SOLUTION BRIEF

Securing Cloud Applications

Overview

Most organizations have discovered the benefits of hosted SaaS applications. No software licenses, no out-of-date software, and simplified deployments make SaaS an enticing method to deliver new functionality without the strings that come with traditional applications. Although many of the "old strings" are gone with SaaS, there are many new ones that must be addressed and managed.

The two major groups of risks are associated with the use of SaaS applications such as Salesforce.com and the use of non-approved applications. These two primary groups share many of the same problems, mostly visibility and control of data once it is outside the perimeter of the network.

Approved applications provide some degree of security and many offer IT administrators tools to manage data; however, these are limited and are on an application-byapplication basis. Unapproved applications represent the highest level of risk because the IT teams have little or no visibility as to what applications are being used, have no insights into the activities or data that are stored in the application, and in many cases are known to be associated with questionable activities.

One of the greatest benefits of SaaS applications is the ease with which they can be deployed by anyone in the organization. This has led to the rise of shadow IT departments where the traditional teams tasked with IT security have little insight into the use and risk posed by applications brought in without their knowledge.

As SaaS continues to grow at a rapid rate, the problems created by SaaS will only get worse. Just because data is no longer stored within the perimeter doesn't excuse the requirement to meet strict compliance guidelines or protect sensitive data from getting into the wrong hands. Organizations need new tools that provide the visibility they need and provide the controls necessary to protect data stored in the cloud.

Challenges/Solution Highlights

Challenges

- Provide Visibility and Control for SaaS Data
- Protect from Cloud-borne Threats
- Extend Compliance to SaaS Applications

Solution

- FortiCASB Cloud Access Security Broker
- FortiOS Cloud Access Security Inspection
- FortiAnalyzer SaaS Reporting

Gain visibility, mitigate threats, and control your data inside and outside the perimeter of the organization with FortiCASB, FortiGate, and FortiAnalyzer.

Challenges Created by SaaS Application

Unlike an application or data warehouse protected safely behind a perimeter firewall, SaaS applications store data and files outside the organization. This creates a new set of problems that must be addressed.

Loss of Visibility and Control

Once outside an organization, data and files are at the mercy of the SaaS provider. Most have some degree of tools to manage files and access, but they don't necessarily mirror the policy controls in place inside the perimeter, nor are they consistent in their methodologies.

Here is where an organization has little understanding of who is accessing information and how it's being shared. Depending on the applications used, there is a risk of sensitive information such as credit cards, social security numbers, and confidential data being stored in the cloud. Most risks here are related to users who accidentally share data with parties they're not supposed to. However, there is always the risk of internal bad actors who can take advantage of the poor controls on easily accessible confidential or proprietary information.

Threats from the Cloud

Most of the major SaaS providers offer some level of security and scan files for threats. These, however, are not bulletproof and can allow infected files to be shared with other users in the cloud or within the perimeter.

Complicated

If an organization knows the SaaS applications in use, it is possible to perform audits; however, it is very difficult, as all services have to be assessed separately with varying tools offered by the SaaS provider. Unapproved applications create a whole new level of compliance issues. Some firewalls can provide visibility for in-line traffic; however, there is no way to perform audits on services used by remote users or on data that is sitting on cloud servers.

Accountability Still Remains

Regardless of where the data resides, the IT organization has the task of maintaining security and compliance. When data is safely stored within the perimeter defenses, that's an easier job. When it's stored on someone else's server outside the organization, the challenges range from figuring out where the data is to what's actually being stored there. If there is an attack on an organization or a data breach, no matter where it originated from, the IT security teams will be held responsible.

Types of SaaS Applications

There are many different methods an IT organization can use to categorize SaaS applications.

For purposes of this document and to maintain consistency with other solutions, the following three supercategories will be used to characterize SaaS application groupings: Sanctioned, Tolerated, and Unsanctioned.

Sanctioned

SaaS applications in this category are defined as those that are approved, sponsored, managed, and in most cases paid for by the organization. Examples of Sanctioned apps could be a corporatewide implementation of Salesforce.com or Microsoft Office 365.

Tolerated

Apps in this category are allowed by the IT organization for use on the network; however, they are not managed or sponsored by the organization. Generally these applications are paid for and managed by the individual and in some cases can be paid for by a department outside of IT. Examples here could include the use of Evernote by an individual to manage documents, or a sales team using Box to send sales information to customers.

Unsanctioned

As the category name suggests, these apps are not tolerated or allowed by the IT organization on the network for any number of reasons including security, competitive, inappropriate con-tent, or even political.

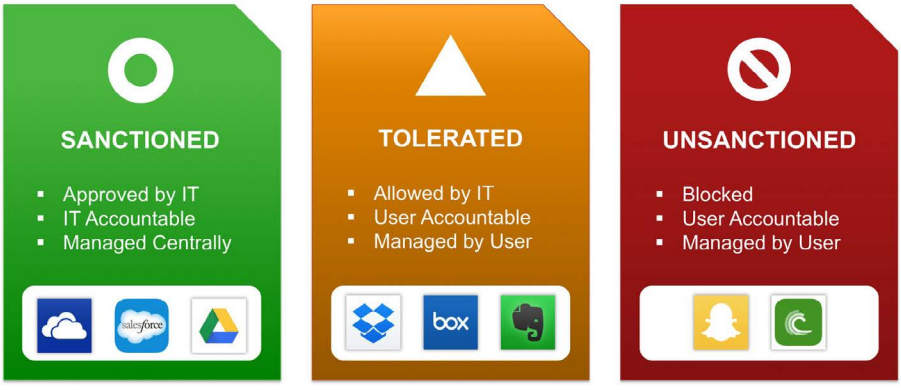

Figure 1: Examples of how an organization group might have SaaS applications for sanctioned, tolerated, and unsanctioned.

Limitations of Firewalls and other Perimeter-based Defenses

Some organizations believe they have the tools they need to manage SaaS application traffic and data with existing tools like a firewall and IPS. These offer some protections, but generally they are limited to in-line deployments. Mobile/remote users who directly access SaaS services aren't covered by these solutions and can represent a sizeable risk. Gartner Research predicts that by 2018, over 25 percent of an organization's traffic will be remote directly to SaaS providers.

An enterprise firewall such as a FortiGate can provide insight into SaaS application traffic and usage. FortiGate offers a Cloud Access Security Inspection (CASI) feature that can detect and manage access to SaaS websites. Sites can be blocked, monitored, or allowed without restriction. This is a great tool; however, it must be deployed in-line and manage traffic that traverses the perimeter. Once outside the organization, the firewall has no visibility as to how the data is used or distributed.

What is a Cloud Access Security Broker?

Cloud access security brokers (CASBs) are security policy enforcement services or devices that are deployed between cloud service providers and users of these services. The types of CASBs can range from onpremise, proxy-based solutions to full cloud-native solutions that use APIs to gain deep access into the data and usage details made available by the cloud service provider.

The primary role of the CASB is to extend and manage an organization's security policies for usage and data housed in cloud-based services. As a majority of organizations adopt hybrid-cloud strategies and deploy SaaS applications such as Salesforce.com and Office 365, there is an urgent need to gain visibility and control for data that is stored outside the traditional IT boundaries. This need is only getting larger as more organizations move to infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) providers.

In organizations that have large shadow IT programs or allow internal groups to buy and manage cloud-based services without IT involvement, CASBs can be a very useful tool for discovery and management. The insights provided by a CASB solution can help an IT organization gain better visibility into cloudbased applications being used and where confidential/proprietary data is stored that could pose risks to the organization.

CASB products typically offer a consolidated set of services for security enforcement including authorization, authentication, device profiling, data loss prevention, malware detection/mitigation, encryption, and tokenization. In addition to security enforcement, CASBs provide in-depth logging, reporting, and analytic of cloud-based services, which are not possible with traditional on-premise network security technologies.

API vs. Proxy-based CASBs

There are two primary forms of CASB services, API-based and proxy-based (forward and reverse modes). Many early CASB market entrants started with reverse proxy-based services that were deployed for users within the perimeter (including VPN), where all traffic is scanned for cloud services activity. As BYOD continues to rapidly erode traditional perimeters, forward proxy modes were introduced.

Forward proxy-based solutions can help cover remote devices, but they can be very cumbersome to manage. The latest CASB services offer API-based controls that are directly linked to the cloud service provider and overcome the need to provide complex device management. This newer approach ensures that all users of the organization's SaaS applications are monitored and protected by the CASB service, no matter where they are or what device they are using.

Benefits of an API-Based CASB

- Greater insights into usage and data within the SaaS application
- Does not interfere with or slow down traffic from the user to the cloud service
- Ability to inspect data previously stored in the cloud and new data being added/modified
- In-depth information on data, users, permissions, and behaviors in the SaaS application
- Device-agnostic and supports nonperimeter access to cloud applications
- Can be used alone or with a proxy-based service for additional perimeter security
- Easy, one-step access that does not require complicated proxy deployments

Benefits of a Proxy-based CASB

- Real-time scanning of usagve and data to/from SaaS provider
- Allows for interception and tokenization of files
- Enables encryption management

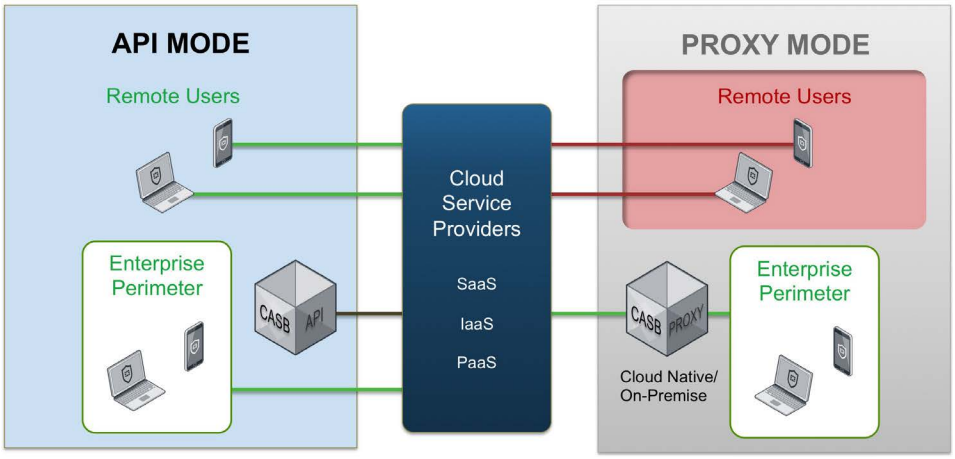

Figure 2: An API-based CASB provides protection for users both within the perimeter and from remote locations.

API is the Future

Although proxy-based CASBs offer some benefits, most organizations prefer the API-based approach. Even vendors that had started out as proxy-based have added API CASBs to their product lines. An APIbased CASB provides most organizations the tools they need; however, there are instances where a proxy-based service may be preferred.

FortiCASB Overview and Features

FortiCASB is a Fortinet developed cloudnative CASB solution that is designed to provide visibility, compliance, data security, and threat protection for cloud-based services employed by an organization.

FortiCASB Features

- API-based model for SaaS data detection, mitigation, analysis, and reporting
- On-demand and stored data threat and data loss prevention scanning
- Comprehensive analytics and reporting including cloud usage, audit results, activity/behavior monitoring, user entitlements, and geolocations
- Full support for major SaaS applications such as Microsoft Office 365 OneDrive and Salesforce.com
- Subscription-based
- Always up-to-date hosted service by Fortinet
- Simplified pricing structure includes all supported applications
- Predefined policies for each SaaS service and configuration assessment tools
- Cloud portal for administrator access

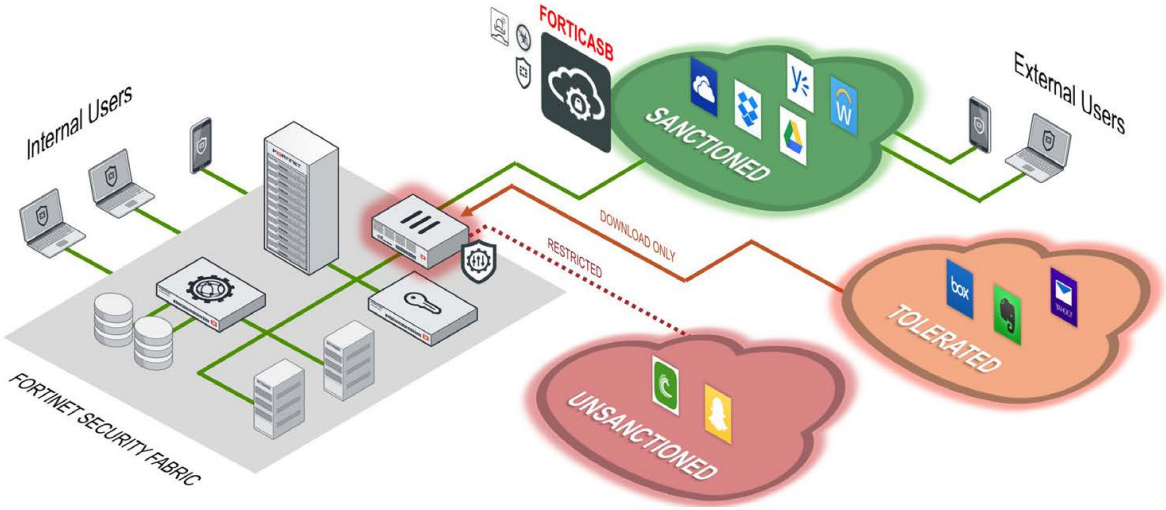

Figure 3: FortiCASB protects sanctioned SaaS applications. FortiGate provides control and visibility for tolerated and unsanctioned SaaS applications.

FortiCASB and the Fortinet Security Fabric

The Fortinet Security Fabric enables protection for all points of the cloud with the existing FortiCloud and FortiHypervisor solutions in addition to tight security integration with cloud infrastructure partners like Amazon AWS and Microsoft Azure. Fortinet's FortiCASB service extends the Fortinet Security Fabric benefits of centralized awareness, threat intelligence, and automated controls to an organization's cloud-native applications and services as part of the FortiCloud service offerings.

With integration into FortiGate, FortiGuard, and FortiAnalyzer, FortiCASB allows deep inspection of cloud-based application usage and stored data and extends security policies to the cloud. Once set up, administrators will have awareness and insight into applications used by the organization and will be able to clearly see where the organization's data may be at risk.

As a cloud-based service hosted by Fortinet, FortiCASB is able to scale to meet the needs of any size organization. Whether it's a business with a few hundred users or a global enterprise with hundreds of thousands of employees, FortiCASB will protect medium and large cloud service deployments without the need to manage hardware constraints. As more users are added, FortiCASB offers convenient, stackable licenses to quickly extend FortiCASB when needed.

Management tools both within the FortiCASB console and FortiGate will enable near-instant alerts to threats or policy violations in cloud-based services. Administrators will have the flexibility and granular capabilities to set actions based on the type of activity encountered, from simple alert notifications to automated actions that can stop threats quickly before they spread within the cloud service to other users or from the cloud to users inside the perimeter.

FortiCASB with Salesforce.com

Salesforce.com is one of the most broadly adopted SaaS applications. FortiCASB directly connects to Salesforce using an API to gain access to data and files stored on the Salesforce platform. Using a master account for the organization, the IT administrator logs into FortiCASB and sets up the access rights, privileges, and data protection policies for the organization. Once set up, each user's account is fully protected, no matter where they log into their account or which type of device they use. Additionally, FortiCASB scrubs the data already stored on Salesforce to ensure information and files are secure and follow all business policies.

Summary

As SaaS application adoption continues to expand, new challenges need to be addressed by IT organizations to ensure data visibility, safety, and compliance. Approved and unapproved SaaS applications present new risks in how data is stored and shared, along with opening new doors to threats to be spread from user to user, inside and outside the traditional perimeter defenses.

A firewall can provide some visibility, but it's limited to devices within the perimeter and can only protect data when it crosses the device. Only a CASB can provide deep access to data and usage for SaaS applications.

Fortinet's FortiCASB solution is the only API-based CASB that is built to operate seamlessly within the Fortinet Security Fabric. FortiCASB's integration with FortiGate, FortiAnalyzer, and FortiGuard Security Services creates a CASB solution that is aware of other Fortinet devices and services, delivers the scale needed for large enterprises, and provides actionable insights into threats and security issues inherent in cloud-based services.

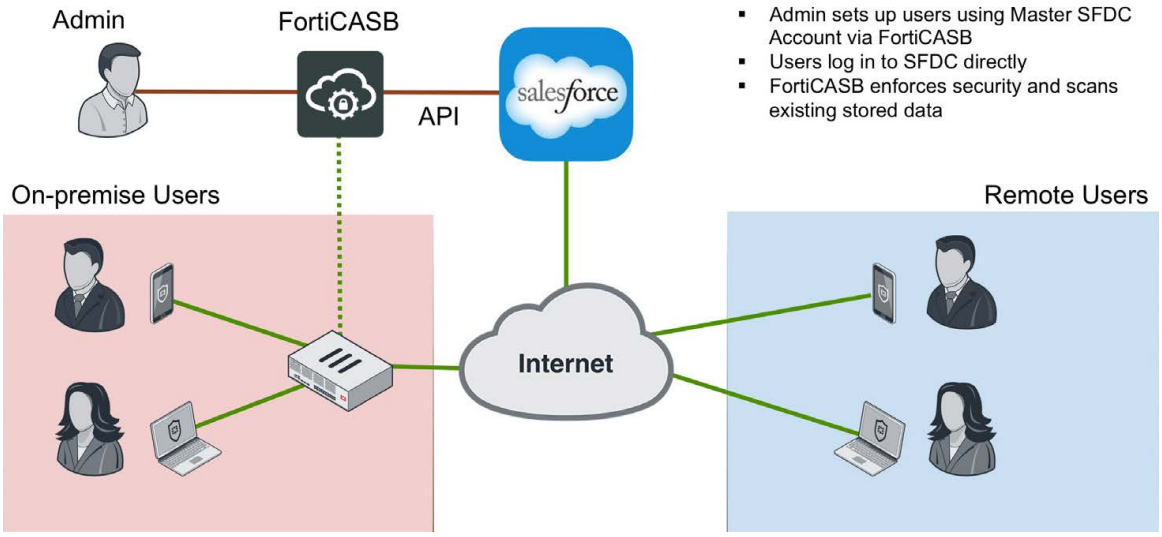

Figure 4: FortiCASB provides protection for on-premise and remote access to salesforce.com by protecting the data centrally. The admin sets up user access and controls through FortiCASB. Users access salesforce.com directly from the internet or from behind the firewall. FortiCASB then manages security directly to salesforce.com using API access.

November 5, 2019 2:42 AM

488935-0-0-EN

D:\Fortinet\Solution Briefs\blue solution briefs\refresh - Securing Cloud Applications\sb-securing-cloud-applications-v1