Palo Alto Networks SaaS Security Posture Management (SSPM)

Protect Sensitive Data from SaaS App Misconfigurations

The transition from the data center to the cloud has left critical business data at risk in constantly changing, complex SaaS apps. Gartner predicted that more than 99% of cloud breaches will be attributed to preventable misconfigurations or mistakes by end users through 2025.[1] With SaaS misconfigurations becoming a leading cause of enterprise data breaches, inefficient manual audits leave SaaS apps misconfigured and data at risk.

The Challenge of Securing Data in SaaS Apps

- Today's typical enterprise uses over 100 sanctioned SaaS apps for core business functions, and app management often sits within departments without an IT or security background.
- The optimal configuration of these constantly changing apps is unclear, with dozens, if not hundreds, of settings for each app.
- InfoSec teams have limited to no visibility into how these apps are configured, and there is a general lack of security management control of the app settings.
- Securing thousands of settings across over a hundred sanctioned SaaS apps is not an easy task. When a SaaS app is compromised due to a vulnerability created by a misconfiguration, its overall security posture is adversely affected, putting the apps' data at risk of a breach.
- Lack of continuous auditing leaves InfoSec teams unaware of SaaS app misconfigurations, putting sensitive data at risk.
- Labor-intensive manual audits are typical and only provide a point-in-time assessment. Performed on a quarterly or annual basis, these audits leave the SaaS app vulnerable to bad actors.

Key Benefits

Reduce app audit time from one week to just 15 minutes: Our SSPM offers system-led, automated remediation to easily fix misconfigurations and avoid time-consuming manual changes.

The most comprehensive app support in the industry: We cover key enterprise and collaboration SaaS apps such as ServiceNow, Microsoft 365, Salesforce, Slack, Dropbox, Okta, Zoom, and over 80 more, or 10 times our competitors, to bring you the most comprehensive SaaS security solution.

Security, not just a compliance check box: Continuous monitoring of security-impacting configurations allows security teams to remediate risks as they arise with a single click and locks security-critical settings into place with Drift Prevention.

Go Beyond Compliance to Secure All Your Critical SaaS Apps, Not Just a Handful

Palo Alto Networks SSPM is focused on delivering true security, not just compliance. To secure SaaS apps today, you need visibility into configurations. We perform continuous, comprehensive monitoring of all security-impacting configurations in SaaS apps and align them to security-oriented best practice recommendations. We enable you to:

- **Reduce the time** it takes to audit an app from a week to just 15 minutes.
- **Quickly adopt best practices** for SaaS configurations.
- **Quickly identify and fix security risks** in a single click with continuous SaaS app monitoring and an intuitive interface.
- **Lock your security-critical settings in place** and avoid regressions often caused by various app administrators with Drift Prevention.
- **Ensure posture security for all your critical SaaS apps**, not just a handful. Your sensitive data and user information span dozens of apps. That's why we offer comprehensive, industry-leading support, over 10 times more than traditional CASB-native SSPM offerings.

From enterprise SaaS apps, collaboration, sales tracking, and development to HR, we've got you covered. Contact Palo Alto Networks to learn more today.

[1] Jay Heiser and Charlie Winckless, *Risk-Based Evaluations of Cloud Provider Security*, Gartner, updated January 16, 2023.

> “Being able to identify, triage, and act on gaps and prevent drift from policy across our critical SaaS applications is a game changer!”
>
> – InfoSec Practitioner, Large Enterprise

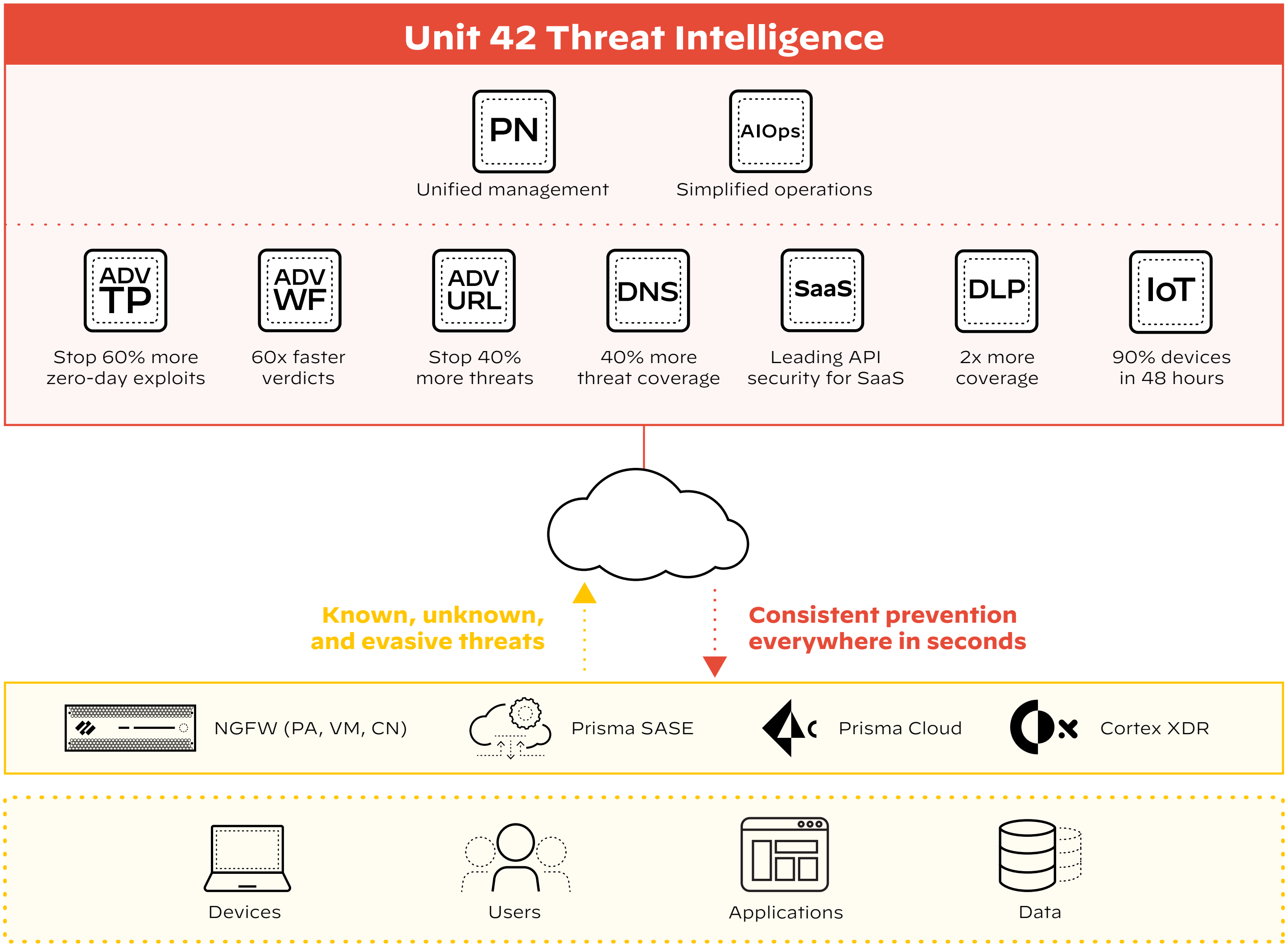

Figure 1: Palo Alto Networks Cloud Delivered Security Services (CDSS)

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