Accurate and Actionable Asset Exposure Insights

© 2025 Zscaler, Inc. All rights reserved.

Solution Brief

Why is cyber asset attack surface management (CAASM) still so hard?

Organizations often struggle to maintain an accurate inventory of their assets, both physical and virtual. As a result, IT and security teams resort to spending hours tracking assets in spreadsheets, making it difficult to assess the risks these assets pose and prioritize remediation efforts. This issue is particularly pressing in highly regulated industries where noncompliance can result in significant fines.

Organizations have dozens of security and IT tools—the average organization has 60–75 different tools.

The number of cyber assets organizations manage increases by 133% on average each year.

Asset information is spread across tools, so it's challenging to create an accurate and up-to-date asset inventory.

Configuration management databases (CMDBs) are difficult to keep updated and are typically incomplete and inaccurate.

Programmatically identifying and fixing asset coverage gaps is impossible without a unified, holistic asset inventory.

Organizations lack the ability to trigger automated remediation workflows and policy adjustments based on asset risk.

SO MANY ASSETS, SO FEW ANSWERS...

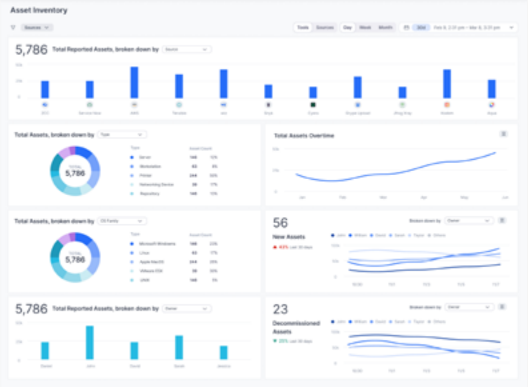
- How many assets do we actually have?
- How accurate is our CMDB?
- Who should be assigned a ticket to remediate a given asset?
- Which assets are missing protective software like EDR?
- Which assets are running end-of-life software?
- Which users are connecting to our key applications with risky assets?
- What level of protection is on each of our crown jewel assets?
- What is the user, geography, department, etc., of each asset?
- What percentage of our assets adheres to corporate policies?

©2025 Zscaler, Inc. All rights reserved.

Get a high-fidelity “golden record” of all your assets with our fundamentally different approach to CAASM.

Zscaler Asset Exposure Management provides the industry’s most complete, accurate, and context-rich asset inventory. Leveraging the data correlation enabled by our patented Data Fabric for Security, our unique approach to CAASM empowers you to identify coverage gaps, automate CMDB hygiene, generate workflows for mitigation, and reduce asset risk. It serves as a single source of asset “truth” for security, IT, and other parts of the business to draw upon to improve security and compliance outcomes, as well as a foundation for continuous threat exposure management (CTEM) solutions.

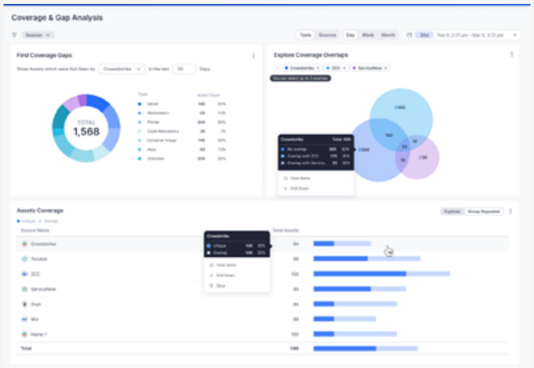
Zscaler Asset Exposure Management offers comprehensive asset risk management, enabling organizations to:


Asset Inventory
Tools
Sources
Day
Week
Month
5,786 Total Reported Assets, broken down by
Total Assets, broken down by
5,786
Total Assets Overtime
Total Assets, broken down by
5,786
56
New Assets
5,786 Total Reported Assets, broken down by
23
Decommissioned Assets

Create an accurate asset inventory

Achieve visibility into all your assets, including endpoints, cloud resources, network devices, and more. Get a complete representation of your asset attack surface by continuously running cross-source deduplication, correlation, and resolution of asset details.

- Leverage 150+ connectors in the Data Fabric for Security
- Synthesize assets reported by multiple disparate tools
- Visually display the relationships between assets
- Correlate all data to create a complete asset view

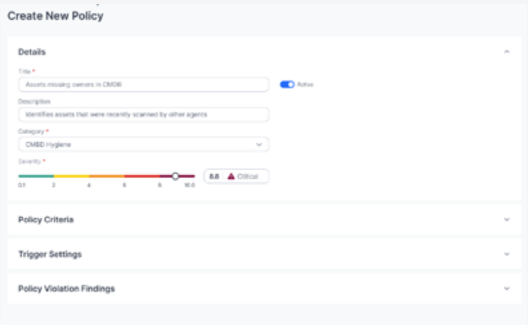


Identify coverage gaps

Easily pinpoint potential compliance issues and misconfigurations (e.g., assets lacking EDR, outdated agent versions), and turn them into actionable tasks to enhance your security posture.

- Understand when proper asset security controls are not sufficient
- Highlight contradicting asset details across different tools
- Define criteria to identify inactive or decommissioned assets
- Uncover potential regulatory issues ahead of your audits

©2025 Zscaler, Inc. All rights reserved.



Create New Policy

Details

Title *: Assets missing owners in CMDB — Active

Description: Identifies assets that were recently scanned by other agents

Category *: CMBD Hygiene

Severity *: 8.8 Critical

Policy Criteria

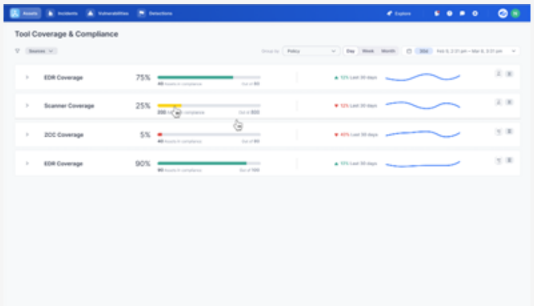
Trigger Settings

Policy Violation Findings

Increase the confidence level in your CMDB

Improve data hygiene by automatically updating the CMDB and resolving data discrepancies across systems.

- Ensure the CMDB records all known organizational assets
- Identify assets not previously known but seen in network traffic
- Ensure critical elements are in the CMDB (domain, serial number, owner, “crown jewel” designation, business unit, geography, etc.)
- Build workflows to automatically update the CMDB



Tool Coverage & Compliance

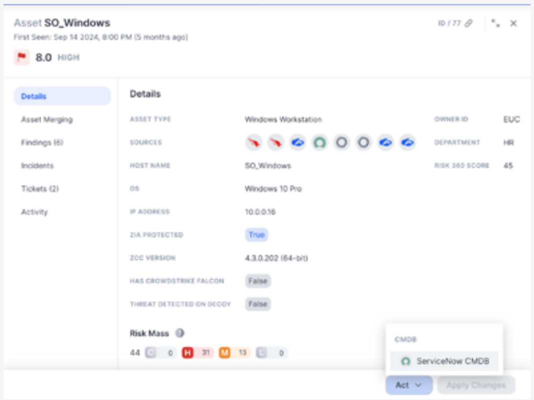
Feb 6, 2:31 pm – Mar 8, 3:31 pm

EDR Coverage	75%	40 Assets in compliance	Out of 80	▲ 12% Last 30 days
Scanner Coverage	25%	200 Assets in compliance	Out of 800	▼ 12% Last 30 days
ZCC Coverage	5%	40 Assets in compliance	Out of 80	▼ 40% Last 30 days
EDR Coverage	90%	90 Assets in compliance	Out of 100	▲ 10% Last 30 days

Improve cross-team collaboration with robust reports and dashboards

Showcase program health status or any other metric, leveraging a library of pre-built and custom dashboards and reports.

- Leverage robust, out-of-the-box asset dashboards and reports
- Design your own dashboards to measure what matters to you
- Report on any data point or broader policy to track KPIs
- Track posture per policy by business unit, team, product, geo, etc.



Asset SO_Windows

First Seen: Sep 14 2024, 8:00 PM (5 months ago)

8.0 HIGH

Details

ASSET TYPE	Windows Workstation	OWNER ID	EUC
SOURCES		DEPARTMENT	HR
HOST NAME	SO_Windows	RISK 360 SCORE	45
OS	Windows 10 Pro		
IP ADDRESS	10.0.0.16		
ZIA PROTECTED	True		
ZCC VERSION	4.3.0.202 (64-bit)		
HAS CROWDSTRIKE FALCON	False		
THREAT DETECTED ON DECOY	False		

Risk Mass

44 C 0 H 31 M 13 L 0

Drive efficient risk mitigation actions

Trigger automated remediation workflows and policy adjustments to restrict access for users associated with risky assets to decrease risk.

- Automatically update the CMDB with missing assets or elements
- Trigger built-in or custom access policies for risky assets
- Initiate automated remediation workflows via ticketing systems
- Assign policy violations to the right owner with actionable information

©2025 Zscaler, Inc. All rights reserved.

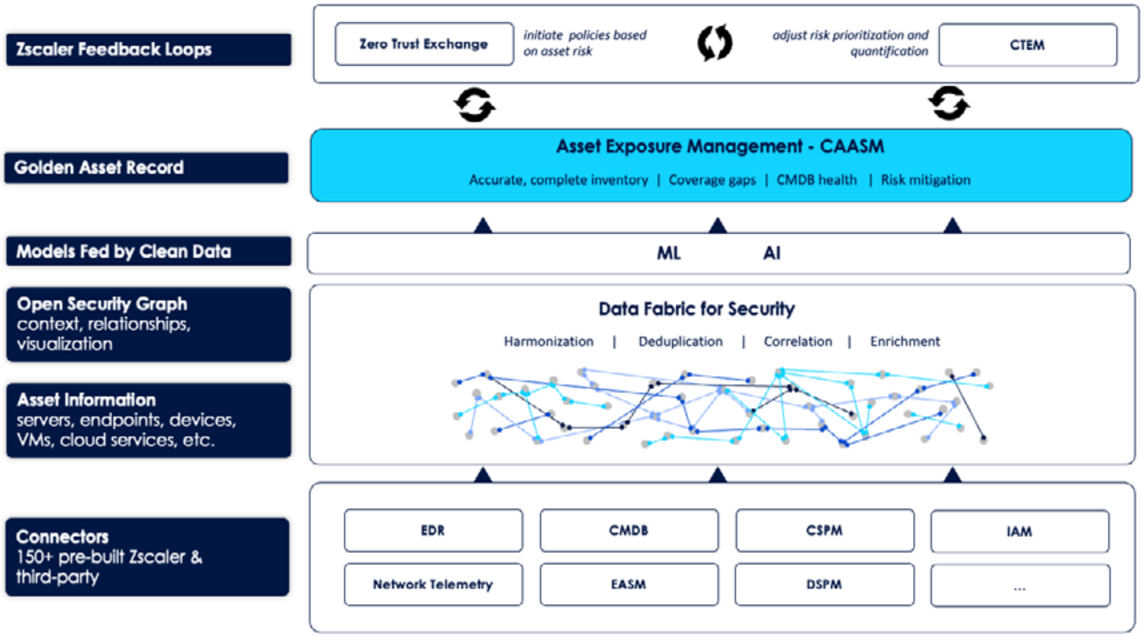
How does it work?

Effective asset exposure management requires discovering and correlating a myriad of previously siloed data sources. Zscaler has pioneered the use of a data fabric that fundamentally transforms the scalability and effectiveness of CAASM.

The Data Fabric for Security seamlessly aggregates and correlates asset information across 150+ security tools and business systems, plus an AnySource connector, which pulls in data from any other application or flat file. The Data Fabric harmonizes, deduplicates, correlates, and enriches these millions of data points to provide a deep understanding of assets, controls, gaps, and misconfigurations.

Once the Data Fabric correlates the data from all your security and IT tools and produces "golden record" of your assets, the Asset Exposure Management application identifies tool coverage gaps or misconfigurations based on your business rules. For example, if your policy dictates that all laptops in the U.S. must be running CrowdStrike, while all laptops in Europe must be running SentinelOne, Asset Exposure Management can tell you which endpoints have the wrong endpoint tool, duplicate tools, or no tool.

Outbound integrations, or "outegrations," allow any finding to initiate a policy. For example, you can automatically raise a bidirectional ticket, kick off an update to your CMDB, or initiate a Zscaler ZIA or ZPA policy to restrict access for a user whose machine is not adhering to company policies or exhibiting risky characteristics.


Zscaler Feedback Loops
Zero Trust Exchange
initiate policies based on asset risk
adjust risk prioritization and quantification
CTEM
Golden Asset Record
Asset Exposure Management - CAASM
Accurate, complete inventory | Coverage gaps | CMDB health | Risk mitigation
Models Fed by Clean Data
ML
AI
Open Security Graph
context, relationships, visualization
Data Fabric for Security
Harmonization | Deduplication | Correlation | Enrichment
Asset Information
servers, endpoints, devices, VMs, cloud services, etc.
Connectors
150+ pre-built Zscaler & third-party
EDR
CMDB
CSPM
IAM
Network Telemetry
EASM
DSPM
...

Get a closer look at Zscaler Asset Exposure Management in action and request your CTEM workshop at **www.zscaler.com/caasm**.

zscaler™ | **Experience your world, secured.™**

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

© 2025 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at **zscaler.com/legal/trademarks** are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.