SOLUTION BRIEF

Protecting Enterprises from the Risks of Software-as-a-Service (SaaS)

Visibility, Insight, and Control for Sanctioned and Unsanctioned Cloud Applications

Executive Summary

Organizations are increasingly adopting cloud-based applications and services for the agility and cost savings they offer. Unfortunately, they are also finding that they have insufficient visibility and control over these services. The risks of Shadow Software-as-a-Service (SaaS) applications can be prevented and detected with the right security controls—and a cloud access security broker (CASB) is a centerpiece of this strategy. Fortinet FortiCASB is a cloud-native CASB with extensive support for major SaaS providers. It tightly integrates with the FortiGate next-generation firewall (NGFW) to increase visibility and provide security-enforcement capabilities, protecting against risks associated with access to both sanctioned and unsanctioned SaaS applications.

Key Benefits of FortiCASB with FortiGate NGFWs

- **Visibility.** Who accessed information, what was accessed, when it was accessed, and from where.
- **Data control.** Discover critical data and classify it under different levels of sensitivity for better protection.
- **Threat protection.** Advanced security services and monitoring of suspicious or irregular user behavior.
- **Compliance.** File content monitoring to find and report on regulated data in the cloud.
- **Total scalability.** A cloud-based operational and subscription model grows with your organization.

The Problem of Shadow Applications

Reliance on cloud-based technologies such as SaaS is on the rise. The enterprise SaaS market is now generating $20B in quarterly revenues, a number that is growing by 32% per year.[1] This trend makes perfect sense on many levels. No software licenses, no out-ofdate software, and simplified deployments make SaaS an enticing method to deliver new functionality without the strings that come with traditional applications. But there are some critical security risks associated with SaaS that many organizations can overlook in favor of the benefits.

One of the greatest advantages of SaaS is the ease with which these applications can be deployed by anyone in the organization. But this ease of use has added to the problem of Shadow IT. Within an organization, Shadow IT refers to technologies used by employees without the knowledge of the IT department—and this includes cloud-based services.

Unapproved SaaS services represent a high level of risk because IT teams have little or no visibility into the applications being used, no insights into the data stored in them, and no ability to spot questionable activities. And as these applications often do not meet enterprise-grade data security and privacy requirements, Shadow SaaS can also introduce compliance risks to enterprises.

Managing Cloud Application Risks with FortiCASB

Whether authorized or not, SaaS applications store data and files outside the organization. And IT organizations must maintain both security and compliance requirements, regardless of where their company data resides. An enterprise firewall can provide insight into SaaS application traffic and usage. Sites can be blocked, monitored, or allowed without restriction. But once an employee accesses a cloud-based service off-network, the firewall has no visibility as to how the data is used or distributed.

A CASB can help address this risk exposure by offering visibility and policy-based controls for data housed in cloud-based services. In organizations with identified Shadow IT problems, CASBs can be a very useful tool for discovery and management of all applications being used across the organization. A CASB typically provides a set of security-enforcement services (e.g., authorization, authentication, device profiling, data loss prevention, malware detection/mitigation, and encryption). In addition, CASBs also should provide in-depth logging, reporting, and analytics of cloud-based services—none of which is possible with traditional on-premises network security technologies.

FortiCASB can be used to see and manage all cloud-based services and applications in use across the enterprise and then implement security policies and controls to protect sensitive data. It provides full support for major cloud providers such as Microsoft Office 365 OneDrive, AWS, Google Drive, and Salesforce.com.

Part of the **FortiGate NGFW Enterprise Protection Bundle**, FortiCASB offers deep integration into the Security Fabric to provide comprehensive visibility, consolidated cloud usage management, and detailed compliance reporting.

Transparent Visibility

FortiCASB works in conjunction with a **FortiGate** NGFW to allow deep inspection of cloud-based application usage and stored data. After deployment, FortiCASB can see which SaaS applications are currently being accessed, which SaaS stored files are being accessed, and whether those files are being shared.

Once applications are visible to the organization, policy-based controls and automated responses can be set to reduce risk exposure and improve security. FortiCASB provides automated access and oversight for sanctioned applications—those that are preapproved by the organization. FortiGate can manage access for tolerated applications (those that are not preapproved but that automatically meet defined policy criteria) and also restrict usage of unsanctioned applications that have risk associations. These features help reduce administrative burdens on limited IT resources.

Integration with **FortiAnalyzer** allows FortiCASB to provide consolidated views in specialized dashboards (Figure 1). This includes a Shadow IT summary of all unsanctioned SaaS applications and associated files. These dashboards help administrators track application traffic, users, and data in real time to reduce the time to resolution in the event of a potential problem or threat incursion.

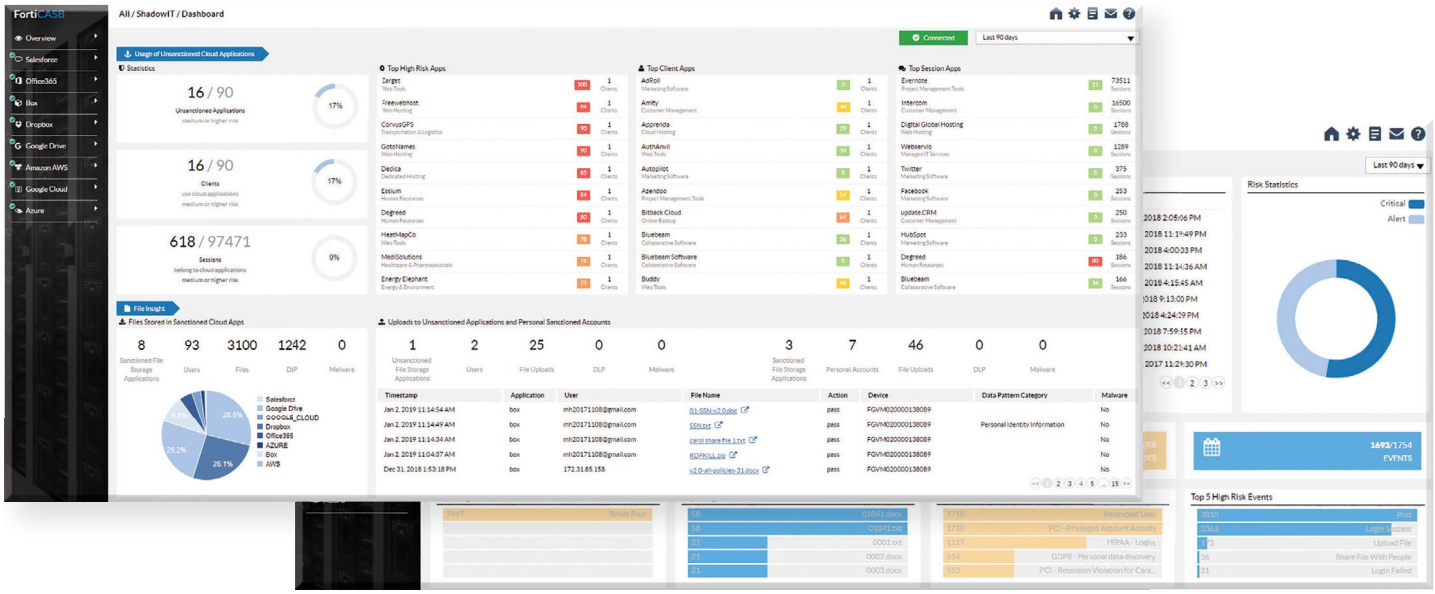

FIGURE 1: FortiCASB dashboards for all SaaS applications in use (shadow it) and application-specific status.

Centralized Visibility

With integration into FortiGate and FortiAnalyzer, FortiCASB allows deep inspection of cloud-based application usage and stored data. The integration also extends security policies to the cloud. Thus, when a user attempts to access an unauthorized SaaS application, FortiGate NGFWs block access based on the application controls set by the administrator. This minimizes risks and helps ensure compliance with the regulations applicable to the respective industry.

The FortiCASB overview dashboard (Figure 2) provides centralized controls over different SaaS applications. It allows security administrators to search based on different timelines and to navigate to specific SaaS applications for more detail. Management tools, both within the FortiCASB console and FortiGate, enable near-instant alerts to threats or policy violations in cloud-based services. Administrators have the flexibility and granular capabilities to set actions based on the type of activity encountered—from simple notifications to automated actions that can stop threats quickly before they spread.

Use of Fortinet Secure SD-WAN, which is built into the FortiGate NGFWs, allows FortiCASB to further extend and implement consistent application-control policies across all distributed branch locations across the organization. It automatically limits user access to only the SaaS applications that comply with the organization's established standards.

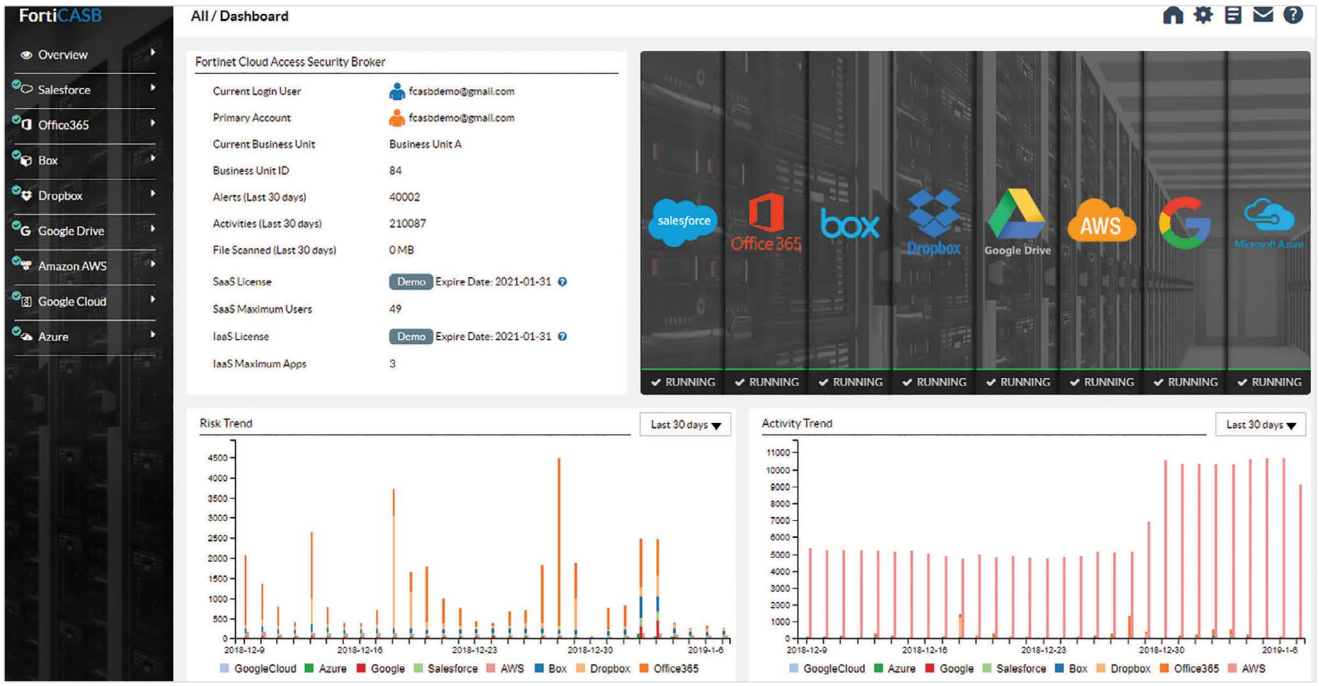

FIGURE 2: FortiCASB overview dashboard—centralized control and management.

With FortiCASB, application-control policies can also be enforced for mobile devices that travel outside the organization's network—beyond the reach of firewall protection. In this case, when combined with **FortiClient**, protection is extended to remote endpoints. Thus, when an off-network endpoint attempts to access an unsanctioned SaaS application via an outside internet connection, FortiClient blocks access based on the predefined application-control policies from FortiGate NGFW.

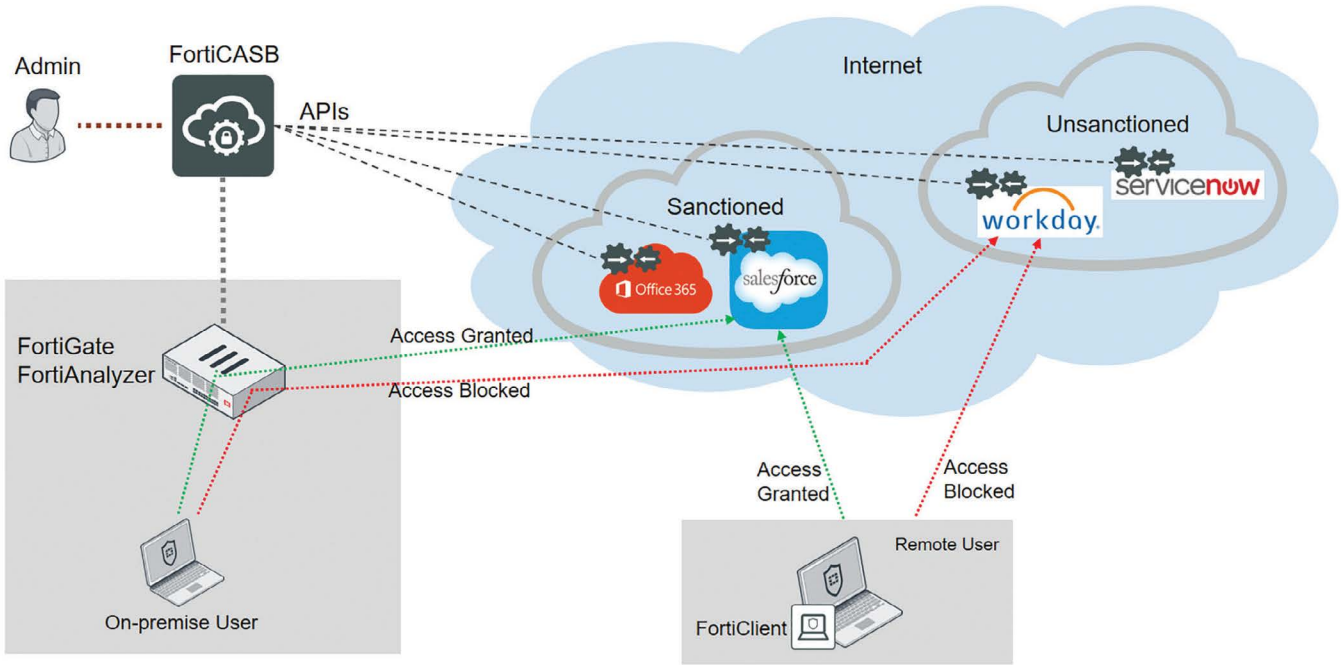

FIGURE 3: FortiCASB provides protection for on-premises and remote access to SaaS applications through its integration with FortiClient.

FortiCASB can also apply controls based on the individual user. Figure 3 uses Salesforce, one of the most widely adopted SaaS applications, as an example. FortiCASB directly connects to Salesforce using an API to establish visibility and control over the platform. The security administrator logs into FortiCASB and establishes access rights for the Salesforce application using a master account for the organization. This includes defining privileges and data-protection policies.

Here, FortiCASB provides protection for both on-premises and remote user access to Salesforce. Each user account is fully protected, regardless of the location where they log into their account or which device they use. Additionally, FortiCASB scrubs the data already stored on Salesforce to ensure information and files are secure and follow all established business policies.

Compliance Report and Tracking

Unapproved SaaS applications create a whole new level of compliance issues. Some firewalls provide visibility for in-line traffic, but there is no way for them to perform audits on unknown services used by remote users. But once all cloud-based applications and services across the organization are visible and controlled with set policies via FortiCASB, they can also be accounted for in terms of compliance.

Beyond monitoring files at the SaaS application API layer, where all direct activity on the cloud application is recorded, FortiCASB follows these files in case they flow through other communication channels beyond the enterprise perimeter. This, in turn, supports comprehensive detection, analysis, and reporting of cloud-based data to ensure that the organization operates within all applicable laws and standards for security and data privacy—at all times and in all places.

In conjunction with the FortiGate NGFW, FortiCASB provides a set of predefined compliance reports. Regulations and compliance standards covered include the EU's General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley/Control Objectives for Information and Related Technologies (SOX/COBIT), Payment Card Industry Data Security Standard (PCI DSS), International Organization for Standardization (ISO) 27001, National Institute of Standards and Technology (NIST) 800/53 U.S. Federal controls, and NIST 800/171 U.S. Non-Federal controls.

Enhancing the Benefits of Cloud-based Applications

To support the enterprise's growing dependence on SaaS, Fortinet combines the advanced visibility capabilities of FortiCASB with the defensive features of FortiGate NGFWs (as well as other key Security Fabric elements like FortiAnalyzer and FortiClient endpoint protection) to deliver complete visibility, control, and compliance reporting for cloud-based applications, services, and data. Tight integration with the Security Fabric helps FortiCASB deliver comprehensive detection, reporting, and protection capabilities that enable enterprises to reduce the risks of both authorized and unauthorized SaaS applications and effectively control application usage on or off the network.

[1] Louis Columbus, "Roundup Of Cloud Computing Forecasts And Market Estimates," Forbes, September 23, 2018.

October 24, 2019 10:24 PM

338980-A-0-EN

D:\Fortinet\Solution Briefs\blue solution briefs\Refresh - Protecting Enterprises from the Risks\sb-protecting-enterprises-from-the-risks-of-software-as-a-service