SEVCO SECURITY

DATASHEET

Sevco Exposure Assessment Platform for Tech Companies

Scale Security at the Speed of Innovation

Key Benefits

Cloud-Native Visibility

Multi-cloud asset discovery across AWS, Azure, GCP, and Kubernetes environments

Rapid Incident Response

Quickly scope security incidents by identifying affected assets and their exposures

Shadow IT Detection

Discover unauthorized cloud services and rogue infrastructure

Security at Scale

Automated workflows and API-first architecture for hypergrowth environments

Sevco Exposure Assessment Platform Use Cases

Built for Fast-Moving Technology Organizations

Tech companies operate differently: rapid deployment cycles, ephemeral infrastructure, distributed teams, multi-cloud architectures, and a culture that prioritizes speed. Sevco's Exposure Assessment Platform is designed for this reality—providing continuous visibility and risk management across dynamic environments without becoming a bottleneck to innovation. Whether you're a SaaS startup, enterprise software company, or hyperscaler, Sevco scales with your growth.

Tech Company Use Cases

☑ **Dynamic Cloud Infrastructure Management**

Maintain real-time inventory of cloud resources that spin up and down automatically. Track virtual servers, microservices, and compute across multiple cloud providers and regions.

☑ **Developer Workstation & Application Governance**

Monitor security posture of developer laptops, track application adoption, identify shadow IT before it becomes a risk. Ensure security tools are deployed without hindering developer productivity.

☑ **SOC 2, ISO 27001 & Customer Trust**

Demonstrate continuous asset management and vulnerability remediation for compliance audits. Provide evidence of security controls to enterprise customers. Automate security questionnaire responses with real-time data.

☑ **M&A Security Due Diligence**

Rapidly assess security posture of acquisition targets. Identify technical debt, security gaps, and integration risks. Accelerate post-acquisition security standardization and tool consolidation.

Sevco Security was founded on the premise that bad data creates bad outcomes. Sevco breaks down siloed tech tools to provide a system of record to support security programs. With Cyber Asset Attack Surface Management (CAASM) as the inventory foundation, Sevco has evolved to include vulnerability assessment, vulnerability prioritization, and threat intelligence—becoming a true Exposure Assessment Platform (EAP) that provides comprehensive data on devices, identities, applications, users and vulnerabilities.

Key Capabilities for Technology Companies

Multi-Cloud Asset Discovery

Automatically discover and inventory assets across AWS, Azure, GCP, and hybrid environments. Track cloud resources, Kubernetes clusters, and deployments in real-time as they scale.

API-First Architecture

Integrate Sevco into your existing workflows via comprehensive APIs. Automate remediation, build custom dashboards, and connect security data to your internal tools. Built for engineers, by engineers.

Developer-Friendly Security

Provide security context without creating friction. Prioritize vulnerabilities based on production exposure, automate ticket creation in Jira/Linear, and verify fixes without manual follow-up. Security that engineers don't hate.

Compliance Automation

Streamline SOC 2, ISO 27001, and customer security reviews with continuous evidence collection. Generate compliance reports automatically and maintain audit-ready documentation without manual effort.

Solve Tech Company Security Challenges

Shadow IT & Application Sprawl

- Discover unauthorized applications
- Identify redundant tools and consolidation opportunities
- Monitor developer productivity tools for exposures

Ephemeral Infrastructure

- Track virtual servers and cloud instances across environments
- Monitor cloud security posture and misconfigurations
- Identify configuration drift
- Maintain inventory despite rapid environment changes

Developer Laptop Security

- Ensure endpoint protection on macOS and Linux devices
- Track vulnerability scanning coverage on workstations
- Monitor compliance with security baselines
- Identify unmanaged or personal devices accessing resources

Customer Security Requirements

- Respond to enterprise security questionnaires quickly
- Demonstrate continuous vulnerability management
- Provide evidence of security control effectiveness
- Maintain SOC 2 Type II and ISO 27001 certifications

Sevco Integrates with the Tech Tools You Already Use

A few examples of the hundreds of integrations Sevco supports:

- Cloud Security & CNAPP
- Development & Ticketing
- Cloud Security
- Identity & Endpoint
- Applications

Use Case Spotlight: SOC 2 Automation

Tech companies pursuing SOC 2 Type II certification need continuous evidence of security controls. Sevco automates evidence collection for critical controls including asset inventory management, vulnerability remediation tracking, and security tool deployment verification.

Automated Evidence for:

- CC6.1: Logical and physical access controls
- CC7.1: System vulnerability detection and monitoring
- CC7.2: Security incident response and remediation

Continuous Monitoring of:

- Endpoint protection deployment coverage
- Vulnerability patching within SLA windows
- Security tool configuration and compliance

Contact Us

sevcosecurity.com

@sevcosecurity

1401 Lavaca Street
#857 Austin, TX 78701

Email: hello@sevcosecurity.com
Phone: 512.270.8949