# AT A GLANCE
# APERTURE FOR SAAS APPLICATIONS

The appeal of SaaS applications, such as Office 365®, G Suite, Box, and Salesforce®, is growing; but so are the hidden threats in SaaS offerings: costly data leaks, regulatory noncompliance, malware propagation, and so on. Aperture™ SaaS security service complements your existing security tools and delivers data classification, data leakage prevention, and threat detection—so you can secure your SaaS applications.

### SaaS Security Challenges

The concept of data residing only in a single, centralized location does not typically apply to today's modern organizations. Data is now distributed across multiple locations, including many that are not under the companies' control. Regardless of the location of the data, IT organizations are still responsible for securing it as it moves. This is the most visible when it comes to SaaS applications. These applications are very hard to control the use of, or have visibility into, with a traditional security implementation. Since they 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 and have control over the applications they use and how they use them, but without the expertise on data or threat risk assessment and prevention.

To gain control of SaaS usage, you need to start by clearly defining the SaaS applications that should be used and which behaviors are allowed within those applications. This requires defining which applications are allowed—or "sanctioned"—and which are not, and then putting solutions measures in place to control their access and usage.

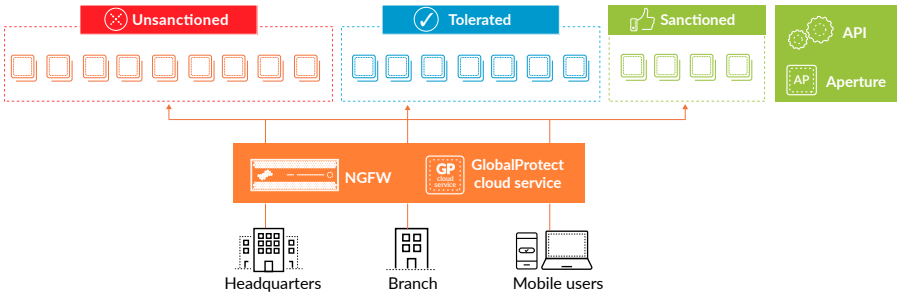
### Safely Enable SaaS Applications with Aperture

Data residing in enterprise-enabled SaaS applications is not visible to an organization's network perimeter. Aperture has the ability to connect directly to sanctioned SaaS applications to provide data classification, sharing/permission visibility, and threat detection within the application. This yields unparalleled visibility, allowing organizations to inspect content for data risk violations and control access to shared data via contextual policy. Safely enabling SaaS applications via Aperture provides full end-to-end security without any additional software, hardware, or network changes required.

Aperture builds upon the existing SaaS visibility and granular control capabilities of App-ID™ technology within our Security Operating Platform with detailed SaaS-based reporting and granular control of SaaS access.

### Aperture Highlights

- **Risk discovery and deep visibility**—complete visibility and analytics across all user, folder, and file activity within SaaS applications to quickly determine if there are any policy violations related to data risk or compliance.
- **Data leak prevention and compliance enablement**—define granular, context-aware DLP policy to drive enforcement as well as quarantine users and data as soon as violations occur.
- **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, indicating credential theft.
- **Deployment simplicity**—fully cloud-delivered, enable comprehensive SaaS protections without the need for any proxies or agents while preserving the end-user experience.
- **Advanced threat prevention**—block known malware, plus identify and block unknown malware within SaaS applications.




Cloud-delivered CASB approach

# AT A GLANCE
# APERTURE FOR SAAS APPLICATIONS

| YOU NEED | WE OFFER |
|---|---|
| Risk discovery and deep visibility | Aperture provides complete visibility across all user, folder, and file activity, generating detailed analysis that helps you transition from a position of speculation to one of full awareness at any given point in time. Deep analytics into day-to-day usage allow you to quickly determine if there are any policy violations related to data risk or compliance. This provides detailed analysis of user and data activity to enable detailed data governance and forensics. |
| Data leak prevention and compliance enablement | Aperture enables you to define granular, context-aware policy control to drive enforcement as well as quarantine users and data as soon as violations occur. This enables you to quickly and easily satisfy data risk compliance requirements, such as those related to PCI and PII data, while still maintaining the benefits of cloud-based applications. |
| User behavior monitoring | Aperture natively provides heuristic-based user behavior monitoring and alerting. You can easily identify suspicious behavior, such as logins from unexpected regions, unusually large usage activity, or multiple failed logins, indicating credential theft. Further, Magnifier behavioral analytics, a cloud-based app for the Palo Alto Networks Application Framework, extends these protections with machine learning by identifying targeted attacks, malicious insiders, and compromised endpoints. |
| Deployment simplicity | Aperture is a cloud-delivered service, without the need for any proxies or agents. Because Aperture communicates directly with SaaS applications, it will look at data from any source, regardless of the device or location from which the data originates. Because Aperture isn't in-line, it doesn't impact latency or bandwidth of applications, and it doesn't affect the end-user experience. |
| Advanced threat prevention | WildFire® malware prevention service, integrated with Aperture, provides advanced threat prevention to block known malware, plus identify and block unknown malware. This integration with WildFire stops threats from spreading through the sanctioned SaaS applications, preventing a new insertion point for malware. New malware discovered by Aperture is shared with the rest of the Security Operating Platform even if it is not in-line with the SaaS applications. |

**CASB Capabilities, Cloud-Delivered**

The Palo Alto Networks Security Operating Platform offers in-line and API-based protection technologies that work together to minimize the wide range of cloud risks that can cause breaches. With a fully cloud-delivered approach to CASB, you can secure your SaaS applications using:

- An in-line approach with Palo Alto Networks GlobalProtect™ cloud service 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, policies based on application risk, DLP, user-based policies, and prevention of known and unknown malware. These comprehensive capabilities span across your on-premises and mobile workforce to prevent the exfiltration of sensitive data across all applications.
- An API approach with Aperture SaaS security service to connect directly to SaaS applications for data classification, DLP, and threat detection. Aperture 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 nonintrusive and does not interfere with or depend on the data path to the cloud application.

To learn more, go to **https://www.paloaltonetworks.com/products/secure-the-cloud/aperture-for-saas**.