Prisma SaaS: At a Glance

SaaS Security Challenges

The concept of an organization’s data residing only in a single, centralized location does not typically apply today. Data is distributed across multiple locations, many not under the organization’s control. Wherever the data is located, IT organizations are still responsible for securing it as it moves. This issue is most visible when it comes to software-as-a-service (SaaS) applications, the use of which is difficult to control, and visibility into which is difficult to maintain, with traditional security. Since SaaS applications are set up and used by end users directly, permission is not needed to access them or move sensitive corporate data to them. This presents a significant challenge with end users who act as their own IT departments, controlling their use of these applications without expertise in data or threat risk assessment and prevention.

Safely Enable SaaS Applications with Prisma SaaS

By offering advanced data protection and consistency across applications, Prisma™ SaaS reins in the risks. It addresses your cloud access security broker (CASB) needs and provide advanced capabilities in risk discovery, data loss prevention, compliance assurance, data governance, user behavior monitoring, and advanced threat prevention. Now, you can stay compliant while preventing data leaks and business disruption through a multi-mode CASB deployment.

Deep cloud risk visibility: Easy-to-navigate SaaS usage dashboards and detailed reporting help rein in shadow IT. Discover risks at a deeper level with complete visibility into all user, folder, and file activity across SaaS applications, generating detailed analysis that helps you quickly determine the presence of any data risk- or compliance-related policy violations.

Data protection and leakage prevention: Define granular, context-aware policy control to drive enforcement as well as quarantine users and data as soon as violations occur. Prisma SaaS can secure your applications by classifying data and monitoring usage through machine learning and an advanced data loss prevention (DLP) engine.

Granular and adaptive access control: Simple-to-manage policies give you granular control over access to SaaS applications to define which are allowed and acceptable behavior within them. This lets you block access for unsanctioned applications while maintaining control of tolerated applications.

Data governance and compliance assurance: You can quickly and easily satisfy data risk compliance requirements, such as those related to GDPR, PCI, PII, or PHI data, while maintaining the benefits of cloud-based applications.

User behavior monitoring: Heuristic-based user behavior monitoring and alerting enables you to easily identify suspicious behavior, such as logins from unexpected regions, unusually large usage activity, or multiple failed logins, that may indicate credential theft.

Advanced threat prevention: Block known malware, plus identify and block unknown malware within SaaS applications.

Cloud-Delivered, Multi-Mode CASB

Prisma SaaS functions as a multi-mode CASB, offering in-line and API-based protection working together to minimize the range of cloud risks that can lead to breaches. With a fully cloud-delivered approach to CASB, you can secure your SaaS applications using:

- **In-line protections** to secure in-line traffic with deep application visibility, segmentation, secure access, and threat prevention. This approach combines user, content, and application inspection features within the security service to enable CASB functions. The inspection technology maps users to applications to deliver granular control over cloud application usage regardless of location or device. Other features include application-specific function control, URL and content filtering, application-risk based policies, user-based policies, DLP, and prevention of known and unknown malware. Forward and reverse proxy support ensures these comprehensive capabilities secure users wherever they and whatever device they use.
- **API-based protections** to connect directly to SaaS applications for data classification, DLP, and threat detection. Prisma SaaS leverages an out-of-band, API-based approach that enables granular inspection of all data at rest in the cloud application as well as ongoing monitoring of user activity and administrative configurations. This deployment mode preserves the user experience for the cloud application because it's non-intrusive and neither interferes with nor depends upon the data path to the cloud application.

To learn more, visit www.paloaltonetworks.com/prisma.

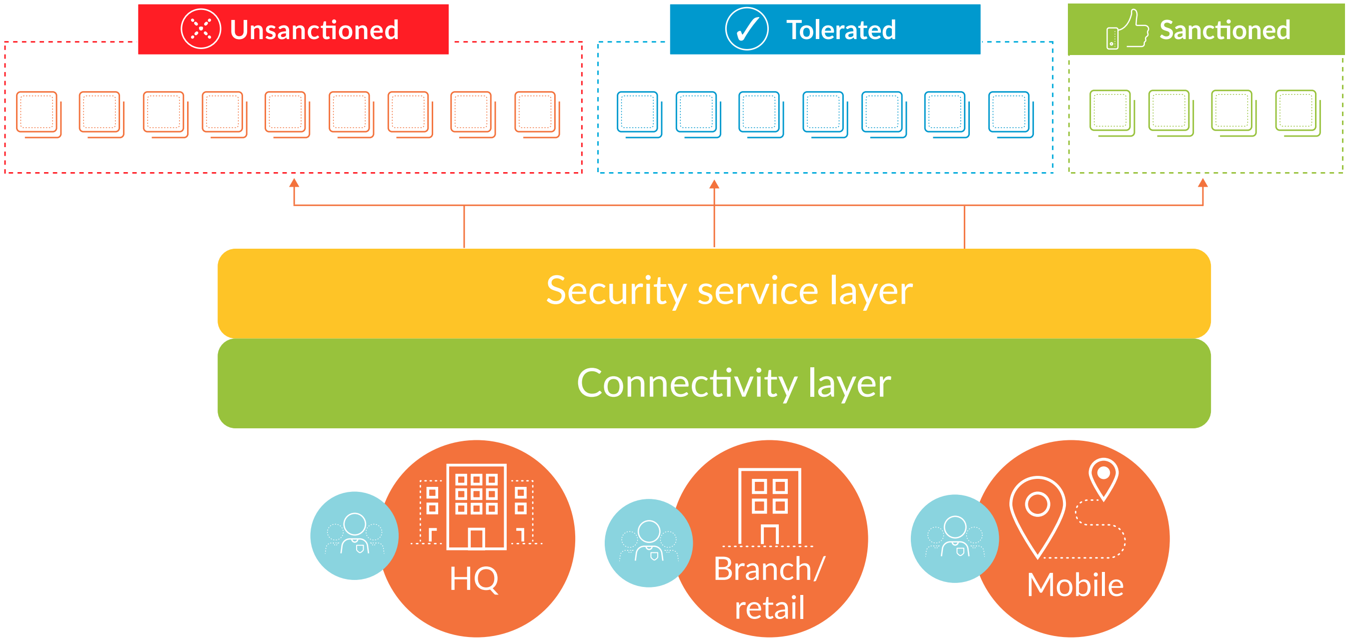

Figure 1: Prisma SaaS model