3 STEPS TO TAKING CONTROL OF SAAS APPS . . .

. . . and Limiting the Risk of Shadow IT

When it comes to the use of software as a service (SaaS) applications within your organization, what you don't know can hurt you. Like wolves in sheep's clothing, unsanctioned or uncontrolled SaaS apps are probably sitting on your network right now, seemingly harmless and unobtrusive, enabling users to collaborate and do their jobs more productively. That is, until suddenly and without warning, they begin wreaking all sorts of havoc on your business, including data exposure, malware distribution and insertion, information leakage, and regulatory non-compliance.

Two main challenges make it critically important for you to get these applications under control:

- Because applications and data move off the enterprise network, it is very difficult to have visibility into them at all times, meaning IT can't monitor them, assess risks, or prevent attacks.
- Their use is growing exponentially through the proliferation of Shadow IT initiatives. This unchecked expansion of Shadow IT exposes your organization to a rapidly growing variety and volume of vulnerabilities that will only get worse over time.

Just to give you a sense of how prevalent the problem is, the latest Application Usage and Threat Report from Palo Alto Networks showed that SaaS-based application usage has grown 46 percent over the past three years, identifying more than 316 apps. The largest portion of these were file storage (40.7%) – a strong indicator that much of this activity involves the use of unknown or uncontrolled apps. To make matters worse, most organizations can't even identify what is in use. According to one survey, 72 percent of IT managers have no idea how many Shadow IT applications are in use within their organizations.[1]

It doesn't have to be this way. There are technologies, tools and strategies you can deploy to get SaaS applications under control and apply enterprise-level security policies to ensure that their use is safe, secure and compliant. How can you get SaaS under control and limit the dangers posed by Shadow IT initiatives? Here's a quick three-step guide.

Step 1. Gain visibility of SaaS usage at the network level

Just to be clear, we are not advocating that you give up valuable and popular business tools, such as Box, Dropbox, Google Drive, Salesforce, or any other application that helps employees to collaborate and be more productive. What we're saying is that you need to be able to identify these applications, and who is using them, and then develop a realistic approach to getting them under control so that their usage does not pose risks to your organization.

The idea is to enable SaaS usage but to control it at the same time. The first step is to use a next-generation firewall to gain visibility at the network level across all user, folder and file activity to get detailed analysis that will help you determine which applications are being used by the users in the network. The goals are to:

- Identify SaaS users and which applications they are using
- Define the behavior of SaaS users (upload, download, etc.)
- Identify the risk of these apps

[1] "You Don't Say? In the Face of Massive Security Breaches, Executives Are Concerned," Forbes, Jan. 9, 2015

Step 2: Control SaaS usage

Once you've identified the unsanctioned applications, you can take the necessary steps to control their usage. One step is to block specific, unsanctioned applications and other Shadow IT initiatives. Another step is to sanction certain SaaS applications you are not already sanctioning. This way you can split usage into sanctioned and unsanctioned groups. But not every SaaS application will fit neatly into one of those two categories, so a third step may be necessary, which is to use your security platform to safely enable SaaS applications that can neither be sanctioned nor blocked.

For example, users in your organization may be working with a third-party vendor and part of their process might be to share documents via the vendor's file sharing application, typically Box or Dropbox. You cannot cut off this application entirely because it is required in the day-to-day work of certain users. This application lives in a gray area: a "tolerated" application. With a next-generation security platform, you can create granular policies that only allow certain users to download from a specific application, while blocking uploads. Once you have these controls in place, you will be able to:

- Safely allow sanctioned cloud applications
- Block unsanctioned applications on your network
- Have granular control of tolerated applications

Step 3: Prevent data and threat risk

It's also important to recognize that, even when a SaaS application is sanctioned, you will face new challenges. Once data is allowed into the cloud where the app resides, that data is no longer under IT's control or visibility. Bad things can happen. For example, many SaaS applications sync files with users automatically, and many users share data with third parties who are out of the control of the company. The combination of these two common activities presents a new insertion point for malware. Not only can malware get in, it can automatically sync those infected shares across the organization without any user intervention. You must be able to:

- Prevent malware insertion
- Prevent data exposure
- Stop data theft

Introducing Aperture by Palo Alto Networks

You need a solution that connects directly to the sanctioned SaaS and provides data exposure, sharing and permission visibility, and threat protection within the application. Aperture™ contextual threat intelligence service gives you this level of visibility with detailed SaaS-based reporting and granular, context-aware policy control. This means you can both inspect content for threat risks and control access to shared data via contextual policy. Aperture enables complete visibility across all user, folder and file activity, so you know exactly what is happening with your SaaS apps at any time. In addition, you can leverage deep analytics to quickly identify, evaluate and address data risk or compliance-related violations.

With the integration of the WildFire™ cloud-based malware analysis service, you get advanced threat protection to block known malware and identify and block unknown malware. This not only prevents threats from spreading through the sanctioned SaaS apps but also allows the sharing of information about new malware discovered in Aperture with the rest of the security platform, thereby protecting the organization from a new insertion point for malware.

Advantages of a Platform Approach

Once you've put the technologies and processes in place to mitigate the risks involved in supporting SaaS applications, you must have tools and processes to maintain constant vigilance. As hackers develop new types of threats, you have to be able to identify and eliminate them before they can do harm to your business. This requires an end-to-end model that incorporates three key elements: a next-generation firewall; a security solution, such as Aperture, designed specifically to address the threats of SaaS applications; and a cloud-based threat intelligence service that provides ongoing vigilance and monitoring of both known and unknown threats.

This is the approach taken in the Palo Alto Networks® Next-Generation Security Platform. The platform includes our Next-Generation Firewall, which inspects all traffic – including applications, threats and content – and ties it to the user, regardless of location or device type. Aperture extends this protection by connecting directly to SaaS applications. This way you never lose visibility into your data or applications and can apply granular policy and control at all times. Through the existing integration of WildFire cloud-based malware analysis, you can prevent known and unknown threats from spreading through your sanctioned SaaS applications.

Taking the Next Step

Don't be fooled by the seemingly innocuous threats presented by the unsanctioned use of SaaS applications. These apps may seem like they are providing value to your organization, and they probably are, until they release an attack that causes a major data breach or significant downtime. And don't assume that you can address the problem simply by sanctioning SaaS apps. You also need to ensure that you have the right technology in place to have unobstructed visibility into these apps, and granular control over your applications and data, wherever they are located.

This is the reality: SaaS applications are not going away. In fact, their usage continues to grow rapidly. This can be a good thing for the business but only if SaaS usage is under IT's control. Make sure your organization leverages the value of SaaS applications without exposing you to their risks.

Learn more about how Aperture uniquely secures SaaS applications as part of the Palo Alto Networks Next-Generation Security Platform by watching this short video: http://go.paloaltonetworks.com/safelyenablesaas

paloalto NETWORKS®

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