CASE STUDY

How a Real Estate Investment Organization Protected Their IT Environment with Sevco

COMPANY: REAL ESTATE INVESTMENT **EMPLOYEES: BETWEEN 2,500-5,000**

Problem: The real estate investment organization was overwhelmed managing vulnerabilities that its security tools surfaced, with no easy way to identify which vulnerabilities to prioritize.

Solution: The Sevco Platform provided asset intelligence and additional context on the vulnerable assets by aggregating asset data from across the Real Estate Org's toolset, enabling them to determine that most vulnerabilities were on a small number of devices and could be easily resolved by making a simple software update. Further, the Real Estate Org could use Sevco's aggregated asset data to prioritize remediation of the remaining vulnerabilities.

Background

In 2022, a major Real Estate Investment Organization launched an initiative to understand exactly how many assets they had and identify any security coverage gaps. Their environment had tens of thousands of assets, including customer-facing systems, operational technology (OT) systems, and IT components.

Initially, they identified a CMDB as the best option to build an asset inventory as it could pull data from various tools. However, they ran into issues due to the staff and time required to implement and maintain the system. The CMDB asset inventory was static—updates had to be run on a discrete basis and then assets were then manually deduplicated. This became an increasingly burdensome process, and never fulfilled the Real Estate Org's requirements.

The Challenge

In 2023, the Real Estate Org decided to take a different approach and kicked off a threat and vulnerability program to truly understand and remediate the risks in their environment. They turned to a channel partner for their expertise.

The Real Estate Org had deployed new Managed Detection and Response (MDR) and Mobile Device Management (MDM) platforms along with a handful of other tools to understand where vulnerabilities existed in their environment. However, these tools identified an overwhelming number of vulnerabilities: more than 80,000 in all.

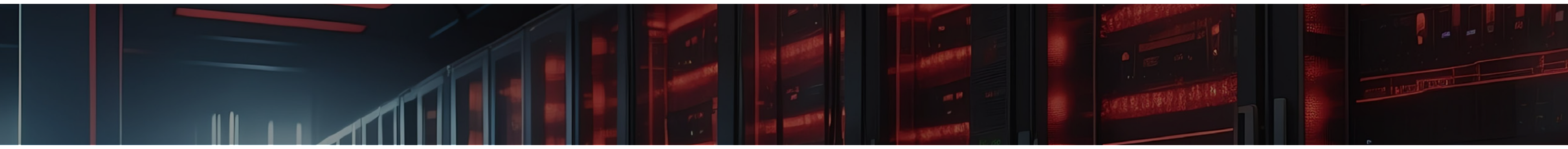
Assessing each of these vulnerabilities individually would have taken months or years. With so many sources of data and no correlation between them, they realized they needed a solution that would provide a comprehensive view of their environment in order to put the vulnerabilities into the proper context, identify the true extent of their risks, and prioritize their remediation efforts. To quickly and effectively address the vulnerabilities, a comprehensive security asset inventory was needed.

The Solution

The Real Estate Org and their channel partner knew that the best way to build a comprehensive and dynamic security asset inventory was with an asset intelligence solution. So they brought in Sevco's cloud-native security asset intelligence platform.

Sevco kicked off an assessment, and in only 30 minutes, they had integrated three sources via API: Directory Services, an Enterprise Mobility Management (EMM) tool, and their MDM. Within 24 hours, the team had integrated 80% of their collecting points, and further integrations were limited only by staff availability.

Immediately after integration, the Real Estate Org team saw that Sevco's platform correlated the data from across all the integrated tools with accuracy and speed that they had never been able to achieve previously.



Within days, the correlated data in Sevco's platform showed the team that tens of thousands of vulnerabilities identified by the MDR actually belonged to only 3,000 devices, and they could resolve nearly all of those CVEs simply by upgrading the operating systems on those specific devices.

Sevco's platform provided the visibility and context (aggregated from across their toolset) to surface the true risk to the Real Estate Org, and identify the most efficient way to remediate that risk. The team saved hundreds of person-hours that would have been spent manually addressing the tens of thousands of vulnerabilities. And all of this was discovered with the Sevco assessment in a matter of days.

Within two months, the Real Estate Org purchased and fully deployed Sevco, enabling them to:

- **Manage their endpoints** to ensure they're properly configured and software is up-to-date
- **Prioritize remediation of vulnerabilities** by leveraging the cross-referenced data and identifiers from across their tools and associating the users and software linked to affected devices
- **Launch a threat hunting campaign** to proactively identify and remediate threats, leveraging data on security gaps, vulnerabilities, patches, tool configuration, and more
- **Drive compliance with regulations** around asset visibility, asset inventory, password updates, and more with proactive alerts when devices or users are out-of-compliance
- **Drive faster and more efficient audits** with the most comprehensive data to run pre-audit exercises to proactively address issues before full audits
- **Identify and decommission obsolete systems**

Sevco has fundamentally changed the way the Real Estate Org approaches cybersecurity. By continuously aggregating data from across their toolset and providing deep context about every asset, Sevco surfaces insights that would not have been discovered without the platform—enabling better security and driving greater efficiencies.

How Sevco Detects and Prioritizes Vulnerabilities

The Sevco Platform provides a comprehensive, multi-source inventory of your assets, the state of their security controls, and vulnerabilities by integrating with your existing security tools to aggregate, correlate, and deduplicate the data in those sources. Because Sevco has visibility and correlates assets and data from across all your tools, it provides a more comprehensive view compared than any single tool—and surfaces important context to assess risk and business impact for each asset.

With this foundation, Sevco automatically detects and proactively alerts your team to vulnerabilities detected in your environment: software vulnerabilities (CVEs), missing or misconfigured security controls (security gaps), and IT hygiene issues (unpatched devices, shadow IT). Sevco finds these vulnerabilities and security gaps quickly and automatically, relieving your team of the laborious and time-intensive manual process of reconciling asset inventories across tools. Instead, they can focus on prioritizing remediation and closing those security gaps quickly.

Schedule time with Sevco today to see what security gaps exist in your organization. After a 30-minute personalized demo, you will receive a no-cost assessment of your assets, the state of your security controls, and vulnerabilities that will provide immediate value and actionable insights.

Contact Us

sevcosecurity.com

@sevcosecurity

1401 Lavaca Street #857
Austin, TX 78701

About Sevco Security

Sevco is the cloud-native CAASM platform delivering the industry's most accurate, real-time IT asset inventory. Hundreds of companies rely on Sevco's 4D Asset Intelligence engine to bridge the gap between IT and security teams. By providing a continuously updated inventory of assets, Sevco autonomously identifies and closes previously unknown security gaps, while dramatically improving incident response. Sevco's patented asset telemetry uncovers significant security gaps and out-of-compliance assets in every deployment without fail. Founded in 2020 and based in Austin, Texas. For more information, visit https://sevcosecurity.com or follow us on LinkedIn.