EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

Pursuant to Local Patent Rule 4-5(d), Plaintiff Taasera Licensing, LLC and Defendants Check Point Software Technologies Ltd., Trend Micro Incorporated (Japan), Fortinet, Inc., Musarubra US LLC, d/b/a Trellix, Palo Alto Networks, Inc., CrowdStrike, Inc. and CrowdStrike Holdings, Inc. jointly submit this Joint Claim Construction Chart containing the agreed and disputed claim terms, phrases, or clauses of U.S. Patent Nos. 6,842,796, 7,673,137, 8,127,356, 8,327,441, 8,819,419, 8,850,517, 8,955,038, 8,990,948, 9,071,518, 9,092,616, 9,118,634, 9,608,997, 9,628,453, 9,860,251, and 9,923,918. In addition, the parties hereby identify the claim number(s) where the terms and phrases appear.

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
1.	'796 Patent, Claim 1 A method of automatically processing an input sequence of data symbols, the method comprising the steps of: identifying at least one **regularly identifiable expression** in the input sequence of data symbols, wherein the at least one **regularly identifiable expression** represents a pattern that is matchable in accordance with a programming	"regularly identifiable expression" / "regular expression" '796 Patent Claim 1	[AGREED]	[AGREED]	Plain and ordinary meaning

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	language that supports such a **regularly identifiable expression**; identifying at least a portion of information associated with the at least one **regularly identifiable expression**; and extracting the portion of information.				
2.	'137 Patent, Claim 1 A system for managing security of a computing device comprising: a **pre-execution module** operable for receiving notice from the computing device's operating system that a new program is being loaded onto the computing device; a validation module coupled to the **pre-execution monitor**	"pre-execution monitor" "pre-execution module" '137 Patent Claims 1-3	[AGREED]	[AGREED]	"pre-execution module"

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	operable for determining whether the program is valid; a detection module coupled to the **pre-execution monitor** operable for intercepting a trigger from the computing device's operating system; and an execution module coupled to the detection module and operable for monitoring, at the operating system kernel of the computing device, the program in response to the trigger intercepted by the detection module. '137 Patent, Claim 2 The system of claim 1, wherein the **pre-execution module** is further operable for suspending loading of the program onto the computing device.				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	'137 Patent, Claim 3 The system of claim 1, wherein the **pre-execution module** is further operable for retrieving validation data.				
3.	'137 Patent, Claim 6 A computer implemented method for implementing security for a computing device comprising the steps of: interrupting the loading of a new program for operation with the computing device; validating the new program; **if the new program is validated, permitting the new program to continue loading and to execute in connection with the computing device**;	"if the new program is validated, permitting the new program to continue loading and to execute in connection with the computing device;" '137 Patent Claims 6, 13, 14, and 24	Plain and ordinary meaning	If the new program is (validated, claims 6, 13; the same as the allowed program, claims 14, 24), then it is not monitored while it (loads and executes in connection with the computing device, claims 6, 13; executes on the computing device, claims 14 and 24)	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	if the new program is not validated, monitoring the new program while it loads and executes in connection with the computing device, wherein the step of monitoring the new program while it executes is performed at the operating system kernel of the computing device. '137 Patent, Claim 13 A computer-readable medium having computer-executable instructions for performing the steps recited in claim 6. '137 Patent, Claim 14 A computer-implemented method for implementing security for a computing device, comprising the steps of: identifying an allowed program that is permitted				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	to execute on the computing device; receiving a signal that a new program is going to be executed on the computing device; suspending the execution of the new program on the computing device; determining whether the new program is the same as the allowed program; **if the new program is the same as the allowed program, permitting the new program to execute on the computing device; and** if the new program is not the same as the allowed program, monitoring the new program while allowing it to execute on the computing device, wherein the step of monitoring the new program while allowing it				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	to execute is performed at the operating system kernel of the computing device. '137 Patent, Claim 24 A computer-readable medium having computer-executable instructions for performing the steps recited in claim 14.				
4.	'137 Patent, Claim 1 A system for managing security of a computing device comprising: a pre-execution module operable for receiving notice from the computing device's operating system that a new program is being loaded onto the computing device; a validation module coupled to the pre-execution monitor	"an execution module coupled to the detection module and operable for monitoring, at the operating system kernel of the computing device, the program in response to the trigger intercepted by the detection module" '137 Patent Claim 1	Subject to 112 p. 6 Structure: Software algorithm that performs the steps of FIG. 6 Function: monitoring, at the operating system kernel of the computing device, the program in response to the trigger	Means plus function Function: monitoring, at the operating system kernel of the computing device, the program in response to the trigger intercepted by the detection module	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	operable for determining whether the program is valid; a detection module coupled to the pre-execution monitor operable for intercepting a trigger from the computing device's operating system; and **an execution module coupled to the detection module and operable for monitoring, at the operating system kernel of the computing device, the program in response to the trigger intercepted by the detection module**.		intercepted by the detection module	Algorithm: Indefinite. Alternatively: If the program was not validated, then monitor the nonvalidated program in response to triggers while the program is executing.	
5.	'356 Patent, Claim 1 A computer program product for automatically determining if a packet is a new, exploit candidate, the computer program product comprising:	"network administration traffic" '356 Patent Claims 1, 2, 9, 10, 13, 14, 17, and 18	traffic generated by harmless network administration activities	Indefinite	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	a computer-readable tangible storage device; first program instructions to determine if the packet is a known exploit; second program instructions to determine if the packet is addressed to a broadcast IP address of a network; third program instructions to determine if the packet is **network administration traffic**; fourth program instructions, responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being **network administration traffic**, to determine that the packet is not a new, exploit candidate; and				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	fifth program instructions, responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being **network administration traffic** AND the packet not being another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate; and wherein the first, second, third, fourth and fifth program instructions are stored on the computer-readable tangible storage device. '356 Patent, Claim 2 The computer program product of claim 1 further comprising: sixth program instructions to determine				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	if the packet is web crawler traffic; and wherein the fourth program instructions are responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being **network administration traffic** OR the packet being web crawler traffic, to determine that the packet is not a new, exploit candidate; and the fifth program instructions are responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being **network administration traffic** AND the packet not being web crawler traffic,				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	to determine that the packet is a new, exploit candidate; and the sixth program instructions are stored on the computer-readable tangible storage device. '356 Patent, Claim 9 A computer program product for automatically determining if a packet is a new, exploit candidate, the computer program product comprising: a computer-readable tangible storage device; first program instructions to determine if the packet is a known exploit; second program instructions to determine if the packet is addressed to a broadcast IP address of a network; third program instructions to determine if the packet				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	is **network administration traffic**; fourth program instructions, responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being **network administration traffic**, to determine that the packet is not a new, exploit candidate; and fifth program instructions, responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being **network administration traffic** AND the packet not being another type of traffic known to be benign, to determine and report that the packet is a				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	new, exploit candidate; and wherein the first, second, third, fourth and fifth program instructions are stored on the computer-readable tangible storage device; the second program instructions also determine if the packet has a protocol listed in a list of protocols previously determined to be harmless network broadcast traffic; the fourth program instructions are responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being **network administration traffic** OR the packet having a protocol listed in a list of protocols previously determined to				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	be harmless network broadcast traffic, to determine that the packet is not a new, exploit candidate; and the fifth program instructions are responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being **network administration traffic** AND the packet not having a protocol listed in a list of protocols previously determined to be harmless network broadcast traffic, to determine and report that the packet is a new, exploit candidate. '356 Patent, Claim 10 A computer program product for automatically determining if a packet is				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	a new, exploit candidate, the computer program product comprising: a computer-readable tangible storage device; first program instructions to determine if the packet is a known exploit; second program instructions to determine if the packet is addressed to a broadcast IP address of a network; third program instructions to determine if the packet is **network administration traffic**; fourth program instructions, responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being **network administration traffic**, to determine that the				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	packet is not a new, exploit candidate; and fifth program instructions, responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being **network administration traffic** AND the packet not being another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate; and wherein the first, second, third, fourth and fifth program instructions are stored on the computer-readable tangible storage device; and the third program instructions determine if the packet is **network**				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	administration traffic by comparing an IP protocol and IP address of the packet to a list of combinations of IP protocols and IP addresses previously determined to be **network administration traffic**. '356 Patent, Claim 13 A computer program product for automatically determining if a packet is a new, exploit candidate, the computer program product comprising: a computer-readable tangible storage device; first program instructions to determine if the packet is a known exploit; second program instructions to determine if the packet is addressed to a broadcast IP address of a network;				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	third program instructions to determine if the packet has a protocol listed in a list of protocols previously determined to be harmless broadcast traffic; fourth program instructions to determine if the packet is **network administration traffic**; fifth program instructions, responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being **network administration traffic** OR the packet having a protocol listed in a list of protocols previously determined to be harmless broadcast traffic, to determine that the packet is not a new, exploit candidate; and				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	sixth program instructions, responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being **network administration traffic** AND the packet not having a protocol listed in a list of protocols previously determined to be harmless broadcast traffic, to determine and report that the packet is a new, exploit candidate; and wherein the first, second, third, fourth, fifth and sixth program instructions are stored on the computer-readable tangible storage device. '356 Patent, Claim 14				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	The computer program product of claim 13 further comprising: seventh program instructions to determine if the packet is web crawler traffic; and wherein the fifth program instructions are responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being **network administration traffic** OR the packet being web crawler traffic OR the packet having a protocol listed in a list of protocols previously determined to be harmless broadcast traffic, to determine that the packet is not a new, exploit candidate; and				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	the sixth program instructions are responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being **network administration traffic** AND the packet not being web crawler traffic AND the packet not being other traffic known to be benign AND the packet not having a protocol listed in a list of protocols previously determined to be harmless broadcast traffic, to determine that the packet is a new, exploit candidate; and the seventh program instructions are stored on the computer-readable tangible storage device. '356 Patent, Claim 17				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	A computer system for automatically determining if a packet is a new, exploit candidate, the computer system comprising: one or more processors, one or more computer-readable memories, one or more computer-readable tangible storage devices, and program instructions stored on at least one of the one or more storage devices for execution by at least one of the one or more processors via at least one of the one or more memories, the program instructions comprising: first program instructions to determine if the packet is a known exploit; second program instructions to determine if the packet is addressed				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	to a broadcast IP address of a network; third program instructions to determine if the packet is **network administration traffic**; fourth program instructions, responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being **network administration traffic**, to determine that the packet is not a new, exploit candidate; and fifth program instructions, responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being **network administration traffic**				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	AND the packet not being another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate. '356 Patent, Claim 18 The computer system of claim 17 further comprising: sixth program instructions, stored on at least one of the one or more storage devices for execution by at least one of the one or more processors via at least one of the one or more memories, to determine if the packet is web crawler traffic; and wherein the fourth program instructions are responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	OR the packet being **network administration traffic** OR the packet being web crawler traffic, to determine that the packet is not a new, exploit candidate; and the fifth program instructions are responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being **network administration traffic** AND the packet not being web crawler traffic, to determine that the packet is a new, exploit candidate.				
6.	'356 Patent, Claim 1 A computer program product for automatically determining if a packet is a new, exploit candidate,	"[third/fourth] program instructions to determine if the packet is network administration traffic"	Subject to 112 p. 6 Structure: Software algorithm that	Subject to 112(6). Function: determine if the	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	the computer program product comprising: a computer-readable tangible storage device; first program instructions to determine if the packet is a known exploit; second program instructions to determine if the packet is addressed to a broadcast IP address of a network; **third program instructions to determine if the packet is network administration traffic;** fourth program instructions, responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being network administration traffic, to determine that the packet	'356 Patent Claims 1, 9, 10, 13, and 17	performs the steps of FIG. 7 Function: determine if the packet is network administration traffic	packet is network administration traffic Structure: indefinite	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	is not a new, exploit candidate; and fifth program instructions, responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate; and wherein the first, second, third, fourth and fifth program instructions are stored on the computer-readable tangible storage device. '356 Patent, Claim 9 A computer program product for automatically determining if a packet is				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	a new, exploit candidate, the computer program product comprising: a computer-readable tangible storage device; first program instructions to determine if the packet is a known exploit; second program instructions to determine if the packet is addressed to a broadcast IP address of a network; **third program instructions to determine if the packet is network administration traffic;** fourth program instructions, responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being network administration traffic, to				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	determine that the packet is not a new, exploit candidate; and fifth program instructions, responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate; and wherein the first, second, third, fourth and fifth program instructions are stored on the computer-readable tangible storage device; the second program instructions also determine if the packet				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	has a protocol listed in a list of protocols previously determined to be harmless network broadcast traffic; the fourth program instructions are responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being network administration traffic OR the packet having a protocol listed in a list of protocols previously determined to be harmless network broadcast traffic, to determine that the packet is not a new, exploit candidate; and the fifth program instructions are responsive to the packet not being a known exploit AND the packet not being addressed to a				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	broadcast IP address of a network AND the packet not being network administration traffic AND the packet not having a protocol listed in a list of protocols previously determined to be harmless network broadcast traffic, to determine and report that the packet is a new, exploit candidate. '356 Patent, Claim 10 A computer program product for automatically determining if a packet is a new, exploit candidate, the computer program product comprising: a computer-readable tangible storage device; first program instructions to determine if the packet is a known exploit; second program instructions to determine				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	if the packet is addressed to a broadcast IP address of a network; **third program instructions to determine if the packet is network administration traffic;** fourth program instructions, responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being network administration traffic, to determine that the packet is not a new, exploit candidate; and fifth program instructions, responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	being network administration traffic AND the packet not being another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate; and wherein the first, second, third, fourth and fifth program instructions are stored on the computer-readable tangible storage device; and the third program instructions determine if the packet is network administration traffic by comparing an IP protocol and IP address of the packet to a list of combinations of IP protocols and IP addresses previously determined to be network administration traffic. '356 Patent, Claim 13				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	A computer program product for automatically determining if a packet is a new, exploit candidate, the computer program product comprising: a computer-readable tangible storage device; first program instructions to determine if the packet is a known exploit; second program instructions to determine if the packet is addressed to a broadcast IP address of a network; third program instructions to determine if the packet has a protocol listed in a list of protocols previously determined to be harmless broadcast traffic; **fourth program instructions to determine if the packet**				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	is network administration traffic; fifth program instructions, responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being network administration traffic OR the packet having a protocol listed in a list of protocols previously determined to be harmless broadcast traffic, to determine that the packet is not a new, exploit candidate; and sixth program instructions, responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	AND the packet not having a protocol listed in a list of protocols previously determined to be harmless broadcast traffic, to determine and report that the packet is a new, exploit candidate; and wherein the first, second, third, fourth, fifth and sixth program instructions are stored on the computer-readable tangible storage device. '356 Patent, Claim 17 A computer system for automatically determining if a packet is a new, exploit candidate, the computer system comprising: one or more processors, one or more computer-readable memories, one or more computer-readable tangible storage devices, and program				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	instructions stored on at least one of the one or more storage devices for execution by at least one of the one or more processors via at least one of the one or more memories, the program instructions comprising: first program instructions to determine if the packet is a known exploit; second program instructions to determine if the packet is addressed to a broadcast IP address of a network; **third program instructions to determine if the packet is network administration traffic;** fourth program instructions, responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	network OR the packet being network administration traffic, to determine that the packet is not a new, exploit candidate; and fifth program instructions, responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate.				
7.	'441 Patent, Claim 1 A method of providing an **attestation** service for an application at runtime executing on a computing platform using an	"attestation" '441 Patent Claims 1, 2, 3, 5, and 7	verification	verifying/verifies the identity of an application ('441 Patent)	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	attestation server, comprising: receiving, by the **attestation** server remote from the computing platform: a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application; and a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components; generating, by the **attestation** server, a	'616 Patent Claim 1		verifying/verifies the identity of a device, system, or application ('616 Patent)	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result; and sending, by the **attestation** server, the **attestation** result associated with the application. '441 Patent, Claim 2 The method of claim 1, further comprising: generating, by the **attestation** server, an application artifact as a reference for changes in a subsequent execution context; and sending the generated application artifact such that subsequent changes to the runtime execution context are tracked based				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	on the generated application artifact. '441 Patent, Claim 3 The method according to claim 2, further comprising digitally signing the **attestation** results, wherein the attributes further comprise parent-child process associations of the application. '441 Patent, Claim 5 The method of claim 4, wherein the generating of the report indicating security risks associated with the application includes generating, by the **attestation** server, one or more security assertions that pertain to the received runtime execution context and the received introspective security context.				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	'441 Patent, Claim 7 The method according to claim 1, further comprising controlling a user's transaction with the application by applying a set of authorization rules in accordance with the **attestation** results. '616 Patent, Claim 1 A method of providing an **attestation** service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server, the method comprising: sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored device and				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	applications executing on the monitored device at runtime; receiving, at the trust orchestration server, the dynamic context including the endpoint events of the monitored device and the applications executing on the monitored device at runtime; analyzing, by the trust orchestration server, the received endpoint events; receiving, by the trust orchestration server, third party network endpoint assessments; generating, by the trust orchestration server, temporal events based at least in part on analyzing the third party network endpoint assessments; correlating, by the trust orchestration server, the				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	received endpoint events and the generated temporal events; and generating, by the trust orchestration server, an integrity profile for the system.				
8.	'441 Patent, Claim 1 A method of providing an attestation service for an application at **runtime** executing on a computing platform using an attestation server, comprising: receiving, by the attestation server remote from the computing platform: a **runtime** execution context indicating attributes of the application at **runtime**, wherein the attributes comprise one or more executable file binaries of the application and	"runtime" '441 Patent Claims 1, 2, and 5 '517 Patent Claims 1, 10, 13, and 22 '948 Patent Claims 1 and 5	[AGREED]	[AGREED]	'441/'948 Patents: "the time the application is running" '517 Patent: "the time the application program is running"

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	loaded components of the application; and a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components; generating, by the attestation server, a report indicating security risks associated with the application based on the received **runtime** execution context and the received security context, as an attestation result; and sending, by the attestation server, the attestation result associated with the application. '441 Patent, Claim 2				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	The method of claim 1, further comprising: generating, by the attestation server, an application artifact as a reference for changes in a subsequent execution context; and sending the generated application artifact such that subsequent changes to the **runtime** execution context are tracked based on the generated application artifact. '441 Patent, Claim 5 The method of claim 4, wherein the generating of the report indicating security risks associated with the application includes generating, by the attestation server, one or more security assertions that pertain to the received **runtime** execution context and the				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	received introspective security context. '517 Patent, Claim 1 A method for assessing **runtime** risk for an application program that executes on a device, comprising: storing, in a rules database, a plurality of rules, wherein each rule identifies an action sequence; storing, in a policy database, a plurality of assessment policies, wherein each assessment policy includes at least one rule of the plurality of rules; identifying, using at least one assessment policy, a **runtime** risk for an application program that executes on a device, wherein the identified **runtime** risk indicates a				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	risk or threat of the identified action sequence of the application; and identifying, by a **runtime** monitor including a processing device, a behavior score for the application program that executes on the device based on the identified **runtime** risk, wherein the action sequence is a sequence of at least two performed actions, and each performed action is at least one of: a user action, an application action, and a system action. '517 Patent, Claim 10 The method of claim 1, wherein the **runtime** risk is identified based on matching rules and probabilistic weights and scores of performed actions on the device.				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	'517 Patent, Claim 13 A system for assessing **runtime** risk for an application program that executes on a device, comprising: a rules database storing a plurality of rules, wherein each rule identifies an action sequence; a policy database storing a plurality of assessment policies, wherein each assessment policy includes at least one rule of the plurality of rules; and a **runtime** monitor including a processing device identifying, using at least one assessment policy, a **runtime** risk for an application program that executes on a device, wherein the identified **runtime** risk indicates a				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	risk or threat of the identified action sequence of the application, and identifying a behavior score for the application program that executes on the device based on the identified **runtime** risk, wherein the action sequence is a sequence of at least two performed actions, and each performed action is at least one of: a user action, an application action, and a system action. '517 Patent, Claim 22 The system of claim 13, wherein the **runtime** risk is identified based on matching rules and probabilistic weights and scores of performed actions on the device. '948 Patent, Claim 1				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	A method of providing real-time operational integrity of an application on a native computing environment, the method comprising: monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a **runtime** configuration of the application, resource utilization by the application, and integrity of the application; generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity processor, an event correlation matrix, a risk				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	correlation matrix, and a trust supervisor; correlating, by the event and risk correlation matrix, threat classifications based on the temporal sequence of the generated real-time behavior based events; and displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for operational integrity of the application. '948 Patent, Claim 5 The method of claim 1, wherein the plurality of **runtime** dashboards are a plurality of application runtime reputation score dashboards that comprise one or more of: a global view dashboard;				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	a system configuration dashboard; a resource utilization dashboard; an application integrity dashboard; and a network activity dashboard.				
9.	'441 Patent, Claim 1 A method of providing an attestation service for an application **at runtime** executing on a computing platform using an attestation server, comprising: receiving, by the attestation server remote from the computing platform: a runtime execution context indicating attributes of the application **at runtime**, wherein the attributes comprise one or more	"at runtime" '441 Patent Claim 1	[AGREED]	[AGREED]	preamble limiting at least as to "at runtime"; meaning "at the time the application is running"

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	executable file binaries of the application and loaded components of the application; and a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components; generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result; and sending, by the attestation server, the attestation result associated with the application.				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
10.	'616 Patent, Claim 1 A method of providing an attestation service for providing **runtime** operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server, the method comprising: sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored device and applications executing on the monitored device **at runtime**; receiving, at the trust orchestration server, the dynamic context including the endpoint events of the monitored device and the	"[at] runtime" '616 Patent Claim 1	[at] the time the system or device is running	Preamble limiting, at least as to "runtime"; [at] the time the application being monitored is running.	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	applications executing on the monitored device **at runtime**; analyzing, by the trust orchestration server, the received endpoint events; receiving, by the trust orchestration server, third party network endpoint assessments; generating, by the trust orchestration server, temporal events based at least in part on analyzing the third party network endpoint assessments; correlating, by the trust orchestration server, the received endpoint events and the generated temporal events; and generating, by the trust orchestration server, an integrity profile for the system.				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
11.	'616 Patent, Claim 1 A method of providing an attestation service for providing runtime operational integrity of a system using **a computing platform comprising a network trust agent**, an endpoint trust agent, and a trust orchestration server, the method comprising: sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored device and applications executing on the monitored device at runtime; receiving, at the trust orchestration server, the dynamic context including the endpoint events of the monitored device and the	"a computing platform comprising a network trust agent" '616 Patent Claim 1	Plain and ordinary meaning	Limiting preamble; indefinite	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	applications executing on the monitored device at runtime; analyzing, by the trust orchestration server, the received endpoint events; receiving, by the trust orchestration server, third party network endpoint assessments; generating, by the trust orchestration server, temporal events based at least in part on analyzing the third party network endpoint assessments; correlating, by the trust orchestration server, the received endpoint events and the generated temporal events; and generating, by the trust orchestration server, an integrity profile for the system.				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
12.	'616 Patent, Claim 1 A method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server, the method comprising: sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored device and applications executing on the monitored device at runtime; receiving, at the trust orchestration server, the dynamic context including the endpoint events of the monitored device and the	"third party network endpoint assessments" '616 Patent Claims 1, 2, and 4	[AGREED]	[AGREED]	"at least two assessments of a network endpoint provided by one or more third parties"

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	applications executing on the monitored device at runtime; analyzing, by the trust orchestration server, the received endpoint events; receiving, by the trust orchestration server, **third party network endpoint assessments**; generating, by the trust orchestration server, temporal events based at least in part on analyzing the third party network endpoint assessments; correlating, by the trust orchestration server, the received endpoint events and the generated temporal events; and generating, by the trust orchestration server, an integrity profile for the system. '616 Patent, Claim 2				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	The method of claim 1, wherein the **third party network endpoint assessments** are received from an endpoint assessment service. '616 Patent, Claim 4 The method of claim 1, wherein the **third party network endpoint assessments** are received from one or more collaboration services.				
13.	'441 Patent, Claim 1 A method of providing an attestation service for an application at runtime executing on a computing platform using an attestation server, comprising:	"receiving … a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded	Plain and ordinary meaning subject to the construction of "runtime"	Receiving at the time the application is running[1] an execution context that includes the executable file binaries of the application (as	

[1] In their Responsive Brief (Dkt. 259 at 14-15, fn. 15), Defendants corrected this construction to reflect the agreed-upon construction for "at runtime" for the '441 Patent.

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	receiving, by the attestation server remote from the computing platform: **a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application**; and a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components; generating, by the attestation server, a report indicating security risks associated with the	components of the application" '441 Patent Claims 1 and 4		distinct from binary hashes) and loaded components of the application	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	application based on the received runtime execution context and the received security context, as an attestation result; and sending, by the attestation server, the attestation result associated with the application. '441 Patent, Claim 4 The method of claim 1, wherein the received security context is an introspective security context, and wherein the execution analysis is a static, dynamic, or virtual analysis of the **one or more executable file binaries and the loaded components**.				
14.	'441 Patent, Claim 1 A method of providing an attestation service for an application at runtime executing on a computing	"a security context providing security information about the application"	Plain and ordinary meaning	security information about the application provided by a	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	platform using an attestation server, comprising: receiving, by the attestation server remote from the computing platform: a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application; and **a security context providing security information about the application**, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components;	'441 Patent Claims 1, 4, and 5		collaboration service	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received **security context**, as an attestation result; and sending, by the attestation server, the attestation result associated with the application. '441 Patent, Claim 4 The method of claim 1, wherein the received **security context** is an introspective security context, and wherein the execution analysis is a static, dynamic, or virtual analysis of the one or more executable file binaries and the loaded components. '441 Patent, Claim 5				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	The method of claim 4, wherein the generating of the report indicating security risks associated with the application includes generating, by the attestation server, one or more security assertions that pertain to the received runtime execution context and the received introspective **security context**.				
15.	'441 Patent, Claim 2 The method of claim 1, further comprising: generating, by the attestation server, **an application artifact** as a reference for changes in a subsequent execution context; and sending the generated **application artifact** such that subsequent changes to the runtime execution context are tracked based	"an application artifact" '441 Patent Claim 2	Plain and ordinary meaning	data identifying one or more attribute value assertions that describe the application runtime execution context	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	on the generated **application artifact**.				
16.	'441 Patent, Claim 4 The method of claim 1, wherein the received security context is an **introspective security context**, and wherein the execution analysis is a static, dynamic, or virtual analysis of the one or more executable file binaries and the loaded components. '441 Patent, Claim 5 The method of claim 4, wherein the generating of the report indicating security risks associated with the application includes generating, by the attestation server, one or more security assertions that pertain to the received runtime execution context and the	"introspective security context" '441 Patent Claims 4 and 5	Plain and ordinary meaning	a security context based on evaluation of historic state information and measurements [of the remote computing platform] sampled over a period of time; Otherwise, Indefinite.	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	received **introspective security context**.				
17.	'441 Patent, Claim 11 The method according to claim 1, wherein **the application of the restriction on the user's transaction** includes applying routing decisions and redirecting the user to an alternate computer platform.	"the application of the restriction of the user's transaction" '441 Patent Claim 11	Plain and ordinary meaning	Indefinite	
18.	'419 Patent, Claim 1 A method for restricting access to information transmitted over a computing network, said method comprising the steps of: receiving, by a computer at a network location, a resource request for a resource to be located, said resource request containing a universal resource locator (URL);	"return URL" '419 Patent Claims 1, 3, 4, 6, 7, 9, 10, 12, 13, 15, 16, and 19 '634 Patent Claims 1, 3, 4, 5, 6, and 8 '251 Patent Claims 1-6, and 8-10	Plain and ordinary meaning	a new URL for the requested resource that is returned to the requestor's web browser	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	evaluating, by the computer, the URL to determine whether encryption of none, part, or all of the URL is required; determining by the computer, whether the requested resource is available; locating, by the computer, the requested resource contained in the resource request, when the determination is that the requested resource is available; encrypting, the computer, the URL contained in the resource request; and determining, by the computer, whether encryption is required for none, part, or all of a **return URL** of the requested resource that is to be returned to a	'453 Patent Claims 1, 5, 6, 10-12, and 16-18			

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	location of the resource request. '419 Patent, Claim 3 The method as described in claim 2, said method further comprising the steps of: encrypting the computer, the **return URL**; and sending, by the computer, the encrypted URL to the location of the resource request. '419 Patent, Claim 4 A method for restricting access to information transmitted over a computing network, said method comprising the steps of: receiving, by a computer at a network location, a resource request for a resource to be located, said request containing a				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	universal resource locator (URL); evaluating, by the computer, the URL to determine whether encryption of the URL is required; locating, by the computer, the requested resource, when encryption of the URL is not required; determining, by the computer, whether the requested resource is available; encrypting the computer, the URL contained in the resource request; and determining, by the computer, whether encryption of a **return URL** of the requested resource is required, when the requested resource is available. '419 Patent, Claim 6				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	The method as described in claim 4, said method further comprising after the determination that the **return URL** requires encryption the steps of: determining, by the computer, an encrypted value for the **return URL**; and sending, by the computer, a redirect to a browser originating the resource request using the encrypted value for the **return URL**. '419 Patent, Claim 7 The method as described in claim 4, said method further comprising the step of: sending, by the computer, the resource to a browser originating the resource request when encryption of the **return URL** is not required.				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	'419 Patent, Claim 9 The method as described in claim 8, said method further comprising after said locating step, the step of: determining, by the computer, whether encryption of a **return URL** of the requested resource is required, when the requested resource is available. '419 Patent, Claim 10 A computer program product stored in a computer readable hardware storage device for restricting access to information transmitted over a computing network, said computer program product comprising: instructions for receiving at a network location a resource request for a				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	resource to be located, said resource request containing a universal resource locator (URL); instructions for evaluating the URL to determine whether encryption of none, part, or all of the URL is required; instructions for locating the requested resource contained in the resource request; instructions for encrypting the URL contained in the resource request; instructions for determining whether the requested resource is available; and instructions for determining whether encryption of none, part, or all of a **return URL** of the requested resource				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	that is to be returned to a location of the resource request. '419 Patent, Claim 12 The computer program product as described in claim 10, further comprising: instructions for encrypting a **return URL**; instructions for sending the encrypted URL to the location of the resource request. '419 Patent, Claim 13 A computer program product stored in a computer readable hardware storage device for restricting access to information transmitted over a computing network, said computer program product comprising:				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	instructions for receiving at a network location a resource request for a resource to be located, said resource request containing a universal resource locator (URL); instructions for evaluating the URL to determine whether encryption of the URL is required; instructions for locating the requested resource contained in the resource request, when encryption of the URL is not required; instructions for determining whether the requested resource is available; and instructions for determining whether encryption of a **return URL** of the requested resource is required,				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	when the requested resource is available. '419 Patent, Claim 15 The computer program product as described in claim 13, further comprising: instructions for determining an encrypted value for the **return URL** in response to a determination that the **return URL** requires encryption; and instructions for sending a redirect to a browser originating the resource request using the encrypted value for the **return URL**. '419 Patent, Claim 16 The computer program product as described in claim 13, further comprising				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	instructions for sending the resource to a browser originating the resource request when encryption of the **return URL** is not required. '419 Patent, Claim 19 The computer program product as described in claim 17, further comprising instructions for determining whether encryption of a **return URL** of the requested resource is required, when the requested resource is available. '634 Patent, Claim 1 A system comprising a computer and a computer readable hardware storage device, said storage device containing instructions which, upon being executed by the computer, implements a				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	method for restricting access to information transmitted over a computing network, said method comprising: receiving, by the computer at a network location, a resource request for a resource to be located, said resource request containing a universal resource locator (URL); evaluating, by the computer, the URL to determine whether encryption of none, part, or all of the URL is required; determining by the computer, that the requested resource is available and in response, locating, by the computer, the requested resource contained in the resource request; and				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	determining, by the computer, whether encryption is required for none, part, or all of a **return URL** of the requested resource that is to be returned to a location of the resource request. '634 Patent, Claim 3 The system of claim 2, said method further comprising: encrypting, by the computer, the **return URL**; and sending, by the computer, the encrypted URL to the location of the resource request. '634 Patent, Claim 4 A system comprising a computer and a computer readable hardware storage device, said storage device containing instructions which, upon				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	being executed by the computer, implements a method for restricting access to information transmitted over a computing network, said method comprising: receiving, by the computer at a network location, a resource request for a resource to be located, said request containing a universal resource locator (URL); evaluating, by the computer, the URL to determine that encryption of the URL is not required and in response, locating, by the computer, the requested resource; determining, by the computer, that the requested resource is available; encrypting, by the computer, the URL				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	contained in the resource request; and determining, by the computer in response to said determining that the requested resource is available, whether encryption of a **return URL** of the requested resource is required. '634 Patent, Claim 5 The system of claim 4, said method further comprising after a determination that encryption of the **return URL** of the requested resource is required: determining, by the computer, an encrypted value for the **return URL**; and sending, by the computer, a redirect to a browser originating the resource request using the				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	encrypted value for the **return URL**. '634 Patent, Claim 6 The system of claim 4, said method further comprising: sending, by the computer, the resource to a browser originating the resource request in response to a determination that encryption of the **return URL** is not required. '634 Patent, Claim 8 The system of claim 7, said method further comprising after said locating the requested resource: determining, by the computer, whether encryption of a **return URL** of the requested resource is required in response to a determination that the				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	requested resource is available. '251 Patent, Claim 1 A system comprising a computer and a computer readable hardware storage device, said storage device containing instructions executable by the computer to implement a method for restricting access to information transmitted over a computing network, said method comprising: receiving, by the computer at a network location, a resource request for a resource to be located, said resource request containing a universal resource locator (URL); determining by the computer, that the requested resource is available and in response,				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	locating, by the computer, the requested resource contained in the resource request; determining, by the computer, that encryption of the contained URL is required and in response, calculating, by the computer, an encrypted value of the contained URL and sending, by the computer, the encrypted value of the contained URL to the location of the resource request; and determining, by the computer, whether encryption is required for a **return URL** of the requested resource that is to be returned to a location of the resource request and if so then in response, calculating, by the computer, an encrypted value of the **return URL**.				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	'251 Patent, Claim 2 The system of claim 1, said method comprising: determining, by the computer, that encryption of the **return URL** is not required. '251 Patent, Claim 3 The system of claim 1, said method comprising: determining, by the computer, that encryption of the **return URL** is required. '251 Patent, Claim 4 A computer program product, comprising a computer readable hardware storage device containing instructions executable by a computer to implement a method for restricting access to information transmitted over a computing				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	network, said method comprising: receiving, by the computer at a network location, a resource request for a resource to be located, said resource request containing a universal resource locator (URL); determining by the computer, that the requested resource is available and in response, locating, by the computer, the requested resource contained in the resource request; determining, by the computer, that encryption of the contained URL is required and in response, calculating, by the computer, an encrypted value of the contained URL and sending, by the computer, the encrypted value of the contained				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	URL to the location of the resource request; and determining, by the computer, whether encryption is required for a **return URL** of the requested resource that is to be returned to a location of the resource request and if so then in response, calculating, by the computer, an encrypted value of the **return URL**. '251 Patent, Claim 5 The computer program product of claim 4, said method comprising: determining, by the computer, that encryption of the **return URL** is not required. '251 Patent, Claim 6 The computer program product of claim 4, said method comprising:				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	determining, by the computer, that encryption of the **return URL** is required. '251 Patent, Claim 8 The computer program product of claim 7, said method comprising: determining, by the computer, whether encryption is required for a **return URL** of the requested resource that is to be returned to a location of the resource request. '251 Patent, Claim 9 The computer program product of claim 8, said method comprising: determining, by the computer, that encryption of the **return URL** is not required. '251 Patent, Claim 10				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	The computer program product of claim 8, said method comprising: determining, by the computer, that encryption of the **return URL** is required and in response, determining, by the computer, an encrypted value of the **return URL**. '453 Patent, Claim 1 A method for restricting access to information transmitted over a computing network, said method comprising: receiving, by the computer at a network location, a resource request for a resource to be located, said resource request containing a universal resource locator (URL); determining by the computer, that the requested resource is				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	available and in response, locating, by the computer, the requested resource contained in the resource request; determining, by the computer, whether encryption of the contained URL is required; and determining, by the computer, whether encryption is required for a **return URL** of the requested resource that is to be returned to a location of the resource request. '453 Patent, Claim 5 The method of claim 2, said method comprising: determining by the computer, that encryption of the **return URL** is not required. '453 Patent, Claim 6				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	The method of claim 2, said method comprising: determining, by the computer, that encryption of the **return URL** is required and in response, determining, by the computer, an encrypted value of the **return URL**. '453 Patent, Claim 10 The method of claim 7, said method comprising: determining, by the computer, whether encryption is required for a **return URL** of the requested resource that is to be returned to a location of the resource request. '453 Patent, Claim 11 The method of claim 10, said method comprising: determining by the computer, that encryption				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	of the **return URL** is not required. '453 Patent, Claim 12 The method of claim 10, said method comprising: determining, by the computer, that encryption of the **return URL** is required and in response, determining, by the computer, an encrypted value of the **return URL**. '453 Patent, Claim 16 The system of claim 13, said method comprising: determining, by the computer, whether encryption is required for a **return URL** of the requested resource that is to be returned to a location of the resource request. '453 Patent, Claim 17 The system of claim 16, said method comprising:				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	determining by the computer, that encryption of the **return URL** is not required. '453 Patent, Claim 18 The system of claim 16, said method comprising: determining, by the computer, that encryption of the **return URL** is required and in response, determining, by the computer, an encrypted value of the **return URL**.				
19.	'419 Patent, Claim 1 A method for restricting access to information transmitted over a computing network, said method comprising the steps of: receiving, by a computer at a network location, a resource request for a resource to be located, said resource request	"encrypting, the computer, the URL contained in the resource request" '419 Patent Claim 1	[AGREED]	[AGREED]	"encrypting, by the computer, the URL contained in the resource request"

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	containing a universal resource locator (URL); evaluating, by the computer, the URL to determine whether encryption of none, part, or all of the URL is required; determining by the computer, whether the requested resource is available; locating, by the computer, the requested resource contained in the resource request, when the determination is that the requested resource is available; **encrypting, the computer, the URL contained in the resource request**; and determining, by the computer, whether encryption is required for none, part, or all of a				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	return URL of the requested resource that is to be returned to a location of the resource request.				
20.	'419 Patent, Claim 1 A method for restricting access to information transmitted over a computing network, said method comprising the steps of: receiving, by a computer at a network location, a resource request for a resource to be located, said resource request containing a universal resource locator (URL); **evaluating, by the computer, the URL to determine whether encryption of none, part, or all of the URL is required**; determining by the computer, whether the	"evaluating[, by the computer,] the URL to determine whether encryption of [none, part, or all of]the URL is required" "determining, by the computer, whether encryption is required for none, part, or all of a return URL" / "determining[, by the computer,] whether encryption of a return URL of the requested resource is required" / "determining, by the computer, whether	Plain and ordinary meaning	deciding[, by the computer,] whether encryption should be performed on [none, part, or all] of the URL deciding[, by the computer,] [whether / that] encryption should be performed on [none, part, or all of] a return URL / deciding[, by the computer,] whether	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	requested resource is available; locating, by the computer, the requested resource contained in the resource request, when the determination is that the requested resource is available; encrypting, the computer, the URL contained in the resource request; and **determining, by the computer, whether encryption is required for none, part, or all of a return URL** of the requested resource that is to be returned to a location of the resource request. '419 Patent, Claim 4 A method for restricting access to information transmitted over a computing network, said	encryption of a return URL of the requested resource is required" / "determining by the computer, [whether/that] encryption of the contained URL [is/is not] required" / "determining, by the computer, that encryption of the return URL is required" / "determining, by the computer, whether encryption of the contained URL is required" / "determine that encryption of the URL is not required" / "determining by the computer, that encryption		encryption should be performed on a return URL of the requested resource / deciding, by the computer, whether encryption should be performed on the contained URL / deciding, by the computer, that encryption [should / should not] be performed on the contained URL / deciding, by the computer, that encryption should be	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	method comprising the steps of: receiving, by a computer at a network location, a resource request for a resource to be located, said request containing a universal resource locator (URL); **evaluating, by the computer, the URL to determine whether encryption of the URL is required**; locating, by the computer, the requested resource, when encryption of the URL is not required; determining, by the computer, whether the requested resource is available; encrypting the computer, the URL contained in the resource request; and **determining, by the computer, whether**	of the return URL is not required" '419 Patent Claims 1, 4, 10, 13, 17, and 19 '634 Patent Claims 1 and 4 '251 Patent Claims 1-6 and 8-10 '453 Patent Claims 1, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, and 18		performed on the return URL / deciding[, by the computer,] that encryption should not be performed on the [return] URL	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	encryption of a return URL of the requested resource is required, when the requested resource is available. '419 Patent, Claim 10 A computer program product stored in a computer readable hardware storage device for restricting access to information transmitted over a computing network, said computer program product comprising: instructions for receiving at a network location a resource request for a resource to be located, said resource request containing a universal resource locator (URL); instructions for evaluating the URL to **determine whether encryption of none,**				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	part, or all of the URL is required; instructions for locating the requested resource contained in the resource request; instructions for encrypting the URL contained in the resource request; instructions for determining whether the requested resource is available; and instructions for determining whether encryption of none, part, or all of a return URL of the requested resource that is to be returned to a location of the resource request. '419 Patent, Claim 13 A computer program product stored in a computer readable hardware storage device				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	for restricting access to information transmitted over a computing network, said computer program product comprising: instructions for receiving at a network location a resource request for a resource to be located, said resource request containing a universal resource locator (URL); instructions for **evaluating the URL to determine whether encryption of the URL is required**; instructions for locating the requested resource contained in the resource request, when encryption of the URL is not required; instructions for determining whether the				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	requested resource is available; and instructions for **determining whether encryption of a return URL of the requested resource is required**, when the requested resource is available. '419 Patent, Claim 17 A computer program product stored in a computer readable hardware storage device for restricting access to information transmitted over a computing network, said computer program product comprising: instructions for receiving at a network location a resource request for a resource to be located, said resource request containing a universal resource locator (URL);				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	instructions for **evaluating the URL to determine whether encryption of the URL is required**; instructions for encrypting a URL of the network location; instructions for determining whether the requested resource is available; and instructions for locating the requested resource. '419 Patent, Claim 19 The computer program product as described in claim 17, further comprising instructions for **determining whether encryption of a return URL of the requested resource is required**, when the requested resource is available.				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	'634 Patent, Claim 1 A system comprising a computer and a computer readable hardware storage device, said storage device containing instructions which, upon being executed by the computer, implements a method for restricting access to information transmitted over a computing network, said method comprising: receiving, by the computer at a network location, a resource request for a resource to be located, said resource request containing a universal resource locator (URL); **evaluating, by the computer, the URL to determine whether encryption of none, part, or all of the URL is required**;				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	determining by the computer, that the requested resource is available and in response, locating, by the computer, the requested resource contained in the resource request; and **determining, by the computer, whether encryption is required for none, part, or all of a return URL** of the requested resource that is to be returned to a location of the resource request. '634 Patent, Claim 4 A system comprising a computer and a computer readable hardware storage device, said storage device containing instructions which, upon being executed by the computer, implements a method for restricting access to information				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	transmitted over a computing network, said method comprising: receiving, by the computer at a network location, a resource request for a resource to be located, said request containing a universal resource locator (URL); evaluating, by the computer, the URL to **determine that encryption of the URL is not required** and in response, locating, by the computer, the requested resource; determining, by the computer, that the requested resource is available; encrypting, by the computer, the URL contained in the resource request; and				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	determining, by the computer in response to said determining that the requested resource is available, whether encryption of a return URL of the requested resource is required. '251 Patent, Claim 1 A system comprising a computer and a computer readable hardware storage device, said storage device containing instructions executable by the computer to implement a method for restricting access to information transmitted over a computing network, said method comprising: receiving, by the computer at a network location, a resource request for a resource to be located, said resource request containing a				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	universal resource locator (URL); determining by the computer, that the requested resource is available and in response, locating, by the computer, the requested resource contained in the resource request; **determining, by the computer, that encryption of the contained URL is required** and in response, calculating, by the computer, an encrypted value of the contained URL and sending, by the computer, the encrypted value of the contained URL to the location of the resource request; and **determining, by the computer, whether encryption is required for a return URL** of the requested resource that is				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	to be returned to a location of the resource request and if so then in response, calculating, by the computer, an encrypted value of the return URL. '251 Patent, Claim 2 The system of claim 1, said method comprising: **determining, by the computer, that encryption of the return URL is not required**. '251 Patent, Claim 3 The system of claim 1, said method comprising: **determining, by the computer, that encryption of the return URL is required**. '251 Patent, Claim 4 A computer program product, comprising a computer readable hardware storage device				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	containing instructions executable by a computer to implement a method for restricting access to information transmitted over a computing network, said method comprising: receiving, by the computer at a network location, a resource request for a resource to be located, said resource request containing a universal resource locator (URL); determining by the computer, that the requested resource is available and in response, locating, by the computer, the requested resource contained in the resource request; **determining, by the computer, that encryption of the contained URL is**				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	required and in response, calculating, by the computer, an encrypted value of the contained URL and sending, by the computer, the encrypted value of the contained URL to the location of the resource request; and **determining, by the computer, whether encryption is required for a return URL** of the requested resource that is to be returned to a location of the resource request and if so then in response, calculating, by the computer, an encrypted value of the return URL. '251 Patent, Claim 5 The computer program product of claim 4, said method comprising: **determining, by the computer, that**				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	encryption of the return URL is not required. '251 Patent, Claim 6 The computer program product of claim 4, said method comprising: **determining, by the computer, that encryption of the return URL is required**. '251 Patent, Claim 8 The computer program product of claim 7, said method comprising: **determining, by the computer, whether encryption is required for a return URL** of the requested resource that is to be returned to a location of the resource request. '251 Patent, Claim 9 The computer program product of claim 8, said method comprising:				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	determining, by the computer, that encryption of the return URL is not required. '251 Patent, Claim 10 The computer program product of claim 8, said method comprising: **determining, by the computer, that encryption of the return URL is required** and in response, determining, by the computer, an encrypted value of the return URL. '453 Patent, Claim 1 A method for restricting access to information transmitted over a computing network, said method comprising: receiving, by the computer at a network location, a resource request for a resource to be located, said resource				

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	request containing a universal resource locator (URL); determining by the computer, that the requested resource is available and in response, locating, by the computer, the requested resource contained in the resource request; **determining, by the computer, whether encryption of the contained URL is required**; and **determining, by the computer, whether encryption is required for a return URL** of the requested resource that is to be returned to a location of the resource request. '453 Patent, Claim 4 The method of claim 2, said method comprising:				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	determining by the computer, that encryption of the contained URL is required and in response, (i) determining, by the computer, an encrypted value of the contained URL and (ii) sending, by the computer, the encrypted value of the contained URL to the location of the resource request. '453 Patent, Claim 6 The method of claim 2, said method comprising: **determining, by the computer, that encryption of the return URL is required** and in response, determining, by the computer, an encrypted value of the return URL. '453 Patent, Claim 7				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	A method for restricting access to information transmitted over a computing network, said method comprising: receiving, by the computer at a network location, a resource request for a resource to be located, said resource request containing a universal resource locator (URL); determining by the computer, that the requested resource is available and in response, locating, by the computer, the requested resource contained in the resource request; **determining, by the computer, whether encryption of the contained URL is required**; and after said determining that the requested				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	resource is available, determining, by the computer, that encryption of the requested resource is required and in response, determining, by the computer, an encrypted value of the requested resource. '453 Patent, Claim 8 The method of claim 7, said method comprising: **determining by the computer, that encryption of the contained URL is not required**. '453 Patent, Claim 9 The method of claim 7, said method comprising: **determining by the computer, that encryption of the contained URL is required** and in response, (i) determining, by the computer, an encrypted				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	value of the contained URL and (ii) sending, by the computer, the encrypted value of the contained URL to the location of the resource request. '453 Patent, Claim 10 The method of claim 7, said method comprising: **determining, by the computer, whether encryption is required for a return URL** of the requested resource that is to be returned to a location of the resource request. '453 Patent, Claim 11 The method of claim 10, said method comprising: **determining by the computer, that encryption of the return URL is not required**. '453 Patent, Claim 12				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	The method of claim 10, said method comprising: **determining, by the computer, that encryption of the return URL is required** and in response, determining, by the computer, an encrypted value of the return URL. '453 Patent, Claim 13 A system comprising a computer and a computer readable hardware storage device, said storage device containing instructions which, upon being executed by the computer, implements a method for restricting access to information transmitted over a computing network, said method comprising: receiving, by the computer at a network location, a resource request for a resource to				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	be located, said resource request containing a universal resource locator (URL); determining by the computer, that the requested resource is available and in response, locating, by the computer, the requested resource contained in the resource request; **determining, by the computer, whether encryption of the contained URL is required**; and after said determining that the requested resource is available, determining, by the computer, that encryption of the requested resource is required and in response, determining, by the computer, an encrypted value of the requested resource.				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	'453 Patent, Claim 14 The system of claim 13, said method comprising: **determining by the computer, that encryption of the contained URL is not required**. '453 Patent, Claim 15 The system of claim 13, said method comprising: **determining by the computer, that encryption of the contained URL is required** and in response, (i) determining, by the computer, an encrypted value of the contained URL and (ii) sending, by the computer, the encrypted value of the contained URL to the location of the resource request. '453 Patent, Claim 16				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	The system of claim 13, said method comprising: **determining, by the computer, whether encryption is required for a return URL** of the requested resource that is to be returned to a location of the resource request. '453 Patent, Claim 17 The system of claim 16, said method comprising: **determining by the computer, that encryption of the return URL is not required**. '453 Patent, Claim 18 The system of claim 16, said method comprising: **determining, by the computer, that encryption of the return URL is required** and in response, determining, by the computer, an				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	encrypted value of the return URL.				
21.	'419 Patent, Claim 10 A computer program product stored in a computer readable hardware storage device for restricting access to information transmitted over a computing network, said computer program product comprising: instructions for receiving at a network location a resource request for a resource to be located, said resource request containing a universal resource locator (URL); instructions for evaluating the URL to determine whether encryption of none, part, or all of the URL is required;	"determining whether encryption of none, part, or all of a return URL of the requested resource that is to be returned to a location of the resource request" '419 Patent Claim 10	Plain and ordinary meaning	Indefinite	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	instructions for locating the requested resource contained in the resource request; instructions for encrypting the URL contained in the resource request; instructions for determining whether the requested resource is available; and instructions for **determining whether encryption of none, part, or all of a return URL of the requested resource that is to be returned to a location of the resource request**.				
22.	'419 Patent, Claim 2 The method as described in claim 1 further, said method comprising after a determination that the	"determining[, by the computer,] whether the URL of the requested resource is required" '419 Patent Claims 2 and 11	Plain and ordinary meaning	Indefinite	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	requested resource is available, the steps of: determining, by the computer, whether encryption of the requested resource is required; when encryption of the requested resource is required, **determining, by the computer, whether the URL of the requested resource is required**; and determining, by the computer, the encrypted value of the requested resource. '419 Patent, Claim 11 The computer program product as described in claim 10, further comprising: instructions for determining whether encryption of the requested resource is	'634 Patent Claim 2			

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	required in response to a determination that the requested resource is available; instructions for **determining whether the URL of the requested resource is required** when encryption of the requested resource is required; and instructions for determining an encrypted value of the requested resource. '634 Patent, Claim 2 The system of claim 1, said method comprising after said determining that the requested resource is available: determining, by the computer, that encryption of the requested resource is required and in response, **determining,**				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	by the computer, whether the URL of the requested resource is required; and determining, by the computer, the encrypted value of the requested resource.				
23.	'038 Patent, Claim 1 A method for controlling the operation of an endpoint, comprising: providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies; maintaining the plurality of policies in a data store on the computing system; identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor;	"compliance state of the endpoint" '038 Patent Claims 1,12, and 23 '997 Patent Claims 1, 11, and 21 '918 Patent Claims 1, 9, and 17	Plain and ordinary meaning	level of compliance by the endpoint with compliance policy thresholds	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	configuring one or more software agents on the endpoint to monitor the plurality of operating conditions; receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents; determining, by the computing system, **a compliance state of the endpoint** based on the status information and a plurality of compliance policies in the data store; and initiating, by the computing system, based on **the compliance state**, an action identified in at least one rule in the data store, wherein the action				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	is carried out by a processor on the endpoint. '038 Patent, Claim 12 A non-transitory computer readable medium containing computer instructions for controlling the operation of an endpoint, comprising: providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies; maintaining the plurality of policies in a data store on the computing system; identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor; configuring one or more software agents on the				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	endpoint to monitor the plurality of operating conditions; receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents; determining, by the computing system, **a compliance state of the endpoint** based on the status information and a plurality of compliance policies in the data store; and initiating, by the computing system, based on **the compliance state**, an action identified in at least one rule in the data store, wherein the action is carried out by a				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	processor on the endpoint. '038 Patent, Claim 23 A system for controlling the operation of an endpoint, comprising: a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies; a data store, at the computing system, that contains the plurality of policies; one or more software agents on the endpoint configured to monitor a plurality of operating conditions identified in the plurality of policies; and one or more hardware processors at the				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	computing system configured to: receive, across a network, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents, determine **a compliance state of the endpoint** based on the status information and a plurality of compliance policies in the data store, and initiate, based on **the compliance state**, an action identified in at least one rule in the data store, wherein the action is carried out by the hardware processor on the endpoint. '997 Patent, Claim 1				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	A method for controlling the operation of an endpoint, comprising: providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies; maintaining the plurality of policies in a data store on the computing system; identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor; configuring one or more software services provided by an operating system on the endpoint to monitor the plurality of operating conditions; receiving, across a network, at the computing system, status information about the				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	plurality of operating conditions on the endpoint gathered by the one or more software services; determining, by the computing system, **a compliance state of the endpoint** based on the status information and a plurality of compliance policies in the data store; and initiating, remotely by the computing system, based on **the compliance state**, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint, such that the computing system remotely ensures endpoint compliance with the plurality of compliance policies				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	stored in the data store of the computing system. '997 Patent, Claim 11 A non-transitory computer readable medium containing computer instructions for controlling the operation of an endpoint, comprising: providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies; maintaining the plurality of policies in a data store on the computing system; identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor; configuring one or more software services provided by an operating				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	system on the endpoint to monitor the plurality of operating conditions; receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services; determining, by the computing system, **a compliance state of the endpoint** based on the status information and a plurality of compliance policies in the data store; and initiating, remotely by the computing system, based on **the compliance state**, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	endpoint, such that the computing system remotely ensures endpoint compliance with the plurality of compliance policies stored in the data store of the computing system. '997 Patent, Claim 21 A system for controlling the operation of an endpoint, comprising: a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies; a data store, at the computing system, that contains the plurality of policies; one or more software services provided by an operating system on the endpoint configured to monitor a plurality of				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	operating conditions identified in the plurality of policies; and one or more hardware processors at the computing system configured to: receive, across a network, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services, determine **a compliance state of the endpoint** based on the status information and a plurality of compliance policies in the data store, and initiate, remotely by the computing system, based on **the compliance state**, an action identified in at least one rule in the data store, wherein the action is carried out by the				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	hardware processor on the endpoint, such that the computing system remotely ensures endpoint compliance with the plurality of compliance policies stored in the data store of the computing system. '918 Patent, Claim 1 A method for controlling the operation of an endpoint, comprising: providing a user interface, at a computing system that is remote from the endpoint, configured to allow configuration of a plurality of policies; maintaining the plurality of policies in a data store on the computing system; identifying, from the plurality of policies, a plurality of operating				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	conditions on the endpoint to evaluate; configuring one or more software services provided by an operating system on the endpoint to monitor the plurality of operating conditions; receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint, gathered by the one or more software services on the endpoint, and user information that identifies a user of the endpoint; determining, by the computing system, **a compliance state of the endpoint** based on the user information and status information, and a plurality of compliance policies in the data store;				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	authorizing access by the endpoint to a computing resource on the network, authorization being determined by the remote computing system in response to **the compliance state**; and continuing to monitor **the compliance state** by the endpoint and restricting access to the computing resource if **the compliance state** changes. '918 Patent, Claim 9 A non-transitory computer readable medium containing computer instructions for controlling the operation of an endpoint, comprising: providing a user interface, at a computing system that is remote from the endpoint, configured to allow				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	configuration of a plurality of policies; maintaining the plurality of policies in a data store on the computing system; identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to evaluate; configuring one or more software services provided by an operating system on the endpoint to monitor the plurality of operating conditions; receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint, gathered by the one or more software services on the endpoint, and user information that				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	identifies a user of the endpoint; determining, by the computing system, **a compliance state of the endpoint** based on the user information and status information, and a plurality of compliance policies in the data store; authorizing access by the endpoint to a computing resource on the network, authorization being determined by the remote computing system in response to **the compliance state**; and continuing to monitor **the compliance state** by the endpoint and restricting access to the computing resource if **the compliance state** changes. '918 Patent, Claim 17				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	A system for controlling the operation of an endpoint, comprising: a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies; a data store, at the computing system, that contains the plurality of policies; one or more software services provided by an operating system on the endpoint configured to evaluate a plurality of operating conditions identified in the plurality of policies; and one or more hardware processors at the computing system configured to: receive, across a network, at the computing system,				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	status information about the plurality of operating conditions on the endpoint, gathered by the one or more software services on the endpoint, and user information that identifies a user of the endpoint, determine, by the computing system, **a compliance state of the endpoint** based on the user information and status information, and a plurality of compliance policies in the data store, and authorize access by the endpoint to a computing resource on the network, authorization being determined by the remote computing system in response to **the compliance state**.				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
24.	'038 Patent, Claim 1 A method for controlling the operation of an endpoint, comprising: providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies; maintaining the plurality of policies in a data store on the computing system; identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor; configuring one or more software agents on the endpoint to monitor the plurality of operating conditions; receiving, across a network, at the computing system, status	"compliance polic[y/ies]" '038 Patent Claims 1,12, and 23 '997 Patent Claims 1, 11, and 21 '918 Patent Claims 1, 9, and 17	Plain and ordinary meaning	the items on an endpoint to monitor, the analysis methods to use, and the permitted thresholds for the monitored items	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	information about the plurality of operating conditions on the endpoint gathered by the one or more software agents; determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of **compliance policies** in the data store; and initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint. '038 Patent, Claim 12 A non-transitory computer readable medium containing computer instructions for				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	controlling the operation of an endpoint, comprising: providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies; maintaining the plurality of policies in a data store on the computing system; identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor; configuring one or more software agents on the endpoint to monitor the plurality of operating conditions; receiving, across a network, at the computing system, status information about the plurality of operating				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	conditions on the endpoint gathered by the one or more software agents; determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of **compliance policies** in the data store; and initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint. '038 Patent, Claim 23 A system for controlling the operation of an endpoint, comprising: a user interface, provided by a computing system				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	remote from the end point, configured to allow configuration of a plurality of policies; a data store, at the computing system, that contains the plurality of policies; one or more software agents on the endpoint configured to monitor a plurality of operating conditions identified in the plurality of policies; and one or more hardware processors at the computing system configured to: receive, across a network, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents,				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	determine a compliance state of the endpoint based on the status information and a plurality of **compliance policies** in the data store, and initiate, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by the hardware processor on the endpoint. '997 Patent, Claim 1 A method for controlling the operation of an endpoint, comprising: providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies;				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	maintaining the plurality of policies in a data store on the computing system; identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor; configuring one or more software services provided by an operating system on the endpoint to monitor the plurality of operating conditions; receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services; determining, by the computing system, a compliance state of the endpoint based on the status information and a				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	plurality of **compliance policies** in the data store; and initiating, remotely by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint, such that the computing system remotely ensures endpoint compliance with the plurality of **compliance policies** stored in the data store of the computing system. '997 Patent, Claim 11 A non-transitory computer readable medium containing computer instructions for controlling the operation of an endpoint, comprising:				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies; maintaining the plurality of policies in a data store on the computing system; identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor; configuring one or more software services provided by an operating system on the endpoint to monitor the plurality of operating conditions; receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	one or more software services; determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of **compliance policies** in the data store; and initiating, remotely by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint, such that the computing system remotely ensures endpoint compliance with the plurality of **compliance policies** stored in the data store of the computing system. '997 Patent, Claim 21				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	A system for controlling the operation of an endpoint, comprising: a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies; a data store, at the computing system, that contains the plurality of policies; one or more software services provided by an operating system on the endpoint configured to monitor a plurality of operating conditions identified in the plurality of policies; and one or more hardware processors at the computing system configured to: receive, across a network, status information about				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	the plurality of operating conditions on the endpoint gathered by the one or more software services, determine a compliance state of the endpoint based on the status information and a plurality of **compliance policies** in the data store, and initiate, remotely by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by the hardware processor on the endpoint, such that the computing system remotely ensures endpoint compliance with the plurality of **compliance policies** stored in the data store of the computing system.				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	'918 Patent, Claim 1 A method for controlling the operation of an endpoint, comprising: providing a user interface, at a computing system that is remote from the endpoint, configured to allow configuration of a plurality of policies; maintaining the plurality of policies in a data store on the computing system; identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to evaluate; configuring one or more software services provided by an operating system on the endpoint to monitor the plurality of operating conditions; receiving, across a network, at the				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	computing system, status information about the plurality of operating conditions on the endpoint, gathered by the one or more software services on the endpoint, and user information that identifies a user of the endpoint; determining, by the computing system, a compliance state of the endpoint based on the user information and status information, and a plurality of **compliance policies** in the data store; authorizing access by the endpoint to a computing resource on the network, authorization being determined by the remote computing system in response to the compliance state; and continuing to monitor the compliance state by the				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	endpoint and restricting access to the computing resource if the compliance state changes. '918 Patent, Claim 9 A non-transitory computer readable medium containing computer instructions for controlling the operation of an endpoint, comprising: providing a user interface, at a computing system that is remote from the endpoint, configured to allow configuration of a plurality of policies; maintaining the plurality of policies in a data store on the computing system; identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to evaluate;				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	configuring one or more software services provided by an operating system on the endpoint to monitor the plurality of operating conditions; receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint, gathered by the one or more software services on the endpoint, and user information that identifies a user of the endpoint; determining, by the computing system, a compliance state of the endpoint based on the user information and status information, and a plurality of **compliance policies** in the data store; authorizing access by the endpoint to a computing				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	resource on the network, authorization being determined by the remote computing system in response to the compliance state; and continuing to monitor the compliance state by the endpoint and restricting access to the computing resource if the compliance state changes. '918 Patent, Claim 17 A system for controlling the operation of an endpoint, comprising: a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies; a data store, at the computing system, that contains the plurality of policies;				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	one or more software services provided by an operating system on the endpoint configured to evaluate a plurality of operating conditions identified in the plurality of policies; and one or more hardware processors at the computing system configured to: receive, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint, gathered by the one or more software services on the endpoint, and user information that identifies a user of the endpoint, determine, by the computing system, a compliance state of the endpoint based on the user information and				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	status information, and a plurality of **compliance policies** in the data store, and authorize access by the endpoint to a computing resource on the network, authorization being determined by the remote computing system in response to the compliance state.				
25.	'948 Patent, Claim 1 A method of providing **real-time** operational integrity of an application on a native computing environment, the method comprising: monitoring, by a plurality of sensory inputs, one or more of network dialogs	"real-time" "real time" '948 Patent Claims 1 and 2	Plain and ordinary meaning[2]	immediate	

[2] In its Reply Brief (Dkt. 272 at 11-12), Plaintiff changed its construction of the "real-time"/"real time" terms (in '948 Patent claims 1 and 2) from "without intentional delay, given the processing limitations of the system" (Dkt. 256 at 31-35, fn. 4; Dkt. 259 at 27-29) to "plain and ordinary meaning". Therefore, Defendants have not yet had an opportunity to respond to Plaintiff's new construction.

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	of the application, system operations initiated by the application, a runtime configuration of the application, resource utilization by the application, and integrity of the application; generating **real-time** behavior based events for determining the **real-time** operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor; correlating, by the event and risk correlation matrix, threat classifications based on the temporal sequence of the generated **real-time**				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	behavior based events; and displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, **real-time** status indications for operational integrity of the application. '948 Patent, Claim 2 The method of claim 1, wherein the **real-time** operations of applications are monitored continuously.				
26.	'518 Patent, Claim 1 A method for providing device management	"substantially real time"/ "substantially real-time data"	"without intentional delay, given the processing limitations of the system"[3]	Indefinite	

[3] As noted above in footnote 2, Plaintiff originally proposed that the "real-time"/ "real time" terms (in '948 Patent claims 1 and 2) should have the same construction as the "substantially real time"/ "substantially real-time data" terms (in '518 Patent claims 1, 10 and 17). *See* Dkt. 256 at 31-35, fn. 4; Dkt. 259 at 27-29. In its Reply Brief, Plaintiff changed its construction of the "real-time"/"real time" terms (in '948 Patent claims 1 and 2) to "plain and ordinary meaning", while maintaining its construction for the "substantially real time"/ "substantially real-time data" terms (in '518 Patent claims 1, 10 and 17). Dkt. 272 at 11-12. Therefore, Defendants have not yet had an

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	services comprising steps of: gathering, at a server, from a network, status information related to an operating state of each of a plurality of mobile devices, each mobile device utilizing one of a plurality of different mobile operating systems, wherein the status information for each mobile device is gathered from a plurality of sources including each mobile device in a **substantially real time** manner; formatting the status information for each of the mobile devices, such that rules can be substantially uniformly	'518 Patent Claims 1, 10, and 17			

opportunity to respond to Plaintiff's new construction for the "real-time"/ "real time" terms (in '948 Patent claims 1 and 2) or address new arguments raised for the first time in reply relating to the term "substantially real-time."

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	applied to the status information across the plurality of different mobile operating systems; storing the status information in an electronic database accessible to the server; evaluating, at the server, a first compliance state of each of the mobile devices from the status information using a plurality of administrator-defined rules, wherein each of the rules applies to mobile devices regardless of mobile operating system; and initiating, at the server, at least one action defined by the administrator-defined rules in response to the step of evaluating, wherein the step of evaluating is performed by the server				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	automatically, in response to changes in the status information in the electronic database. '518 Patent, Claim 10 A method for providing device management services comprising steps of: receiving, at a server, a plurality of attributes related to an operating state of each of a plurality of mobile devices, each mobile device utilizing one of a plurality of different mobile operating systems, wherein the attributes for each mobile device are gathered from a plurality of sources including each mobile device; making a determination that an attribute of a mobile device has changed;				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	evaluating the attribute, by a processor at the server in response to the determination, to determine if the attribute change triggers at least one of a plurality of administrator-defined rules, which indicates that the attribute is out of compliance, wherein each of the rules applies to mobile devices regardless of mobile operating system; and automatically initiating, at the server, an action defined by the at least one of a plurality of administrator defined rules if the attribute is out of compliance, wherein the attribute is stored in a data store accessible to the server, that includes **substantially real-time data**, gathered from the plurality of sources on a				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	network and pertaining to a plurality of attributes of a plurality of mobile devices, wherein the **substantially real-time data** is formatted, such that the rules can be substantially uniformly applied to the plurality of attributes across the plurality of different mobile operating systems. '518 Patent, Claim 17 A system for providing device management services comprising: a data store configured to be accessible by a server; a CPU of the server coupled to a memory configured to execute computer readable instructions; computer readable instructions for execution on the server comprising				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	instructions configured to: automatically make a determination that an attribute of a mobile device stored in the data store has changed; evaluate the attribute, in response to the determination, to determine if the attribute change triggers at least one of a plurality of administrator-defined rules, which indicates that the attribute is out of compliance, wherein each of the rules applies to mobile devices regardless of mobile operating system; and automatically initiate an action defined by the at least one of a plurality of administrator defined rules if the attribute is out of compliance,				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	wherein the data store is configured to gather **substantially real-time data** pertaining to a plurality of attributes related to an operating state of each of the plurality of mobile devices, the attributes for each mobile device being gathered from a plurality of sources including each mobile device, wherein each mobile device utilizes one of a plurality of different mobile operating systems, and the **substantially real-time data** is formatted, such that the rules can be substantially uniformly applied to the plurality of attributes across the plurality of different mobile operating systems.				
27.	'948 Patent, Claim 1 A method of providing real-time operational	"which includes a network analyzer, an integrity processor, an event correlation matrix,	Plain and ordinary meaning	Indefinite	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	integrity of an application on a native computing environment, the method comprising: monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime configuration of the application, resource utilization by the application, and integrity of the application; generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment **which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor**;	a risk correlation matrix, and a trust supervisor" '948 Patent Claim 1			

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	correlating, by the event and risk correlation matrix, threat classifications based on the temporal sequence of the generated real-time behavior based events; and displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for operational integrity of the application.				
28.	'948 Patent, Claim 1 A method of providing real-time **operational integrity of an application** on a native computing environment, the method comprising: monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system	"operational integrity of the application" '948 Patent Claim 1	Plain and ordinary meaning	the level of threat or contextual trustworthiness of the application	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	operations initiated by the application, a runtime configuration of the application, resource utilization by the application, and integrity of the application; generating real-time behavior based events for determining the real-time **operational integrity of the application** executing on the native computing environment which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor; correlating, by the event and risk correlation matrix, threat classifications based on the temporal sequence of the generated real-time behavior based events; and				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for **operational integrity of the application**.				
29.	'948 Patent, Claim 1 A method of providing real-time operational integrity of an application on a native computing environment, the method comprising: monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime configuration of the application, resource utilization by the application, and integrity of the application;	"an event correlation matrix" '948 Patent Claim 1	Plain and ordinary meaning	"A matrix which maps integrity warnings to endpoint events, and the rows or columns represent an application instance on the monitored system."	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity processor, **an event correlation matrix**, a risk correlation matrix, and a trust supervisor; correlating, by the **event** and risk **correlation matrix**, threat classifications based on the temporal sequence of the generated real-time behavior based events; and displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	operational integrity of the application.				
30.	'948 Patent, Claim 1 A method of providing real-time operational integrity of an application on a native computing environment, the method comprising: monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime configuration of the application, resource utilization by the application, and integrity of the application; generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which	"a risk correlation matrix" '948 Patent Claim 1	Plain and ordinary meaning	"A matrix which maps endpoint events to system warning classes, system warnings, and/or integrity warnings, and the rows or columns represent a machine identifier or application instance identifier of the monitored system."	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	includes a network analyzer, an integrity processor, an event correlation matrix, **a risk correlation matrix**, and a trust supervisor; correlating, by the event and **risk correlation matrix**, threat classifications based on the temporal sequence of the generated real-time behavior based events; and displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for operational integrity of the application.				
31.	'948 Patent, Claim 1 A method of providing real-time operational integrity of an application on a native computing	"correlating, by the event and risk correlation matrix"	Plain and ordinary meaning	Indefinite	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	environment, the method comprising: monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime configuration of the application, resource utilization by the application, and integrity of the application; generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor; **correlating, by the event and risk correlation**	'948 Patent Claim 1			

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	matrix, threat classifications based on the temporal sequence of the generated real-time behavior based events; and displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for operational integrity of the application.				
32.	'518 Patent, Claim 1 A method for providing device management services comprising steps of: gathering, at a server, from a network, status information related to an operating state of each of a plurality of mobile devices, each mobile device utilizing one of a plurality of different	"initiating… at least one action" / "initiate an action" '518 Patent Claims 1, 10, and 17	Plain and ordinary meaning	Initiating: automatically causing to begin in real time	

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	mobile operating systems, wherein the status information for each mobile device is gathered from a plurality of sources including each mobile device in a substantially real time manner; formatting the status information for each of the mobile devices, such that rules can be substantially uniformly applied to the status information across the plurality of different mobile operating systems; storing the status information in an electronic database accessible to the server; evaluating, at the server, a first compliance state of each of the mobile devices from the status information using a				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	plurality of administrator-defined rules, wherein each of the rules applies to mobile devices regardless of mobile operating system; and **initiating**, at the server, **at least one action** defined by the administrator-defined rules in response to the step of evaluating, wherein the step of evaluating is performed by the server automatically, in response to changes in the status information in the electronic database. '518 Patent, Claim 10 A method for providing device management services comprising steps of: receiving, at a server, a plurality of attributes related to an operating				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	state of each of a plurality of mobile devices, each mobile device utilizing one of a plurality of different mobile operating systems, wherein the attributes for each mobile device are gathered from a plurality of sources including each mobile device; making a determination that an attribute of a mobile device has changed; evaluating the attribute, by a processor at the server in response to the determination, to determine if the attribute change triggers at least one of a plurality of administrator-defined rules, which indicates that the attribute is out of compliance, wherein each of the rules applies to mobile devices regardless				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	of mobile operating system; and automatically **initiating**, at the server, **an action** defined by the at least one of a plurality of administrator defined rules if the attribute is out of compliance, wherein the attribute is stored in a data store accessible to the server, that includes substantially real-time data, gathered from the plurality of sources on a network and pertaining to a plurality of attributes of a plurality of mobile devices, wherein the substantially real-time data is formatted, such that the rules can be substantially uniformly applied to the plurality of attributes across the plurality of different mobile operating systems.				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	'518 Patent, Claim 17 A system for providing device management services comprising: a data store configured to be accessible by a server; a CPU of the server coupled to a memory configured to execute computer readable instructions; computer readable instructions for execution on the server comprising instructions configured to: automatically make a determination that an attribute of a mobile device stored in the data store has changed; evaluate the attribute, in response to the determination, to determine if the attribute change triggers at least one of a plurality of				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	administrator-defined rules, which indicates that the attribute is out of compliance, wherein each of the rules applies to mobile devices regardless of mobile operating system; and automatically **initiate an action** defined by the at least one of a plurality of administrator defined rules if the attribute is out of compliance, wherein the data store is configured to gather substantially real-time data pertaining to a plurality of attributes related to an operating state of each of the plurality of mobile devices, the attributes for each mobile device being gathered from a plurality of sources including each mobile device, wherein each mobile device utilizes one of a plurality				

EXHIBIT A - JOINT CLAIM CONSTRUCTION CHART

#	Claim Language	Claim Term(s), Phrase(s), or Clause(s)	Taasera's Proposed Construction	Defendants' Proposed Construction	Court's Construction
	of different mobile operating systems, and the substantially real-time data is formatted, such that the rules can be substantially uniformly applied to the plurality of attributes across the plurality of different mobile operating systems.				