SAFELY ENABLE YOUR SAAS APPLICATIONS

The appeal of software-as-a-service applications is growing, but so are the hidden threats in SaaS offerings: costly data leaks, regulatory noncompliance, malware propagation, and so on. Palo Alto Networks 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.

The New Reality of Cloud Adoption

The concept of data residing only in a single, centralized location does not typically apply to modern organizations. Data is now distributed across multiple locations, including many outside a given organization's control. Wherever the data is located, IT organizations are still responsible for securing it as it moves. When it comes to SaaS applications, which are difficult to control and maintain visibility into with traditional security, this is especially demanding. Since end users directly set up and use SaaS applications, they don't need permission 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 use of these applications without necessarily having expertise in data or threat risk assessment and prevention.

Organizations need to embrace the new reality and plan to address the new risks introduced with adoption of cloud applications:

- **Globally distributed workforce:** Most large organizations have employees around the globe looking to access tools and data in the cloud. These users employ multiple devices and access applications from various locations while collaborating with other internal or external users.

  Security implication: Consistent security is required for any device, anytime, anywhere.

- **Apps procured directly by end users:** Traditionally, IT departments have been responsible for procuring applications employees need. With the exponential growth of SaaS applications, the consumption model of these applications has shifted, and many can be purchased as subscriptions with a credit card. Today, lines of businesses within organizations typically purchase productivity and collaboration tools as needed, without following IT procurement processes. These off-the-shelf applications, if not vetted, can introduce blind spots for various security teams.

  Security implication: Organizations need visibility into "shadow IT" and the ability to manage risk.

- **User-controlled information sharing:** The biggest challenge of handing end users the power of data sharing is the huge risk of sensitive data exposure. This can be as simple as an employee sharing with someone else who also has share privileges, snowballing to a public share. A mistyped name can lead to sharing with the wrong person or group, even external. "Ghost shares" can happen when information is shared with ex-employees or former vendors whose accounts have not been deactivated. Less common but still a threat, malicious internal users may purposely share data by setting folders to be shared publicly or with an external email address.

  Security implication: Advanced data loss prevention (DLP) is required for data stored in the cloud while enabling cloud-based collaboration.

Requirements for Safely Adopting SaaS Apps

Taking advantage of SaaS applications while keeping your organization secure necessitates careful consideration of several requirements:

- **Application discovery:** Most organizations do not realize the extent of shadow IT risk in their user bases. The typical way to solve this is to manually export logging data from a firewall or web proxy to a visibility tool or security information and event management (SIEM) provider. This needs to be done periodically to keep track of new apps or usage patterns, requiring significant administrator time. The right approach is automated and real-time, without any management overhead.
- **Data protection:** With the adoption of cloud applications and sensitive data stored outside the traditional perimeter, organizations need to rethink their data protection strategies. SaaS vendors, such as Microsoft and Box, Inc., provide basic security features within their applications, but these features are typically not enterprise-grade and can get cumbersome to manage as they force you to manage policies separately for each application. With most large organizations today adopting twenty to thirty sanctioned applications, management overhead can get quickly become complex. Ensuring a consistent security feature set across all applications requires third-party security.
- **Comprehensive security:** Traditional in-line DLP tools or web proxies deliver some security capabilities, but they have limited context for cloud apps. For instance, when a user uploads a file to SharePoint®, proxies will tell you that data was uploaded to SharePoint, but they cannot tell you if it was uploaded to a publicly exposed folder or if the access rules constitute a compliance violation. These kinds of questions can only be answered if you deploy an in-line, API-based approach to SaaS security.
- **Maintaining user experience:** Cloud application vendors invest heavily in optimizing the user experience, seamless user onboarding processes, and quick application response. As organizations adopt new security tools, it is important to ensure that they do not affect the user experience by forcing additional steps or introducing significant latencies in the use of applications.
- **Protecting users:** With the ease of collaboration and the power of sharing in the hands of the users, sensitive data can get exposed due to improper access permissions. Managing access rights to data in the cloud is complex, and security tools are required to monitor and govern sharing permissions to avoid costly data leaks.

Turning to a Cloud Access Security Broker

It would be extremely challenging for most organizations to meet all the aforementioned requirements with their existing security tools—particularly those tools already deployed to secure on-premises environments. Instead, more and more companies are deploying cloud access security brokers (CASBs), which deliver broader visibility and better control over the usage of cloud applications as well as compliance and protection for cloud-based data. Unlike other security tools your organization may use, CASBs offer cloud-specific capabilities that address security gaps in your organization's use of cloud services.

CASBs can be deployed in two different modes, depending on your organization's requirements:

- **In-line approach:** With an in-line approach, a CASB can use either forward or reverse proxy. With forward proxy, the CASB forwards cloud traffic to an appliance or service that can provide application visibility and control capabilities. Forward proxy capabilities are not limited to traditional proxies, such as secure web gateways. Powerful application control can be enforced using a cloud-based security service or next-generation firewall. Organizations that already have an NGFW deployed as an internet gateway for on-premises or cloud-based security services for remote users can avoid the additional management overhead and complexity of using the traditional proxies most CASB vendors offer. For a reverse proxy, a CASB can use single sign-on, or sometimes DNS, to reroute users to an in-line CASB service to enforce policies.
- **API-based approach:** Quickly becoming the preferred method of implementing a CASB, the API-based approach provides visibility into an organization's data within the cloud application or service while complementing security services "in between" the cloud traffic. This out-of-band approach supports 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 does not interfere with or depend on the data path to the cloud application. In addition to applying policies for any future violations, an API-based CASB is the only way to inspect existing data stored in the cloud as well as remediate existing DLP violations and threats.

Introducing Palo Alto Networks CASB Offering

The Palo Alto Networks Security Operating Platform offers in-line and API-based protection technologies that work 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:

- **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, application-risk based policies, user-based policies, DLP, and prevention of known and unknown malware. These comprehensive capabilities span your on-premises and mobile workforce to prevent 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 non-intrusive and neither interferes with nor depends upon the data path to the cloud application.

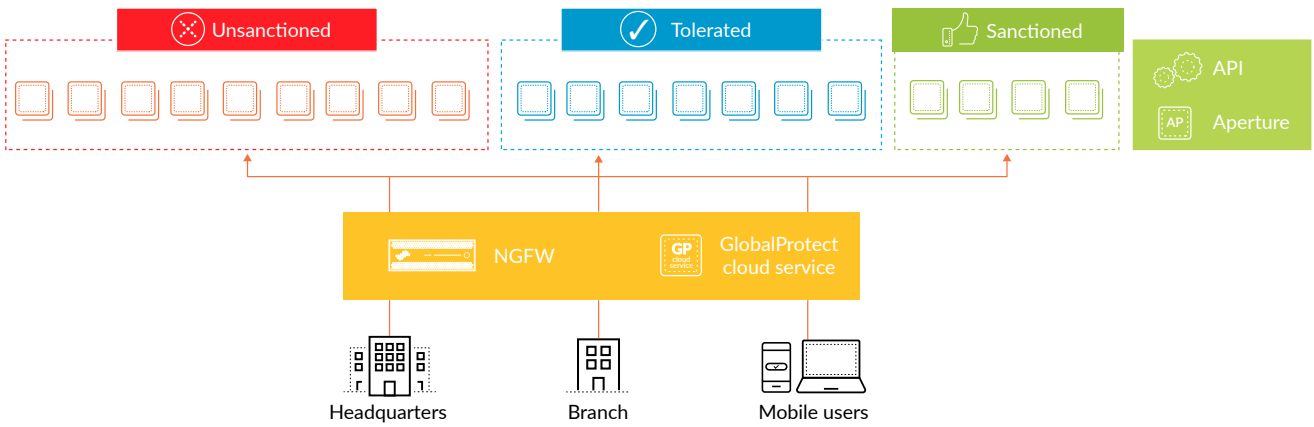

Figure 1: Cloud-delivered CASB approach

An Overview of SaaS Security Capabilities

Deep SaaS Usage Visibility

Businesses can scan all network traffic and detect all applications in use on the network, as well as identify what data is being transferred to the cloud. The Security Operating Platform was built from the ground up to provide unparalleled visibility and precise control of all applications, including details on application usage across the network. SaaS is one of many application categories supported through an extensive library of application signatures that allow immediate classification and fine-grained control. Easy-to-navigate SaaS usage dashboards and detailed reporting help reign in shadow IT risk and get you started on your journey to securing SaaS applications.

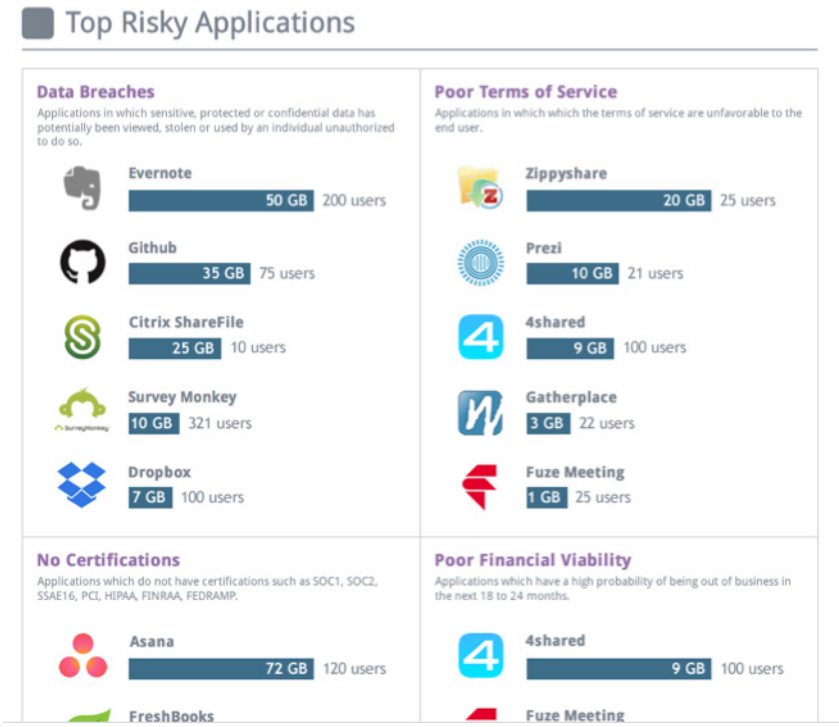

Figure 2: SaaS usage reporting

Granular and Adaptive Access Control

Simple-to-manage policies let you control access to SaaS applications at a granular level, defining which applications are allowed as well as the acceptable behavior within them. Once you have properly classified your SaaS applications, security policies establish access and usage controls at the network, device, and user levels. This lets you block access for unsanctioned applications while maintaining granular control of tolerated applications.

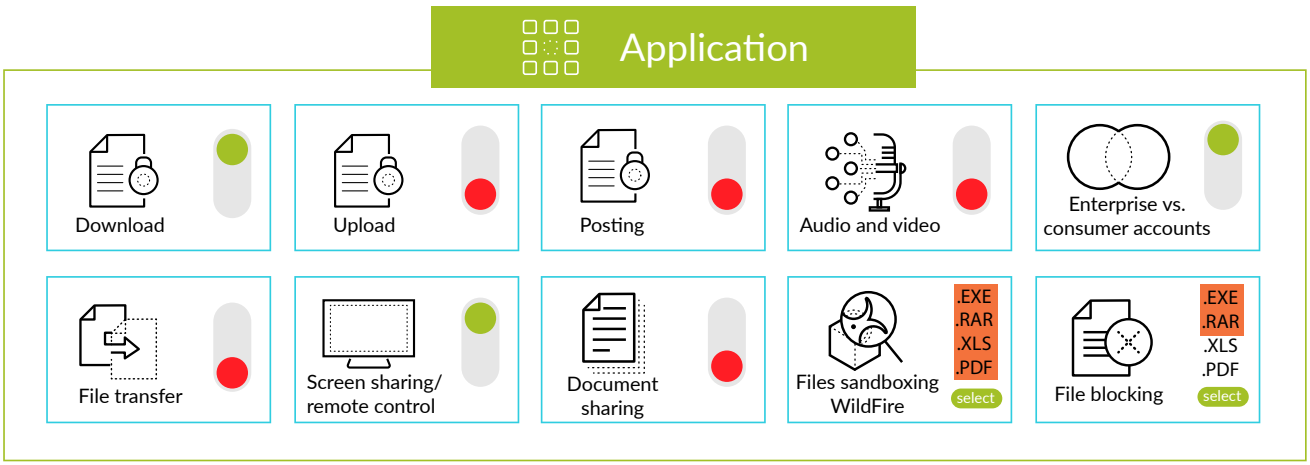

Figure 3: Granular application controls

Data and Risk Discovery

Through the Security Operating Platform, you can scan all data stored within SaaS applications and classify the data based on predefined or custom data patterns. You can also take advantage of supervised machine learning algorithms to categorize data and identify any sensitive files. Once all information is discovered, the assets are checked for any incidents, exposures, and compliance with regulations or corporate policies.

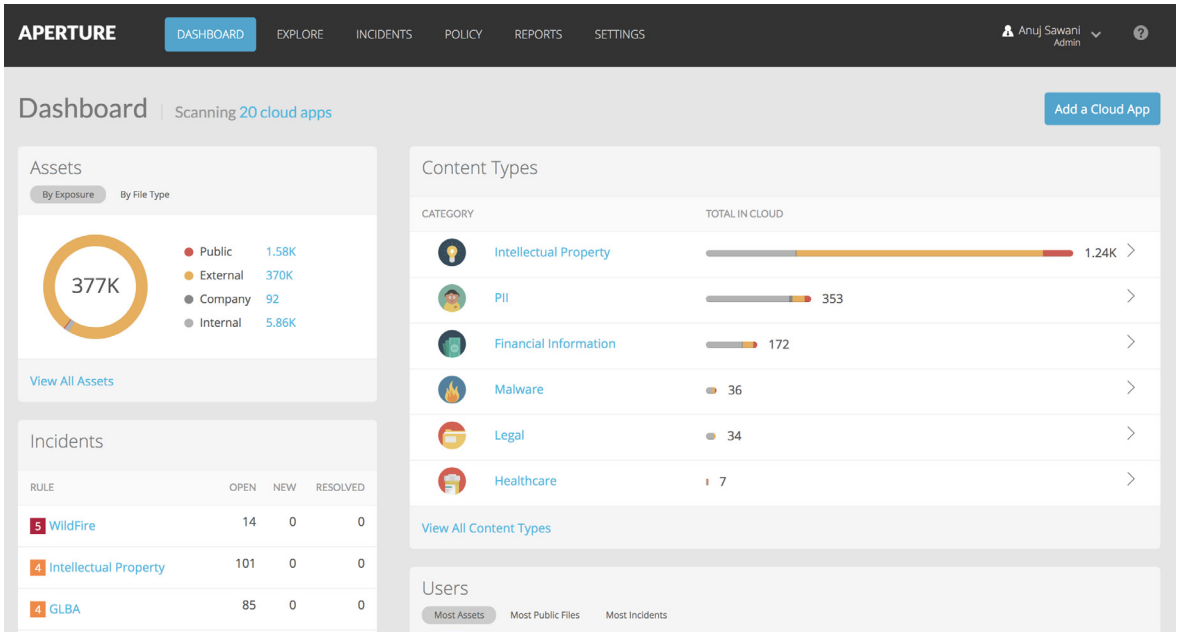

Figure 3: SaaS usage dashboard

Advanced DLP and Compliance

Powerful controls enable you to enforce granular DLP policies based on keywords, file characteristics, and other content patterns. Data loss policies allow you to identify, monitor, and automatically protect sensitive information. Predefined policy templates are available to help you maintain compliance with industry standards and regulations. For specific business needs, you can define custom policies based on business needs, such as policies to classify and control content that includes credit card numbers, tax IDs, or other sensitive information. Content classification is performed using:

- **Matching data patterns:** To help prevent data loss, content scanning can identify potential matches based on data and text patterns defined in policies. You can use predefined patterns or develop custom patterns, known as "regular expressions."
- **Machine learning:** It's not always possible to create a pattern for all data types or appearances. Machine learning algorithms can come to understand what sensitive data looks like over time.

Secure Unmanaged/BYOD Access

As your workforce expands around the world, your users increasingly access SaaS applications from remote locations and devices. Palo Alto Networks supports reverse proxy capabilities using single sign-on to seamlessly reroute users to the in-line security gateway to enforce policies. This functionality can be applied to secure access from any unmanaged or personal device that uses an internet browser to access SaaS applications.

Detect Anomalous User Activity

Stolen credentials or malicious intent may lead to unusual behavior, such as large data downloads or multiple user login attempts from varying locations within a short period. You can implement alerts for these types of anomalous activities as well as suggest remedial actions.

Find and Remove Malware

WildFire® malware prevention service, integrated with Aperture, provides advanced threat prevention to block known malware as well as identify and block unknown malware. This integration stops threats from spreading through sanctioned SaaS applications, eliminating a new insertion point for malware. New malware found through this integration is shared with the rest of the Security Operating Platform even if the platform is not in-line with the SaaS applications.

Simple Deployment and Broader Context

As a cloud-delivered service, Aperture does not need any proxies or agents. Because it communicates directly with SaaS applications, it will look at data from any source, regardless of device or location of origin. Furthermore, because Aperture isn't in-line, it doesn't affect latency, application bandwidth, or the user experience.

With Aperture, your organization can reduce false positives and false negatives with broader context than other agents, devices, or security tools.

Featured App Integrations

Office 365	G Suite	Box.com
GitHub	Slack	ServiceNow
Dropbox	Workplace by Facebook	Salesforce
Confluence	Jive	Citrix ShareFile

Securing Your Cloud Environment

Palo Alto Networks lets you deliver consistent, automated protections across public and private clouds so you can adopt SaaS apps, rapidly roll out cloud-delivered services and apps, and avoid business disruption. Employing the industry's most comprehensive security capabilities, the Security Operating Platform protects SaaS applications, public and private cloud environments, and endpoints with a comprehensive array of products and services.

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

© 2019 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.
safely-enable-your-saas-applications-wp-010919