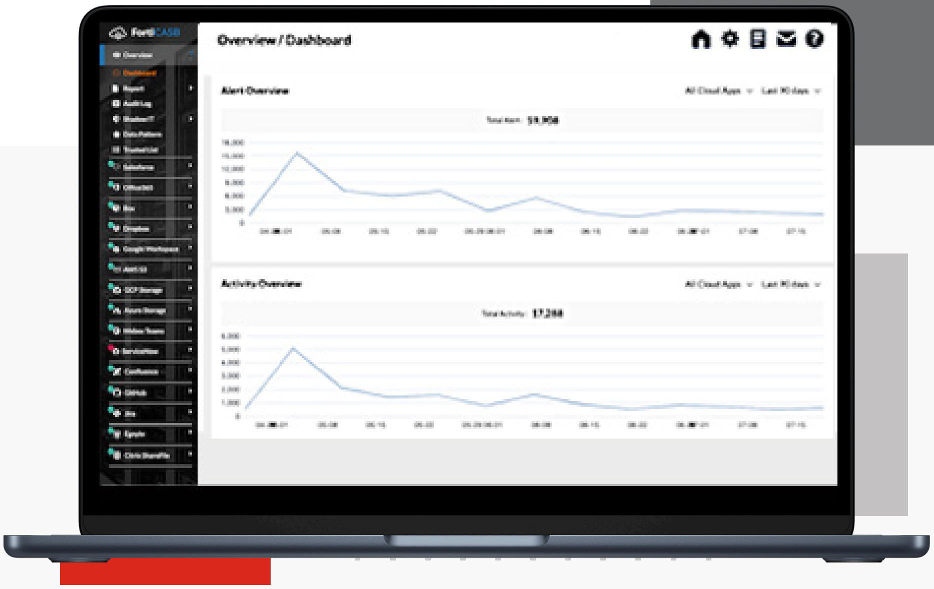
FORTINET

Data Sheet

FortiCASB™



Key Features

FortiCASB provides visibility and protection for SaaS applications

- Centralized visibility
- Extends security protection from on-prem to the cloud
- Simplify compliance against many industry standards such as PCI DSS, HIPAA, SOC2 and GDPR with predefined policies and reports
- Monitor user behaviors and activities and manage user entitlement
- Data loss prevention (DLP) and threat detection tools
- FortiGuard integration for advanced threat detection

Visibility, Insight, and Control for SaaS Applications and Data

Many organizations have enabled the use of software as a service (SaaS) cloud-based applications and services to increase productivity and efficiency. Consequently, this ability has also expanded the attack surface with the proliferation of devices, locations and applications. Security solutions must protect all the data and applications that make up the new landscape. And in order to set the appropriate security controls, Organizations will need visibility to all the devices, applications, users and events occurring in their environment.

Available in

Cloud

Feature Highlights

FortiCASB is a Fortinet-developed cloud-native Cloud Access Security Broker (CASB) and Data Security Policy Management (DSPM) solution designed to provide visibility, compliance, data security, and threat protection for cloud-based services employed by an organization. FortiCASB provides policy-based insights into users, behaviors, and data stored in major SaaS applications. For organizations that are required to comply with regulatory requirements and industry mandates, FortiCASB has predefined policies for common regulatory standards to detect violations along with reports for auditing and tracking.

Additionally FortiCASB provides a granular Data Security Policy module that allows organizations to customize the response to different data related activities such as sharing, editing or downloads based on the actual content and characteristics of the data.

Equipped with predefined out-of-the-box security policies, FortiCASB monitors for multiple security risks, examples depicted at left.

Malicious Traffic

Malware

Data Exfiltration

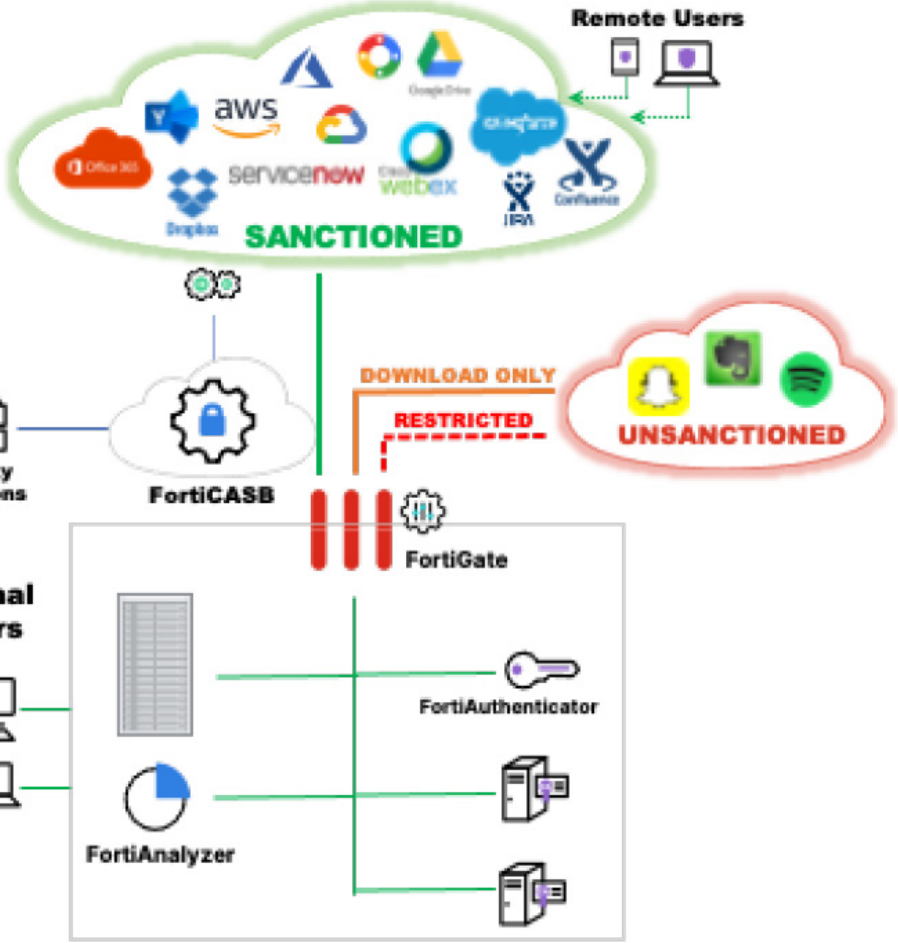
Suspicious User Activity

Compliance Violations

Sensitive Data Leakage

API-based Approach

Using an API-based approach, FortiCASB is directly connected to leading SaaS providers to access usage and data stored in the cloud. This connection enables administrators the ability to scan provisioned cloud resources for potential threats as well as SaaS application data for threats, proprietary information, or sensitive customer records. This approach ensures that all users of the organization's SaaS applications are monitored and protected by FortiCASB no matter where they are or what device they are on.



Feature Highlights

Fortinet Security Fabric

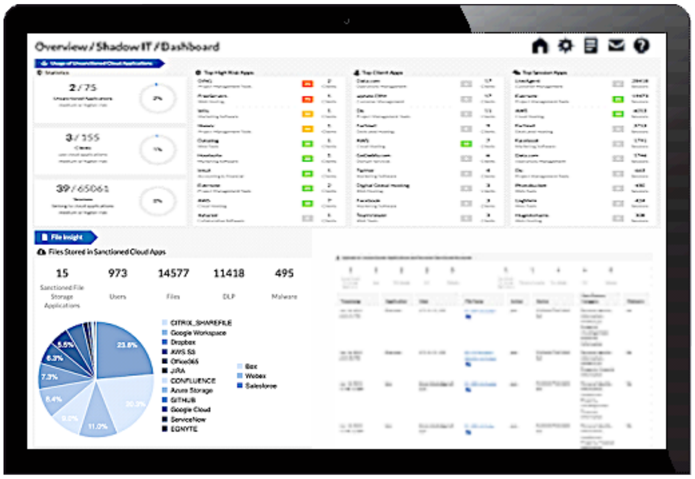
FortiCASB is a component in the Fortinet Security Fabric and an integral part of the Fortinet CASB and SaaS security solution. Fortinet CASB solution is comprised of the FortiGate and FortiProxy powered inline CASB capabilities as well as the FortiCASB API CASB and DSPM protection.

Data Protection

FortiCASB offers a highly customizable suite of data protection capabilities that help protect from data related breaches and compromises by providing a granular data protection policy engine. Using the broad set of FortiGuard DLP signatures as well as a customizable pattern and policy engine, in conjunction with an advanced and accurate DLP content analysis engine organizations can achieve the best possible data security posture to meet their needs. FortiCASB can be configured for nearly any policy to meet data protection needs and provide tailored reports on DLP activities. For organizations that must meet compliance standards, FortiCASB offers predefined reports for standards including SOX, GDPR, PCI, HIPAA, NIST, and ISO27001, to provide organizations visibility into policy violations so they can be tracked and remediated.

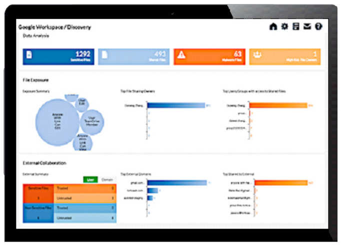
Shadow IT Discovery

FortiCASB has seamless integrations with FortiGate and FortiAnalyzer to provide a comprehensive view of the risk posture and usage for all sanctioned and unsanctioned (Shadow IT) cloud applications used in an organization, enabling administrators with insights to enforce policy-based access controls for risky applications.



FortiCASB Shadow IT Dashboard

Feature Highlights



FortiCASB Usage and File Insight Overview

User Insights and Policies

FortiCASB offers many tools to provide insights into user behaviors and their activities on cloud-based applications. Administrators can monitor usage as needed and have the ability to view user entitlements, dormant users, and conduct detailed configuration assessments.

FortiGuard Integration for Advanced Threat Protection

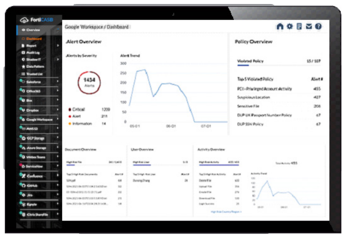
FortiCASB automatically includes award-winning FortiGuard and DLP services to scan files stored in the cloud. This service is at no extra cost to FortiCASB subscribers

Extendable Threat Detection Capabilities

Extend Fortinet Threat Detection Capabilities for your SaaS environment with additional solutions from the Fortinet Security Fabric. The Fortinet Security Fabric portfolio provides a broad range of security solutions that can be implemented to increase SaaS security. These solutions can be implemented separately or along with FortiCASB.

The Fortinet FortiCNP solution provides insights into the security and risk posture for cloud workloads, user activity, resources, network traffic, and data storage. For organizations leveraging container-based workloads, the FortiCNP Container Protection automates and embeds security throughout the software development lifecycle, allowing DevOps teams to focus on more critical aspects of the application build cycle.

FortiSASE SIA extends networking and security capabilities to support a “work from anywhere” workforce by enabling visibility, security, and orchestrated policy control for secure internet access regardless of their location, ensuring consistent protection across dynamic and distributed networks.



FortiCASB SaaS Analytics

Advanced SaaS Analytics

FortiCASB offers a comprehensive set of analysis tools to manage SaaS usage and data storage. Detailed user monitoring helps to quickly identify risks and automated tools help to manage incidents as they occur.

Cloud Applications Support

FortiCASB offers a full API integration with leading SaaS and cloud services that include AWS, Azure Storage, Box, Citrix ShareFile, Confluence, Dropbox Business, Egnyte, Facebook Workplace, Github, Google Workspace, Google Cloud Storage, Jira, Office 365, Salesforce, SAP, ServiceNow, and Cisco Webex Teams.

Ordering Information

The FortiCASB SaaS Protection license is required to enable visibility and protection for SaaS applications and data.

FortiCASB Cloud Platform Protection add-on license is required for visibility into data stored in public cloud environments.

Product	SKU	Description
FortiCASB SaaS Protection	FC1-10-FCASB-145-02-DD	FortiCASB SaaS Protection 100 User SKU. Includes 1TB of Data Security scanning capacity per year.
	FC2-10-FCASB-145-02-DD	FortiCASB SaaS Protection 500 User SKU. Includes 5TB of Data Security scanning capacity per year.
FortiCASB Data Protection	FC1-10-FCASB-307-02-DD	FortiCASB Data Protection 100GB, add-on subscription license for malware/sensitive data scan/DLP on SaaS platforms, requires one of FC1-10-FCASB-145-02-DD or FC2-10-FCASB-145-02-DD or FortiClient ZTNA licenses.
	FC5-10-FCASB-307-02-DD	FortiCASB Data Protection 1 TB, add-on subscription license for malware/sensitive data scan/DLP on SaaS platforms, requires one of FC1-10-FCASB-145-02-DD or FC2-10-FCASB-145-02-DD or FortiClient ZTNA licenses.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.

FORTINET®

www.fortinet.com

April 17, 2024