Seceon SSPM Capabilities

AI/ML-Powered SaaS Security Posture Management

SSPM in 2024

The rapid shift to SaaS applications for an increasing number of use cases and workflows across organizations is putting pressure on security, governance and risk professionals to modernize their operations for the SaaS-powered world. And with 78% of organizations storing sensitive data in SaaS applications including PII, financials, customer details etc., and the average mid-size organization's employees using over 375 SaaS applications, many security and risk personnel are applying custom controls and policies on an application by application level.

Driving this rapid change a single focus on on-premises infrastructure and application security to SaaS security is research from the Cloud Security Alliance (CSA) found that SaaS misconfigurations caused 63% of security incidents.

Challenges Security, Risk, and Compliance Teams Face

Security teams need unified visibility into users, privileges, activity, configuration status across SaaS applications to defend against risks and threats. They must be able to correlate SaaS security events and alerts with security telemetry from across their infrastructure, networks, and users.

- Threat actors are increasingly focused on targeting SaaS applications which are often in-use across an organization and not always under the central control or provide visibility to IT and Security Operations teams.
- Administrators of SaaS applications in an organization are not always aware of or focusing on maintaining best practice configuration and management practices for SaaS applications.
- Governance and Risk teams need visibility and assurance that controls and policies are being followed and when they are not, they need to be alerted, logged and when possible remediated.

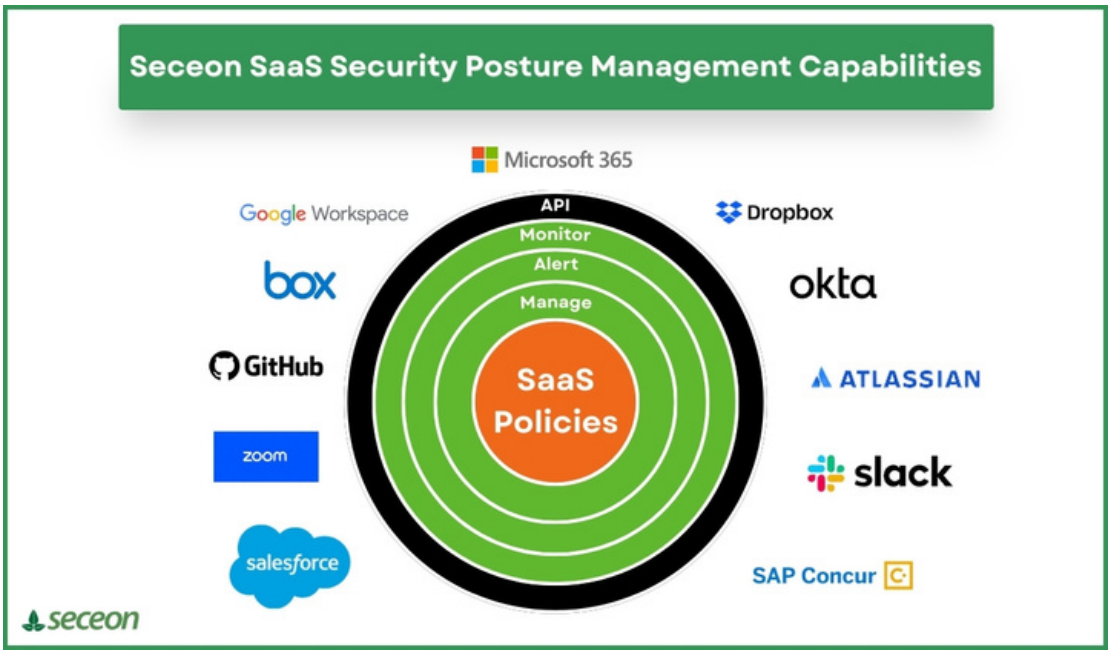
How Seceon Supports SSPM

Seceon's aiSIEM and aiSIEM-CGuard and it's AI/ML-powered ability to enrich, detect and respond to threats in real-time spans cloud, on-premises, networks, endpoints and popular SaaS applications. The platform's ability to correlate indicators of compromise, indicators of behaviors with identities and policy violations.

- Seceon has developed the capability to provide customers seamless access to Seceon's enriched, normalized SaaS security visibility for some of today's most popular and widely adopted SaaS applications. Security teams can be more efficient, reduce the financial overhead needed to sort and clean logs, but also gain a holistic understanding of the actors, activities and relationships in their cloud environments.

- When Seceon's SSPM capabilities are combined with polices on supported SaaS applications like Microsoft 365 (Email, OneDrive, SharePoint etc.), Dropbox, Okta, GitHub, Zoom, Salesforce, SAP Concur, etc. individual SaaS organizations benefit from the safest way to integrate security with their department or business goals, paving the path for sustained productivity and innovation.

- Seceon customers can store and access historical visibility of data and alerts for policy violations enabling automated or security analyst driven incident response, threat hunting, and audits.



Seceon SSPM Overview

Seceon SSPM Key Benefits

Automate SaaS Security Policy Monitoring and Management

- Rapidly implement your policies for supported SaaS applications. Seceon's powerful platform enables security and GRC teams to apply posture monitoring across access, privileges, configuration options and more. (Varies by application). Seceon's aiSIEM and aiSIEM-CGuard are continuously monitoring for data control, data security, and data exfiltration. Alerting and stopping data theft or sharing PII or PHI.
- Seceon customers can store and access historical visibility of data and alerts for policy violations enabling automated or security analyst-driven incident response, threat hunting, and audits. Seceon also provides analysts with detailed threat analysis with the MITRE ATT&CK framework.

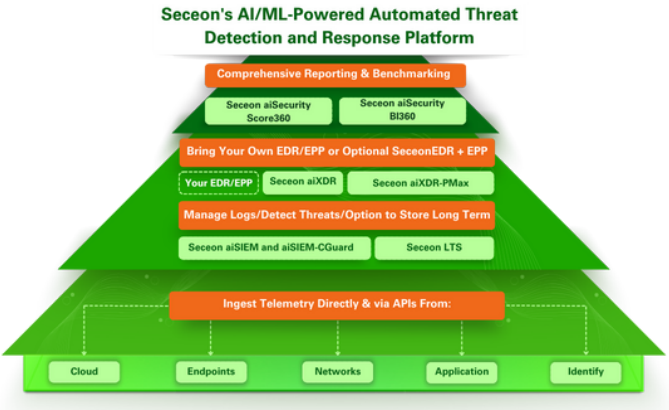
Automate Remediation for Policy Violations

- Seceon's real-time policy monitoring can detect violations and alert security analysts or incident responders and/or automatically respond by blocking, stopping, quarantine or remediate the configuration or violation that was against the posture's policy.

Faster Audit Reporting

- Seceon enables standard posture monitoring reports and with Seceon aiSecurity BI360, custom reports and dashboards. Seceon's platform features support for many existing security frameworks and their controls and audit support reports, including NIST, GDPR, CMMC, HIPAA, PCI, and many other regional and industry frameworks.

About Seceon



About Seceon

Seceon enables MSPs, MSSPs, and IT teams to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. Seceon augments and automates MSP and MSSP security services with an AI and ML-powered aiSIEM and aiXDR platform. It delivers gapless coverage by collecting telemetry from logs, identity management, networks, endpoints, clouds, and applications. It's all enriched and analyzed in real-time with threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 430 partners are reselling and/or running high-margin, efficient security services with automated cyber threat remediation and continuous compliance for over 7,800 clients.

Learn more about Seceon SSPM Capabilities

Schedule a Demo www.seceon.com/contact/