AT A GLANCE
APERTURE

The use of software-as-a-service applications is creating new risks and gaps in security visibility for malware propagation, data leakage and regulatory non-compliance. Aperture™ SaaS security service delivers complete visibility and granular enforcement across all user, folder and file activity within sanctioned SaaS applications, providing detailed analysis and analytics on usage without requiring any additional hardware, software or network changes.

SaaS Security Challenges

The concept of data residing only in a single, centralized location does not typically apply to today's modern networks. Networks have become inverted with data that's spread throughout 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 department 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. Even skilled users with security experience can run into problems with SaaS applications if they don't have the right tools that provide visibility into data exposure and threat insertions that SaaS can introduce.

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

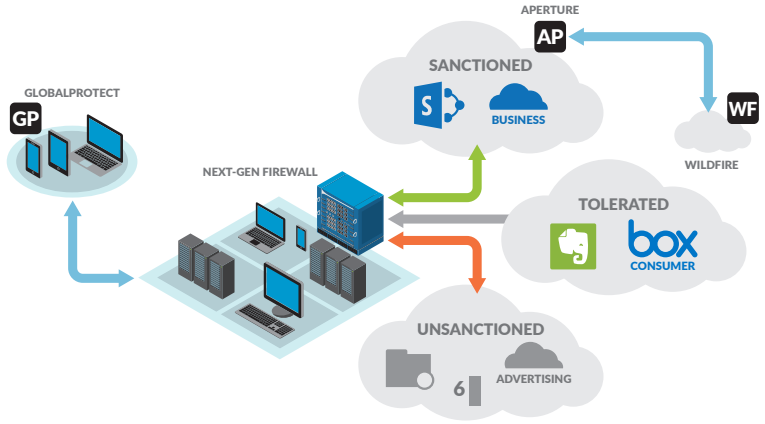
Safely Enable SaaS Applications With Aperture

Data resident within 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 a contextual policy.

Aperture builds upon the existing SaaS visibility and granular control capabilities of App-ID™ application identification technology within our Next-Generation Security Platform with detailed SaaS-based reporting and granular control of SaaS access. Adding visibility and control within the SaaS applications via Aperture provides a full end-to-end security solution without any additional software, hardware or network changes required.

Aperture Highlights

- Complete visibility across all user, folder and file activity, providing detailed analysis that helps you transition from a position of speculation to one of knowing exactly what's happening at any given point in time
- Retroactive analysis of data exposure that doesn't just look at data in-line but also from the creation of the SaaS account itself, no matter how long ago that was
- Deep analytics into day-to-day usage that allow you to quickly determine if there are any data risks or compliance-related policy violations
- Granular, context-aware policy control that provides you with the ability to drive enforcement and quarantine users and data as soon as a violation occurs
- Advanced threat protection to block known malware and identify and block unknown malware



Impacts of sanctioned and unsanctioned SaaS applications

AT A GLANCE
APERTURE

YOU NEED	WE OFFER
SaaS threat prevention	WildFire™ cloud-based threat analysis service integrated with Aperture provides advanced threat prevention to block known malware and identify and block unknown malware. This integration with WildFire prevents 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 Next-Generation Security Platform, even if it is not in-line with the SaaS applications.
Data exposure visibility	Aperture provides complete visibility across all user, folder and file activity, providing detailed analysis that helps you transition from a position of speculation to one of knowing exactly what's happening at any given point in time. This gives you the ability to view deep analytics into day-to-day usage, which allows you to quickly determine if there are any data risk or compliance-related policy violations. This provides detailed analysis of user and data activity to enable detailed data governance and forensics.
Contextual data exposure control	Aperture enables you to define granular, context-aware policy control that provides you with the ability to drive enforcement and the quarantine of users and data as soon as a violation occurs. This enables you to quickly and easily satisfy data risk compliance requirements, such as PCI and PII, while still maintaining the benefits of cloud-based applications.
Completely automated SaaS security	Aperture is a completely cloud-based solution without the need for any proxies or agents. Because Aperture communicates directly with the SaaS applications, it will look at data from any source, regardless of the device or location from where the data came. Because Aperture isn't in-line, it doesn't impact latency or the bandwidth of applications and has no impact on the end-user experience. It just works.

Next-Generation Security Platform

Aperture adds another dimension of security to the Palo Alto Networks Next-Generation Security Platform, providing key insight into data and threat exposure within sanctioned SaaS applications. When Aperture is included, the capabilities increase substantially to provide an all-encompassing SaaS solution with true visibility into all applications, including sanctioned and unsanctioned SaaS applications, with granular control of access and usage. With Aperture, you can:

1. Gain full visibility into all applications.
2. Have granular control of applications.
3. Extend security to all users all of the time.
4. Prevent threats everywhere.

The Next-Generation Security Platform provides data protection, regardless of location. Whether data resides on-premise, has been virtualized and needs protection in a private cloud (NSX®, ACI™, KVM, OpenStack®), is extended to a public cloud (IaaS/PaaS) such as AWS®, or has been moved to a SaaS application, we can protect it.

To learn more, go to **http://www.paloaltonetworks.com/products/aperture.html.**