

EXHIBIT B

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

Claim 1

U.S. Patent No. 8,051,460	Cisco's Identity Services Engine
[Claim 1 – preamble] A method of granting access to a protected network, the method comprising:	Cisco infringes this claim by making, using, testing, offering for sale, and selling the ISE product and system and through performance of each of the claimed steps and/or providing instructions and data from its servers to third-parties to perform at least one of the claimed steps. Further, subsequent to Cisco's making, using, testing, offering for sale, and selling of the ISE, Cisco offers services to third-parties and customers with respect to the ISE. For example, these can include "Technical Services," "Advisory Services," and "Cisco Talos Incident Response" services. (https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/ise-licensing-guide-og.html). For technical services, for example, Cisco encourages customers to purchase "Cisco Smart Net Total Care" for Cisco ISE physical appliances and Software Support (SWSS) contracts for Cisco ISE virtual machines. For advisory services, Cisco offers Expert Services to address "your business objectives with the technology we offer" (including ISE). <i>Id.</i> And for the Talos Incident Response, Cisco provides a full suite of proactive and emergency services to help third-parties prepare, respond, and recover from a cybersecurity breach. Cisco explains that third-parties can "order and transact Cisco Talos Incident Response when ordering Cisco ISE subscriptions." <i>Id.</i> Additionally, and as set forth in InfoExpress's 3-1 disclosures, Cisco's ISE also includes Cisco's ISE (NAC) appliance. Specifically, these are Cisco-provided tangible hardware and "virtual appliances" on which ISE can be deployed. A list of accused ISE (NAC) Appliances (also referred to as "hardware platforms") which ISE supports, are disclosed in InfoExpress's Disclosure of Asserted Claims and Infringement Contentions per Patent L.R. 3-1 and 3-2 at Section II.B.2. These ISE (NAC) Appliances are listed in Cisco's Identity Services Engine

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

[1 – c] using the gatekeeper to determine if requirements of the security policy are satisfied by the access device, and	Cisco's ISE "us[es] the gatekeeper to determine if requirements of the security policy are satisfied by the access device," and induces others to do so. Cisco explains how generally, "ISE allows you to check for compliances, also known as posture, of endpoints, before allowing them to connect to your network." ISE 3.0 Admin Guide at 2. By "check[ing] for compliance" of an endpoint, ISE "uses [its] gatekeeper to determine if requirements of the security policy are satisfied by the access device. <i>See id.</i> • Secure Access: Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods. • Segmentation: Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation. • Posture or Compliance: Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services. ISE 3.0 Admin Guide at 2; <i>see also id.</i> at 1 ("Cisco Identity Services Engine (ISE) is an identity-based network access control and policy enforcement system. It functions as a common policy engine that enables endpoint access control and network device administration for enterprises. . . You can leverage Cisco ISE to ensure compliance . . .") Cisco also provides various examples of how ISE's gatekeeper "determine[s] if requirements of the security policy are satisfied by the access device[.]" Cisco's ISE can obtain the "<i>hardware attributes of an endpoint.</i>" ISE 3.0 Admin Guide at 174; <i>see also id.</i> at 174-5 (listing attributes), 176 ("Cisco ISE profiles the hardware attributes of a
---	--

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	client's system, however, there may be a few hardware attributes Cisco ISE does not profile. . . . The hardware inventory data collection interval can be controlled The default interval is 5 minutes."). Cisco further discloses that one can "check posture compliance" with respect to these hardware attributes – that is, to see if the access device's hardware satisfies requirements that are set in ISE. ISE 3.0 Admin Guide at 1032, 1051; <i>see also id.</i> at 2 ("Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network."). "By "check[ing] for compliance," ISE "us[es] the gatekeeper to determine if requirements of the security policy are satisfied by the access device." Cisco's ISE can also obtain "<i>endpoint attribute data</i>" which further includes "Profiling attributes: the Multi-Factor Classification attributes – Hardware Manufacturer, Hardware Model, Operating System, and Endpoint Type[;] Trust Score attributes: Attributes related to Random MAC addresses, profiling changes, spoofing detection, and other behaviors that are monitored by Cisco AI Endpoint Analytics to calculate comprehensive Trust Scores for endpoints.[';] . . . Endpoint Trust Score [and] [Configuration Management Database ("CMDB")] attributes" <i>Id.</i> at 874-75; <i>see also</i> Randomized Changing MAC at 44 (listing six examples of device attributes). Cisco further discloses that "a Cisco ISE administrator can then create specific authorization rules using these values" – which meet the claimed "requirements of a security policy." <i>See</i> ISE 3.0 Admin Guide at 874. It follows that Cisco ISE can then determine if the endpoint attribute data complies with the "specific authorization rules" – and thus ISE "us[es] the gatekeeper to determine if requirements of the security policy are satisfied by the access device." Cisco's ISE can also obtain "simple posture conditions," including file conditions, registry conditions, application conditions, service conditions, and USB conditions on the client (the claimed "access device"). <i>Id.</i> at 1027. And because it was established that "Cisco ISE allows
--	---

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network[,]” (<i>id.</i> at 2), by “check[ing] for compliance,” ISE “us[es] the gatekeeper to determine if requirements of the security policy are satisfied by the access device.” With respect to Cisco’s own and third-party (i.e. non-Cisco) access points, ISE “validates endpoint compliance [and] . . . authorizes the endpoint” – that is, it “us[es] the gatekeeper to determine if requirements of the security policy are satisfied by the access device.” ISE 3.0 Admin Guide at 804.
--	--

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

3. The method of claim 1, further comprising obtaining system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.	Cisco performs "[t]he method of claim 1, further comprising obtaining system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy" and induces others to do so. As explained above with respect to claim element 1-c, Cisco ISE "uses [its] gatekeeper to determine if requirements of the security policy are satisfied by the access device. Furthermore with respect to that same element were provided several examples of how Cisco does so: • By obtaining the "hardware attributes of an endpoint," • By obtaining "endpoint attribute data," • By obtaining "simple posture conditions," • By, with respect to Cisco's own and third-party (i.e. non-Cisco) access points, "validat[ing] endpoint compliance [and] . . . authoriz[ing] the endpoint," and • By, with respect to guest devices, providing "the posture agent that checks their posture profile and verifies if their device is compliant." These examples of attributes, posture conditions and the like also constitute examples of "system data," which Cisco's ISE "obtain[s] . . . from the access device." And furthermore, just as Cisco ISE "use[s] [its] gatekeeper to determine if requirements of the security policy are satisfied by the access device," it so to "appl[ies] [its] security policy [by] using the system data to determine that the access device satisfies the requirements of the security policy."
--	---

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

4. The method of claim 3, wherein the system data includes antivirus software status.	Cisco's ISE performs "[t]he method of claim 3, wherein the system data includes antivirus software status." Cisco discloses that ISE can "check[] for the latest OS patch, antivirus and antispymware packages with current definition file variables (version, date, etc.).]" Thus, the "system data" (which is used "to determine that the access device satisfies the requirements of the security policy") includes antivirus software status. <table><tr><td>Endpoint posture service</td><td> • Performs posture assessments to endpoints connected to the network. • Enforces the appropriate compliance policies for endpoints through a persistent client-based agent, a temporal agent, or a query to an external MDM/EMM. • Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, antivirus and antispymware packages with current definition file variables (version, date, etc.). antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PIN-lock, rooted or jailbroken status, application presence, and USB-attached media. • Supports automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies. • Provides hardware inventory for full network visibility. • Requires the AnyConnect 4.x agent for posture assessment on these OS platforms: • Windows 10 and later • Mac OS X 10.13 and later • Linux (RedHat Enterprise Linux, SUSE Linux Enterprise Service and Ubuntu) </td></tr></table> See also ISE 3.0 Admin Guide at 1057-58 (posture assessment options include Antivirus Installation and Antivirus Version/ Antivirus Definition Date).	Endpoint posture service	• Performs posture assessments to endpoints connected to the network. • Enforces the appropriate compliance policies for endpoints through a persistent client-based agent, a temporal agent, or a query to an external MDM/EMM. • Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, antivirus and antispymware packages with current definition file variables (version, date, etc.). antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PIN-lock, rooted or jailbroken status, application presence, and USB-attached media. • Supports automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies. • Provides hardware inventory for full network visibility. • Requires the AnyConnect 4.x agent for posture assessment on these OS platforms: • Windows 10 and later • Mac OS X 10.13 and later • Linux (RedHat Enterprise Linux, SUSE Linux Enterprise Service and Ubuntu)
Endpoint posture service	• Performs posture assessments to endpoints connected to the network. • Enforces the appropriate compliance policies for endpoints through a persistent client-based agent, a temporal agent, or a query to an external MDM/EMM. • Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, antivirus and antispymware packages with current definition file variables (version, date, etc.). antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PIN-lock, rooted or jailbroken status, application presence, and USB-attached media. • Supports automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies. • Provides hardware inventory for full network visibility. • Requires the AnyConnect 4.x agent for posture assessment on these OS platforms: • Windows 10 and later • Mac OS X 10.13 and later • Linux (RedHat Enterprise Linux, SUSE Linux Enterprise Service and Ubuntu)		

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

5. The method of claim 1, further comprising communicating between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy.	Cisco's ISE performs "[t]he method of claim 1, further comprising communicating between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy[.]" and induces others to do so. As disclosed above with respect to claim element 1-b, Cisco's ISE uses "posture agents" (the claimed "agent executing on the access device"). These include: • The <i>AnyConnect Agent</i> (which can "report[] a complete list of running and installed applications" on the access device, ISE 3.0 Admin Guide at 1102-03; <i>see also id.</i> at 1057-58); • The <i>AnyConnect Stealth Agent</i> (which reports certain information back to ISE, <i>id.</i> at 1010-11); and • The <i>Cisco Temporal Agent</i>, (which is a "temporary executable file that is run on the client to check the compliance status" and which "is removed from the client machine after the login session is terminated"). Furthermore, as disclosed above with respect to claim 3, Cisco performs the "method of claim 1, further comprising <i>obtaining system data</i> from the access device, and wherein applying the security policy includes using the <i>system data</i> to determine that the access device satisfies the requirements of the security policy[.]" Cisco also discloses several non-limiting examples of "system data." Therefore, these (1) agents (1) "execut[e] on the access device to obtain system data from the access device, and (2) "communicat[e] that system data to ISE's gatekeeper so that (3) ISE can
---	--

U.S. Patent No. 8,051,460 (Cisco's Identity Services Engine)

	"apply[] the security policy [] using th[at] system data to determine that the access device satisfies the requirements of the security policy," Cisco and/or ISE "communicat[e]between the gatekeeper and an agent executing on the access device to obtain system data from the access device, and wherein applying the security policy includes using the system data to determine that the access device satisfies the requirements of the security policy."
6. The method of claim 5, wherein the system data includes information regarding devices connected to the access device.	Cisco's ISE performs "[t]he method of claim 5, wherein the system data includes information regarding devices connected to the access device" and induces others to do so. Cisco states, with respect to "hardware attributes," that they include a field for "attached devices." ISE 3.0 Admin Guide at 174-75. Cisco further explains that "You can click the number in the Attached Devices column that corresponds to an endpoint to view the Name, Category, Manufacturer, Type, Product ID, and Vendor ID of the USB devices that are currently attached to the endpoint." <i>Id.</i>; <i>see also id.</i> 1027 (USB Conditions), 1051 (USB Condition Settings), 1057 (USB_Block "[e]nsures that the endpoint device does not have any USB storage devices connected"). Thus, because Cisco's ISE can determine "attached devices" such as a USB (which are so attached to the endpoint), the system data includes information regarding devices connected to the access device.
10. The method of claim 1, wherein the access point is a network switch.	Cisco's ISE performs "[t]he method of claim 1, wherein the access point is a network switch. and induces others to do so. Cisco explains that with respect to mobile device management (MDM) server integration with ISE, "ISE is the enforcement point . . . [that] then applies the appropriate access control policies to <i>switches</i>, access routers, wireless access points, and other network access points." Randomized and Changing MAC Deployment Guide at 43; <i>see also</i> ISE 3.0 Admin Guide at 830