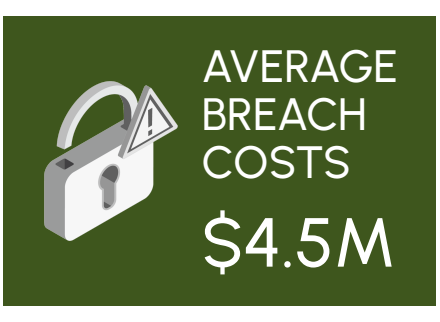
Reduce Compliance Liability and Risk While Curtailing Costs

The recent SEC case against the SolarWinds CISO shows that organizations have to prove their security controls are in place, working effectively—and most importantly enforceable with evidence-based-data.

How Are You Addressing CIS Critical Security Control 1: Inventory and Control of Enterprise Assets?



When the average breach costs **$4.5 million**, just one unprotected asset can present significant liability and risk. Having complete visibility and control of a comprehensive security asset inventory is control number one in every security framework, but achieving that control is extremely challenging. Tools and teams are siloed, providing disparate views of an organization's assets. There hasn't been a single source of truth—until Sevco.

"Asset inventory is critical. It's the number one thing on most regulatory and compliance frameworks. If you're talking NIST, the CRI profile, FFIEC CAT, the first thing they're asking you about is how well are you managing your inventory. We have to know what our assets are to protect them."

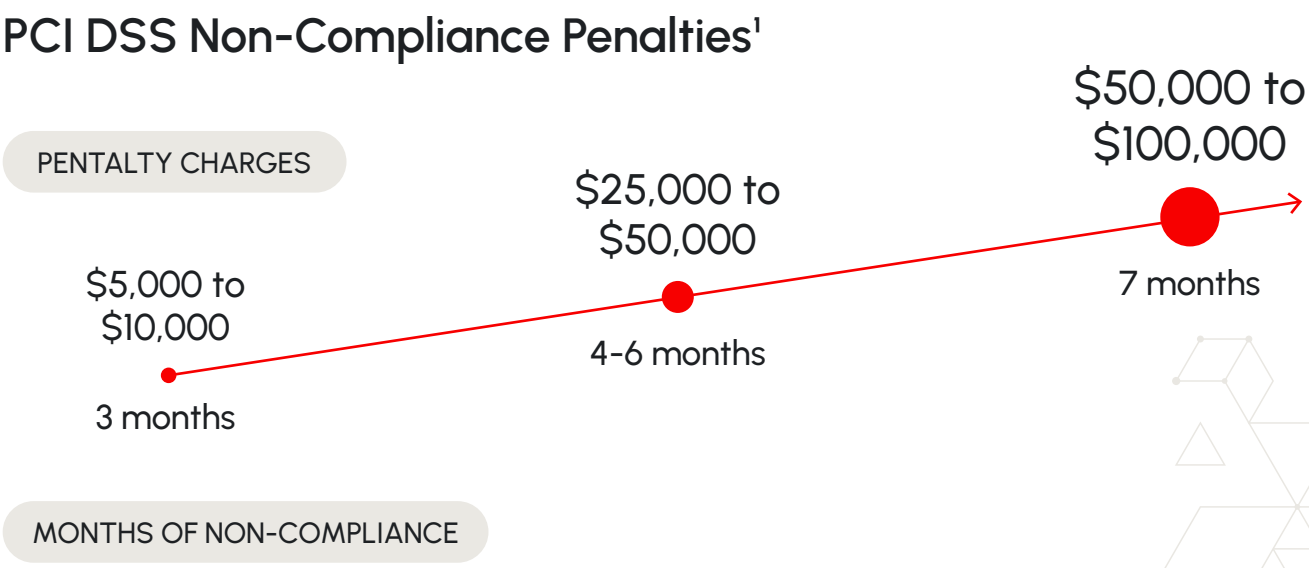
Steve Lodin, VP of Cybersecurity and IAM, Sallie Mae

The Costs Associated With Non-Compliance Are High

There are numerous associated costs with non-compliance including:

- Loss of Shareholder Value
- Regulatory Fines
- Legal Fees
- Greater/increased Future Audit Scrutiny
- Loss of Reputation
- Customer Impact
- Data Breach Reporting

PCI DSS Non-Compliance Penalties[1]



SEC Charges SolarWinds and Chief Information Security Officer With Fraud, Internal Control Failures

"As the complaint alleges, SolarWinds' public statements about its cybersecurity practices and risks were at odds with its internal assessments, including a 2018 presentation prepared by a company engineer and shared internally, including with Brown, that SolarWinds' remote access set-up was "not very secure" and that someone exploiting the vulnerability "can basically do whatever without us detecting it until it's too late," which could lead to "major reputation and financial loss" for SolarWinds."[2]

2023 U.S. Department of Health and Human Services Office for Civil Rights (OCR) Settlement Announcement

HHS Office for Civil Rights Settles HIPAA Investigation With Arizona Hospital System Following Cybersecurity Hacking[3]

Organization: Banner Health
Fine total: $1,250,000

Regulations by Type That Businesses Must Consider in a Modern Regulatory World

Industry

- PCI DSS
- HIPAA
- SOX-GLBA
- NERC-CIP
- CIS CSC
- FFIEC-CAT

Government

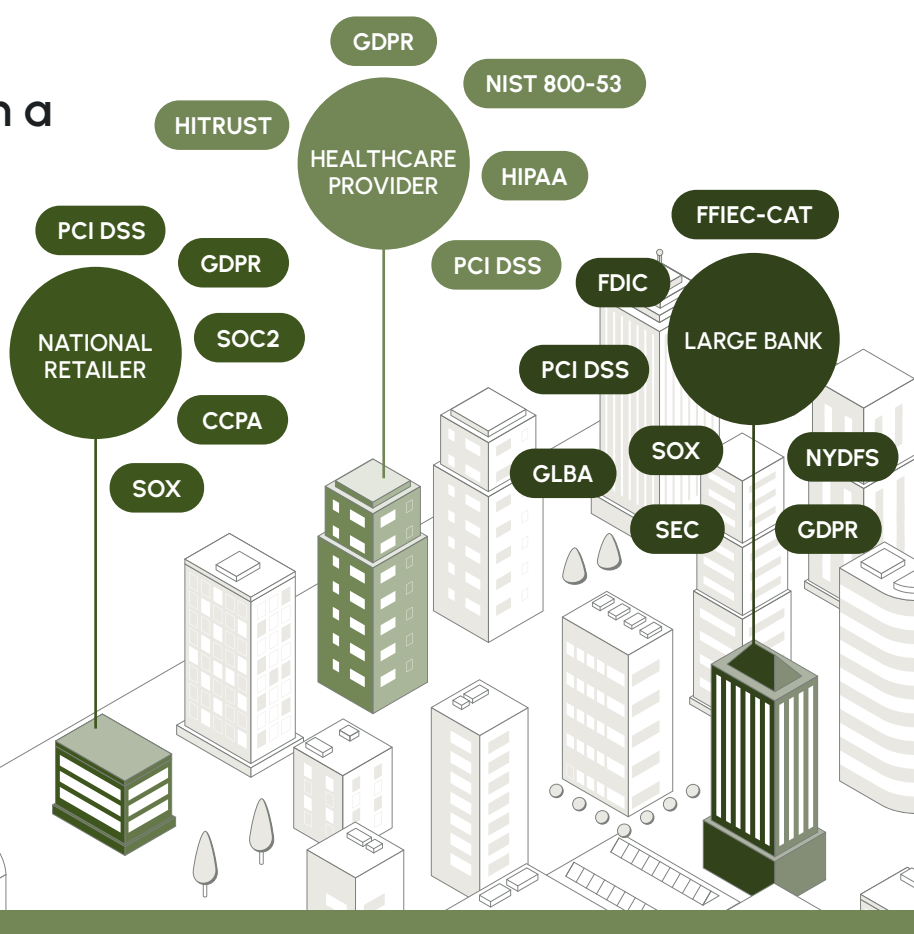
- CMMC
- FDIC
- GDPR
- FTC
- NIST 800-53/171
- SEC

Partner

- Third-party risk policy enforcement
- Risk assessment
- Supply chain certification

Corporate

- SOC Type 2
- Data privacy
- Data protection
- Licensing

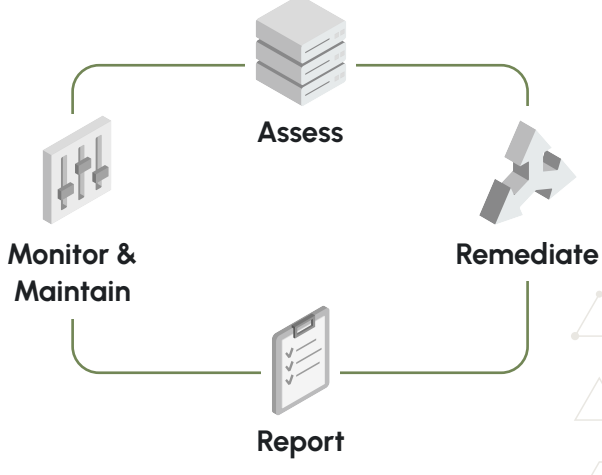


"Asset intelligence is so essential to financial services because it's so heavily regulated. It's not the asset that you can see - it's the asset that you can't see that typically gets you in trouble."

Brandon Pinzon, SVP and Chief Security Officer of Argo Group

Validate Continuous Compliance

Sevco's Asset Intelligence Platform provides a comprehensive real time view into an organization's environment that directly addresses security assessment and audit requirements including gap analysis, ensuring the security of the enterprise stack, automating vulnerability analysis and prioritization, and providing posture reporting to provide comprehensive data to prove findings, and enrich risk assessment.



Regulatory Requirements That Sevco Supports

To learn more, contact us at: info@sevco.io or book a demo at:

www.sevcosecurity.com/book-a-demo/

Regulations	Sections
PCI DSS v4.0	• **2.1** - Processes and mechanisms for applying secure configurations to all system components are defined and understood. • **2.2** - System components are configured and managed securely. • **12.2** - PCI DSS scope is documented and validated.
CIS CSC	• **Requirement 1.0** - Inventory and Control of Enterprise Assets • **Requirement 2.0** - Inventory and Control of Software Assets • **Requirement 4.0** - Secure Configuration of Enterprise Assets and Software
NIST	**ID.AM-1** - Physical devices and systems within the organization are inventoried
OCIE Cybersecurity Resiliency (SEC)	**Governance and Risk Management** - Risk Assessment
GDPR / LGPD	**Article 32 1 d** - Security of processing
HIPAA	**164.308 (a)(1)** - Security Management Process
NY State DFS Cybersecurity Requirements	**Section 500.03 a through m** - Cybersecurity Policy
NERC CIP	**010-3, 010-2 - Cyber Security** - Configuration Change Management and Vulnerability Assessments

Sevco Coverage Details

Sevco discovers, inventories, and conducts cross-asset correlation on a wide range of asset types including physical and virtual systems, applications, identities, and vulnerabilities. These assets can be local, remote, and cloud-based.

Sevco continuously validates and reports on the presence and configuration state of controls operating on regulated assets.

Applying priorities predicated on risk assessment, Sevco can remediate exceptions discovered during validation and integrate with risk management processes and cybersecurity policies such as change management and vulnerability assessments.

Regulatory Requirements Supported by Sevco

PCI DSS - Requirements 1, 2, 5, 6, 8, 10, 11, 12
SOX - Sections 105, 404
CIS CSC 20 - Controls 1, 2, 3, 4, 6, 7, 13
NIST CSF - SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
GDPR / LGPD - Articles 25, 32, 33, 35
FFIEC CAT
NERC CIP Standard - CIP 005-5, CIP 008-5, CIP-010-2

"As we think of about what connections out, the exporting feature is fantastic - especially when you want to provide that for auditors."

Albert Attias, Senior Director of Enterprise Security, Workday

1.https://blog.rsisecurity.com/pci-fines-and-penalties-for-non-compliance/ 2.https://www.sec.gov/news/press-release/2023-227 3. https://compliancy-group.com/hipaa-fines-directory-year/