APERTURE

Safely Enable Your SaaS Applications

The use of SaaS (Software as a Service) applications is creating gaps in security visibility and new risks for threat propagation, data leakage and regulatory noncompliance.

Challenge

Gain visibility and control of SaaS usage to prevent threat propagation and data leakage.

Solution

Palo Alto Networks® has established a rich history of safely enabling applications by helping IT organizations secure these higher risk, unsanctioned services through superior classification and granular policy control across the network.

Aperture adds to the Palo Alto Networks Next-Generation Security Platform, providing a unique approach to securing sanctioned SaaS applications. Aperture adds complete visibility across all user, folder and file activity within the SaaS application and provides detailed analysis and analytics on usage to prevent data risk and compliance violations. Even more importantly, it allows granular context-aware policy control within these SaaS applications to drive enforcement and quarantine of users and data as soon as a violation occurs.

Integration of Aperture with Palo Alto Networks WildFire™ threat intelligence cloud prevents known and unknown threats from spreading through the sanctioned SaaS applications, preventing a new insertion point for malware.

The concept of data residing only in a single centralized location does not apply in today's modern networks. The network has become inverted with data spread throughout multiple locations, including many that are not under the organization's control. Regardless of the location of the data, the IT team is still responsible for securing it as it moves. This is the most visible when it comes to SaaS (Software as a Service) applications. The use of these applications is very hard to control, or have visibility of once the data has left the network perimeter. This presents a significant challenge, with end users now acting as their own IT department that has control over the applications they use and how they use them, but without the expertise on data or threat risk assessment and prevention. Without the right tools to enable visibility into data exposure and threat insertions, even skilled users with security experience can run into problems with SaaS applications.

To gain control of SaaS application usage, you need to start by clearly defining the SaaS applications that should be used and

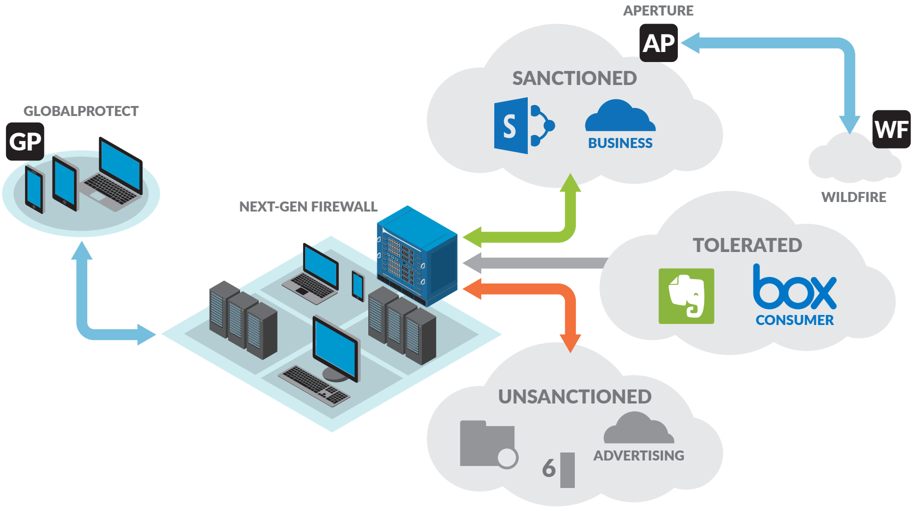

Figure 1: Impacts of sanctioned and unsanctioned SaaS applications

which behaviors within those applications are allowed. This requires: a clear definition of which applications are allowed and provided by IT (sanctioned); which are not provided by IT but are allowed with restrictions (tolerated) because of a legitimate business need; and which are not allowed (unsanctioned), and then put solutions in place to control their usage.

Sanctioned SaaS Introduces Unique Risks

Once a SaaS application is defined as sanctioned, and data is allowed into the cloud where that application resides, there are new challenges that emerge. The data is no longer under the organization's control, and visibility is often lost. The SaaS vendors do their best to protect the data in their applications; but, ultimately it is not their responsibility. Just like any other part of the network, it is the IT team's responsibility to protect and control the data, regardless of the location.

Malicious Outsiders

The most common source of breaches for networks overall is also a critical concern for SaaS application security. The SaaS application becomes a new entry and distribution point for malware used by malicious external users. Some malware will even target SaaS applications themselves, changing their shares to public so the data can be retrieved externally.

Accidental Data Exposure

End users are often one of the most common risks with SaaS applications. While well-meaning, they are often untrained and unaware of the risks their actions pose. Because the SaaS applications used are designed for easy sharing, it is understandable that the data becomes unintentionally exposed in a variety of ways. By far the biggest risks with SaaS applications are the three types of end-user accidental data exposures, which are surprisingly common. They are:

Accidental share: This is when a share was meant for a particular person but was accidently sent to the wrong person or group. This is common when a name auto-fills, or is mistyped, which may be pointing to an old email address or the wrong name, group or even an external user.

Promiscuous share: This is when a legitimate share was created but the user went on to share it with other people who shouldn't have access to it. This often ends with the data being publicly shared because it can go well beyond the control of the original owner.

Ghost/Stale sharing: Another very common accidental share is known as a ghost share. This is when employees and vendors are no longer working with the company, or should no longer have access, but their shares still remain. Without the right tools in place to give you visibility and control of the shares, it is very difficult to track and fix these to keep up with the validity of the accounts.

Malicious Insiders

The least common of the three, but still a SaaS application concern, is the malicious internal user who purposely shares data for theft or revenge. This can be as simple as an employee who is leaving the company and sets up all the folders to be shared publicly or via an external email address in order to steal the data from a remote location.

SaaS Security Requirements

To gain control of sanctioned SaaS application usage, a few key requirements are needed.

Threat Protection

Protection from malware is a common concern for network security, and it is no different with the use of SaaS applications. SaaS applications, in fact, introduce new threat risks that also need to be understood and controlled. One of the biggest risks of SaaS applications is that many of them sync files with users automatically. On top of that, many people use SaaS applications to share data with third parties that are out of control of the company. The combination of these two common uses of SaaS applications presents a new insertion point for malware, one that not only can get in from external shares but also can sync those infected files across the organization automatically without any user intervention required.

To properly deal with the new danger of SaaS-based threats, you need a solution that can prevent the files from residing in the sanctioned SaaS application, whether it is known or unknown malware, regardless of the source of the file. Stop the threat at the source before it has a chance to propagate to other locations.

Visibility and Data Exposure Control

With SaaS application usage defined and controlled with a granular policy, there will be data moving to applications that the company has deemed as sanctioned. Once the data has reached the cloud service, it will reside within the SaaS application and will no longer be visible to an organization's network perimeter. This is traditionally a blind spot for IT. Changes, such as malware from third parties and improper sharing, can still be a danger, as mentioned earlier in the "Sanctioned SaaS Introduces Unique Risks" section, and companies need to protect themselves. An additional set of controls specific to data exposure is needed to specially address these risks unique that are unique to SaaS. The focus needs to be on data protection in this environment, so a deep understanding of users, the data they have shared, and how they have shared it, are key.

Prevent Risk, Don't Just Respond

Unlike a traditional firewall, the threat and data exposure protections should not be an in-line function only looking at future events. Instead, they need to look back at all the previous data and shares in the applications, even before a policy has been put in place. This way, all improper data shares are caught and resolved well before a negative, real-time event triggers the need for a manual response.

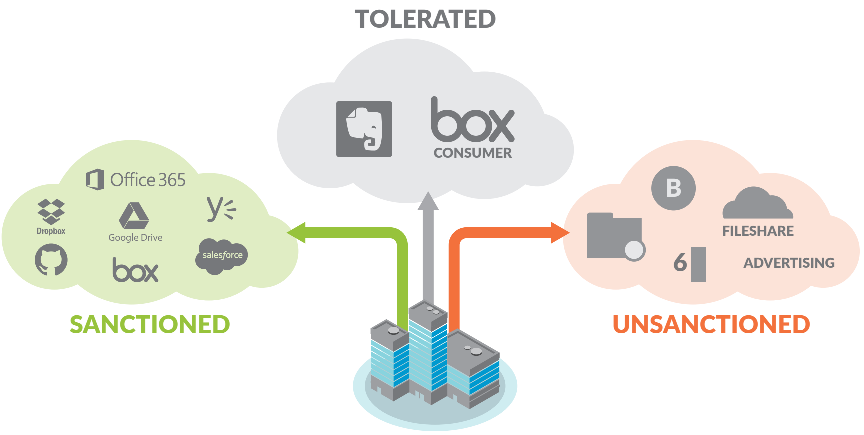

Figure 2: Sanctioned SaaS security with Aperture

Introducing Aperture by Palo Alto Networks

Data residing within enterprise-enabled SaaS applications is not visible to an organization's network perimeter. Aperture adds 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 the Next-Generation Security Platform provided through App-ID™ with detailed SaaS-based reporting and granular control of SaaS usage. Aperture adds visibility and control within SaaS applications and provides a full end-to-end security solution without any additional hardware, software or network changes required.

SaaS Threat Prevention

WildFire threat cloud integration with Aperture provides advanced threat prevention to block known malware and identify and block unknown malware. This extends the existing integration of WildFire to prevent 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 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. With the ability to view deep analytics into day-to-day usage, you can quickly determine if there are any data risk or compliance-related policy violations. This detailed analysis of user and data activity allows for granular data governance and forensics.

Because Aperture connects directly to the applications themselves, it provides continuous silent monitoring of the risks within the sanctioned SaaS applications, with detailed visibility that was previously unseen.

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.

Data does not have to be based only on hosted files, either (unstructured data). Data can be application entries (structured data), such as Salesforce.com entries. Aperture prevents data exposure in either case, supporting the common issue of hosted-file exposure, as well as application entries residing in the applications themselves. Both are common forms of improper data shares.

Advanced Document Classification

Aperture inspects documents for common sensitive data strings, such as credit card numbers, SSH keys, and Social Security numbers, flagging them as risks if improperly shared. Unique to Aperture is the ability to identify documents by type, through advanced document classification regardless of the data that is contained in the document itself. Aperture has been pre-designed to identify sensitive documents, such as medical, tax and legal, automatically. The document classification engine does not only support predefined document type classification but also can support the uploading of custom documents for classification that, in turn, supports customer-specific data risk control.

For example: A blank purchase order can be loaded into Aperture for document classification, so policy and visibility can be set for the document itself. If the form is exposed, it will be flagged as high-risk, regardless of whether there is sensitive data contained within it.

Retroactive Policy

Aperture has a unique approach to policy that is not dependent on time. A typical network security policy is only effective for data seen after the policy is set because it only sees in-line data and applies the policy from that point forward. This doesn't work for SaaS data exposure security, however, since the data that is shared today may have been originally shared years ago. Instead, policies created in Aperture will apply to all users and data from the beginning of the account's creation to identify any violations. There is no need to wait for someone to try to access the data to resolve it; it is proactively found for resolution, no matter how old the data or share may be.

User	Document Type	Sensitive Data	Share Type	Threat
Individual/ Group	Financial and Legal	SSH Keys, API Keys, CC Numbers, SS Numbers	Internal, External, Public, Company	Malware Present

Policies are context-driven to allow for granular definitions of data exposure risks. This is necessary to enable SaaS usage by users while still preventing accidental data exposure. Policies take into context a number of factors to create an overall data exposure risk. One or two factors may not provide enough insight into the potential risk of the share. It is only after comprehending the full context of the share that we can determine the overall risk of exposure.

Risks are calculated by user type, document type, sensitive data contained, how they are shared, and whether there is malware present. See the chart below. This provides the ability to control the exposure at a granular level based on a number of important factors.

For example: A financial team may be able to share financial data with other people on their team–but not beyond that. Even though the original share is allowed, they must not share data with malware. Finance may, however, be allowed to share non-sensitive data company-wide or, in some cases, with external vendors. The key to allowing this kind of granularity is the ability to look at the share in context of all the factors.

The most common need with SaaS security is to ensure compliance of PCI and PII standards within an organization. Aperture has accounted for that with predefined policies to address these common compliance requirements.

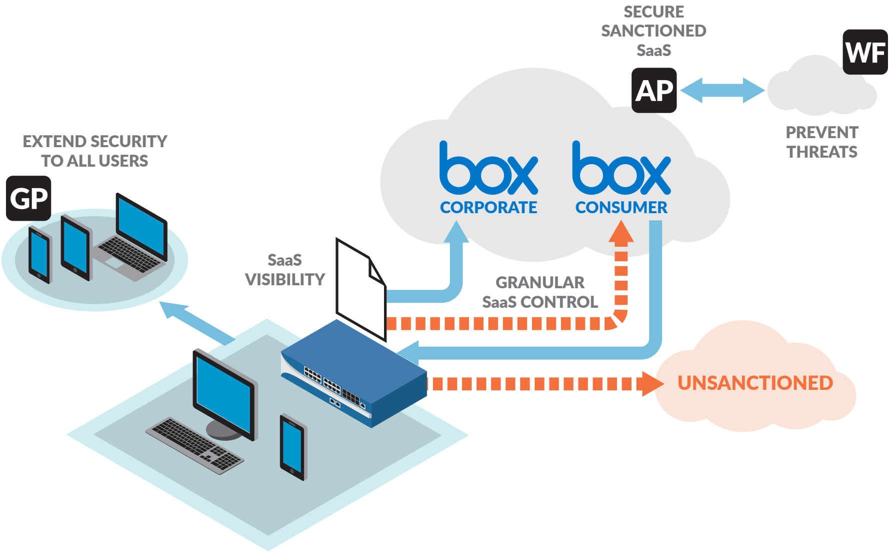

Figure 3: Complete SaaS visibility and control by Palo Alto Networks

No User or Network Impact

Aperture is a completely cloud-based solution without the need for any proxies or agents for it to work. Because Aperture communicates directly with the SaaS applications themselves, it will look at data from any source, regardless of the device or location from which the data came. Because Aperture isn't an in-line service, it doesn't impact latency or the bandwidth of applications and has no impact on the end-user experience. Native applications on mobile devices are also unaffected, so your users aren't limited to using only web-based access. With no network changes needed or proxies to set up, it has no impact on network configurations. No new software or hardware needs to be installed to use Aperture. It just works.

Beyond Sanctioned SaaS

Aperture adds another dimension of security to the Palo Alto Networks Next-Generation Security Platform, providing key insight into data and threat exposure with sanctioned SaaS applications. When Aperture is included as part of a larger solution with a next-generation firewall, the capabilities increase substantially to provide an all-encompassing SaaS solution with true visibility into all applications. This includes both sanctioned and unsanctioned SaaS, with granular control of application usage. (See diagram below.)

Full Visibility into All Applications

Palo Alto Networks Next-Generation Firewall technology was built from the ground up to provide unparalleled visibility and control of all applications, including details on application usage across the network. SaaS is one of the many application categories that is supported today through an extensive library of App-ID instances that provide immediate classification and fine-grained controls.

Application	Control	Feature
Box	Box – Personal	App-ID
	Box – Corporate	App-ID
	Upload control	File Blocking
	Download control	File Blocking
	Malware detection	WildFire & protection profile
	User-based control	User-ID

Example of granular controls supported with App-ID

Granular Control of All Applications

Palo Alto Networks Next-Generation Firewall with App-ID provides the industry-leading granular control to and from SaaS applications. This provides organizations with the ability to control access to SaaS applications at a granular level, defining not just which applications are allowed but also the acceptable behavior within the application. Once SaaS applications have been properly classified, security policies establish access and usage controls at the network, device and user levels. This not only enables the ability to block access for unsanctioned applications but also provides the granular control of tolerated applications; which, in turn, allows control of how they are used to ensure business is unaffected while providing assurances of their safe use.

Extend Security to All Users All of the Time

With Palo Alto Networks GlobalProtect™ mobile security, users are connected to the network all of the time, eliminating the large number of users roaming off the enterprise network. GlobalProtect works by connecting a user's device to the closest next-generation firewall, so that full network security can be performed, regardless of the user's physical location. And with the VM-Series being consumable in public cloud services like Amazon® AWS, the closest next-gen firewall can be very close to the user.

Prevent Threats Everywhere

WildFire is designed to identify known and unknown malware residing within the network and then share that data with the rest of the Next-Generation Security Platform. Aperture adds that malware visibility into SaaS applications directly.

Full Data Security Regardless of Location

Aperture is part of a larger cloud solution that, with the Next-Generation Security Platform, allows for data protection regardless of location. Whether data resides on-premises; has been virtualized and needs protection in a private cloud (NSX™, ACI, Hyper-V®, KVM/OpenStack®); has extended to the public cloud (AWS, Azure™, vCloud® Air™); or has been moved to a SaaS application, Palo Alto Networks can protect it.

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com