Cisco SecureX device insights

Q

What is SecureX device insights?

A

SecureX device insights provides you with a unified view of the devices in your organization by consolidating inventories from integrated data sources such as:

- Duo
- Meraki Systems Manager
- Orbital
- Secure Endpoint
- Umbrella
- Cisco Secure Client (coming soon)

Device insights also supports other third-party, non-Cisco sources such as:

- Jamf Pro
- Microsoft Intune
- MobileIron
- VMware Workspace ONE (formerly AirWatch)

Q

What is the customer challenge that device insights addresses?

A

With the increasingly distributed and complex nature of customers' security environments, visibility has become an even bigger challenge. With a focus on security resilience and expanding visibility, this new device insights feature is designed to consolidate, discover, normalize, and work with their device inventory within SecureX.

Q

What does device insights cost?

A

It is an included feature within SecureX. SecureX is provided as an entitlement to Customers of qualifying Cisco Secure products (Secure Endpoint (AMP), Umbrella, Firepower, Kenna, Duo, etc.)

Q

What are the benefits of using device insights?

A

Device insights helps you answer these questions and more:

- What types of devices are connected to your environment or organization?
- What users have been accessing those devices?
- Where are those devices located?
- What vulnerabilities are associated with those devices?
- Which security agents are installed?
- Is your security software up to date?

Q

How does device insights get this data from my sources?

A

Device insights utilizes native APIs of all supported sources.

- **Full inventory sync** – A process that involves a standard API call to the source which results in the download of the full asset inventory of this source.
- **Delta sync** – When supported, Device Insights uses API calls that return only changes since the last sync. Assets timestamps like 'last updated' are used to identify what has been changed after the last sync.
- **Webhooks** – If supported by the source, device insights configures a Webhook programmatically through the source's API. This instructs the source to proactively send events/changes directly to device insights, not having to wait until the next scheduled sync.

Device Insights Sources	REST API Full Sync	REST API Delta Sync	Webhooks
Cisco Secure Endpoint (AMP)	Yes	No	Yes
Cisco Umbrella	Yes	Yes	No
Cisco Orbital	No	No	No
Cisco DUO	Yes	Yes	No
Cisco Meraki System Manager*	Yes	No	No
Microsoft Intune	Yes	No	No
MobileIron	Yes	No	No
JAMF	Yes	No	Yes
AirWatch	Yes	Yes	No
Cisco Secure Client (aka: Unified Agent)	Yes	No	Yes
Custom	No	No	No

Q **How does device insights avoid duplicate endpoints when they are reported by multiple sources?**

A One of the primary functions of device insights is to merge endpoint data from various sources into a single endpoint record to present administrators and investigators with a consolidated view of any endpoint. The goal when merging endpoints is to not only merge correctly, but to do so with no false positives.

Q **How does device insights define “Out of Date” and “End of Life” in the OS support filter?**

A Device insights leverages a special feed from Duo Security which provides OS lifecycle information and then applies it to our non-server inventory. This does not require a Duo integration into SecureX. The functions are provided behind the scenes as a service to all SecureX Customers using device insights.

Q **Where do the vulnerabilities come from that are reported in device insights?**

A Currently, any reported vulnerabilities come exclusively from Cisco Secure Endpoint. More advances are road mapped as Cisco integrates Kenna more tightly into SecureX.

Q **Are there any plans to add a host detected by FTD in device insights?**

A We are investigating this for a possible addition to the roadmap.

Q **Are there any limits as to how many devices device insights can support?**

A There are no defined limits to the number of endpoints in device insights yet. We have tested environments that had over 1,000,000 devices.

Q **We expect to have tens of thousands of devices appearing in device insights. What are my options for sorting through this data?**

A Device insights includes Quick Filters, Simple Boolean searches and –in the near-future – Advanced Searches that allow for full Lucene search queries.

Q **Can I save the filters that I create for reuse?**

A Yes. The filters will persist so that they can be selected from the pull-down. They will be available to anyone in your organization that has access to device insight. This is highly valuable for the most common filters.

Q **What is the difference between the basic (boolean) searches and the Advanced Search capability?**

A Basic (Boolean) search uses Elasticsearch; AND, OR and NOT.
Advanced Search is based on the Lucene Query Language; Field, Term, Operator, or modifier and provides for more extensive searches. e.g., avDefinitionsOutOfDate OR isCompromised:true OR hasFaults:true AND NOT hostname:Demo* Please see the official documentation for details.

Q

Will I have insight into servers and not just desktops?

A

The device type classifications used by device insights are Desktop, Server, Mobile and Virtual. Devices can be classified this way, when detectable. The Operating System detection and classification contains a category type of "other" as well.

Q

How does Secure Endpoint enrich Device Insights?

A

Integrating Secure Endpoint as a key source to device insights answers the following:

- Are definitions up to date?
- Is the endpoint isolated?
- Is Orbital enabled?
- Does the endpoint have any current vulnerabilities?
- What Is the currently assigned Group and Policy assigned to the endpoint?

In addition, the GUID assigned to the endpoint is reported and the admin can pivot on the GUID directly to the Secure Endpoint console Device Trajectory to obtain a better idea of what the endpoint has been up to.

Q

When integrating Secure Endpoint (AMP) can I get Group and Policy information?

A

The status 'seen in sources' for Secure Endpoint when you view a particular device will give you both the Group and Policy. In addition, you can filter on the main inventory table for the Secure Endpoint Policy to see a list of devices that share the same policy. Not all the integrating products support sharing the Group, Labels, Tags, or Policies that an endpoint is using in the source product.

Q

What is Orbital?

A

Orbital is a service that adds Osquery to Secure Endpoint to support detailed and fast queries. Device insights leverages Orbital to provide you and your applications with information about your hosts. Osquery is an open-source project that captures nearly all aspects of Windows, macOS and Linux operating systems, cataloging those attributes in a database that is query-able through a universal query language like SQL (structured query language). While Orbital uses Osquery in the agent, there is much more to Orbital than just Osquery – including a secure always-on connection between the cloud service and the agent on the endpoint.

For more on Orbital, please see the product page, or this intro video: https://www.cisco.com/c/en/us/products/security/threatwise-tv-demos/sd-wan/endpoint-security-evolution.html?dtid=osscdc000283

Q **We have Secure Endpoint but currently do not have Orbital. How do we get Orbital to take advantage of the detailed data on the endpoints, such as the Windows Security Center configurations?**

A Secure Endpoint Advantage customers can deploy Orbital on supported platforms with a simple configuration change in the Secure Endpoint console. Up to 30 minutes later, Orbital will be available and ready for queries.

Once deployed, Orbital can provide detailed forensic snapshots, run live queries, and schedule periodic queries. Orbital works well in combination with Secure Endpoint host isolation to provide a means of quarantining a suspicious host while performing an investigation.

See How Do I Get Orbital?

Q **What is the OS support for Orbital?**

A While Orbital itself supports Windows, macOS & Linux, SecureX device insights will only support Windows at the GA (General Availability) release. macOS and Linux will be fast follow-on's post GA.

Q **Can I have more than one integration-module per integration type, such as having multiple integration-modules for my device managers (e.g.: 2 different instances of Jamf Pro)?**

A Yes, this supported.

Q **What license is required for DUO to integrate with device insights as a source?**

A DUO Access & Beyond.

Q **How often can we configure device insights to sync with the sources**

A An admin can schedule a sync one time per day. The "Sync Now" button for manual syncs will be available for use as required to help during investigations, as is the "Update from Orbital Live Query" capability in the device details page. Note: when the source supports Webhooks, there is no limitation to the proactive notifications sent to Device Insights.

Q **For accessing my onPrem MDM through my firewall, what IP addresses do I need to allow?**

A
- North America: 35.168.234.165, 35.172.5.95, 34.225.249.84
- EU: 34.251.83.242, 52.49.85.99, 52.208.164.206
- Asia Pacific, Japan, China: 54.248.49.240, 52.198.165.128, 52.196.126.178

Q **I am new to device insights as well as SecureX. What is the ribbon at the bottom of the screen?**

A SecureX has a distributed set of capabilities presented in the form of apps and tools in the SecureX ribbon. The ribbon is in the lower portion of the page and persists as you move between the dashboard and other security products in your environment. To aid in your research and investigation, use the ribbon to access the casebook, apps, settings, search observables for enrichment, and view incidents.

Q **Can the data obtained by device insights enrich threat hunting with SecureX threat response?**

A Yes. This is known as Asset Resolution, and you can view asset details in the Assets section on the Details page in the investigation Results pane, so the details are displayed in-line during investigations. You can also click the View in device insights link to view the details.

Q **How can I easily identify compromised endpoints in device insights?**

A From the Edit Column's pull-down to ensure Compromised Endpoints is selected. This displays devices where Secure Endpoint has detected a compromised artifact. Note: this does not mean that your other endpoints are not compromised.

Q **My endpoints are shown as unmanaged. What does it mean to be Managed or Unmanaged?**

A Managed means that the device is enrolled with an MDM/EMM product such as Meraki SM and is configured as a Source and sending device insights this data.

Q **Which action can I take directly from device insights?**

A Some sources provide the ability to pivot to their respective consoles to further investigate the endpoint. Secure Endpoint, Umbrella and Duo are viable options today.

Q **What is the definition of a "Compromised Artifact" shown for an Endpoint?**

A If an endpoint in device insights has been determined to be compromised this is due to data from Secure Endpoint. A compromise is a collection of one or more detections on a machine.

Q **How can I figure out which "Compromised Artifact" triggered the alert in device insight?**

A Click the link on the device in the Secure Endpoint section of the device details screen. This will pivot you to the device trajectory page for the endpoint in the Secure Endpoint Cloud Console.

Q **Is there any information shown in device insights if multiple Compromised Artifacts have been identified by Secure Endpoint?**

A No. If one or more compromised artifacts exist on the endpoint, the endpoint will be flagged as having a compromised artifact. For more details on these, you would need to pivot to the endpoint's device trajectory screen in the Secure Endpoint cloud by clicking on the link in the Secure Endpoint section of the device details page.

Q **What are the recommended steps for an analyst if device insights indicate a device as having a compromise?**

A Click on the GUID of the machine shown in device insights which will pivot you to Secure Endpoint Device Trajectory as a starting point.

Q **Are there any other scenarios beside Secure Endpoint where a device might be designated as compromised in device insights?**

A No, not today but stay tuned.

Q **Is there an option to force an information update for an endpoint from all configured sources?**

A No. The frequency of the Source Syncs is configured per Source.

Q **Is there an option to enable logging to review which information is provided from a specific source for a specific host?**

A No, not today but that is planned. After the GA there is a planned UI refresh for the device details page that will more clearly and more wholly clarify which information is being sent from each source.

Q **I am in a company they replaced a lot of endpoints and devices; 1,000 notebooks within a month and approximately 600 devices managed by MDM. How can I clean this up using device insight?**

A Today this data needs to age out which is set to 90 days. Sources typically have a set date to deem an endpoint inactive in their respective product.

Q **What is the best approach to add possible compromised endpoints from device insight to the Casebook in the SecureX Ribbon?**

A You can use the Find Observables option in the ribbon and based on the findings add to a casebook or choose to investigate further in threat response. Optionally, you can pivot from the ribbon to threat response, manually initiate an investigation and search on it (e.g., hostname:Thorsten-Tandy100).

C67-745083-00 03/22