MICROSOFT EXHIBIT 1089
Microsoft v. Qomplx
IPR2026-00182

EXHIBIT E
U.S. Patent No. 12,301,627

As used herein and with respect to the ’627 Patent, the term “Accused ’627 MSEM Products” means:

(a) Microsoft products that incorporate, rely upon, interact with, or otherwise utilize Microsoft Security Exposure Management (“MSEM”), including at least MSEM itself;

(b) Any other systems, services, or products that utilize the libraries, applications, scripts, packages, or other modules that implement the functionality described below in a manner not materially different with respect to the claims charted below;

(c) any other products that infringe the asserted claims for analogous reasons to those described below; and,

(d) Microsoft products that practice one of more claims of the ’627 Patent.

This claim chart for the ’627 Patent covers all Accused ’627 MSEM Products. The theory of infringement described below in connection with the Asserted Claims is analogous to the theory of infringement for all the Accused ’627 MSEM Products.

I. Claim 1

A computer system comprising: a hardware memory, wherein the computer system is configured to execute software instructions stored on nontransitory machine-readable storage media comprising software instructions that:	The Accused ’627 MSEM Products include a computer system comprising a hardware memory, wherein the computer system is configured to execute software instructions stored on nontransitory machine-readable storage media comprising software instructions that perform as discussed below. For example, MSEM is a cloud software platform.[1] Microsoft’s documentation explains that MSEM “consolidates security posture information and insights from” multiple Microsoft services and “connect[s] to external data sources to further enrich and extend your security posture management. . . . Integration of non-Microsoft security tools will be a consumption-based cost based on number of assets in the connected security tool.”[2] One of skill in the art would understand that such ingestion and processing occurs on computers systems comprising a hardware memory.
store in the hardware memory a representation of a first graph, wherein the representation of the first graph comprises representations of a first plurality of nodes corresponding to a first plurality of entities and further comprises	The software instructions of the Accused ’627 MSEM Products store in the hardware memory a representation of a first graph, wherein the representation of the first graph comprises representations of a first plurality of nodes corresponding to a first plurality of entities and further comprises representations of a first plurality of edges. For example, MSEM stores graphs, including the “enterprise exposure graph” consisting of nodes and edges stored in a pair of tables. The graph may be represented in part as `ExposureGraphNodes` and `ExposureGraphEdges`:[3]

[1] Microsoft, *What is Microsoft Security Exposure Management*, available at `https://learn.microsoft.com/en-us/security-exposure-management/microsoft-security-exposure-management` [hereinafter *What is MSEM?*].

[2] Microsoft, *Integration and licensing for Microsoft Security Exposure Management*, available at `https://learn.microsoft.com/en-us/security-exposure-management/integration-licensing` [hereinafter *MSEM Integration*].

[3] Microsoft, *Schemas and operators overview*, available at `https://learn.microsoft.com/en-us/security-exposure-management/schemas-operators` [hereinafter *Schemas and Operators*].

representations of a first plurality of edges,	**Schema tables** The exposure graph relies on the following tables: • *ExposureGraphNodes* • *ExposureGraphEdges* Microsoft's documentation explains that "`ExposureGraphNodes` contains organizational entities and their properties. These include entities like devices, identities, user groups, and cloud assets such as virtual machines (VMs), storage, and containers. Each node corresponds to an individual entity and encapsulates information about its characteristics, attributes, and security related insights within the organizational structure."[4] **ExposureGraphNodes** *ExposureGraphNodes* contains organizational entities and their properties. These include entities like devices, identities, user groups, and cloud assets such as virtual machines (VMs), storage, and containers. Each node corresponds to an individual entity and encapsulates information about its characteristics, attributes, and security related insights within the organizational structure. Microsoft's documentation further explains that `ExposureGraphEdges` "provides visibility into relationships between entities and assets in the graph."[5]

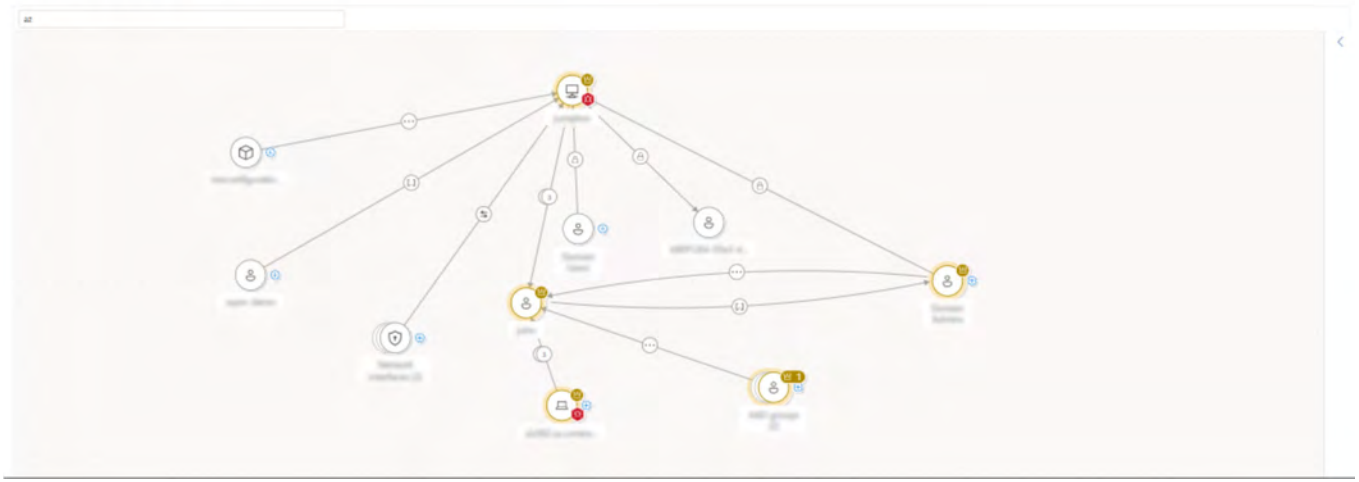
[4] *Schemas and Operators.*

[5] *Id.*

	ExposureGraphEdges The *ExposureGraphEdges* schema, along with the complementing *ExposureGraphNodes* schema, provides visibility into relationships between entities and assets in the graph. Many hunting scenarios require exploration of entity relationships and attack paths. For example, when hunting for devices exposed to a specific critical vulnerability, knowing the relationship between entities, can uncover critical organizational assets. The following are *ExposureGraphEdges* column names, labels, and descriptions: • `EdgeId` (`string`) - The unique identifier for the relationship/edge. • `EdgeLabel` (`string`) - The edge label. Examples: "affecting," "routes traffic to," "is running," and "contains." You can view a list of edge labels by querying the graph. For more information, see List all edge labels in your tenant. • `SourceNodeId` (`string`) - Node ID of the edge's source. Example: "12346aa0-10a5-587e-52f4-280bfc014a08" • `SourceNodeName` (`string`) - The source node display name. Example: "mdvmaas-win-123" • `SourceNodeLabel` (`string`) - The source node label. Example: "microsoft.compute/virtualmachines" • `SourceNodeCategories` (`Dynamic` (json)) - The categories list of the source node. • `TargetNodeId` (`string`) - The node ID of the edge's target. Example: "45676aa0-10a5-587e-52f4-280bfc014a08" • `TargetNodeName` (`string`) - Display name of the target node. Example: gke-test-cluster-1 • `TargetNodeLabel` (`string`) - The target node label. Example: "compute.instances" • `TargetNodeCategories` (`Dynamic` (json)) - The categories list of the target node. • `EdgeProperties` (`Dynamic` (json)) - Optional data relevant for the relationship between the nodes. Example: For the `EdgeLabel` "routes traffic to" with `EdgeProperties` of `networkReachability`, provide information about the port and protocol ranges that are used to transfer traffic from point A to B. Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
wherein the first graph is a directed graph,	The first graph of the Accused ’627 MSEM Products is a directed graph.

	For example, Microsoft’s documentation explains that the `ExposureGraphEdges` table schema includes information about “source nodes” and “target nodes”:[6] **ExposureGraphEdges** The *ExposureGraphEdges* schema, along with the complementing *ExposureGraphNodes* schema, provides visibility into relationships between entities and assets in the graph. Many hunting scenarios require exploration of entity relationships and attack paths. For example, when hunting for devices exposed to a specific critical vulnerability, knowing the relationship between entities, can uncover critical organizational assets. The following are *ExposureGraphEdges* column names, labels, and descriptions: • `EdgeId` (`string`) - The unique identifier for the relationship/edge. • `EdgeLabel` (`string`) - The edge label. Examples: "affecting," "routes traffic to," "is running," and "contains." You can view a list of edge labels by querying the graph. For more information, see List all edge labels in your tenant. • `SourceNodeId` (`string`) - Node ID of the edge's source. Example: "12346aa0-10a5-587e-52f4-280bfc014a08" • `SourceNodeName` (`string`) - The source node display name. Example: "mdvmaas-win-123" • `SourceNodeLabel` (`string`) - The source node label. Example: "microsoft.compute/virtualmachines" • `SourceNodeCategories` (`Dynamic` (json)) - The categories list of the source node. • `TargetNodeId` (`string`) - The node ID of the edge's target. Example: "45676aa0-10a5-587e-52f4-280bfc014a08" • `TargetNodeName` (`string`) - Display name of the target node. Example: gke-test-cluster-1 • `TargetNodeLabel` (`string`) - The target node label. Example: "compute.instances" • `TargetNodeCategories` (`Dynamic` (json)) - The categories list of the target node. • `EdgeProperties` (`Dynamic` (json)) - Optional data relevant for the relationship between the nodes. Example: For the `EdgeLabel` "routes traffic to" with `EdgeProperties` of `networkReachability`, provide information about the port and protocol ranges that are used to transfer traffic from point A to B.

[6] *Id.*

	As another example, Microsoft's documentation shows that MSEM contains an "attack surface map" which comprises a directed graph:[7] **Attack surface map**  Based on Qomplx's analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
wherein the first plurality of entities comprises a plurality of accounts and a plurality of resources, and	The first plurality of entities of the Accused '627 MSEM Products comprise a plurality of accounts and a plurality of resources.

[7] Microsoft, *Overview of critical asset management*, available at `https://learn.microsoft.com/en-us/security-exposure-management/critical-asset-management` [hereinafter *Critical Asset Management*].

	For example, the `ExposureGraphNodes` schema table, as discussed above, "contains organizational entities and their properties" including "entities like devices, identities, user groups, and cloud assets such as virtual machines (VMs), storage, and containers." Microsoft's documentation explains that "[e]ach node corresponds to an individual entity and encapsulates information about its characteristics, attributes, and security related insights within the organizational structure."[8] **ExposureGraphNodes** *ExposureGraphNodes* contains organizational entities and their properties. These include entities like devices, identities, user groups, and cloud assets such as virtual machines (VMs), storage, and containers. Each node corresponds to an individual entity and encapsulates information about its characteristics, attributes, and security related insights within the organizational structure. As another example, MSEM "provides an out-of-the-box catalog of predefined critical asset classifications for assets that include devices, identities, and cloud resources," including "assets such as file servers and domain controllers," "[d]atabases with sensitive data," "identity groups such as Power Users," and "[u]ser roles like Privileged Role Administrator."[9]

[8] *Schemas and Operators*.

[9] *Critical Asset Management*.

	Predefined classifications Security Exposure Management provides an out-of-the-box catalog of predefined critical asset classifications for assets that include devices, identities, and cloud resources. Predefined classifications include: • Critical cyber-security assets such as file servers and domain controllers • Databases with sensitive data • Identity groups such as Power Users • User roles like Privileged Role Administrator In addition, you can create custom critical assets to prioritize what your organization considers to be critical when assessing exposure and risk. Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
wherein each edge of the first plurality of edges corresponds to a respective relationship between a respective pair of entities;	Each edge of the first plurality of edges of the Accused ’627 MSEM Products corresponds to a respective relationship between a respective pair of entities. For example, Microsoft’s documentation explains that the `ExposureGraphEdges` schema table, as discussed above, “provides visibility into relationships between entities and assets in the graph.” Microsoft’s documentation explains that these relationships include, for example, `EdgeLabel` values such as “affecting,” “routes traffic to,” “is running,” and “contains.” Similarly, `EdgeProperties` represent “[o]ptional data relevant for the relationship between the nodes”:[10]

[10] *Schemas and Operators*.

ExposureGraphEdges

The *ExposureGraphEdges* schema, along with the complementing *ExposureGraphNodes* schema, provides visibility into relationships between entities and assets in the graph. Many hunting scenarios require exploration of entity relationships and attack paths. For example, when hunting for devices exposed to a specific critical vulnerability, knowing the relationship between entities, can uncover critical organizational assets.

The following are *ExposureGraphEdges* column names, labels, and descriptions:

- `EdgeId` (`string`) - The unique identifier for the relationship/edge.
- `EdgeLabel` (`string`) - The edge label. Examples: "affecting," "routes traffic to," "is running," and "contains." You can view a list of edge labels by querying the graph. For more information, see List all edge labels in your tenant.
- `SourceNodeId` (`string`) - Node ID of the edge's source. Example: "12346aa0-10a5-587e-52f4-280bfc014a08"
- `SourceNodeName` (`string`) - The source node display name. Example: "mdvmaas-win-123"
- `SourceNodeLabel` (`string`) - The source node label. Example: "microsoft.compute/virtualmachines"
- `SourceNodeCategories` (`Dynamic` (json)) - The categories list of the source node.
- `TargetNodeId` (`string`) - The node ID of the edge's target. Example: "45676aa0-10a5-587e-52f4-280bfc014a08"
- `TargetNodeName` (`string`) - Display name of the target node. Example: gke-test-cluster-1
- `TargetNodeLabel` (`string`) - The target node label. Example: "compute.instances"
- `TargetNodeCategories` (`Dynamic` (json)) - The categories list of the target node.
- `EdgeProperties` (`Dynamic` (json)) - Optional data relevant for the relationship between the nodes. Example: For the `EdgeLabel` "routes traffic to" with `EdgeProperties` of `networkReachability`, provide information about the port and protocol ranges that are used to transfer traffic from point A to B.

Graph Kusto Query Language (KQL) operators

Microsoft Security Exposure Management relies on exposure graph tables and unique exposure graph operators to enable operations over graph structures. The graph is built from tabular data using the `make-graph` operator, and then queried using graph operators.

Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents.

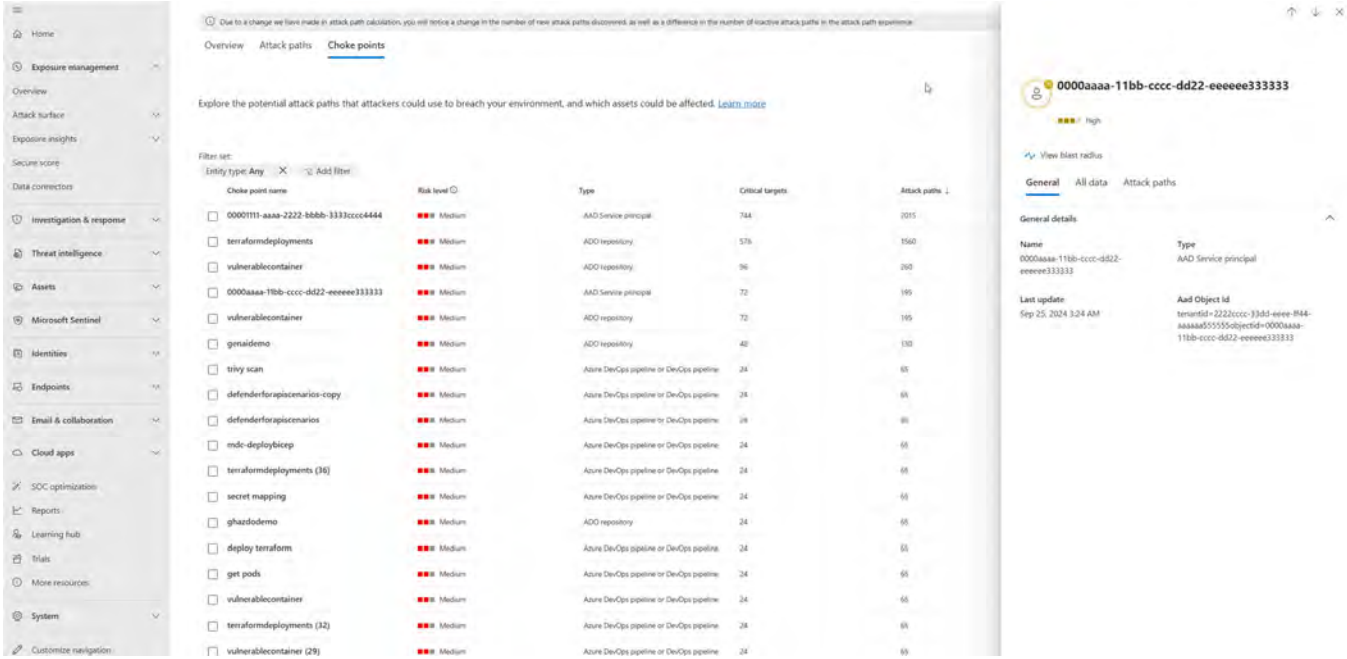
	For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
receive streaming data comprising time-stamped data about events relating to one or more entities of the first plurality of entities,	The software instructions of the Accused ’627 MSEM Products receive streaming data comprising time-stamped data about events relating to one or more entities of the first plurality of entities. For example, Microsoft’s documentation explains that MSEM collects data from a large set of sources, including “Microsoft Defender for Endpoint, Microsoft Defender for Identity, Microsoft Defender for Cloud, Microsoft Entra ID, and others.”[11] **Overview** Microsoft Security Exposure Management consolidates security posture data from all your digital assets, enabling you to map your attack surface and focus your security efforts on areas at greatest risk. Data from Microsoft Security products like Microsoft Defender for Endpoint, Microsoft Defender for Identity, Microsoft Defender for Cloud, Microsoft Entra ID, and others are automatically ingested and consolidated within Exposure Management. You can further enrich and extend this data by connecting to a range of external data sources. To provide coverage of all your assets and security signals and to help you establish a comprehensive, single source of truth for your assets, Exposure Management provides data connectors that ingest data from other security or asset management products deployed in your environment. Benefits include: • Normalized within exposure graph • Enhancing device inventory • Mapping relationships • Revealing new attack paths • Providing comprehensive attack surface visibility • Incorporating asset criticality • Enriching context with business application or operational affiliation • Visualizing through the Attack Map tool • Exploring using advanced hunting queries via KQL

[11] Microsoft, *Overview*, available at `https://learn.microsoft.com/en-us/security-exposure-management/overview-data-connectors` [hereinafter *Overview of Data Connectors*].

	Microsoft's documentation explains that MSEM collects and processes "different types of telemetry data, such as user-login events, device domain membership information, and various network signals . . . to create a comprehensive understanding of the criticality of each domain entity."[12]
	
	As another example, MSEM "continuously discovers assets and workloads, and gathers discovered data into a unified and up-to-date view of your inventory and attack surfaces."[13]
	
	What can I do with Security Exposure Management?
	
	With Security Exposure Management you can:
	
	• **Get a unified view across the organization:** Security Exposure Management continuously discovers assets and workloads, and gathers discovered data into a unified and up-to-date view of your inventory and attack surface.
	
	• **Manage and investigate attack surfaces:** Visualize, analyze, and manage cross-workload attack surfaces.
	  ○ The enterprise exposure graph gathers information to provide a comprehensive view of security posture and exposure across the business.
	  ○ Graph schemas provide contextual information about specific organizational entities such as devices, identities, machines, and storage.
	  ○ Query the enterprise exposure graph to explore assets, assess risk, and hunt for threats across on-premises, hybrid, and multicloud environments.
	  ○ Visualize your environment and graph queries with the attack surface map.

[12] Microsoft, *Critical Asset Protection with Microsoft Security Exposure Management*, available at `https://techcommunity.microsoft.com/blog/microsoft-security-blog/critical-asset-protection-with-microsoft-security-exposure-management/4122645` [hereinafter *Critical Asset Protection]*.

[13] *What is MSEM?*

	As another example, in the screenshot below from Microsoft's documentation, the entity "0000aaaa-11bb-cccc-dd2-eeeeee3333333" has a "[l]ast update" date of "Sep 25, 2024, 3:24 AM."[14]  Based on Qomplx's analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.

[14] Microsoft, *Review attack paths*, available at `https://learn.microsoft.com/en-us/security-exposure-management/review-attack-paths` [hereinafter *Review Attack Paths*].

based on a first portion of the streaming data, identify a first entity that does not correspond to any of the first plurality of nodes, wherein the first entity is not of the first plurality of entities,	Based on a first portion of the streaming data, the software instructions of the Accused ’627 MSEM Products identify a first entity that does not correspond to any of the first plurality of nodes, wherein the first entity is not of the first plurality of entities.
	
	For example, Microsoft’s documentation explains that MSEM “continuously discovers assets and workloads, and gathers discovered data into a unified and up-to-date view of your inventory and attack surface. . . . The enterprise exposure graph gathers information to provide a comprehensive view of security posture and exposure across the business”:[15]
	
	What can I do with Security Exposure Management?
	
	With Security Exposure Management you can:
	
	• **Get a unified view across the organization**: Security Exposure Management continuously discovers assets and workloads, and gathers discovered data into a unified and up-to-date view of your inventory and attack surface.
	
	• **Manage and investigate attack surfaces**: Visualize, analyze, and manage cross-workload attack surfaces.
	  ○ The enterprise exposure graph gathers information to provide a comprehensive view of security posture and exposure across the business.
	  ○ Graph schemas provide contextual information about specific organizational entities such as devices, identities, machines, and storage.
	  ○ Query the enterprise exposure graph to explore assets, assess risk, and hunt for threats across on-premises, hybrid, and multicloud environments.
	  ○ Visualize your environment and graph queries with the attack surface map.
	
	The enterprise exposure graph “includes assets, findings, and entity relationships from” a number of sources, including Defender for Cloud, Defender for Endpoint, Defender Vulnerability Management, Defender for Identity, and Entra ID.[16]

[15] *What is MSEM?*

[16] Microsoft, *Overview of attack surface management*, available at `https://learn.microsoft.com/en-us/security-exposure-management/cross-workload-attack-surfaces` [hereinafter *Overview of Attack Surface Management*].

	As another example, MSEM’s graph representation is “automatically generate[d] . . . based on the data collected across assets and workloads,” and “can fluctuate due to the dynamic nature of IT environments. Our system dynamically generates attack paths based on the real-time conditions of each customer’s environment. Changes such as the addition or removal of assets, updates to configurations, a user logging on or off from a machine, a user added or removed to a group, and the implementation of new network segmentation or security policies can all influence the number and types of attack paths identified”:[17]
	
	Identifying and resolving attack paths
	
	Here's how Exposure Management helps you to identify and resolve attack paths.
	
	• **Attack path generation:** Security Exposure Management automatically generates attack paths based on the data collected across assets and workloads. It simulates attack scenarios, and identifies vulnerabilities and weaknesses that an attacker could exploit.
	  ◦ The number of attack paths visible in the portal can fluctuate due to the dynamic nature of IT environments. Our system dynamically generates attack paths based on the real-time conditions of each customer's environment. Changes such as the addition or removal of assets, updates to configurations, a user logging on or off from a machine, a user added or removed to a group, and the implementation of new network segmentation or security policies can all influence the number and types of attack paths identified.
	  ◦ This approach ensures that the security posture we provide is both accurate and reflective of the latest environment state, accommodating the agility required in today's IT environments.
	
	As another example, MSEM includes a device inventory. “During the onboarding process, the Devices list is gradually populated with devices as they begin to report sensor data”:[18]

[17] Microsoft, *Overview of attack paths*, `https://learn.microsoft.com/en-us/security-exposure-management/work-attack-paths-overview` [hereinafter *Overview of Attack Paths*].

[18] Microsoft, *Device inventory*, available at `https://learn.microsoft.com/en-us/defender-endpoint/machines-view-overview` [hereinafter *Device Inventory*] (emphasis omitted).

	During the onboarding process, the **Devices list** is gradually populated with devices as they begin to report sensor data. Use this view to track your onboarded endpoints as they come online, or download the complete endpoint list as a CSV file for offline analysis. Further, Microsoft’s documentation explains that MSEM performs “device discovery”:[19] **Device discovery overview** 05/08/2025 • Applies to: Microsoft Defender for Endpoint Plan 2 Protecting your environment requires taking inventory of the devices that are in your network. However, mapping devices in a network can often be expensive, challenging, and time-consuming. Microsoft Defender for Endpoint provides a device discovery capability that helps you find unmanaged devices connected to your corporate network without the need for extra appliances or cumbersome process changes. Device discovery uses onboarded endpoints, in your network to collect, probe, or scan your network to discover unmanaged devices. The device discovery capability allows you to discover: • Enterprise endpoints (workstations, servers, and mobile devices) that aren't yet onboarded to Defender for Endpoint • Network devices like routers and switches • IoT devices like printers and cameras MSEM’s “Device Inventory” interface includes a summary of devices discovered in the last 7 days:[20]

[19] Microsoft, *Device discovery overview*, available at `https://learn.microsoft.com/en-us/defender-endpoint/device-discovery` [hereinafter *Device Discovery*].

[20] *Device Discovery*.

	 Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
based on a second portion of the streaming data, wherein the second portion is not identical to the first portion, identify a first relationship between a pair of entities of the first plurality of entities that does not correspond to	Based on a second portion of the streaming data, wherein the second portion is not identical to the first portion, the software instructions of the Accused ’627 MSEM Productsidentify a first relationship between a pair of entities of the first plurality of entities that does not correspond to any of the first plurality of edges. For example, as explained above, Microsoft’s documentation explains that MSEM “continuously discovers assets and workloads, and gathers data into a unified and up-to-date view of your inventory and attack surface.”[21] The graph representation of MSEM is “automatically generate[d] . . . based on the data collected across assets and workloads[,]” and “can fluctuate due to the dynamic nature of IT

[21] *What is MSEM?*

any of the first plurality of edges,	environments.”[22] MSEM “dynamically generates attack paths based on the real-time conditions of each customer’s environment. Changes such as the addition or removal of assets, updates to configurations, a user logging on or off from a machine, a user added or removed to a group, and the implementation of new network segmentation or security policies can all influence the number and types of attack paths identified”:[23]
	
	Identifying and resolving attack paths
	
	Here's how Exposure Management helps you to identify and resolve attack paths.
	
	• **Attack path generation**: Security Exposure Management automatically generates attack paths based on the data collected across assets and workloads. It simulates attack scenarios, and identifies vulnerabilities and weaknesses that an attacker could exploit.
	  ○ The number of attack paths visible in the portal can fluctuate due to the dynamic nature of IT environments. Our system dynamically generates attack paths based on the real-time conditions of each customer's environment. Changes such as the addition or removal of assets, updates to configurations, a user logging on or off from a machine, a user added or removed to a group, and the implementation of new network segmentation or security policies can all influence the number and types of attack paths identified.
	  ○ This approach ensures that the security posture we provide is both accurate and reflective of the latest environment state, accommodating the agility required in today's IT environments.
	
	Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.

modify, in the hardware memory, the representation of the first graph to generate a	The software instructions of the Accused ’627 MSEM Products modify, in the hardware memory, the representation of the first graph to generate a modified representation of the first graph, wherein the modified representation of the first graph comprises a representation of a first node corresponding to the

[22] *Overview of Attack Paths*.

[23] *Id*.

modified representation of the first graph, wherein the modified representation of the first graph comprises a representation of a first node corresponding to the first entity and a representation of a first edge corresponding to the first relationship, wherein the first node is not of the first plurality of nodes and the first edge is not of the first plurality of edges,	first entity and a representation of a first edge corresponding to the first relationship, wherein the first node is not of the first plurality of nodes and the first edge is not of the first plurality of edges. For example, as explained above, MSEM’s graph representation is continuously updated “based on the data collected across assets and workloads,” and “can fluctuate due to the dynamic nature of IT environments. Our system dynamically generates attack paths based on the real-time conditions of each customer’s environment. Changes such as the addition or removal of assets, updates to configurations, a user logging on or off from a machine, a user added or removed to a group, and the implementation of new network segmentation or security policies can all influence the number and types of attack paths identified.”[24] An example of MSEM’s “attack surface map” is shown below:[25]

[24] *Id*.

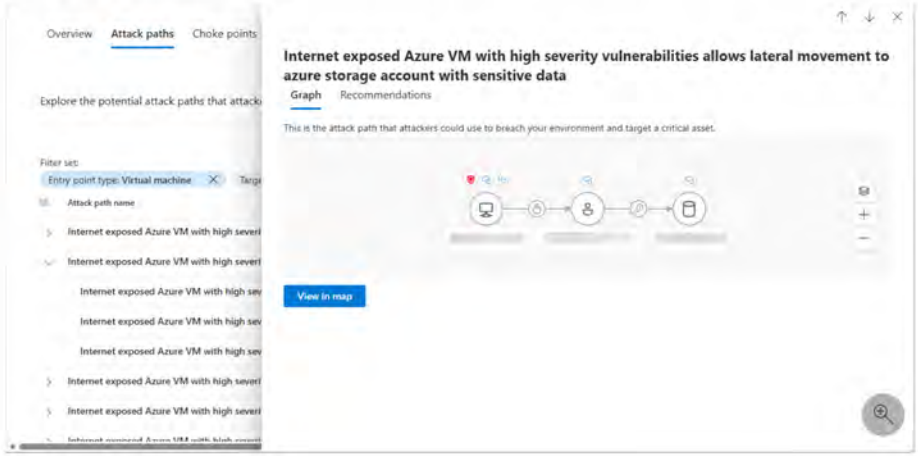
[25] Microsoft, *Getting value from your data connectors*, available at `https://learn.microsoft.com/en-us/security-exposure-management/value-data-connectors` [hereinafter *Value From Your Data Connectors*].

	Exposure graph To explore your assets and enrichment data retrieved from external data products, you can also view this information in the Exposure Graph. Within the Attack Surface map, you can view the nodes representing assets discovered by your connectors, with built-in icons showing the discovery sources for each asset. Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
identify, based on the modified representation of the first graph, an attack path that could be involved in an attack involving the first entity,	Based on the modified representation of the first graph, the software instructions of the Accused ’627 MSEM Products identify an attack path that could be involved in an attack involving the first entity. For example, MSEM uses the continuously updated graph representation to identify attack paths, which are updated along with the graph representation. MSEM “automatically generates attack paths based on

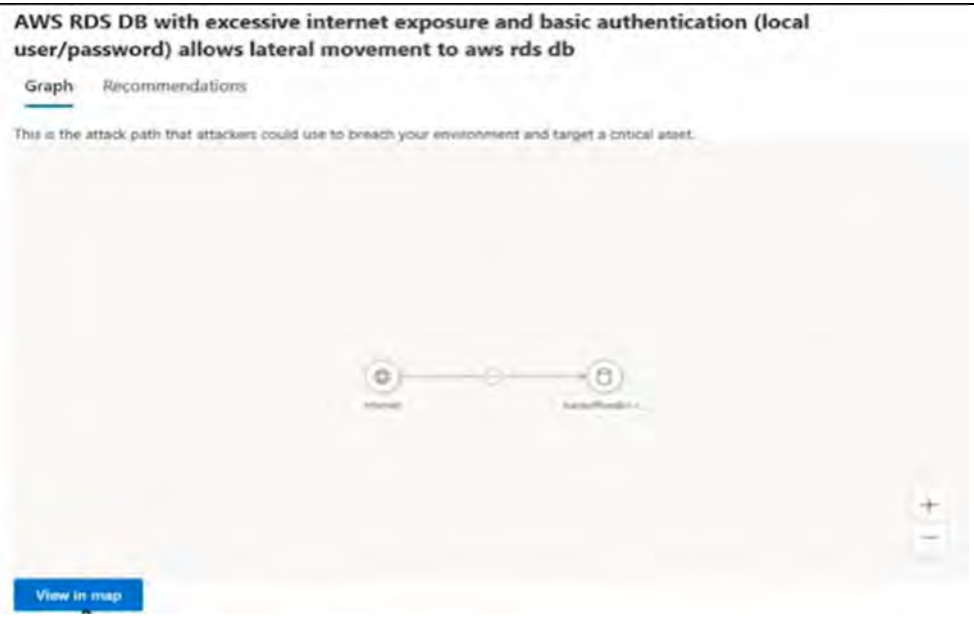
wherein identifying the attack path comprises:	the data collected across assets and workloads. . . . The attack path graph view uses enterprise exposure graph data to visualize the attack path to understand how potential threats might unfold":[26]
	
	Identifying and resolving attack paths
	
	Here's how Exposure Management helps you to identify and resolve attack paths.
	
	• **Attack path generation**: Security Exposure Management automatically generates attack paths based on the data collected across assets and workloads. It simulates attack scenarios, and identifies vulnerabilities and weaknesses that an attacker could exploit.
	  ○ The number of attack paths visible in the portal can fluctuate due to the dynamic nature of IT environments. Our system dynamically generates attack paths based on the real-time conditions of each customer's environment. Changes such as the addition or removal of assets, updates to configurations, a user logging on or off from a machine, a user added or removed to a group, and the implementation of new network segmentation or security policies can all influence the number and types of attack paths identified.
	  ○ This approach ensures that the security posture we provide is both accurate and reflective of the latest environment state, accommodating the agility required in today's IT environments.
	
	• **Attack path visibility**: The attack path graph view uses enterprise exposure graph data to visualize the attack path to understand how potential threats might unfold.
	  ○ Hovering over each node and connector icon provides you with additional information about how the attack path is build. For instance, from an initial virtual machine containing TLS/SSL keys all the way to permissions to storage accounts.
	  ○ The enterprise exposure map extends how you can visualize attack paths. Along with other data, it shows you multiple attack paths and choke points, nodes that create bottlenecks in the graph or map where attack paths converge. It visualizes exposure data, allowing you to see what assets are at risk, and where to prioritize your focus.
	
	As another example, in the screenshot below, MSEM identifies an "attack path that attackers could use to breach your environment and target a critical asset," described as "Internet exposed Azure VM with high severity vulnerabilities allows lateral movement to azure storage account with sensitive data":[27]

[26] *Overview of Attack Paths*.

[27] *Value From Your Data Connectors*

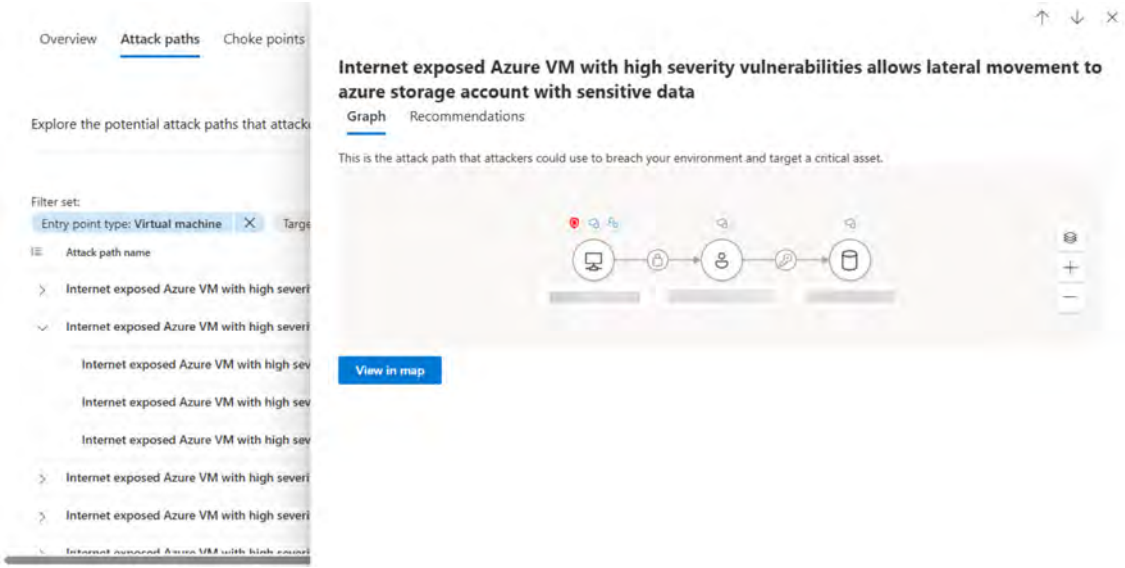
	Attack paths Security Exposure Management automatically generates attack paths based on the data collected across assets and workloads, including data from external connectors. It simulates attack scenarios, and identifies vulnerabilities and weaknesses that an attacker could exploit. As you explore attack paths in your environment, you can view the discovery sources that contributed to this attack path based on the graphical view of the path.  As another example, the following screenshot from a Microsoft video shows an example attack path described as "AWS RDS DB with excessive internet exposure and basic authentication (local user/password) allows lateral movement to aws rds db."[28]

[28] Microsoft, *Transform your defense: Microsoft Security Exposure Management | Microsoft Secure Tech Accelerator*, available at `https://www.youtube.com/watch?v=vY_VmZ9LLgg` (at 19:25).

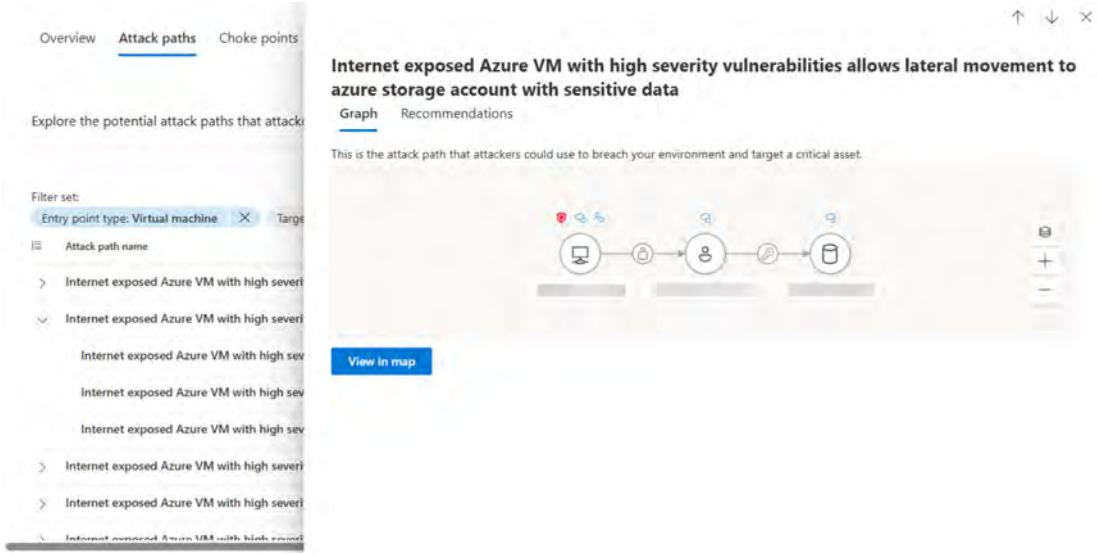
	 As another example, MSEM includes “Cloud Attack paths,” which “illustrate routes that adversaries could exploit to move laterally within your environment, starting from external exposure and progressing toward meaningful impact within your environment”:[29]

[29] *Overview of Attack Paths.*

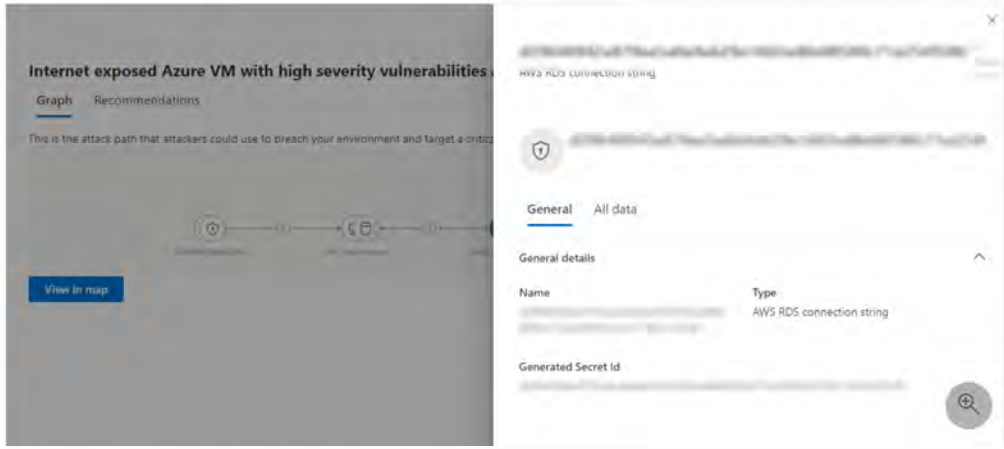
	Cloud attack paths Cloud Attack paths illustrate routes that adversaries could exploit to move laterally within your environment, starting from external exposure and progressing toward meaningful impact within your environment. They help security teams visualize and prioritize real-world risks across their attack surface, focusing on externally-driven, exploitable threats that adversaries could use to compromise your organization. Cloud attack paths reflect real, externally driven and exploitable risks, helping you cut through the noise and act faster. The paths focus on external entry points and how attackers could progress through your environment reaching business-critical targets. Attack Path expands cloud threat detection to cover a broad range of cloud resources, including storage accounts, containers, serverless environments, unprotected repositories, unmanaged APIs, and AI agents. Each attack path is built from a real, exploitable weakness such as exposed endpoints, misconfigured access settings, or leaked credentials, ensuring that identified threats reflect genuine risk scenarios. By analyzing cloud configuration data and performing active reachability scans, the system validates whether exposures are accessible from outside the environment, reducing false positives and emphasizing threats that are both real and actionable. Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
identifying a second entity that can be reached using the first entity, wherein the second entity corresponds to a second node, and the second node is related by one or more edges to the first node corresponding to the first entity in the modified	Identifying the attack path comprises identifying a second entity that can be reached using the first entity, wherein the second entity corresponds toa second node, and the second node is related by one or more edges to the first node corresponding to the first entity in the modified representation of the first graph.

representation of the first graph; and,	For example, in the example attack path “Internet exposed Azure VM with high severity vulnerabilities allows lateral movement to azure storage account with sensitive data,” shown below, the Accused ’627 MSEM Products identify a first and second node related by an edge:[30]  Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
identifying a third entity that can be reached using the second entity, wherein the	The software instructions of the Accused ’627 MSEM Products identify a third entity that can be reached using the second entity, wherein the third entity corresponds to a third node, and the third node is related by one or more edges to the second node in the modified representation of the first graph.

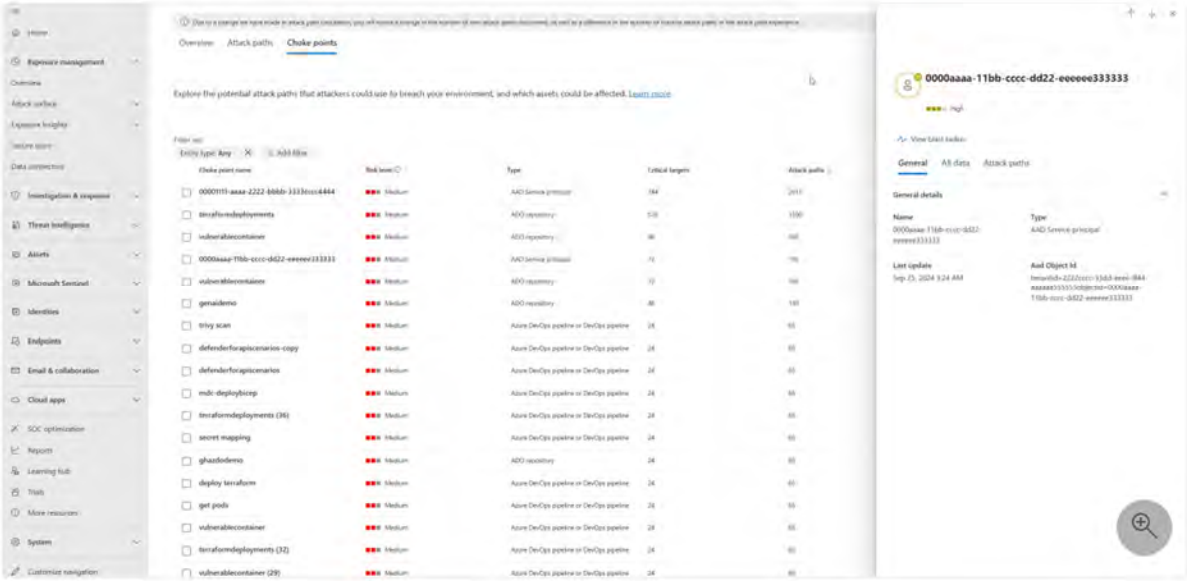
[30] *Value From Your Data Connectors.*

third entity corresponds to a third node, and the third node is related by one or more edges to the second node in the modified representation of the first graph; and	For example, in the example attack path “Internet exposed Azure VM with high severity vulnerabilities allows lateral movement to azure storage account with sensitive data,” shown above, MSEM identifies a third node that is related to a second node by an edge.[31]  Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
generate a report comprising an identification of the first entity and at least one of the	The software instructions of the Accused ’627 MSEM Products generate a report identifying the first entity and at least one of the second and third entities.

[31] *Id.*

second entity and the third entity.	For example, Microsoft's documentation explains that MSEM provides "additional information about how the attack path is built" and "actionable recommendations to mitigate the identified attack paths":[32] **Examine an attack path** 1. Select a specific attack path to examine it further for potential exploitable vulnerabilities. 2. In the **Attack Path** graph, hover over a node or edge (connector) icon to see additional information about how the attack path is built.  **Review recommendations** 1. Select the **Recommendations** tab to view the list of actionable recommendations to mitigate the identified attack paths. 2. Sort recommendations by heading or select a specific recommendation, to open the recommendation screen. 3. Review recommendation details, and then select **Manage** to remediate the recommendation in the correct workload interface.

[32] *Review Attack Paths*.

	As another example, in the screenshot below from Microsoft's documentation, "[g]eneral details" are provided for AAD Service principal entity "0000aaaa-11bb-cccc-dd2-eeeeee3333333."[33] **View choke points and blast radius** 1. Go the choke points tab to view a list of choke points on the attack path dashboard. By focusing on these choke points, you can reduce risk by addressing high-impact assets, thus preventing attackers from progressing through various paths. 2. Select a choke point to open the side panel, select **View blast radius** and explore the attack paths from a choke point. The blast radius provides a detailed visualization showing how the compromise of one asset could affect others. This enables security teams to assess the broader implications of an attack and prioritize mitigation strategies more effectively. 

[33] *Id.*

	Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.

II. Claim 5

The computer system of claim 1	See above for an analysis of Claim 1.
wherein the modified representation of the first graph comprises a representation of a node corresponding to the first entity, wherein the first entity is identified based on active reconnaissance results.	The modified representation of the first graph of Claim 1 comprises a representation of a node corresponding to the first entity, wherein the first entity is identified based on active reconnaissance results. For example, Microsoft's documentation explains that MSEM "perform[s] active reachability scans" to "validate[] whether exposures are accessible from outside the environment":[34] **Cloud attack paths** Cloud Attack paths illustrate routes that adversaries could exploit to move laterally within your environment, starting from external exposure and progressing toward meaningful impact within your environment. They help security teams visualize and prioritize real-world risks across their attack surface, focusing on externally-driven, exploitable threats that adversaries could use to compromise your organization. Cloud attack paths reflect real, externally driven and exploitable risks, helping you cut through the noise and act faster. The paths focus on external entry points and how attackers could progress through your environment reaching business-critical targets. Attack Path expands cloud threat detection to cover a broad range of cloud resources, including storage accounts, containers, serverless environments, unprotected repositories, unmanaged APIs, and AI agents. Each attack path is built from a real, exploitable weakness such as exposed endpoints, misconfigured access settings, or leaked credentials, ensuring that identified threats reflect genuine risk scenarios. By analyzing cloud configuration data and performing active reachability scans, the system validates whether exposures are accessible from outside the environment, reducing false positives and emphasizing threats that are both real and actionable. As another example, MSEM "consolidates security posture data from all your digital assets," including "[d]ata from Microsoft Security products like Microsoft Defender for Endpoint, Microsoft

[34] *Overview of Attack Paths.*

	Defender for Identity, Microsoft Defender for Cloud, Microsoft Entra ID, and others."[35] Defender for Endpoint, for example, includes "Standard discovery," a "device discovery capability that helps you find unmanaged devices connected to your corporate network." Standard discovery "uses smart, active probing to discover additional information about observed devices to enrich existing device information."[36] For example, Standard discovery "uses various PowerShell scripts to actively probe devices in the network. Those PowerShell scripts are Microsoft signed and are executed from the following location: `C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Downloads\*.ps`. For example, `C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Downloads\UnicastScannerV1.1.0.ps1`."[37] Based on Qomplx's analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.

[35] *Overview of Data Connectors*.

[36] *Device Discovery*.

[37] Microsoft, *Configure device discovery in Defender for Endpoint*, available at `https://learn.microsoft.com/en-us/defender-endpoint/configure-device-discovery`.

III. Claim 6

The computer system of claim 1	See above for an analysis of Claim 1.
wherein the modified representation of the first graph comprises a representation of a node corresponding to the first entity, wherein the first entity is identified based on passive reconnaissance results.	The modified representation of the first graph of Claim 1 comprises a representation a node corresponding to the first entity, wherein the first entity is identified based on passive reconnaissance results. For example, as noted above, MSEM “consolidates security posture data from all your digital assets,” including “[d]ata from Microsoft Security products like Microsoft Defender for Endpoint, Microsoft Defender for Identity, Microsoft Defender for Cloud, Microsoft Entra ID, and others.”[38] Defender for Endpoint includes “Basic discovery,” a “device discovery capability that helps you find unmanaged devices connected to your corporate network.”[39] Basic discovery “passively collect[s] events in your network and extract[s] device information from them,” “us[ing] the `SenseNDR.exe` binary for passive network data collection and no network traffic is initiated. Endpoints extract data from all network traffic seen by an onboarded device.”[40] Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.

[38] *Overview of Data Connectors*.

[39] *Device Discovery*.

[40] *Id.*

IV. Claim 11

The computer system of claim 1,	See above for an analysis of Claim 1.
wherein the computer system is further configured to execute software instructions stored on nontransitory machine-readable storage media comprising software instructions that determine whether an event, of the events relating to one or more entities of the first plurality of entities, is anomalous, wherein determining whether the event is anomalous comprises: determining that the event relates to the first entity,	The software instructions of the Accused ’627 MSEM Products determine whether an event, of the events relating to one or more entities of the first plurality of entities, is anomalous, wherein determining whether the event is anomalous comprises determining that the event relates to the first entity, determining at least one behavior pattern associated with the first entity, and comparing the event to the at least one behavior pattern. For example, MSEM “consolidates cloud security posture information and insights from workloads that include,” among others, “Microsoft Defender for Cloud Apps.”[41] Defender for Cloud Apps “combin[es] multiple detection methods, including anomaly, behavioral analytics (UEBA), and rule-based activity detections, to provide a broad view of how your users use apps in your environment.”[42] Microsoft’s documentation explains that Defender for Cloud Apps’ detection methods determine behavioral patterns associated with entities and compare events related to such entities to behavioral patterns. For example, Defender for Cloud Apps uses “user and entity behavioral analytics (UEBA) and machine learning (ML)” to “target[] numerous behavioral anomalies across your users and the machines and devices connected to your network.”[43]

[41] *MSEM Integration*.

[42] Microsoft, *Tutorial: Detect suspicious user activity with behavioral analytics (UEBA)*, available at `https://learn.microsoft.com/en-us/defender-cloud-apps/tutorial-suspicious-activity` [hereinafter *Detect Suspicious User Activity*].

[43] Microsoft, *Create Defender for Cloud Apps anomaly detection policies*, available at `https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy` [hereinafter *Anomaly Detection Policies*].

determining at least one behavior pattern associated with the first entity, and comparing the event to the at least one behavior pattern.	As another example, Defender for Cloud apps “[d]etects multiple file download activities in a single session with respect to the baseline learned,” and “[d]etects multiple administrative activities in a single session with respect to the baseline learned.”[44] **Phase 2: Tune anomaly detection policies** Several built-in anomaly detection policies are available in Defender for Cloud Apps that are preconfigured for common security use cases. You should take some time to familiarize yourself with the more popular detections, such as: • **Impossible travel** Activities from the same user in different locations within a period that is shorter than the expected travel time between the two locations. • **Activity from infrequent country** Activity from a location that wasn't recently or never visited by the user. • **Malware detection** Scans files in your cloud apps and runs suspicious files through Microsoft's threat intelligence engine to determine whether they're associated with known malware. • **Ransomware activity** File uploads to the cloud that might be infected with ransomware. • **Activity from suspicious IP addresses** Activity from an IP address that has been identified as risky by Microsoft Threat Intelligence. • **Suspicious inbox forwarding** Detects suspicious inbox forwarding rules set on a user's inbox. • **Unusual multiple file download activities** Detects multiple file download activities in a single session with respect to the baseline learned, which could indicate an attempted breach. • **Unusual administrative activities** Detects multiple administrative activities in a single session with respect to the baseline learned, which could indicate an attempted breach. As another example, the “impossible travel” detection “uses a machine-learning algorithm” that “learns a new user’s activity pattern” and “identifies unusual and impossible user activity between two locations.” Similarly, the “infrequent country” detection “stores information about previous locations used by the user. An alert is triggered when an activity occurs from a location that wasn’t

[44] *Detect Suspicious User Activity.*

	recently or never visited by the user.”[45] As another example, the “unusual activities (by user)” detection “look for activities within a single session with respect to the baseline learned, which could indicate on a breach attempt. These detections leverage a machine-learning algorithm that profiles the users log on pattern and reduces false positives. These detections are part of the heuristic anomaly detection engine that profiles your environment and triggers alerts with respect to a baseline that was learned on your organization’s activity”:[46]

[45] *Anomaly Detection Policies.*

[46] *Id.*

	Unusual activities (by user) These detections identify users who perform: • Unusual multiple file download activities • Unusual file share activities • Unusual file deletion activities • Unusual impersonated activities • Unusual administrative activities • Unusual Power BI report sharing activities (preview) • Unusual multiple VM creation activities (preview) • Unusual multiple storage deletion activities (preview) • Unusual region for cloud resource (preview) ⓘ Note As part of ongoing improvements to Defender for Cloud Apps alert threat protection capabilities, the policy with the title "Suspicious file access activity (by user)" has been disabled, migrated to the new dynamic model and renamed to **Suspicious file access indicative of lateral movement** and **Suspicious file access from untrusted ISP and user agent with malicious IP indicator**. If you previously configured governance actions or email notifications for this policy, you can re-enable it at any time in the Microsoft Defender portal > Cloud Apps > Policy management page. These policies look for activities within a single session with respect to the baseline learned, which could indicate on a breach attempt. These detections leverage a machine-learning algorithm that profiles the users log on pattern and reduces false positives. These detections are part of the heuristic anomaly detection engine that profiles your environment and triggers alerts with respect to a baseline that was learned on your organization's activity. Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.

V. Claim 12

The computer system of claim 11,	See above for an analysis of Claim 11.
wherein comparing the event to the at least one behavior pattern comprises using a threshold.	Comparing the event to the at least one behavior pattern of Claim 11 comprises using a threshold. For example, Defender for Cloud Apps uses tuning and thresholds to determine whether to flag an event as anomalous. Microsoft Defender for Cloud Apps allows users to set "dynamic thresholds" for anomaly detection.[47] Next, you want to tune your policies. The following policies can be fine-tuned by setting filters, dynamic thresholds (UEBA) to help train their detection models, and suppressions to reduce common false positive detections: • Anomaly detection • Cloud discovery anomaly detection • Rule-based activity detection As another example, the "impossible travel" detection discussed above contains a "sensitivity slider" to "determine[] the level of suppressions applied to anomalous behavior before triggering an impossible travel alert[,]" offering "Low," "Medium," and "High" sensitivity levels.[48]

[47] *Detect Suspicious User Activity.*

[48] *Id.*

	3. **Tune sensitivity of impossible travel** Configure the sensitivity slider that determines the level of suppressions applied to anomalous behavior before triggering an impossible travel alert. For example, organizations interested in high fidelity should consider increasing the sensitivity level. On the other hand, if your organization has many users that travel, consider lowering the sensitivity level to suppress activities from a user's common locations learned from previous activities. You can choose from the following sensitivity levels: • **Low**: System, tenant, and user suppressions • **Medium**: System and user suppressions • **High**: Only system suppressions As another example, Defender for Cloud Apps offers the ability to tune "the volume of activity required before the detection raises an alert."[49] **Phase 4: Tune rule-based detection (activity) policies** Rule-based detection policies give you the ability to complement anomaly detection policies with organization-specific requirements. We recommend creating rules-based policies using one of our Activity policy templates (go to **Control** > **Templates** and set the **Type** filter to **Activity policy**) and then configuring them to detect behaviors that aren't normal for your environment. For example, for some organization that don't have any presence in a particular country/region, it may make sense to create a policy that detects the anomalous activities from that country/region and alert on them. For others, who have large branches in that country/region, activities from that country/region would be normal and it wouldn't make sense to detect such activities. 1. **Tune activity volume** Choose the volume of activity required before the detection raises an alert. Using our country/region example, if you have no presence in a country/region, even a single activity is significant and warrants an alert. However, a single sign-in failure could be human error and only of interest if there are many failures in a short period. 2. **Tune activity filters** Set the filters you require to detect the type of activity you want to alert on. For example, to detect activity from a country/region, use the **Location** parameter. 3. **Tune alerts** To prevent alert fatigue, set the **daily alert limit**. Based on Qomplx's analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be

[49] *Id.*

	insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.

VI. Claim 14

The computer system of claim 1,	See above for an analysis of Claim 1.
wherein the computer system comprises a plurality of physical computing machines.	The computer system of Claim 1 comprises a plurality of physical computing machines. For example, as explained above, MSEM is a cloud software platform that “consolidates security posture information and insights from workloads that include” a wide variety of Microsoft products and services and “connect[s] to external data sources to further enrich and extend your security posture management. . . . Integration of non-Microsoft security tools will be a consumption-based cost based on number of assets in the connected security tool.”[50] One of skill in the art would understand that such ingestion and processing occurs on a plurality of physical computing machines. Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.

[50] *MSEM Integration.*

VII. Claim 16

The computer system of claim 1,	See above for an analysis of Claim 1.
wherein at least one entity of the first plurality of entities is at least one of a user, a place, a device, a resource, a group, or a service.	At least one entity of the first plurality of entities of Claim 1 is at least one of a user, a place, a device, a resource, a group, or a service. For example, as explained above, MSEM represents graph nodes using the `ExposureGraphNodes` table. Microsoft's documentation explains that "`ExposureGraphNodes` contains organizational entities" such as "devices, identities, user groups, and cloud assets such as virtual machines (VMs), storage, and containers.[51] **ExposureGraphNodes** *ExposureGraphNodes* contains organizational entities and their properties. These include entities like devices, identities, user groups, and cloud assets such as virtual machines (VMs), storage, and containers. Each node corresponds to an individual entity and encapsulates information about its characteristics, attributes, and security related insights within the organizational structure. Based on Qomplx's analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.

[51] *Schemas and Operators.*

VIII. Claim 18

A computer system comprising: a hardware memory, wherein the computer system is configured to execute software instructions stored on nontransitory machine-readable storage media comprising software instructions that:	The Accused ’627 MSEM Products include a computer system comprising a hardware memory, wherein the computer system is configured to execute software instructions stored on nontransitory machine-readable storage media comprising software instructions that perform as discussed below. For example, MSEM is a cloud software platform.[52] Microsoft’s documentation explains that MSEM “consolidates cloud security posture information and insights from” multiple Microsoft services and “connect[s] to external data sources to further enrich and extend your security posture management. . . . Integration of non-Microsoft security tools will be a consumption-based cost based on number of assets in the connected security tool.”[53] One of skill in the art would understand that such ingestion and processing occurs on computers systems comprising a hardware memory.
store in the hardware memory a representation of a first graph, wherein the representation of the first graph comprises representations of a first plurality of nodes corresponding to a first plurality of entities and further comprises representations of a first plurality of edges,	The software instructions of the Accused ’627 MSEM Products store in the hardware memory a representation of a first graph, wherein the representation of the first graph comprises representations of a first plurality of nodes corresponding to a first plurality of entities and further comprises representations of a first plurality of edges. For example, MSEM stores graphs, including the “enterprise exposure graph” consisting of nodes and edges stored in a pair of tables. The graph may be represented in part as `ExposureGraphNodes` and `ExposureGraphEdges`:[54]

[52] *What is MSEM?*.

[53] *MSEM Integration.*

[54] *Schemas and Operators*.

	Schema tables The exposure graph relies on the following tables: • *ExposureGraphNodes* • *ExposureGraphEdges* Microsoft's documentation explains that "`ExposureGraphNodes` contains organizational entities and their properties. These include entities like devices, identities, user groups, and cloud assets such as virtual machines (VMs), storage, and containers. Each node corresponds to an individual entity and encapsulates information about its characteristics, attributes, and security related insights within the organizational structure."[55] **ExposureGraphNodes** *ExposureGraphNodes* contains organizational entities and their properties. These include entities like devices, identities, user groups, and cloud assets such as virtual machines (VMs), storage, and containers. Each node corresponds to an individual entity and encapsulates information about its characteristics, attributes, and security related insights within the organizational structure. Microsoft's documentation further explains that `ExposureGraphEdges` "provides visibility into relationships between entities and assets in the graph."[56]

[55] *Id.*

[56] *Id.*

	ExposureGraphEdges The *ExposureGraphEdges* schema, along with the complementing *ExposureGraphNodes* schema, provides visibility into relationships between entities and assets in the graph. Many hunting scenarios require exploration of entity relationships and attack paths. For example, when hunting for devices exposed to a specific critical vulnerability, knowing the relationship between entities, can uncover critical organizational assets. The following are *ExposureGraphEdges* column names, labels, and descriptions: • `EdgeId` (`string`) - The unique identifier for the relationship/edge. • `EdgeLabel` (`string`) - The edge label. Examples: "affecting," "routes traffic to," "is running," and "contains." You can view a list of edge labels by querying the graph. For more information, see List all edge labels in your tenant. • `SourceNodeId` (`string`) - Node ID of the edge's source. Example: "12346aa0-10a5-587e-52f4-280bfc014a08" • `SourceNodeName` (`string`) - The source node display name. Example: "mdvmaas-win-123" • `SourceNodeLabel` (`string`) - The source node label. Example: "microsoft.compute/virtualmachines" • `SourceNodeCategories` (`Dynamic` (json)) - The categories list of the source node. • `TargetNodeId` (`string`) - The node ID of the edge's target. Example: "45676aa0-10a5-587e-52f4-280bfc014a08" • `TargetNodeName` (`string`) - Display name of the target node. Example: gke-test-cluster-1 • `TargetNodeLabel` (`string`) - The target node label. Example: "compute.instances" • `TargetNodeCategories` (`Dynamic` (json)) - The categories list of the target node. • `EdgeProperties` (`Dynamic` (json)) - Optional data relevant for the relationship between the nodes. Example: For the `EdgeLabel` "routes traffic to" with `EdgeProperties` of `networkReachability`, provide information about the port and protocol ranges that are used to transfer traffic from point A to B. Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
wherein the first graph is a directed graph,	The first graph of the Accused ’627 MSEM Products is a directed graph.

For example, Microsoft's documentation explains that the `ExposureGraphEdges` table schema includes information about "source nodes" and "target nodes":[57]

ExposureGraphEdges

The *ExposureGraphEdges* schema, along with the complementing *ExposureGraphNodes* schema, provides visibility into relationships between entities and assets in the graph. Many hunting scenarios require exploration of entity relationships and attack paths. For example, when hunting for devices exposed to a specific critical vulnerability, knowing the relationship between entities, can uncover critical organizational assets.

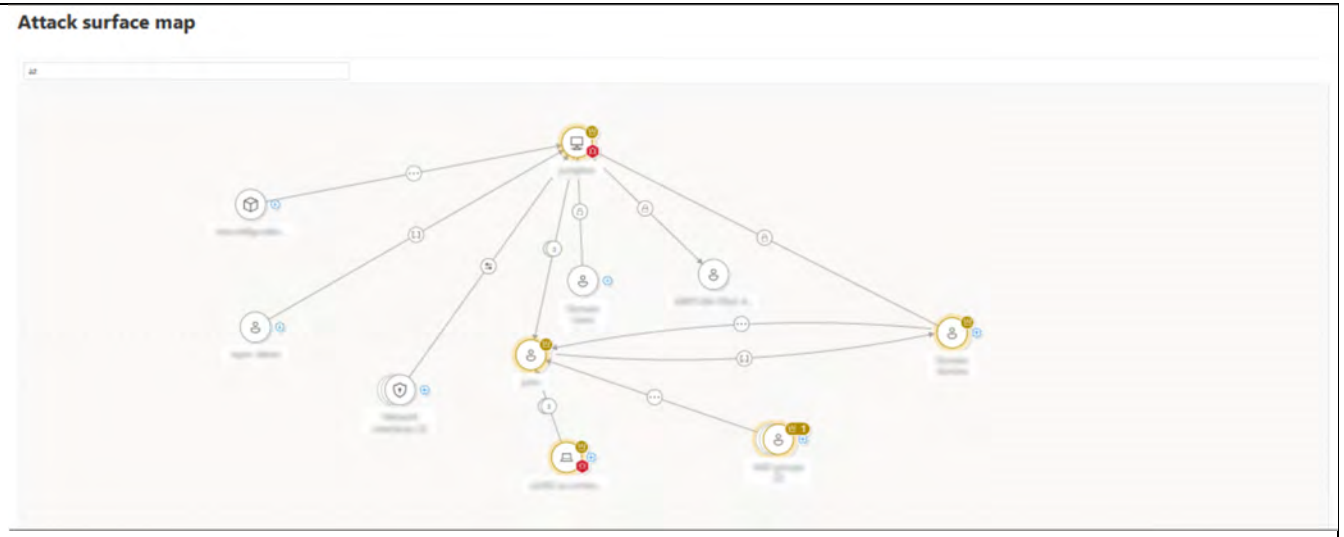
The following are *ExposureGraphEdges* column names, labels, and descriptions:

- `EdgeId` (`string`) - The unique identifier for the relationship/edge.
- `EdgeLabel` (`string`) - The edge label. Examples: "affecting," "routes traffic to," "is running," and "contains." You can view a list of edge labels by querying the graph. For more information, see List all edge labels in your tenant.
- `SourceNodeId` (`string`) - Node ID of the edge's source. Example: "12346aa0-10a5-587e-52f4-280bfc014a08"
- `SourceNodeName` (`string`) - The source node display name. Example: "mdvmaas-win-123"
- `SourceNodeLabel` (`string`) - The source node label. Example: "microsoft.compute/virtualmachines"
- `SourceNodeCategories` (`Dynamic` (json)) - The categories list of the source node.
- `TargetNodeId` (`string`) - The node ID of the edge's target. Example: "45676aa0-10a5-587e-52f4-280bfc014a08"
- `TargetNodeName` (`string`) - Display name of the target node. Example: gke-test-cluster-1
- `TargetNodeLabel` (`string`) - The target node label. Example: "compute.instances"
- `TargetNodeCategories` (`Dynamic` (json)) - The categories list of the target node.
- `EdgeProperties` (`Dynamic` (json)) - Optional data relevant for the relationship between the nodes. Example: For the `EdgeLabel` "routes traffic to" with `EdgeProperties` of `networkReachability`, provide information about the port and protocol ranges that are used to transfer traffic from point A to B.

As another example, Microsoft's documentation shows that MSEM contains an "attack surface map" which comprises a directed graph.[58]

[57] *Id.*

[58] *Critical Asset Management.*

	 Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
wherein the first plurality of entities comprises a plurality of accounts and a plurality of resources, and	The first plurality of entities of the Accused ’627 MSEM Products comprise a plurality of accounts and a plurality of resources. For example, the `ExposureGraphNodes` schema table, as discussed above, “contains organizational entities and their properties” including “entities like devices, identities, user groups, and cloud assets such as virtual machines (VMs), storage, and containers.” Microsoft’s documentation

	explains that "[e]ach node corresponds to an individual entity and encapsulates information about its characteristics, attributes, and security related insights within the organizational structure."[59] **ExposureGraphNodes** *ExposureGraphNodes* contains organizational entities and their properties. These include entities like devices, identities, user groups, and cloud assets such as virtual machines (VMs), storage, and containers. Each node corresponds to an individual entity and encapsulates information about its characteristics, attributes, and security related insights within the organizational structure. As another example, MSEM "provides an out-of-the-box catalog of predefined critical asset classifications for assets that include devices, identities, and cloud resources," including "assets such as file servers and domain controllers," "[d]atabases with sensitive data," "[i]dentity groups such as Power Users," and "[u]ser roles like Privileged Role Administrator."[60] **Predefined classifications** Security Exposure Management provides an out-of-the-box catalog of predefined critical asset classifications for assets that include devices, identities, and cloud resources. Predefined classifications include: • Critical cyber-security assets such as file servers and domain controllers • Databases with sensitive data • Identity groups such as Power Users • User roles like Privileged Role Administrator In addition, you can create custom critical assets to prioritize what your organization considers to be critical when assessing exposure and risk.

[59] *Schemas and Operators.*

[60] *Critical Asset Management.*

	Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
wherein each edge of the first plurality of edges corresponds to a respective relationship between a respective pair of entities;	Each edge of the first plurality of edges of the Accused ’627 MSEM Products corresponds to a respective relationship between a respective pair of entities. For example, Microsoft’s documentation explains that the `ExposureGraphEdges` schema table, as discussed above, “provides visibility into relationships between entities and assets in the graph.” Microsoft’s documentation explains that these relationships include, for example, `EdgeLabel` values such as “affecting,” “routes traffic to,” “is running,” and “contains.” Similarly, `EdgeProperties` represent “[o]ptional data relevant for the relationship between the nodes”:[61]

[61] *Schemas and Operators*.

ExposureGraphEdges

The *ExposureGraphEdges* schema, along with the complementing *ExposureGraphNodes* schema, provides visibility into relationships between entities and assets in the graph. Many hunting scenarios require exploration of entity relationships and attack paths. For example, when hunting for devices exposed to a specific critical vulnerability, knowing the relationship between entities, can uncover critical organizational assets.

The following are *ExposureGraphEdges* column names, labels, and descriptions:

- `EdgeId` (`string`) - The unique identifier for the relationship/edge.
- `EdgeLabel` (`string`) - The edge label. Examples: "affecting," "routes traffic to," "is running," and "contains." You can view a list of edge labels by querying the graph. For more information, see List all edge labels in your tenant.
- `SourceNodeId` (`string`) - Node ID of the edge's source. Example: "12346aa0-10a5-587e-52f4-280bfc014a08"
- `SourceNodeName` (`string`) - The source node display name. Example: "mdvmaas-win-123"
- `SourceNodeLabel` (`string`) - The source node label. Example: "microsoft.compute/virtualmachines"
- `SourceNodeCategories` (`Dynamic` (json)) - The categories list of the source node.
- `TargetNodeId` (`string`) - The node ID of the edge's target. Example: "45676aa0-10a5-587e-52f4-280bfc014a08"
- `TargetNodeName` (`string`) - Display name of the target node. Example: gke-test-cluster-1
- `TargetNodeLabel` (`string`) - The target node label. Example: "compute.instances"
- `TargetNodeCategories` (`Dynamic` (json)) - The categories list of the target node.
- `EdgeProperties` (`Dynamic` (json)) - Optional data relevant for the relationship between the nodes. Example: For the `EdgeLabel` "routes traffic to" with `EdgeProperties` of `networkReachability`, provide information about the port and protocol ranges that are used to transfer traffic from point A to B.

Graph Kusto Query Language (KQL) operators

Microsoft Security Exposure Management relies on exposure graph tables and unique exposure graph operators to enable operations over graph structures. The graph is built from tabular data using the `make-graph` operator, and then queried using graph operators.

Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.

identify, based on the representation of the first graph, a first plurality of attack paths comprising a first entity of the first plurality of entities, wherein each attack path of the first plurality of attack paths targets a second entity of the first plurality of entities,	Based on the representation of the first graph, the software instructions of MSEM identify a first plurality of attack paths comprising a first entity of the first plurality of entities, wherein each attack path of the first plurality of attack paths targets a second entity of the first plurality of entities.
	
	For example, MSEM “automatically generates attack paths based on the data collected across assets and workloads. . . . The attack path graph view uses enterprise exposure graph data to visualize the attack path to understand how potential threats might unfold”.[62]
	
	Identifying and resolving attack paths
	
	Here's how Exposure Management helps you to identify and resolve attack paths.
	
	• **Attack path generation**: Security Exposure Management automatically generates attack paths based on the data collected across assets and workloads. It simulates attack scenarios, and identifies vulnerabilities and weaknesses that an attacker could exploit.
	  ○ The number of attack paths visible in the portal can fluctuate due to the dynamic nature of IT environments. Our system dynamically generates attack paths based on the real-time conditions of each customer's environment. Changes such as the addition or removal of assets, updates to configurations, a user logging on or off from a machine, a user added or removed to a group, and the implementation of new network segmentation or security policies can all influence the number and types of attack paths identified.
	  ○ This approach ensures that the security posture we provide is both accurate and reflective of the latest environment state, accommodating the agility required in today's IT environments.
	
	• **Attack path visibility**: The attack path graph view uses enterprise exposure graph data to visualize the attack path to understand how potential threats might unfold.
	  ○ Hovering over each node and connector icon provides you with additional information about how the attack path is build. For instance, from an initial virtual machine containing TLS/SSL keys all the way to permissions to storage accounts.
	  ○ The enterprise exposure map extends how you can visualize attack paths. Along with other data, it shows you multiple attack paths and choke points, nodes that create bottlenecks in the graph or map where attack paths converge. It visualizes exposure data, allowing you to see what assets are at risk, and where to prioritize your focus.
	
	Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be

[62] *Overview of Attack Paths*.

	insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
receive streaming data comprising time-stamped data about events relating to one or more entities of the first plurality of entities,	The software instructions of the Accused ’627 MSEM Products receive streaming data comprising time-stamped data about events relating to one or more entities of the first plurality of entities. For example, Microsoft’s documentation explains that MSEM collects data from a large set of sources, including “Microsoft Defender for Endpoint, Microsoft Defender for Identity, Microsoft Defender for Cloud, Microsoft Entra ID, and others.”[63]

[63] *Overview of Data Connectors.*

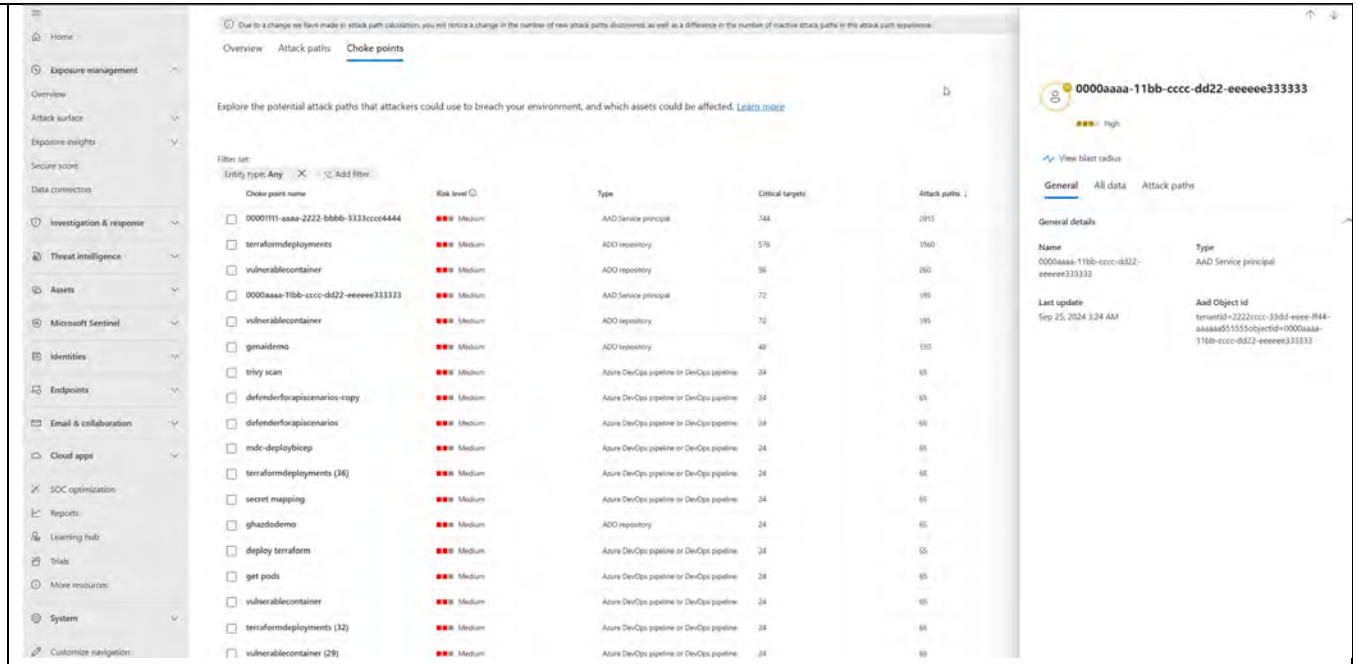
	Overview Microsoft Security Exposure Management consolidates security posture data from all your digital assets, enabling you to map your attack surface and focus your security efforts on areas at greatest risk. Data from Microsoft Security products like Microsoft Defender for Endpoint, Microsoft Defender for Identity, Microsoft Defender for Cloud, Microsoft Entra ID, and others are automatically ingested and consolidated within Exposure Management. You can further enrich and extend this data by connecting to a range of external data sources. To provide coverage of all your assets and security signals and to help you establish a comprehensive, single source of truth for your assets, Exposure Management provides data connectors that ingest data from other security or asset management products deployed in your environment. Benefits include: • Normalized within exposure graph • Enhancing device inventory • Mapping relationships • Revealing new attack paths • Providing comprehensive attack surface visibility • Incorporating asset criticality • Enriching context with business application or operational affiliation • Visualizing through the Attack Map tool • Exploring using advanced hunting queries via KQL Microsoft's documentation explains that MSEM collects and processes "different types of telemetry data, such as user-login events, device domain membership information, and various network signals . . . to create a comprehensive understanding of the criticality of each domain entity."[64] As another example, MSEM "continuously discovers assets and workloads, and gathers discovered data into a unified and up-to-date view of your inventory and attack surfaces."[65]

[64] *Critical Asset Protection.*

[65] *What is MSEM?*

	What can I do with Security Exposure Management?
	
	With Security Exposure Management you can:
	
	• **Get a unified view across the organization**: Security Exposure Management continuously discovers assets and workloads, and gathers discovered data into a unified and up-to-date view of your inventory and attack surface.
	
	• **Manage and investigate attack surfaces**: Visualize, analyze, and manage cross-workload attack surfaces.
	  ○ The enterprise exposure graph gathers information to provide a comprehensive view of security posture and exposure across the business.
	  ○ Graph schemas provide contextual information about specific organizational entities such as devices, identities, machines, and storage.
	  ○ Query the enterprise exposure graph to explore assets, assess risk, and hunt for threats across on-premises, hybrid, and multicloud environments.
	  ○ Visualize your environment and graph queries with the attack surface map.
	
	As another example, in the screenshot below from Microsoft's documentation, the entity "0000aaaa-11bb-cccc-dd2-eeeeee3333333" has a "[l]ast update" date of "Sep 25, 2024, 3:24 AM."[66]

[66] *Review Attack Paths*.

	 Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
based on a first portion of the streaming data, identify a third entity that does not correspond to any of the first plurality of nodes, wherein the third entity is	Based on a first portion of the streaming data, the software instructions of the Accused ’627 MSEM Products identify a third entity that does not correspond to any of the first plurality of nodes, wherein the third entity is not of the first plurality of entities.

not of the first plurality of entities,	For example, MSEM "continuously discovers assets and workloads, and gathers discovered data into a unified and up-to-date view of your inventory and attack surface.":[67]
	
	What can I do with Security Exposure Management?
	
	With Security Exposure Management you can:
	
	• **Get a unified view across the organization:** Security Exposure Management continuously discovers assets and workloads, and gathers discovered data into a unified and up-to-date view of your inventory and attack surface.
	
	• **Manage and investigate attack surfaces:** Visualize, analyze, and manage cross-workload attack surfaces.
	  ○ The enterprise exposure graph gathers information to provide a comprehensive view of security posture and exposure across the business.
	  ○ Graph schemas provide contextual information about specific organizational entities such as devices, identities, machines, and storage.
	  ○ Query the enterprise exposure graph to explore assets, assess risk, and hunt for threats across on-premises, hybrid, and multicloud environments.
	  ○ Visualize your environment and graph queries with the attack surface map.
	
	The enterprise exposure graph "includes assets, findings, and entity relationships from" a number of sources, including Defender for Cloud, Defender for Endpoint, Defender Vulnerability Management, Defender for Identity, and Entra ID.[68]
	
	As another example, MSEM's graph representation is "automatically generate[d] . . . based on the data collected across assets and workloads," and "can fluctuate due to the dynamic nature of IT environments."[69] Microsoft's documentation further explains that the graph representation is updated to reflect "[c]hanges such as the addition or removal of assets, updates to configurations, a user

[67] *What is MSEM?*

[68] *Overview of Attack Surface Management.*

[69] *Overview of Attack Paths*.

	logging on or off from a machine, a user added or removed to a group, and the implementation of new network segmentation or security policies."[70]
	
	Identifying and resolving attack paths
	
	Here's how Exposure Management helps you to identify and resolve attack paths.
	
	• **Attack path generation**: Security Exposure Management automatically generates attack paths based on the data collected across assets and workloads. It simulates attack scenarios, and identifies vulnerabilities and weaknesses that an attacker could exploit.
	  ○ The number of attack paths visible in the portal can fluctuate due to the dynamic nature of IT environments. Our system dynamically generates attack paths based on the real-time conditions of each customer's environment. Changes such as the addition or removal of assets, updates to configurations, a user logging on or off from a machine, a user added or removed to a group, and the implementation of new network segmentation or security policies can all influence the number and types of attack paths identified.
	  ○ This approach ensures that the security posture we provide is both accurate and reflective of the latest environment state, accommodating the agility required in today's IT environments.
	
	As another example, MSEM's device inventory "is gradually populated with devices as they begin to report sensor data":[71]
	
	During the onboarding process, the **Devices list** is gradually populated with devices as they begin to report sensor data. Use this view to track your onboarded endpoints as they come online, or download the complete endpoint list as a CSV file for offline analysis.
	
	Microsoft's documentation further explains that MSEM performs "device discovery":[72]

[70] *Id.*

[71] *Device Inventory* (emphasis omitted).

[72] *Device Discovery*.

Device discovery overview

05/08/2025 • Applies to: Microsoft Defender for Endpoint Plan 2

Protecting your environment requires taking inventory of the devices that are in your network. However, mapping devices in a network can often be expensive, challenging, and time-consuming.

Microsoft Defender for Endpoint provides a device discovery capability that helps you find unmanaged devices connected to your corporate network without the need for extra appliances or cumbersome process changes. Device discovery uses onboarded endpoints, in your network to collect, probe, or scan your network to discover unmanaged devices. The device discovery capability allows you to discover:

- Enterprise endpoints (workstations, servers, and mobile devices) that aren't yet onboarded to Defender for Endpoint
- Network devices like routers and switches
- IoT devices like printers and cameras

MSEM’s “Device Inventory” interface includes a summary of devices discovered in the last 7 days:[73]

[73] *Device Discovery*.

	Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
based on a second portion of the streaming data, wherein the second portion is not identical to the first portion, identify a first relationship between a pair of entities of the first plurality of entities that does not correspond to any of the first plurality of edges, modify, in the hardware memory, the representation of the first graph to generate a modified representation of the first graph, wherein the modified representation of the first graph comprises a representation of a node corresponding to the third entity and an edge corresponding to the first relationship, wherein the node is not of the first plurality of nodes and the edge is	Based on a second portion of the streaming data, wherein the second portion is not identical to the first portion, the software instructions of the Accused ’627 MSEM Products identify a first relationship between a pair of entities of the first plurality of entities that does not correspond to any of the first plurality of edges, modify, in the hardware memory, the representation of the first graph to generate a modified representation of the first graph, wherein the modified representation of the first graph comprises a representation of a node corresponding to the third entity and an edge corresponding to the first relationship, wherein the node is not of the first plurality of nodes and the edge is not of the first plurality of edges, and identify, based on the modified representation of the first graph, a second plurality of attack paths comprising the first entity, wherein each attack path of the second plurality of attack paths targets the second entity, and wherein an attack path of the second plurality of attack paths comprises the third entity. For example, as explained above, Microsoft’s documentation explains that MSEM “continuously discovers assets and workloads, and gathers discovered data into a unified and up-to-date view of your inventory and attack surface.”[74] MSEM’s graph representation is “automatically generate[d] . . . based on the data collected across assets and workloads[,]” and “can fluctuate due to the dynamic nature of IT environments.”[75] Microsoft’s documentation further explains that MSEM “dynamically generates attack paths based on the real-time conditions of each customer’s environment,” based on “[c]hanges such as the addition or removal of assets, updates to configurations, a user logging on or

[74] *What is MSEM?*.

[75] *Overview of Attack Paths*.

not of the first plurality of edges, and
 	
identify, based on the modified representation of the first graph, a second plurality of attack paths comprising the first entity, wherein each attack path of the second plurality of attack paths targets the second entity, and wherein an attack path of the second plurality of attack paths comprises the third entity.
	off from a machine, a user added or removed to a group, and the implementation of new network segmentation or security policies."[76]
	
	Identifying and resolving attack paths
	
	Here's how Exposure Management helps you to identify and resolve attack paths.
	
	• **Attack path generation**: Security Exposure Management automatically generates attack paths based on the data collected across assets and workloads. It simulates attack scenarios, and identifies vulnerabilities and weaknesses that an attacker could exploit.
	  ○ The number of attack paths visible in the portal can fluctuate due to the dynamic nature of IT environments. Our system dynamically generates attack paths based on the real-time conditions of each customer's environment. Changes such as the addition or removal of assets, updates to configurations, a user logging on or off from a machine, a user added or removed to a group, and the implementation of new network segmentation or security policies can all influence the number and types of attack paths identified.
	  ○ This approach ensures that the security posture we provide is both accurate and reflective of the latest environment state, accommodating the agility required in today's IT environments.
	
	Based on Qomplx's analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.

[76] *Id.*

IX. Claim 22

The computer system of claim 18,	See above for an analysis of Claim 18.
wherein a portion of the representation of the first graph is derived from reconnaissance data received by the computer system from a plurality of computer systems,	A portion of the representation of the first graph of Claim 18 is derived from reconnaissance data received by the computer system from a plurality of computer systems. For example, as explained above, Microsoft’s documentation explains that MSEM collects data from a large set of sources, including, among others, Microsoft Defender for Endpoint.[77] Defender for Endpoint includes a “device discovery capability” that “uses onboarded endpoints, in your network, to collect, probe, or scan your network to discover unmanaged devices. The device discovery capability allows you to discover: Enterprise endpoints (workstations, servers, and mobile devices) that aren’t yet onboarded to Defender for Endpoint[;] Network devices like routers and switches[;] IoT devices like printers and cameras.”[78] Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
wherein a first computer system of the plurality of computer systems performs passive reconnaissance, and	A first computer system of the plurality of computer systems performs passive reconnaissance. For example, as noted above, MSEM “consolidates security posture data from all your digital assets,” including “[d]ata from Microsoft Security products like Microsoft Defender for Endpoint, Microsoft Defender for Identity, Microsoft Defender for Cloud, Microsoft Entra ID, and others.”[79] Defender for

[77] *Overview of Data Connectors*.

[78] *Device Discovery*.

[79] *Overview of Data Connectors*.

	Endpoint includes “Basic discovery,” a “device discovery capability that helps you find unmanaged devices connected to your corporate network.”[80] Defender for Endpoint “passively collect[s] events in your network and extract[s] device information from them. Basic discovery uses the `SenseNDR.exe` binary for passive network data collection and no network traffic is initiated. Endpoints extract data from all network traffic seen by an onboarded device.”[81] Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
wherein a second computer system of the plurality of computer systems performs active reconnaissance.	A second computer system of the plurality of computer systems performs active reconnaissance. For example, Defender for Endpoint includes a “[n]etwork device discovery” capability in which a “designated Microsoft Defender for Endpoint device is used on each network segment to perform periodic authenticated scans of preconfigured network devices. Once discovered, vulnerability management capabilities in Defender for Endpoint provide integrated workflows to secure discovered switches, routers, WLAN controllers, firewalls, and VPN gateways. . . . These types of devices require an agentless approach where a remote scan obtains the necessary information from the devices. Depending on the network topology and characteristics, a single device or a few devices onboarded to Microsoft Defender for Endpoint performs authenticated scans of network devices using SNMP (read-only).”[82] Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be

[80] *Device Discovery.*

[81] *Id.*

[82] Microsoft, *Network device discovery and vulnerability management*, available at `https://learn.microsoft.com/en-us/defender-endpoint/network-devices`.

	insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.

X. Claim 27

The computer system of claim 18,	See above for an analysis of Claim 18.
wherein the representation of the first graph comprises an identification of the third entity as a sensitive resource, and	The representation of the first graph of Claim 18 comprises an identification of the third entity as a sensitive resource. For example, Microsoft’s documentation explains that the attack surface map contains “[i]con indicators” that “show node type and edge type. Visual indicators show information such as the high criticality crown or a vulnerability bug, providing visual input to where critical organizational data is at risk.”[83] As another example, MSEM “provides an out-of-the-box catalog of predefined critical asset classifications for assets that include devices, identities, and cloud resources,” including among others “[c]ritical cyber-security assets such as file servers and domain controllers” and “[d]atabases with sensitive data.”[84]

[83] Microsoft, *Explore with the attack surface map*, available at `https://learn.microsoft.com/en-us/security-exposure-management/enterprise-exposure-map` [hereinafter *Attack Surface Map*].

[84] *Critical Asset Management*.

Predefined classifications

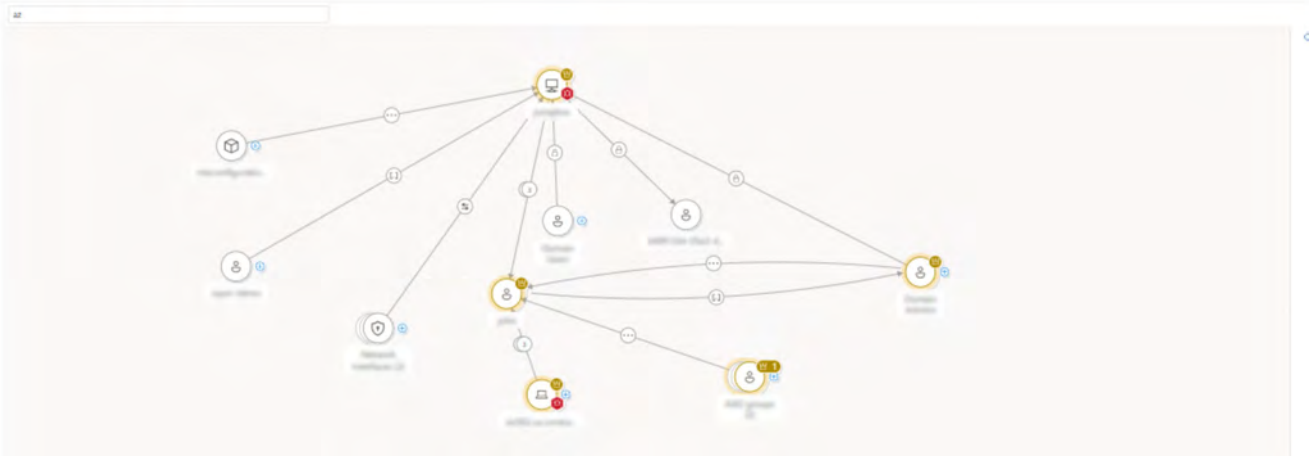
Security Exposure Management provides an out-of-the-box catalog of predefined critical asset classifications for assets that include devices, identities, and cloud resources. Predefined classifications include:

- Critical cyber-security assets such as file servers and domain controllers
- Databases with sensitive data
- Identity groups such as Power Users
- User roles like Privileged Role Administrator

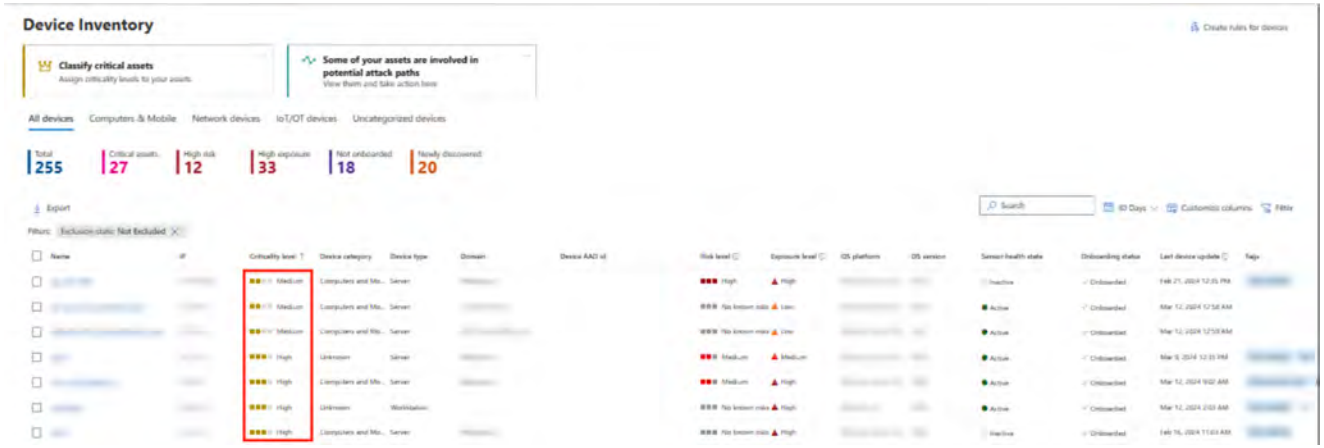
In addition, you can create custom critical assets to prioritize what your organization considers to be critical when assessing exposure and risk.

In the example from Microsoft's documentation shown below, multiple nodes are identified as critical assets:[85]

Attack surface map



[85] *Id.*

wherein the computer system is further configured to execute software instructions stored on nontransitory machine-readable storage media comprising software instructions that generate a report that identifies the third entity as a sensitive resource.	The computer system of Claim 18 is further configured to execute software instructions stored on nontransitory machine-readable storage media comprising software instructions that generate a report that identifies the third entity as a sensitive resource. For example, Microsoft’s documentation explains that “[a]fter business critical assets are defined and identified, asset criticality appears with your asset information. Asset criticality is integrated into other experiences in the Defender portal, such as in advanced hunting, the device inventory, and in attack paths that involve critical assets. For example, in the Device Inventory, a criticality level is shown.”[86]  Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.

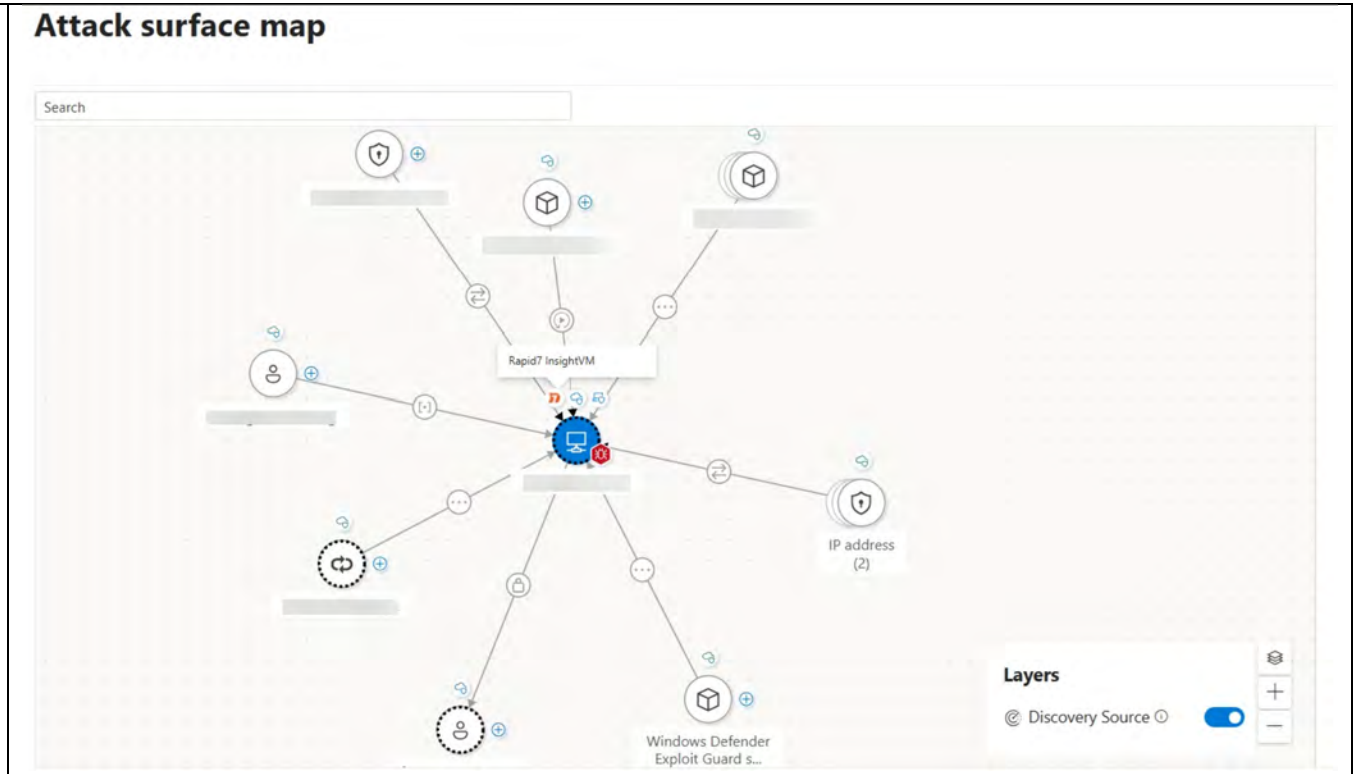
[86] *Id.* (emphasis omitted).

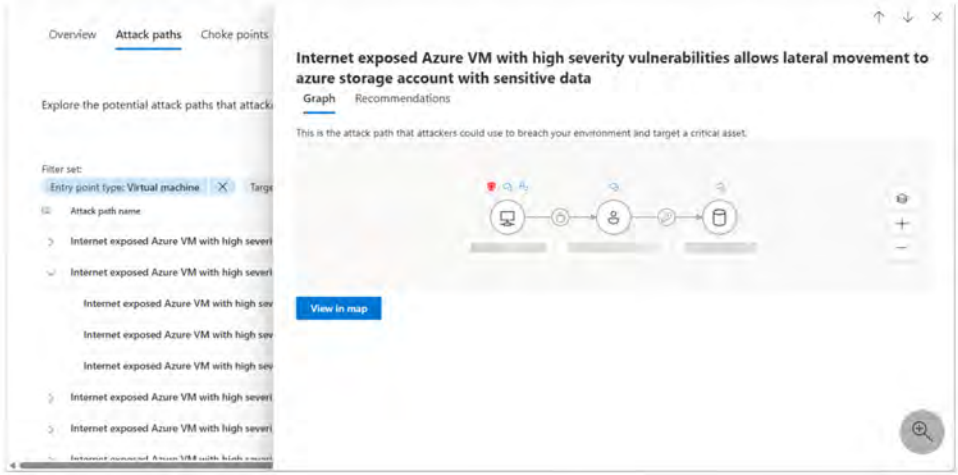
XI. Claim 28

The computer system of claim 18,	See above for an analysis of Claim 18.
wherein the representation of the first graph comprises an identification of a security vulnerability associated with the third entity, and	The representation of the first graph of Claim 18 comprises an identification of a security vulnerability associated with the third entity. For example, as explained above, MSEM graph representation contains “[i]con indicators” that “show node type and edge type[,]” as well as “[v]isual indicators” that “show information such as … a vulnerability bug, providing visual input to where critical organizational data is at risk.”[87] In the example from Microsoft’s documentation shown below, a node is identified with a red visual indicator.[88]

[87] *Attack Surface Map*.

[88] *Id*.

	 Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
wherein an attack path of the second plurality of attack paths	An attack path of the second plurality of attack paths of Claim 18 is based on the security vulnerability.

is based on the security vulnerability.	For example, Microsoft's documentation explains that MSEM "automatically generates attack paths based on the data collected across assets and workloads, including data from external connectors. It simulates attack scenarios, and identifies vulnerabilities and weaknesses that an attacker could exploit."[89] In the example from Microsoft's documentation shown below, MSEM identifies an "attack path that attackers could use to breach your environment and target a critical asset[,] described as "Internet exposed Azure VM with high severity vulnerabilities allows lateral movement to azure storage account with sensitive data."[90] **Attack paths** Security Exposure Management automatically generates attack paths based on the data collected across assets and workloads, including data from external connectors. It simulates attack scenarios, and identifies vulnerabilities and weaknesses that an attacker could exploit. As you explore attack paths in your environment, you can view the discovery sources that contributed to this attack path based on the graphical view of the path. 

[89] *Value From Your Data Connectors.*

[90] *Id.*

	Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.