FortiCASB-SaaS Visibility and Control for the Cloud

Executive Summary

Software-as-a-Service (SaaS) applications are a key factor in the business agility that the marketplace requires today. However, the ease with which lines of business can stand up applications—with or without help from IT—can result in inconsistent policy and usage management, inadequate security controls, and siloed access control. These issues can significantly increase an organization's risk. Powered by Fortinet solutions, organizations have a transparent view of all applications from a single console, consistent security policies and practices across the network, and best practices regarding governance and compliance.

SaaS Visibility and Control From FortiCASB

- Full visibility of SaaS application usage
- Malware and sensitive data monitoring
- Consistent governance and policy management
- Resource consumption visibility and control
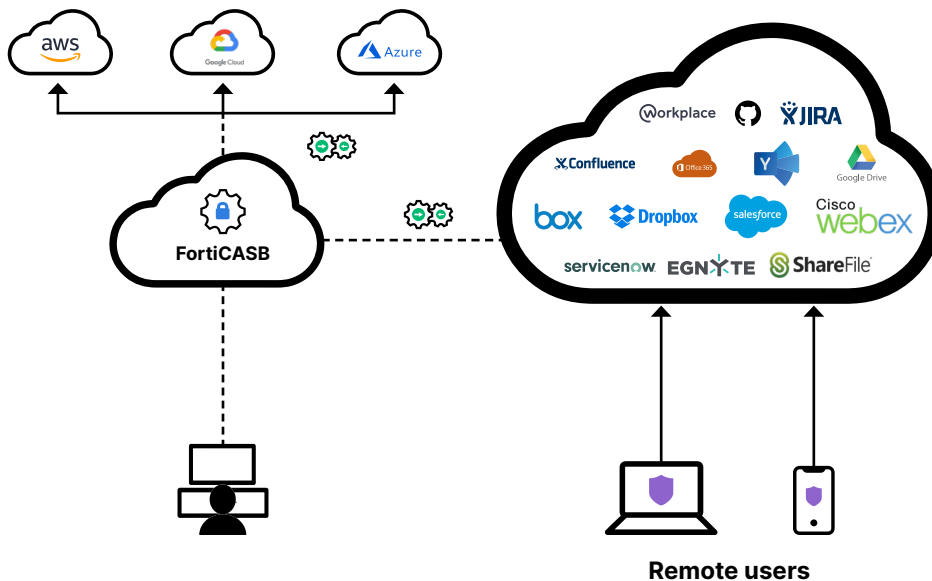- Full support for major SaaS applications

Figure 1: FortiCASB-SaaS management API for uniform application visibility and control.

Instant IT for Anyone With a Credit Card

IT teams and line-of-business leaders alike have embraced SaaS as a flexible, scalable, cost-effective way to deploy applications needed by the business. Without the need to deploy and manage applications on an on-premises server, line-of-business leaders, department managers, and even individual program owners can procure and manage their applications—at a fraction of the time and cost required to roll out an on-premises service.

Despite these clear benefits, the broad embrace of SaaS over the past decade has resulted in virtually unmanageable cloud sprawl at many organizations.[1] Often, security teams have a siloed view of SaaS applications and may have no visibility at all into some.

Security controls, configurations, and other policies are inconsistent, increasing risk to the organization. And with major SaaS providers primarily focused on delivering business requirements and functionality, they may not be fully armed with the proper guidance to secure these applications properly.[2] This puts a greater need for organizations to implement a centralized, comprehensive approach to SaaS security by users of their applications.

Achieving Uniform Governance Across All SaaS Applications With Fortinet

The FortiCASB-SaaS Cloud Access Security Broker service leverages application programming interfaces (APIs) for SaaS applications to monitor all activity and configuration settings across all SaaS services. It provides centralized, detailed visibility into usage, enabling organizations to have uniform access control, resource consumption, configuration, and security policies. It scans stored files for malware and advanced persistent threats, reducing the risk that these files would spread through the network.

Centralizing control of SaaS applications with Fortinet enables organizations to deploy best practices concerning compliance and governance, helps them protect sensitive data in these applications from advanced threats, and brings shadow IT applications under centralized control. It also enables consistent application-control policies across all of the company's branch locations. Providing adequate levels of security also helps reduce latency and provide the level of performance that users expect.

Leveraging Visibility To Provide Protection

SaaS applications bring a variety of benefits to businesses, including quick deployment, minimal management hassles, and scalability on the fly. But left unmonitored, they present multiple security risks. Fortinet FortiCASB provides full visibility and control so that organizations can leverage the benefits of SaaS without increasing risk.

---

[1] Emil Sayegh, "The Dangers Of Cloud Sprawl: When There's Too Much Cloud Going On," Forbes, April 28, 2020.

[2] Ian Sharpe, "How secure are your SaaS applications?," Cloud Security Alliance, October 19, 2020.

November 2, 2021 7:19 AM

377060-A-0-EN