SaaS Security

The Industry's Leading SASE-Native SaaS Security Solution

Almost every organization today uses technology, adopting SaaS applications at a record pace and moving vast amounts of data and operations to the cloud. This distributed digital ecosystem extends to apps and data as well as to the users who access it. They come from headquarters, remote locations, and homes as well as through a range of devices, introducing a level of digital complexity that invites new threats and data loss vectors.

Palo Alto Networks SaaS Security tackles the rapid growth of SaaS and generative AI (GenAI) apps, protects data across all SaaS control points, and enables businesses to operate securely without compromise.

Main Business Benefits

- Automatically see and secure new SaaS applications, including GenAI and modern collaboration apps.
- Cover every network and web transmission for all users everywhere, across branch offices and remote users, for consistent enforcement and user experience.
- Proactively discover and prevent sensitive data leakage to SaaS and GenAI apps to preserve data integrity and compliance.
- Stop known, unknown, and zero-day threats, including malicious insiders, in real time and with Zero Trust.
- Streamline operations with a fully integrated solution instead of having multiple point products that increase complexity and cost.

Risks with Conventional Approaches

When security teams secure their cloud-based SaaS applications and data, they typically turn to cloud access security brokers (CASBs). However, current CASB solutions struggle to keep up with modern security and business needs.

Lack of Visibility and Automation Across SaaS

Traditional CASBs face significant limitations when discovering new SaaS and GenAI apps due to their outdated design and reliance on static methods. They depend on manual signature updates and static application libraries—often derived from a limited user base, leaving many shadow SaaS apps undetected. What's more, the process to audit and verify hundreds or thousands of SaaS configuration settings within sanctioned apps can be manual, running the risk of misconfigurations that lead to security vulnerabilities.

Compliance and Security Risks from Inaccurate Data Classification

The rise in SaaS-originated data—such as from collaboration workspaces, email, and chat, coupled with hard-to-detect data embedded within screenshots and images—heightens the risk of data loss or theft. With current data detection challenges, threat actors have shifted from traditional vectors to target SaaS apps such as Google Workspace, Slack, and Microsoft Teams. These platforms facilitate rapid data sharing, making it hard for legacy CASB solutions to accurately stop incidents without disrupting legitimate business workflows.

Friction and Poor User Experience from Operational Complexity

Legacy CASBs are also constrained by their deployment models, such as proxies, which only monitor traffic routed through specific infrastructures. This approach fails to capture SaaS usage from unmanaged devices or outside corporate networks, which is a common scenario in modern work environments. They also lack integration with broader security architectures, leading to disjointed policy enforcement and management.

An Intelligent and Proactive Approach

IT security teams face the growing challenge of securing an increasing number of SaaS and GenAI applications, safeguarding sensitive data, and ensuring consistent compliance across multicloud environments. To address these demands, they require comprehensive SaaS security solutions that include the following capabilities:

- **Comprehensive visibility and control over all SaaS consumption:** Automatically detect all SaaS applications in use across the enterprise, including corporate, unsanctioned, and GenAI apps. They should extend to marketplaces, providing insights into risks posed by marketplace extensions, plugins, and interconnected apps.
- **Accurate and real-time sensitive data detection:** Accurately discover, classify, and monitor sensitive data across all SaaS control points, ensuring compliance and minimizing risks. It should use AI/ML to reduce false positives, enforce granular security policies, and prevent unauthorized access or sharing of data in real time.
- **Zero Trust defense against insider threats and advanced attacks:** Proactive threat detection, antimalware, behavior analytics, and Zero Trust access controls defend against malicious insiders and sophisticated threat actors. They must safeguard against advanced threats that target SaaS collaboration tools and be able to uncover threats in GenAI responses.

Palo Alto Networks SaaS Security Solution

Palo Alto Networks SaaS Security is a SASE-native solution that delivers broad visibility and real-time control over all SaaS applications, including GenAI apps. Moreover, it provides robust data protection by monitoring and securing the unapproved movement and storage of sensitive data across various SaaS platforms.

Palo Alto Networks SaaS Security—offered as a solution bundle—is a consolidated offering that includes the core products listed in table 1.

Table 1: Products and Use Cases

Product	Use Case
SaaS Security	Gain visibility into all SaaS applications in use, including shadow IT and various tenants. Visibility and control extend to interconnected apps and plugins sourced from SaaS platforms and their associated marketplaces, providing a holistic view of the SaaS ecosystem. It prevents SaaS misconfigurations with posture security and management, mitigating the risk of security vulnerabilities.
AI Access Security™	Gain a clear view of GenAI usage across the enterprise, identifying which apps are in use, by whom, and for what purpose—ensuring there are no blind spots. Leverage bespoke risk scores to make data-driven decisions about GenAI apps and apply granular controls, while protecting sensitive data from being leaked into GenAI apps and their training models. Confidently manage GenAI adoption while maintaining stringent data security standards.
Enterprise DLP	Discover, monitor, and protect sensitive data across every network, cloud, and user. Advanced detections augmented by AI and ML revolutionize data classification to reduce false positives by more than 90% for near-perfect accuracy. Organizations can simplify operations with unified policies enforced consistently across multiple layers in the security stack.

Key Components and Capabilities

Table 2 lists the core components and capabilities of the Palo Alto Networks SaaS Security bundled offering.

Table 2: Features and Capabilities

Capability	Description
SaaS Inline	Provides granular SaaS application visibility and control of unsanctioned apps and tenants through advanced analytics, reporting, visualization, categorization, and security policy authoring to minimize security risks. Discover and control SaaS consumption with visibility into over 73K SaaS apps, automatically identified via ML and crowdsourced from a firewall community of over 70K customers.
AI Access	Enables the safe use of GenAI by providing real-time visibility into GenAI apps, user access controls, data protection, and continuous risk monitoring. With an industry-leading catalog of over 1.8K GenAI apps and insights from 70+ app attributes, it proactively prevents sensitive data loss and enables safe GenAI adoption. It includes posture management for 12+ GenAI apps, inline DLP controls for 90+ apps, and SaaS inline tenancy control for 12 GenAI apps.
Network DLP	Network DLP automatically discovers, monitors, and protects sensitive data in motion across branch offices and remote users. With a focus on preventing exposure of sensitive data within SaaS apps, it leverages over 100+ inline DLP integrations to monitor data flows and user activities.
SaaS API	SaaS API addresses sensitive data stored in corporate SaaS applications or data that might be incorrectly shared with SaaS apps. APIs enable the scanning of data within SaaS apps, as well as control access permissions and monitor activities, such as changes in user permissions.

Table 2: Features and Capabilities (continued)	
Capability	**Description**
SaaS Security Posture Management (SSPM)	SSPM mitigates risk to corporate SaaS apps and the data within them by finding and fixing misconfigurations—including extensions and plugins, preventing configuration drift, and ensuring secure posture for all sanctioned apps. SSPM is available for over 95 SaaS applications.
Behavior Threats	The cloud-based user entity and behavior analytics (UEBA) feature proactively identifies anomalous behaviors and simplifies monitoring with dynamic user risk scores, predefined situational policies, detailed incident reports, user watchlists, and more.
Email DLP*	AI-powered Email DLP analyzes email communications in real time, scanning for sensitive information and preventing unauthorized data transfers to swiftly block or encrypt emails inline.
AI-Powered Data Classification	Data classification techniques include regular expressions, dictionaries, data validation, Indexed Document Matching, Exact Data Matching—scalable to billions of records, natural language processing, and optical character recognition for images. Context-aware ML models combined with LLM-based natural language are augmented across 300+ data classifiers to interpret semantics and reduce false positives. Over 100+ pretrained ML models and customer-trainable ML models further enhance detection accuracy.
End-User Coaching	Coach end users when they access unapproved apps or if sensitive data is detected. Enhanced with XSOAR integration, notifications can ensure swift response to potential incidents via Slack, Microsoft Teams, and email services (e.g., Gmail, Microsoft, etc.). Administrators can also implement trigger exemptions and business justification workflows to improve the end-user experience.

* Available via an add-on SKU. It will be included in the bundle by mid-2025.

Building on Zero Trust with SaaS Security

When implementing an effective Zero Trust security strategy for cloud-enabled enterprises, factor in a least-privileged access strategy for SaaS applications and their sensitive data. Palo Alto Networks SaaS Security is a fundamental part of the Palo Alto Networks Zero Trust architecture. It enables organizations to consistently secure access to SaaS applications, GenAI apps, and enterprise data across highly distributed environments.

Palo Alto Networks SaaS Security is delivered on the Strata™ platform via Prisma® Access and Next-Generation Firewalls (cloud-based, software, and hardware form factors). Simple and flexible deployment models help organizations enable the safe adoption of SaaS and AI in today's digital-first world.

Privacy and Licensing

Table 3: Privacy and Licensing	
Trust and Privacy	**Licensing and Support Requirements**
Palo Alto Networks has strict privacy and security controls in place to prevent unauthorized access to sensitive or personally identifiable information. We apply industry-standard best practices for security and confidentiality. Find further information in our privacy datasheets.	• The CASB-X or CASB-PA bundles include SaaS Inline Security, SaaS API Security, DLP Inline, Data Security (formerly SaaS API and DLP for SaaS API), SSPM, and AI Access Security, which can also be licensed individually. • NGFW (hardware or virtual) and/or Prisma Access • Strata Logging Service

Global Customer Services

Global Customer Services delivers the guidance, expertise, and resources necessary to maximize the value of your investment. Professional Services, Customer Success, support, ongoing education, and adoption tools ensure protection from intruders at every stage of your cybersecurity journey. Contact your Palo Alto Networks account manager to obtain the services that fit your needs.

Deploying a consistent and integrated SaaS Security solution—as part of an SSE or SASE architecture—won't only stop sophisticated cyberattacks, but it will streamline operations and improve user experience. Securely connect your employees to the internet and all business-critical SaaS apps, including GenAI apps, with the highest level of security without compromise.

To learn more about Palo Alto Networks SaaS Security, visit our webpage or contact your Palo Alto Networks representative.

3000 Tannery Way
Santa Clara, CA 95054

Main:	**+1.408.753.4000**
Sales:	**+1.866.320.4788**
Support:	**+1.866.898.9087**

www.paloaltonetworks.com