

One Platform - Continuous Exposure Management

Sevco at a Glance

- Gain visibility across your entire attack surface—**internal, external, cloud, end users.**
- Prioritize the exposures that matter—**misconfigurations, vulnerabilities, security gaps.**
- Streamline your cross-functional remediation—**automated actions, workflows, resolution tracking.**

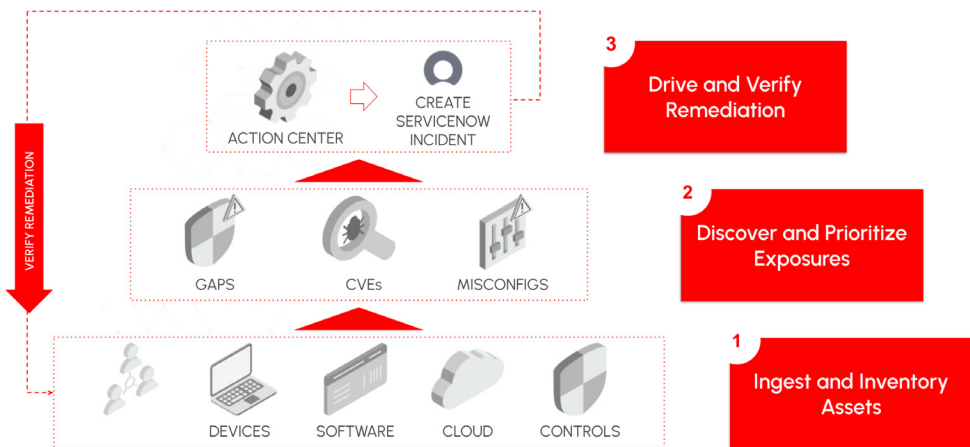
“Sevco Security’s ability to report believable metrics across the entire vulnerability lifecycle is powerful and utterly unique. A closed ticket doesn’t mean a vulnerability was actually fixed. Sevco surfaces those challenges, allowing teams to collaborate across departments to continuously improve our security posture and mature operations.”

Jeffrey M. Vinson, Sr.
Former CISO
Harris Health

Mission Control for Security Teams: The Sevco Exposure Assessment Platform

Leverage 1000+ integrations to scope your attack surface and discover all of your assets. Identify high risk exposures associated with your assets, correlate them with threat intelligence, and prioritize them according to business context. Take action against critical exposures and verify their remediation. Sevco combines the power of CAASM, Vulnerability Management, and Cloud Security Posture Management in one robust Exposure Assessment Platform.

Continuous Monitoring of the Entire Exposure Life Cycle



Core Use Cases

Asset Inventory

- Aggregate, correlate, and deduplicate assets in real-time via API from your existing security investments
- Automatically maintain the relationship between your assets in a visual graph of your attack surface
- Monitor the presence and state of security controls to optimize agent deployment, scan coverage, and asset compliance

Vulnerability Management

- Unify your vulnerability assessment data with the full context of your asset inventory
- Instantly correlate threat and exploit intelligence to every vulnerability
- Customize prioritization based on asset criticality, severity, exploitability, and business impact

Cloud Security Posture Management

- Inventory cloud resources across multiple cloud providers via integrations with your CNAPP tools
- Prioritize cloud security findings—misconfigurations, sensitive data, overprivileged accounts, and more
- Remediate the highest risk attack paths to reduce cloud cyber risk

Exposure Management

- Normalize risk across different types of exposures—security controls gaps, CVEs, cloud—for one holistic view of attack surface risk
- Go beyond ticket closure and verify remediation actions on assets and exposures
- Track the health of your security program with custom dashboards and reports

Unify your siloed data to reduce risk

Reduce the number of alerts, the fatigue of detection, and the complexity of siloed data analysis. Sevco's Exposure Assessment Platform automates the discovery of critical exposures that pose a real threat to the attack surface, quantifies risk and prioritizes different classes of exposures, and accelerates remediation with automated actions. From a single pane of glass, security teams can track the progress of remediation efforts, verify the resolution of risk—going beyond the closure of a ticket, and assess the overall health trend of their security program over time.

Exposure Management

Severity: Based on risk to the environment

Open: Number of assets impacted by vulnerability needing action

Total: Total number of assets impacted by vulnerability including those that are snoozed or accepted as risky

Avg age & compliance: Avg number of days assets have been associated w/ vulnerability and impacted assets within or outside SLA

The dashboard screenshot shows a summary of assets to review (5,372), new today (146), and assets in remediation (129). It includes a donut chart for severity levels (Low, Medium, High, Critical) and a table of vulnerability categories such as 'At risk admin devices', 'At risk admins', and 'No endpoint security'. An 'Aging trend' bar chart shows the number of assets over time from March 8th to today. A table at the bottom provides details for specific vulnerabilities, including their descriptions, counts, 7-day changes, and SLAs.

Status detail of impacted assets

7-day change: Increase or decrease in the number of assets based on remediation effectiveness + new findings

View, add, or change actions like automated remediation workflows

Additional vulnerability description and details including observation, impact, and recommendations

Contact Us