6 Mistakes to Avoid in Building an Exposure Management Program

EBOOK

6 Mistakes to Avoid in Building an Exposure Management Program

In the rapidly evolving landscape of enterprise technology, understanding and securing the attack surface has become increasingly difficult. The scale and complexity of operations create stale asset inventories and siloed tools that produce findings without context, preventing the clarity required for proactive cybersecurity.

Today's enterprise environments frequently consist of tens of thousands of internet-exposed assets, ranging from websites and source code repositories to SSL certificates and S3 buckets. Additionally, modern infrastructure must account for Internet of Things (IoT) devices, operational technology (OT) systems, cloud-based SaaS applications, and assets from third-party vendors and partners. This intricate web of interconnected technologies leads to blind spots in inventories, disjointed exposure findings, and fragmented business context. As a result, security teams spend countless hours manually prioritizing an incomplete view of exposures.

Exposure management programs are designed to secure the organization proactively, but building an effective program is challenging. This eBook highlights six critical mistakes to avoid in this process. By understanding and avoiding these common pitfalls, security professionals can achieve more effective visibility, strengthen their defensive posture, and ensure a comprehensive approach to mitigating risks across the attack surface.

Mistake **#1: Failure to Define Scope**

Mistake **#2: Blind Spots in the Asset Inventory**

Mistake **#3: Failing to Apply Asset Security Controls**

Mistake **#4: Failing to Apply Asset Context in Prioritizing Vulnerabilities**

Mistake **#5: Failing to Leverage Automation in Remediation Workflows**

Mistake **#6: Leaving Responsibility and Ownership in Silos**

Let’s take a closer look at each one.

Mistake #1: Failure to Define Scope

Scoping entails making a business decision about which assets your exposure management program will cover.

“Why not all assets?”

Ideally, your program will be comprehensive—eventually. The most important assets to include initially are the ones connected to business-critical operations, compliance mandates, or other strategic goals. Start by defining your most critical asset categories, then evaluate which of these assets are currently being discovered and tracked by an existing tool or program, such as a Configuration Management Database, Active Directory, or Endpoint Detection and Response (EDR) tool.

You may discover visibility gaps during the scoping process. For instance, you may have data on devices, network infrastructure, and some applications, but might not be able to cover online code repositories or software supply chains. Or, a financial services company may have excellent data for on-prem assets at headquarters, but a recent acquisition has poor asset hygiene.

When making scoping decisions, stakeholders need to balance the severity of business risks with the feasibility of data collection. The more data you have access to, the more assets you can include in your inventory. In a perfect world, you’d have complete data on all your assets. If you don’t have this—at least at the beginning—you can limit the initial scope of your inventory.

Over time, as your program matures and you integrate data from additional sources, you can include more assets in your inventory and broaden the scope of your program with investments in asset discovery tools.

Leveling up your exposure management program:

Stage of maturity:	Assets to include:
Initial	• Endpoints • Network-connected assets • External attack surface • SaaS apps
Intermediate	• Code repositories • Third-party risk • Cloud assets
Advanced	• Digital risk protection • Deep and dark web sources • AI and LLMs

Scoping enables you to build a program with clear boundaries and objectives. It also allows you to establish benchmarks against which you can measure success.

Mistake #2: Blind Spots in the Asset Inventory

The attack surface evolves in only one direction: towards greater complexity. The number of assets that organizations manage continues to increase every year, while increasing use of open-source code and cloud development all further increase attack surface complexity.

Corporate growth through acquisition leads to subsidiaries with external-facing assets that are unknown to the organization's central vulnerability management team. The gateway for a bad actor could sit within a subsidiary, running one legacy application on a forgotten server under a desk.

Unfortunately, most security leaders believe that their organization's asset inventory is incomplete, and a majority acknowledge that it is probably missing critical assets.

According to Gartner® research[1]:

30% of IT assets are missing from inventories

30% of newly-purchased assets are never entered into the system of record

24% of organizations haven't verified their IT asset inventories within the past five years

[1] Gartner Research, "Create an Asset Management Practice as a First Step in Reducing Cost and Audit Risks," January 2023.

One of the primary causes of visibility issues is an over-reliance on limited data sources. Security teams often rely on a CMDB, an EDR tool, or a database like Active Directory to build an inventory of assets to secure. While these are all useful sources of asset data, it takes all of these tools (and then some) to drive complete visibility.

As you revisit the initial scope of your program, consider all of the data sources that might enrich the asset records within scope, including:

- EDR solutions
- Configuration Management Database (CMDB)
- Vulnerability scanning tools
- IT databases like Active Directory
- Cloud security posture management (CSPM) and data security posture management (DSPM) solutions
- External attack surface management (EASM) solutions
- Network telemetry
- Spreadsheets

The more data sources feeding your inventory, the closer you'll get to maximum visibility and complete asset context. You'll also know exactly which assets are missing coverage from vulnerability scanners and EDR tools. Consider a solution with built-in connectors to all relevant data sources, including files, databases and even spreadsheets. It should harmonize, deduplicate, correlate, and enrich asset records across sources to create a uniform "golden record" of assets with the context required to enforce proper security controls.

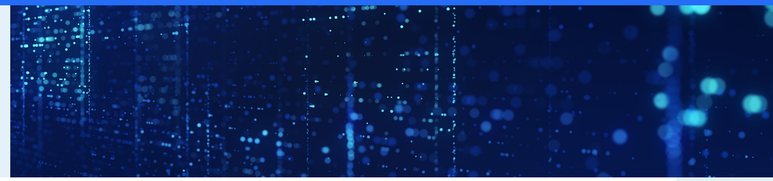
Even the most reliable individual asset management tools have gaps, blind spots, and incomplete context on their own. By combining the data from various sources, security teams can close those visibility gaps and improve the hygiene of every contributing source.

The **configuration management database (CMDB)** is a key source of asset data on the IT operations side of the house, but there are important gaps when it comes to security:

- They are often blind to asset categories covered above (especially cloud resources and external-facing assets from subsidiaries).
- IT teams often update them manually, leading to out-of-date asset records and missing properties such as owner, location, and who's responsible for maintenance.
- They have no way to assess risk context or identify exposures such as missing security controls, risky open ports, and unauthorized software.

While the CMDB should be ONE source of asset data for your exposure management program, it is not a record of truth for asset inventory.

In fact, an ideal approach would be to feed asset data back from your exposure management program to the CMDB, ensuring IT's primary source of asset data is always up-to-date.



Mistake #3: Failing to Apply Asset Security Controls

An inventory answers the question, *What assets do we own?* But to manage your attack surface effectively, you need to ask:

- *Where do we have coverage gaps or missing security controls?*
- *Which operating systems are approaching end-of-life?*
- *Can we apply mitigations or configuration changes to reduce the risk?*

An effective Cyber Asset Attack Surface Management (CAASM) solution can answer these questions with important asset context, helping your team design policies, compliance benchmarks, and mitigation processes to harden your technology environment at the foundation. This sets the foundation for your entire exposure management program.

Identifying coverage gaps

When assets have misconfigurations, missing agents (such as EDR or vulnerability scanning), or misalignment with the CMDB, they are at greater risk to the organization. Your program should systematically identify assets out of compliance with your coverage and control policies, surfacing violations for swift remediation.

Proactive management of EOL/EOS operating systems

End-of-life (EOL) and end-of-support (EOS) technology can contain unpatchable vulnerabilities. When vendors discontinue maintenance or support of an operating system, it is imperative that IT and security teams upgrade technology before it introduces exposures. Obsolete technology is not only a burden on users and business operations, it is a target for attackers. You should track upcoming EOL/EOS operating systems, prioritize according to business criticality, and provide your organization ample time to plan and budget for upgrades.

Mitigate exposures at the asset level

While vulnerability management is a critical program for proactive cyber defense, it's not the *only* way to reduce the likelihood of an attack. CAASM solutions should streamline mitigation workflows to address exposures such as misconfigurations, outdated or missing agents, or missing CMDB owners. By integrating your CAASM solutions with ITSM and CMDB tools, you can put rich asset data to work to initiate proactive mitigation workflows.

Mistake #4: Failing to Apply Asset Context in Prioritizing Vulnerabilities

Vulnerability management programs often fall into the trap of being overly focused on Common Vulnerabilities and Exposures (CVEs). CVEs are reported centrally, and relatively simple to find them, count them, and measure your progress in remediating them.

One reason security programs become over-reliant on CVEs is that they rely on scanning methods that provide context only for the vulnerability, not the asset on which it exists. In other words, they don't prioritize asset context because they don't *have* asset context.

In the real world, not all CVEs are created equal. Imagine if you have two CVEs, each with a severity rating of "9." One is on an internal server, in a development environment that is not exposed to the internet, and the server is running an EDR agent. The other is on a production instance of a web application, where any customer (or attacker) could find and access it, and crucial protective controls are misconfigured. Which one would you patch first?

It is essential that the data model used by your exposure management solution be flexible and expansive enough to include information about the presence (or absence) of compensating security controls for every asset. This makes it possible to map exposures against compensating controls, so that you can identify coverage gaps in real time.

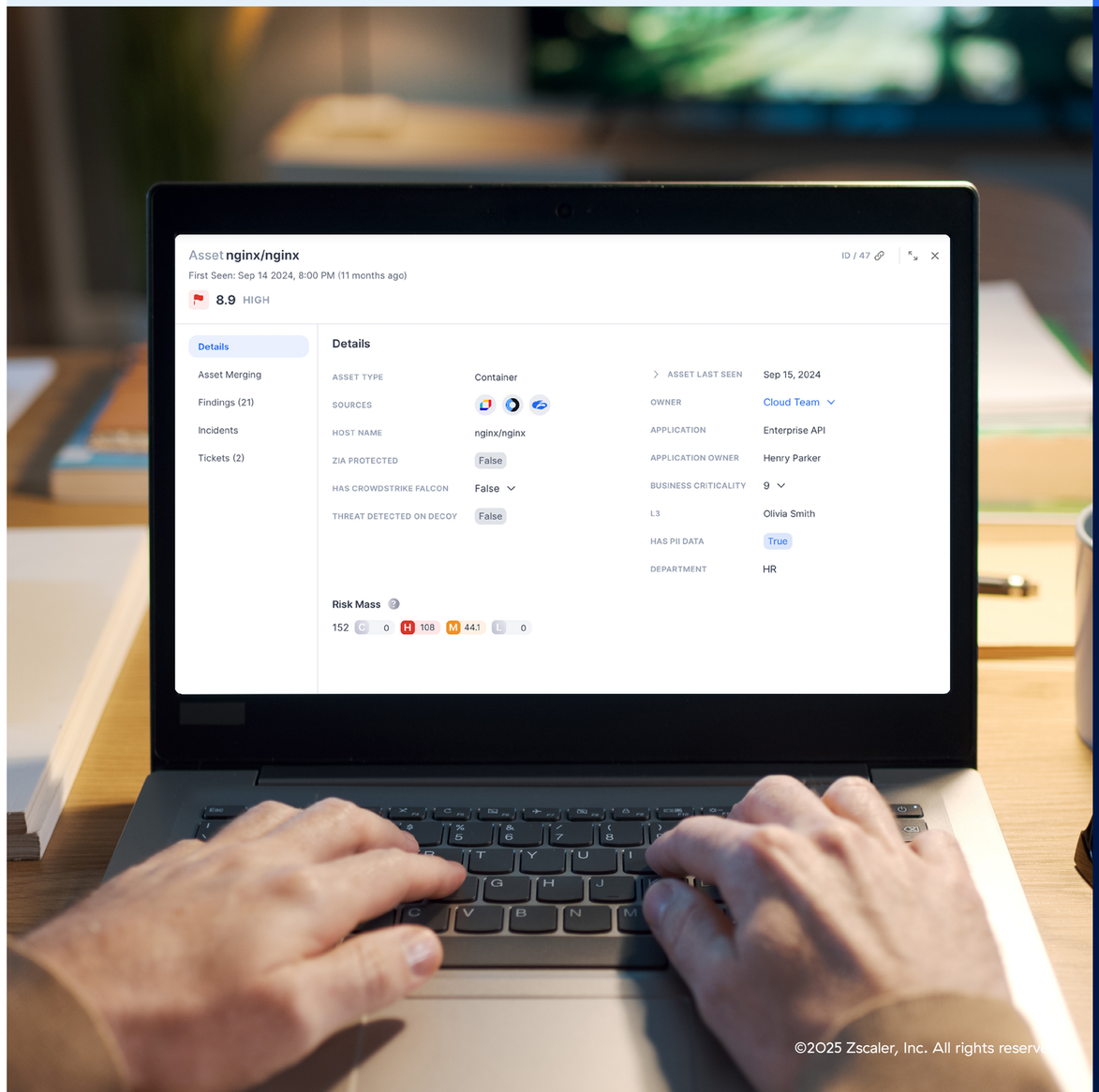
Your solution should enable users to see every asset in the environment, along with rich contextual data about that asset, including:

- Who owns it?
- What operating system is it running?
- Where is it located?

More importantly, though, you should also be able to visualize the extent of your security coverage inside the solution. It should have an easy-to-use dashboard that lets you instantly answer questions like:

- Which assets have been scanned for vulnerabilities in the last 10 days?
- Which assets are missing EDR agents?
- Which assets are protected by a Zero Trust-based Network Access (ZTNA) or secure connectivity solution?

When the solution provides a clear visualization illustrating where you have coverage, where coverage is multi-layered, and where it is absent, you have an easy way to identify your most pressing risks. This enables you to prioritize remediation efforts in ways that truly address the greatest risks first.



Mistake #5: Failing to Leverage Automation in Remediation Workflows

Proactive security requires two key ingredients to deal with the quantity of exposure data: prioritization and efficiency. By now, you should have some actionable tips for prioritization in your exposure management program, so let's talk about efficiency.

The wealth of asset and exposure data creates the opportunity to automate simple decisions and repetitive tasks in the remediation workflow.

Examples include:

- Who owns this ticket?
- What is the Service Level Agreement (SLA)?
- Is this resolved?

You can also initiate tasks such as:

- Restrict user access due to a critical vulnerability
- Update this asset record in the CMDB
- Retire this asset from our inventory

Your solution should support automated assignment for vulnerability and policy violation tickets, SLA setting, and ticket status updates with robust bi-directional integrations with IT ticketing tools. It should also have "outegrations" with secure access or zero trust providers to automate mitigating actions, such as restricting user access when the device has a critical vulnerability or additional risk factors.

You may never reach zero exposures, but a tightly integrated exposure management solution can drive automation and efficiency, helping your teams maximize its resources for risk reduction.

Mistake #6: Leaving Responsibility and Ownership in Silos

Exposure management is a team sport. The most successful organizations foster cross-functional collaboration between IT, security, compliance and risk management teams, and the business as a whole.

Democratizing information access is a key first step in building open, transparent communication, which is at the heart of strong collaborative relationships. When a solution offers robust reporting and easy-to-use, easy-to-share dashboards, it makes it simple to measure what matters most to the organization. Even better, it simplifies communicating key metrics and progress to stakeholders, executive leadership, and the board.

When there's an array of granular reports and dashboards to choose from out of the box, it's easy to share information about policy effectiveness or any other Key Performance Indicators (KPIs). Flexible reporting also makes it possible to track asset posture by business unit, team, product, geographic location, and many other factors.

Information-sharing contributes to the creation of a culture of accountability. Your exposure management platform should drive stronger prioritization of exposures AND generate remediation workflows designed for your organization's cross-functional processes.

How Can Exposure Management Help Our Enterprise Reduce Real-World Risks?

Continuous Threat Exposure Management (CTEM) is a framework for achieving proactive cyber risk reduction. The term was coined by Gartner, Inc. to describe an integrated, iterative approach to risk-based vulnerability reduction and security posture improvement. Incorporating people, processes, and technologies, CTEM is a cyclical five-step process that enables an organization to continually re-evaluate the accessibility, exposure, and exploitability of its digital and physical assets.[2] The five steps are **scoping, discovery, prioritization, validation,** and **mobilization.** Learn more about building an effective CTEM program in this ebook.

Ultimately, effective exposure management leads to faster remediation, improved compliance, and a measurable, demonstrable reduction in risk.

Zscaler's Exposure Management platform includes all of these comprehensive capabilities, together in a single solution.

[2] Gartner, *Implement a Continuous Threat Exposure Management Program*, October 2023.

ZSCALER EXPOSURE MANAGEMENT IS ENABLING LEADING ORGANIZATIONS TO:

- **Create an accurate asset inventory**
  Get a complete representation of your asset attack surface by continuously running cross-source deduplication, correlation, and resolution across all assets, including endpoints, cloud resources, network devices, IoT, and more.
- **Identify coverage gaps**
  Easily pinpoint potential compliance issues and misconfigurations (e.g., assets lacking EDR, outdated agent versions) and turn these into actionable tasks to enhance your security posture.
- **Prioritize the riskiest vulnerabilities and exposures**
  Unify findings from every source in the environment, harmonizing exposure data and enriching with business context and threat intelligence.
- **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.
- **Reduce risk with AI-powered remediation and custom workflows**
  Group related findings or policy violations into smart tickets, connect tickets to custom service requests or ITSM workflows, and leverage an AI copilot for tailored remediation plans.

Zscaler Exposure Management delivers a holistic approach to help security teams identify, prioritize, and close their riskiest exposures. Request a demo to see this consolidated view for yourself.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 www.zscaler.com