AXONIUS

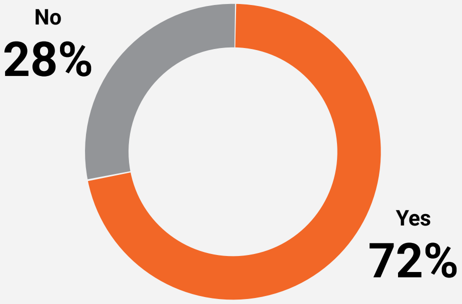
5 Tips to Maximize your CMDB ROI with Cyber Asset Attack Surface Management (CAASM)

If you work in IT or Security, you're very familiar with the configuration management database (CMDB), which helps organizations understand the relationships across the hardware and software in IT environments.

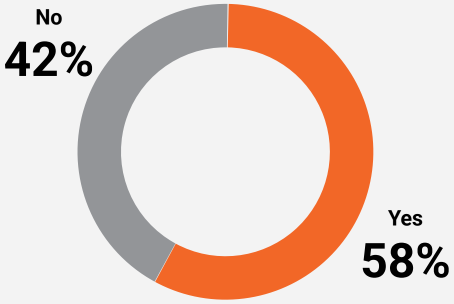
CMDBs are a great tool for IT Service Management needs - so why do so many companies lack confidence in their asset inventory?

CMDBs are valuable, but they were never built to secure the evolving attack surface. CMDBs don't provide security-related insights to support effective risk analysis and mitigation or to be a valuable tool for security teams to take action on their cyber assets. That's where Cyber Asset Attack Surface Management (CAASM), working alongside your CMDB, can help.

Q: Are security data and IT data siloed in your organization?



Q: Does siloed data weaken your organization's security posture?



There's a disconnect between asset data managed by IT vs asset data managed by Security

2024 State of Cybersecurity Report | Ivanti

Only **17%**

organizations can clearly identify and inventory a majority (95% or more) of their assets

2024 Gartner Innovation Insight: Attack Surface Management

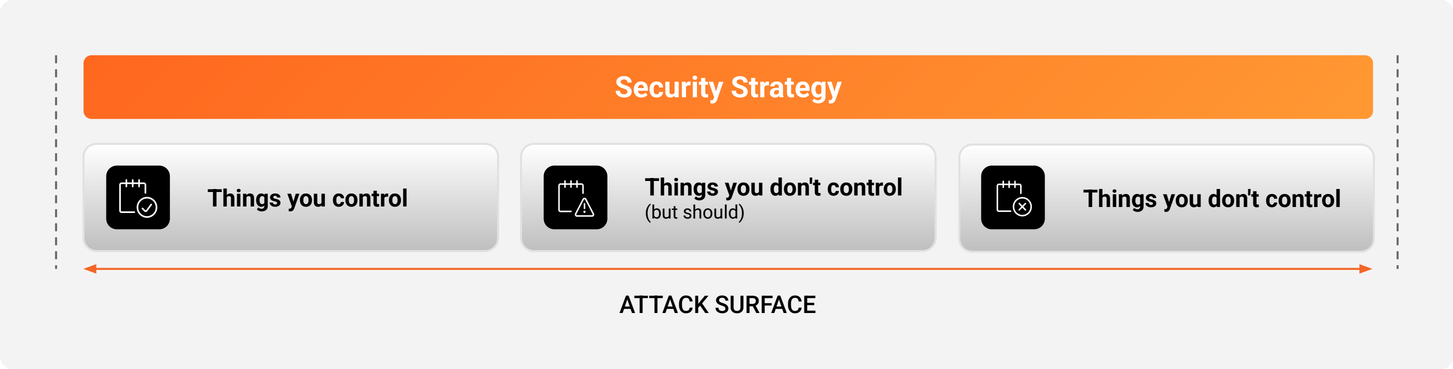
01

Centralize your asset inventory

The things you control, things you don’t control (but should), and things you can’t control, all in one place.

Many IT environments support a bring-your-own-device (BYOD) environment to provide employees flexibility. But personal phones and laptops still interact with enterprise IT systems, and pose potential hazards. A CMDB’s information about these devices isn’t typically comprehensive. Unmanaged devices can elude CMDB capture altogether, and key information about enterprise devices can be missing as well, for example when hardware is missing key antivirus protection or apps are unprotected by SSO.

CAASM closes this gap by shifting shadow or unmanaged enterprise assets out of the “things you can’t control” category and into a reliable, unified view of all assets, where they can be monitored and managed. It automates the critical process of finding and analyzing every device operating in the enterprise environment, collecting and correlating details from a wide variety of identity solutions and other systems. And it can correct errors, like duplicate database entries generated by different source formats, simplifying management and remediation.



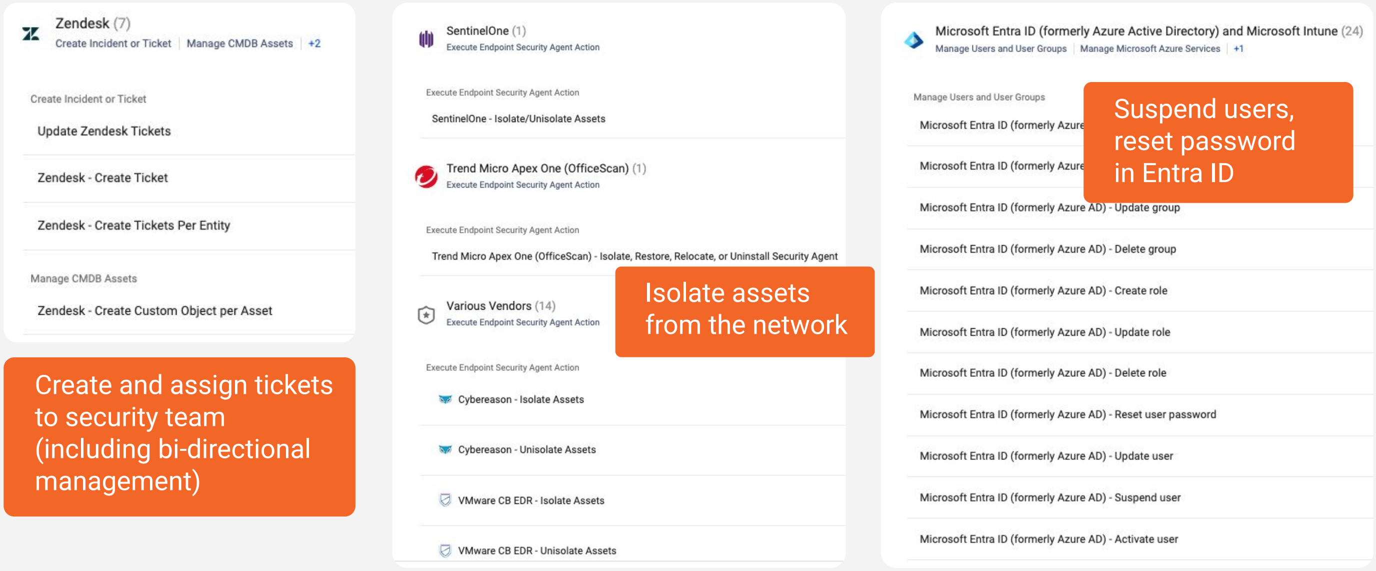
02

Support Incident RCA

When reacting to a security incident, gathering context quickly is vital for root cause analysis. A CMDB will provide some pertinent information, like spotting risky CIs based on software version or hardware modification issues. But the database might contain data from disparate sources which haven’t been updated in time to spot emerging vulnerabilities, such as a new IP address or a zero-day exploit.

Adding a CAASM solution fills in these knowledge gaps. It can catalogue ephemeral devices, such as virtual machines, containers and other assets, can zero in on attack path, vulnerability and misconfiguration details, and can discover when devices don’t have endpoint protection and when they were first identified on the network. This additional context lets enterprises confidently automate remediation, like forcing password resets, isolating devices, and blocking suspicious users.

Examples of responding to incidents with Axonius



Zendesk (7)
Create Incident or Ticket | Manage CMDB Assets | +2

Create Incident or Ticket

- Update Zendesk Tickets
- Zendesk - Create Ticket
- Zendesk - Create Tickets Per Entity

Manage CMDB Assets

- Zendesk - Create Custom Object per Asset

Create and assign tickets to security team (including bi-directional management)

SentinelOne (1)
Execute Endpoint Security Agent Action

Execute Endpoint Security Agent Action

- SentinelOne - Isolate/Unisolate Assets

Trend Micro Apex One (OfficeScan) (1)
Execute Endpoint Security Agent Action

Execute Endpoint Security Agent Action

- Trend Micro Apex One (OfficeScan) - Isolate, Restore, Relocate, or Uninstall Security Agent

Various Vendors (14)
Execute Endpoint Security Agent Action

Execute Endpoint Security Agent Action

- Cybereason - Isolate Assets
- Cybereason - Unisolate Assets
- VMware CB EDR - Isolate Assets
- VMware CB EDR - Unisolate Assets

Isolate assets from the network

Microsoft Entra ID (formerly Azure Active Directory) and Microsoft Intune (24)
Manage Users and User Groups | Manage Microsoft Azure Services | +1

Manage Users and User Groups

- Microsoft Entra ID (formerly Azure
- Microsoft Entra ID (formerly Azure
- Microsoft Entra ID (formerly Azure AD) - Update group
- Microsoft Entra ID (formerly Azure AD) - Delete group
- Microsoft Entra ID (formerly Azure AD) - Create role
- Microsoft Entra ID (formerly Azure AD) - Update role
- Microsoft Entra ID (formerly Azure AD) - Delete role
- Microsoft Entra ID (formerly Azure AD) - Reset user password
- Microsoft Entra ID (formerly Azure AD) - Update user
- Microsoft Entra ID (formerly Azure AD) - Suspend user
- Microsoft Entra ID (formerly Azure AD) - Activate user

Suspend users, reset password in Entra ID

03

Help IT Compliance and Audit

CAASM enriches CMDBs by correlating asset data continuously in the background, providing an always up-to-date inventory in real time. Security teams can spot known exploits identified by CISA, can query devices that are running out-of-date builds, find orphaned assets or users who need to be credentialed, and review the business's vulnerability remediation history. Not only does this help to keep up with compliance needs, but CAASMs also enable Security and IT to act quickly on any issues, automating response actions like deploying patches, running commands and scripts, etc with their CAASM.

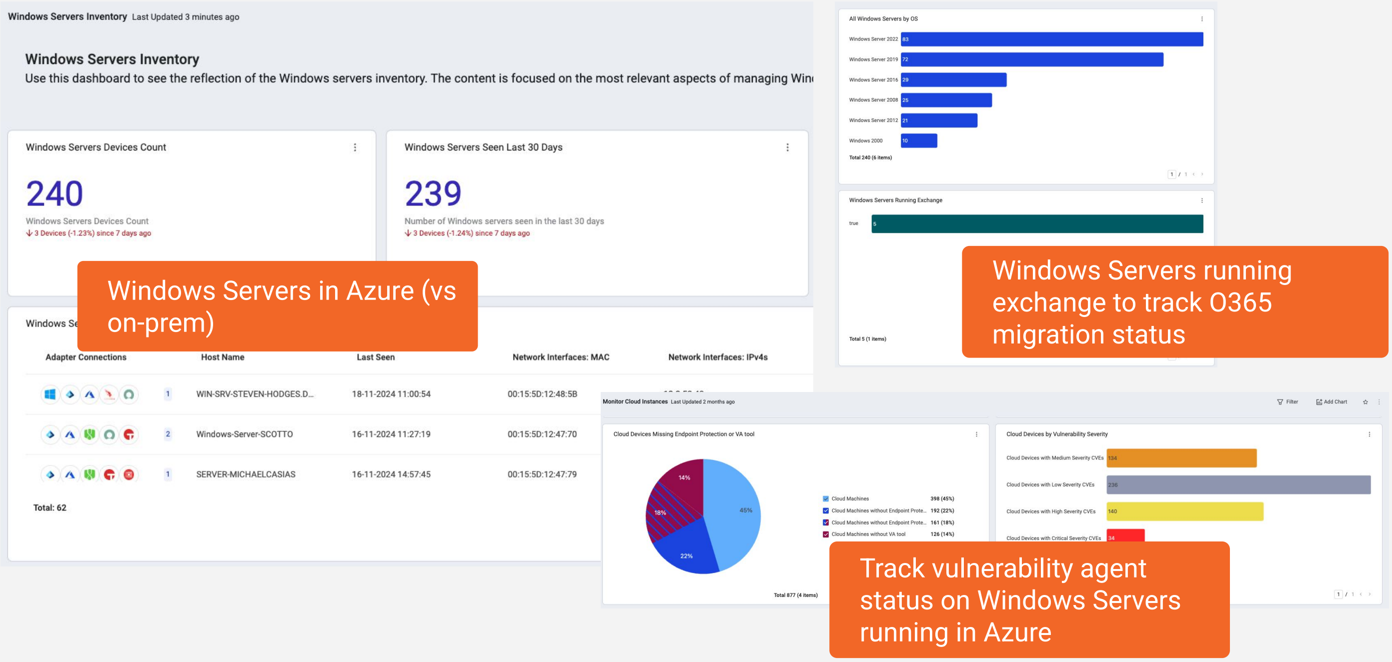
04

Accelerate modernization and cloud migration

Over time, organizations replace and reconfigure data sources as they introduce new technology to grow their businesses. Each new integration increases the complexity of the company's network of CIs, and these changes can have knock-on impacts across the entire system, including opening new vulnerabilities that bad actors can exploit.

Yes, a CMDB can be used to analyze IT assets and dependencies during an update or cloud migration. But CAASM goes further, capturing information like vulnerability agent status on servers being migrated to Azure or AWS, or unsupported operating systems. By building dedicated dashboards to track cloud infrastructure status, businesses whose cyber assets are integrated with CAASM solutions can manage mitigating risks that may result from the upgrade.

Example dashboards created with Axonius



Windows Servers Inventory Last Updated 3 minutes ago

Windows Servers Inventory

Use this dashboard to see the reflection of the Windows servers inventory. The content is focused on the most relevant aspects of managing Win

Windows Servers Devices Count

240

Windows Servers Devices Count

↓ 3 Devices (-1.23%) since 7 days ago

Windows Servers Seen Last 30 Days

239

Number of Windows servers seen in the last 30 days

↓ 3 Devices (-1.24%) since 7 days ago

Windows Se

Adapter Connections		Host Name	Last Seen	Network Interfaces: MAC	Network Interfaces: IPv4s
	1	WIN-SRV-STEVEN-HODGES.D...	18-11-2024 11:00:54	00:15:5D:12:48:5B	
	2	Windows-Server-SCOTTO	16-11-2024 11:27:19	00:15:5D:12:47:70	
	1	SERVER-MICHAELCASIAS	16-11-2024 14:57:45	00:15:5D:12:47:79	

Total: 62

All Windows Servers by OS
Windows Server 2022
83
Windows Server 2019
72
Windows Server 2016
29
Windows Server 2008
25
Windows Server 2012
21
Windows 2000
10
Total 240 (6 items)
1 / 1
Windows Servers Running Exchange
true
5
Total 5 (1 items)
Monitor Cloud Instances Last Updated 2 months ago
Filter
Add Chart
Cloud Devices Missing Endpoint Protection or VA tool
14%
18%
45%
22%
☑ Cloud Machines 398 (45%)
☑ Cloud Machines without Endpoint Prote... 192 (22%)
☑ Cloud Machines without Endpoint Prote... 161 (18%)
☑ Cloud Machines without VA tool 126 (14%)
Total 877 (4 items)
Cloud Devices by Vulnerability Severity
Cloud Devices with Medium Severity CVEs
134
Cloud Devices with Low Severity CVEs
236
Cloud Devices with High Severity CVEs
140
Cloud Devices with Critical Severity CVEs
34
1 / 1

Windows Servers in Azure (vs on-prem)

Windows Servers running exchange to track O365 migration status

Track vulnerability agent status on Windows Servers running in Azure

05

Identify IT policy configuration gaps

CAASM delivers a comprehensive view across cyber assets that may not be discovered solely via a CMDB. Examples include discovering users with expired passwords, users and admins are not enrolled in MFA, and network devices with your AV agent. Your IT teams can see at a glance which devices have which specific agents installed, keep track of outdated clients and servers, and make informed access decisions including enabling various forms of automated remediation.

Bonus

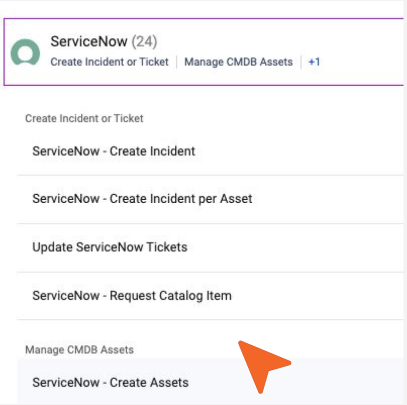
Accelerate CMDB reconciliation

Let’s end on everyone’s “favorite” topic - CMDB reconciliation. We’ll cover how Axonius, specifically, can help here. There is not much variability in CMDB reconciliation pain points across companies. Most teams will experience a form of these three challenges

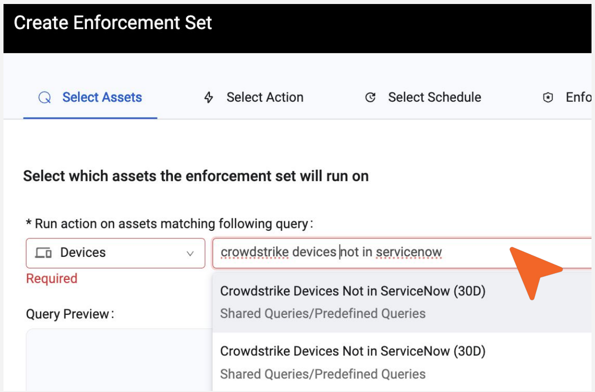
1. Lack of completeness - where is the asset I am looking for?
2. Lack of details - why can’t I see more information about this asset?
3. Obsolete data - the name and IP address of a device are outdated, a vulnerability has already been patched, user ownership has changed, etc.

CAASMs like Axonius connect to a breadth of data sources (including the CMDB itself) to build your complete asset inventory. Reconciliation is then a simple task of asking the question - “Show assets known to Axonius that are not in ServiceNow,” or “Show assets in both ServiceNow and Axonius where only Axonius has a specific asset parameter” (IP Address, open ports, MAC address etc that may be missing from the CMDB). From here, you can utilize Axonius’s Enforcement Center to create new assets in ServiceNow, even going into the specifics of choosing with table names to add new assets to.

Example dashboards created with Axonius


ServiceNow (24)
Create Incident or Ticket | Manage CMDB Assets | +1
Create Incident or Ticket
ServiceNow - Create Incident
ServiceNow - Create Incident per Asset
Update ServiceNow Tickets
ServiceNow - Request Catalog Item
Manage CMDB Assets
ServiceNow - Create Assets

Step 1
Choose the Create Assets action



Select which assets the enforcement set will run on

* Run action on assets matching following query:

Devices | crowdstrike devices not in servicenow

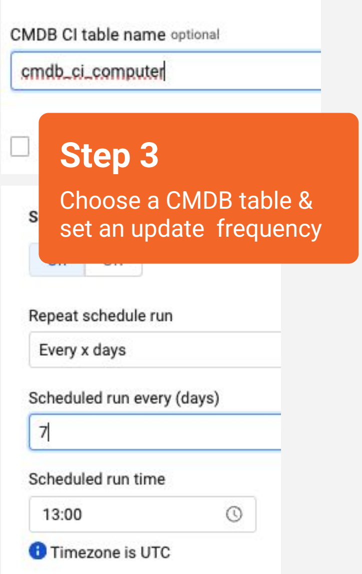
Required

Query Preview:

Crowdstrike Devices Not in ServiceNow (30D)
Shared Queries/Predefined Queries

Crowdstrike Devices Not in ServiceNow (30D)
Shared Queries/Predefined Queries

Step2
Specify your saved query



CMDB CI table name optional: cmdb_ci_computer

Repeat schedule run: Every x days

Scheduled run every (days): 7

Scheduled run time: 13:00

Timezone is UTC

Step 3
Choose a CMDB table & set an update frequency

Learn more about how Axonius can complement your CMDB.

Learn more

AXONIUS