POSITION PAPER

Emerging trends in security posture management (SPM)

Contents

Executive summary 3

The need for security posture management 4

What is security posture management? 4

What are the common, current approaches? 5

Why SPM needs to evolve 5

What are the new themes emerging? 6

Current and upcoming use cases 8

Conclusion: Importance of SPM in the context of cyber resilience 10

Executive summary

This position paper explores the growing importance of security posture management (SPM) in today's complex digital landscape.

NIST defines an organization's security posture as its cybersecurity fitness, reflecting resources (people, tools, policies) and threat adaptability.

This document describes the limitations of traditional reactive security measures and emphasizes the need for a proactive approach to security posture management.

Security posture management:

- Provides visibility of vulnerabilities across identity, data, and applications—including multi-cloud environments and AI models.
- Prioritizes risks based on real-world threats and business impacts, ensuring efficient resource allocation.
- Leverages behavioral analytics to detect anomalies and insider threats, improving threat detection accuracy.
- Automates security responses to expedite incident mitigation and streamline security operations.
- Secures new attack surfaces like the cloud and Internet of Things (IoT).

In short, this position paper illustrates that proactive SPM is an enabler of cyber resilience.

The need for security posture management

Organizations face multifaceted challenges in maintaining their security posture amid the complexities of managing data, applications, identity/access, cloud, and external pressures from evolving cybersecurity regulations. The rapid pace of application deployment, remote work, and supply chain vulnerabilities are expanding the attack surface and cyberthreat susceptibility.

Meanwhile, increasing regulatory demands not only impose financial penalties but also mandate specific safeguards and swifter breach notifications on executives like CSOs and CISOs.

SPM is essential for several reasons:

- **Risk mitigation:** SPM helps proactively identify potential security risks and implement strategies to mitigate them, reducing overall downtime.
- **Incident response**: Effective incident response plans and procedures minimize damage during security breaches or attacks. Learning from incidents ensures continuous improvement.
- **Compliance and governance:** Adhering to industry standards, regulations, and data security laws—such as HIPAA, GLBA, CCPA, GDPR, NIS2, DORA, etc.—demonstrates accountability and builds trust with regulatory bodies and customers.
- **Security architecture:** Properly designed and implemented security controls protect sensitive data, applications, and identity. Additionally, the minimization and sanitization of data reduce storage costs and mitigate risk.
- **Employee training:** Frequently educating employees on security protocols ensures consistent adherence to best practices.

Note that an organization's security posture is dynamic, evolving alongside technology and emerging threats. Assessing and strengthening it is crucial for maintaining resilience and safeguarding assets.

What is security posture management?

SPM is a comprehensive strategy for organizations to defend against evolving cyber threats, offering a holistic, best-practice-based approach to bolster defenses against risks like data and credential breaches, application and data vulnerabilities, and compliance failures.

SPM focuses on securing applications, data, digital identities, and cloud configuration/policies while emphasizing continuous risk management and proactive defenses.

By implementing AI-driven SPM, organizations can build a cyber-resilient infrastructure that adapts to new threats, reduces the attack surface, and maintains compliance and trust.

Automated response and orchestration minimize attackers' dwell time and operational windows, while continuous optimization ensures the security posture evolves with emerging threats and organizational changes.

What are the common, current approaches?

While firewalls, rule-based SIEMs, anti-malware software, strong password policies, vulnerability management, and disaster recovery plans remain foundational security practices, they represent a reactive approach with inherent limitations.

These methodologies excel at mitigating known threats, but today's cyber adversaries are increasingly sophisticated. Here is why relying solely on reactive measures can leave your organization vulnerable:

- Reactive tools struggle to identify and contain AI-generated attacks, zero-day attacks, or novel malware variants.
- Delayed detection and response take valuable time, potentially allowing attackers to exfiltrate data or disrupt operations.
- Reactive measures often involve downtime and resource allocation to address breaches, impacting productivity and revenue.
- Data loss can trigger regulatory fines and customer lawsuits, which also damage the organization's reputation.

Why SPM needs to evolve

Proactive SPM focuses on prevention, continuous monitoring, and rapid response. It leverages threat intelligence and advanced analytics to prevent emerging threats such as AI-driven phishing and social engineering attacks. It also prioritizes vulnerability management and employs behavioral analytics for anomaly detection.

Automated response and orchestration minimize attackers' dwell time and operational windows, while continuous optimization ensures the security posture evolves with emerging threats and organizational changes.

What are the new themes emerging?

AI integration

- **Visibility and discovery:** AI Integration with SPM allows organizations to discover and maintain an inventory of all AI models used across their multi-cloud environments. It tracks associated resources, data sources, and pipelines involved in training or fine-tuning these models. This prevents shadow AI models, compliance violations, and data exfiltration through AI-powered applications.

- **Data governance:** AI-focused legislation mandates strict controls around AI usage and customer data. AI-integrated SPM inspects data sources used for training AI models, identifying sensitive or regulated data (such as personally identifiable information) that might be exposed through model outputs or interactions.

- **Risk management:** AI-integrated SPM identifies vulnerabilities and misconfigurations in the AI supply chain. By analyzing the full supply chain (source data, libraries, APIs, etc.), it ensures proper encryption, logging, licensing, authentication, and authorization settings.

- **Runtime monitoring and detection:** AI-integrated SPM monitors and protects sensitive data in model outputs, implementing data-centric security measures and output validation processes.

Risk prioritization

Risk prioritization is a critical aspect of SPM. It ensures that resources are focused on critical issues with the highest impact. When you prioritize risk, you prevent spreading resources too thin across minor problems while leaving major vulnerabilities unaddressed.

The following best practices help you with risk prioritization:

- **Understand risks:** Not all vulnerabilities pose the same risk to every organization. Assessing severity in the context of your specific business environment is essential. Factors like data sensitivity, environment, and business context play a role.

- **Leverage threat intelligence:** Prioritize vulnerabilities based on actual risk. Understand which vulnerabilities are actively exploited and could harm your organization.

- **Maximize impact through correlation:** Address high- and medium-risk issues with many related findings. Correlation between multiple tools that are reporting the same finding with contextual information validates and simplifies resolution.

- **Frameworks and tools:** Consider aligning with frameworks like the NIST Cybersecurity Framework (CSF). The CSF provides a comprehensive structure for governing, identifying, protecting, detecting, responding to, and recovering from cyberattacks.

Proactive SPM goes beyond firewalls and continuously monitors clouds to identify vulnerabilities and enforce best practices.

Behavioral analytics

Behavioral analytics plays a vital role in enhancing an organization's security posture. By harnessing the power of AI and machine learning (ML), they analyze patterns in user behavior to identify potential security threats while maintaining data privacy:

- **Data collection and transformation:** Gather data from various sources (network traffic logs, access logs, database user activity records) and transform it into a suitable format for analysis. Relevant sensitive data must be protected using encryption, masking, or tokenization to maintain data privacy.
- **Data analysis:** Employ unsupervised ML algorithms to analyze data and detect anomalies that deviate from normal behavior.
- **Alerting and remediation:** When an anomaly is detected, an integrated alert system notifies security teams, providing necessary information for remediation.

Behavioral analytics helps detect insider threats and unknown threats, and reduces false positives, ultimately strengthening an organization's security defenses.

Response automation

Response automation is a critical aspect of SPM. It enables organizations to efficiently address security threats by automating routine tasks.

- **Efficiency:** By automating repetitive actions, security teams can focus on more complex threats, improving overall efficiency.
- **Incident response time:** Automated responses reduce incident response time, allowing faster mitigation of security issues.
- **SOAR Tools:** Security orchestration, automation, and response (SOAR) tools collect and analyze security data, enabling automated responses to low-level threats.

In summary, response automation enhances an organization's security posture by streamlining processes and freeing up resources for strategic security tasks.

New and emerging attack surfaces

Traditional security struggles with defending against the vast attack surfaces of the cloud and IoT. Proactive SPM goes beyond firewalls and continuously monitors clouds to identify vulnerabilities and enforce best practices. Micro-segmentation isolates data in clouds, limiting breach damage.

For IoT, identity and access management integration coupled with AI analytics introduces real-time visibility, allowing anomaly detection and compromised device isolation and control of access and permissions for IoT devices. This approach, including threat hunting and automated response, is crucial for a resilient security posture.

Continuous validation and governance

Governance in SPM bridges business priorities with technical implementation, including architecture, standards, and policy. Governance teams provide oversight and monitoring to sustain and improve security posture over time. They also report their compliance status as required by regulating bodies.

Continuous security validation extends SPM across all connections by combining attack surface management, security control validation, and automated red teaming. This approach ensures ongoing assessment, quick issue identification, and proactive mitigation—rather than waiting for external threats to exploit weaknesses.

Current and upcoming use cases

Application security

- Centralizes and contextualizes security findings from AppSec testing tools (SAST, DAST, SCA), offering tailored views for effective collaboration across security, development, engineering, and executive teams.
- Prioritizes vulnerabilities in code by leveraging AI to significantly reduce false positives, enabling organizations to increase developer productivity and focus on risks with the highest business impact.
- Enhances organizational productivity by reducing tool sprawl and aligns cybersecurity management with business objectives.

Data security

- Leverages AI-driven analytics to automate the discovery and classification of sensitive or dark data across multi-cloud environments.
- Reduces data storage costs using data minimization and data usage monitoring to identify only the most relevant structured or unstructured data to store.
- Mitigates large-language-model (LLM) training data theft risks by automating comprehensive data hygiene and sensitive data protection measures, such as encryption, masking, and hashing.

Identity security

- Reduces the identity attack surface by implementing the principle of least privilege. This allows access to the right resource, for the right person, and for the right amount of time before the access is revoked.
- Establishes the fundamentals of zero trust by implementing multi-factor authentication and passwordless authentication.
- Provides governance through automated workflow approvals for secure onboarding and offboarding of human and non-human identities.

Security operations

SPM involves several critical aspects of security operations, including automated risk mitigation, real-time SIEM correlation integrated with behavioral analytics, and proactive threat hunting:

- **Prioritizing vulnerabilities:** By integrating AI- or ML-driven behavioral analytics into SPM, organizations can identify critical vulnerabilities out of millions of events based on their potential impact, exploitability, and ease of mitigation. By focusing on high-impact risks, security teams can allocate resources effectively.
- **Automated risk mitigation:** SPM solutions automate the process of identifying and addressing security issues. Real-time insights allow for swift responses to threats, reducing the window of exposure.
- **Threat intelligence and proactive hunting:** Leveraging threat intelligence feeds and advanced analytics, SPM empowers security teams to proactively hunt for indicators of compromise and emerging threats. This allows them to identify and neutralize potential attacks before they cause damage.
- **Reporting and tracking:** SPM tools report identified vulnerabilities, track remediation efforts, and monitor progress. This ensures accountability and continuous improvement in an organization's security posture.

SPM plays a crucial role in safeguarding against misconfigurations, unauthorized access, compliance gaps, and other security risks across cloud environments.

Conclusion: Importance of SPM in the context of cyber resilience

Cyber resilience refers to an organization’s ability to withstand, adapt to, and recover from cyberthreats and incidents. SPM represents an organization’s overall security strength and resilience. It encompasses the collective status of security mechanisms, policies, and procedures.

SPM enables cyber resilience by:

- **Reducing vulnerabilities:** A strong security posture minimizes vulnerabilities, making it harder for attackers to exploit gaps.
- **Effective incident response:** SPM ensures efficient incident handling and system restoration.
- **Quick recovery:** When breaches occur, a robust posture helps restore affected systems promptly.
- **Business reputation and trust:** Maintaining a strong posture builds trust with customers and partners. It also helps organizations comply with regulatory requirements and maintain data privacy.

In summary, SPM plays a pivotal role in enhancing cyber resilience by fortifying defenses, minimizing impact, and ensuring business continuity even in the face of evolving threats.

Learn more about SPM solutions:

Data Privacy and Protection
Visit the website ›

Application Security
Visit the website ›

IGA Buyer’s Guide
Read the guide ›