Security-as-a-Service with FortiCloud

Key Elements and Common Use Cases to Better Secure and Manage Your IT Infrastructure
## Contents

Executive Summary .................................................. 3  
The Need for Security Delivered as-a-Service ................. 3  
FortiCloud: The key elements of a Security-as-a-Service product suite ............... 4  
  FortiGate Cloud ................................................. 4  
  FortiWeb Cloud .................................................. 4  
  FortiCWP .......................................................... 5  
  FortiCASB ......................................................... 5  
  FortiMail Cloud .................................................. 5  
  FortiSandbox ...................................................... 5  
Common Use Cases for FortiCloud ................................ 6  
  Cloud-based Management ........................................ 6  
  Securing and Managing Cloud-only Infrastructures ............. 6  
  Securing Small and Medium Businesses ......................... 6  
  Enhance On-premises Security with FortiCloud .................. 7  
Solution ............................................................. 7  
Conclusion ............................................................ 7
Executive Summary

Organizations large and small are grappling with the cost and the complexity of securing their infrastructure. Security delivered “as-a-service” can improve your overall security posture, protect cloud-based workloads, and ease the burden of managing security policies. It can also help simplify global deployments and policy management without the cost of additional hardware for management systems.

FortiCloud has been designed to meet the needs of businesses of all sizes as they seek more efficient and effective ways to secure their applications and infrastructure, both on-premises and in the cloud.

The Need for Security Delivered as-a-Service

It has often been noted that the concept of perimeter-based security—security systems that seek to harden all ingress and egress points—is passé as the rise of the Internet of Things and mobile computing has moved the “perimeter” from gateway devices to nearly any device. Security professionals often say that the perimeter is everywhere. Therefore, the concept of on-premises security must evolve as the distinction between cloud and data center and devices fades. Today, your desktop, laptop, and even your mobile device can receive and serve content to sites and users anywhere connected to the internet. Not only is the perimeter everywhere, the cloud itself is also everywhere—and so your security must be everywhere as well.

Traditional security solutions such as next-generation firewalls and endpoint protection will always be critical for securing your campus and your data center. But these traditional solutions must also be enhanced with cloud-based security offerings to be truly effective in the modern era.

The truth is, there is nothing new about cloud-based tools enhancing local security. Nearly every antivirus solution sold over the past 20 years, for example, has depended on updated signature files and on various types of threat feeds delivered from the cloud. But even as distinctions remain between on-premises and the cloud, the need for cloud-based security solutions continues to grow.

Cloud-based, or at least cloud-“enhanced,” security has the advantages of being accessible and manageable from anywhere, as well as highly scalable. An email security product in the cloud won’t be overwhelmed by a surge of email the way an on-premises appliance might. And a cloud-based sandbox will be able to scale as the number and complexity of files to be examined grows. Even on-premises solutions can benefit from integration with tools that are better sourced in the cloud, such as artificial intelligence (AI)-based threat analytics. Finally, many organizations consume at least some cloud-based services such as Microsoft 365, Salesforce, or Google Drive. These applications are best secured by a cloud access security broker (CASB) solution.

FortiCloud Offerings:

- FortiCare
- FortiGate Cloud
- FortiCASB
- FortiCWP
- FortiManager
- FortiAnalyzer
- FortiSwitch Cloud
- FortiToken
- FortiAP Cloud
- FortiPresence
- FortiMail Cloud
- FortiExtender
- FortiWeb Cloud
- FortiInsight
- FortiClient
- FortiConverter
- FortiGSLB
- FortiPAM
FortiCloud: The key Elements of a Security-as-a-Service Product Suite

FortiCloud is a broad platform for delivering Security-as-a-Service. Unlike competitive approaches, FortiCloud addresses all elements of securing cloud-native applications, and it does so in a manner that is both effective and scalable. FortiCloud provides three categories of tools:

- Tools that deliver Security-as-a-Service such as FortiWeb Cloud and FortiCASB
- Tools for managing other security tools such as FortiGate Cloud and FortiManager
- FortiCare for tracking assets, licensees, RMAs, support tickets, and more

FortiCloud is an important part of the Fortinet Security Fabric. The Fortinet Security Fabric ties Fortinet security solutions together to collect, coordinate, and respond to malicious behavior wherever it occurs.

The core of a security fabric is an upstream FortiGate located at the edge of the network, with several internal FortiGates functioning as internal segmentation firewalls (ISFWs). A Security Fabric can be used to coordinate the behavior of other Fortinet products in your network, including FortiAnalyzer, FortiManager, FortiClient, FortiClient EMS, FortiWeb, FortiSwitch, and FortiAP.

It is the Security Fabric that sets Fortinet apart from other security vendors. The Fortinet Security Fabric covers:

- Endpoint client security
- Secure wired, wireless, and VPN access
- Network security
- Data-center security (physical and virtual)
- Application (OTS and custom) security
- Cloud security
- Content (email and web) security
- Infrastructure (switching and routing) security

Cloud security may only be one part of the broader issue of cybersecurity, but its importance can’t be overstated. Key components of the FortiCloud offering suite for cloud security include:

**FortiGate Cloud**

FortiGate Cloud is a cloud-based management platform for your FortiGate Unified Threat Management devices. It simplifies the initial deployment, setup, and ongoing management while providing you with visibility of your entire deployment. It enables FortiGate to manage software-defined wide-area networking (SD-WAN), unified threat management (UTM) features, FortiSwitch, and FortiAP deployments to extend functionality, and delivers rich analytics and actionable reports. FortiGate Cloud is generally used for managing Fortinet solutions at small and medium businesses.

**FortiWeb Cloud**

Designed for web applications that demand the highest level of protection, FortiWeb Cloud provides robust security that is simple to deploy, easy to manage, and cost-effective. With FortiWeb Cloud, DevOps teams and security architects alike have access to the same proven detection techniques used in other FortiWeb form factors without the need for costly capital investments. Unlike solutions that simply spin up virtual machines for each customer and increase the management workload on already-stretched teams, FortiWeb Cloud delivers a true Software-as-a-Service (SaaS) solution that leverages the leading public clouds to offer highly scalable and low-latency application security.
At the heart of FortiWeb is an AI-based detection engine that uses machine learning to identify requests that stray from normal patterns, taking action to protect applications from known and unknown zero-day threats. FortiWeb also integrates with FortiSandbox, which further utilizes AI to detect new or previously unknown threats as well as the MITRE ATT&CK framework, OWASP Top 10 vulnerability inspection, and real-time threat feeds from FortiGuard Labs.

FortiWeb will protect web-based applications and the application programming interfaces (APIs) they rely on. FortiWeb Cloud is a true SaaS application, delivered from the cloud, allowing you to pay only for what you use, and requiring no additional hardware.

FortiCWP

FortiCWP offers security administrators and DevOps teams the ability to evaluate their cloud configuration security posture, detect potential threats originating from misconfiguration of cloud resources, analyze traffic across cloud resources (in and out of the cloud), and evaluate cloud configuration against best practices. It enables the ability to manage risk throughout multi-cloud infrastructures, provides regulatory compliance reporting, and integrates remediation into the cloud infrastructure life-cycle automation framework.

FortiCASB

FortiCASB is a Fortinet-developed cloud-native cloud access security broker (CASB) subscription with an extensive set of cloud security posture management (CSPM) capabilities that are 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 as well as comprehensive reporting tools. FortiCASB offers a full API integration with leading SaaS and cloud services including Microsoft 365, Microsoft OneDrive, Google Drive, Salesforce.com, Dropbox, and Box as well as compliance reporting and Shadow IT detection.

FortiMail Cloud

FortiMail Cloud delivers comprehensive email security to protect your employees and data from cyberattacks. It provides the industry’s most independently validated security effectiveness. Delivered as a SaaS solution, it is easy to enable and requires minimal ongoing management—most of which can be easily extended to end-users. FortiMail delivers a greater-than-99.5% spam detection rate and multiple layers of malware detection, all with extremely few false positives. Fully managed by Fortinet, FortiMail Cloud allows you to focus on your business while Fortinet secures your email.

FortiSandbox

Top-rated AI-powered FortiSandbox is part of the Fortinet breach protection solution, which integrates with the Fortinet Security Fabric platform to address rapidly evolving and more targeted threats including ransomware, crypto-malware, and others across a broad digital attack surface. Specifically, it delivers real-time actionable intelligence through the automation of zero-day, advanced malware detection and response. FortiSandbox improves zero-day threat detection efficacy and performance by leveraging two machine-learning models—patent-pending enhanced random forest with boost tree and least squares optimization applied to static and dynamic analysis of suspicious objects. It also accelerates threat investigation and management processes by adhering to standards based on the MITRE ATT&CK framework for malware reporting.
Common Use Cases for FortiCloud

Cloud-based Management

Organizations of all sizes are seeking more efficient and more cost-effective ways to access and manage devices. FortiCloud provides a web-based portal to manage Fortinet physical and virtual devices—both on-premises and in the cloud. It also provides access to FortiCare for device-based support, providing firmware updates, technical support, and foundational FortiGuard subscriptions for dynamic policies. Components of this use case listed below must be purchased separately.

Key Components

FortiCare—Managed Fortinet devices, account-based services, access to professional services, licenses, support tickets, RMAs, and more

FortiManager Cloud—Simplify zero-touch provisioning and management with a rich set of tools to centrally manage any number of devices from a single console

FortiAnalyzer Cloud—Cloud-based system analytics, events management, and health monitoring services

FortiAP Cloud—Centralizes the life-cycle management of standalone FortiAPs with a simple, intuitive, and easy-to-use cloud interface

FortiSwitch Cloud—Centralizes the life-cycle management of standalone FortiSwitch Ethernet switches with a simple, intuitive, and easy-to-use cloud interface

companies are prioritizing cloud-based services over deploying more hardware. FortiCloud offerings deliver Security-as-a-Service from the cloud. FortiCloud includes tools for protecting cloud-based data and workloads as well as helping to secure the use of SaaS-based applications such as Salesforce and Microsoft 365. FortiCloud also provides cloud-based management for your Fortinet physical and virtual devices. Components of this use case listed below must be purchased separately.

Key Components

FortiWeb Cloud—SaaS-based web application firewall

FortiCWP—SaaS-based cloud-workload cloud data protection

FortiCASB—Secure SaaS applications such as Microsoft 365 and Salesforce and Shadow IT discovery

FortiMail Cloud—SaaS-based, top-rated secure email gateway

Public Clouds

On-premises

Remote

MSSP

Securing Small and Medium Businesses

Small and medium businesses face the same threats as large enterprises—except they have fewer resources and personnel to handle them. The FortiCloud offering suite delivers Security-as-a-Service from the cloud. It includes easy-to-configure and easy-to-use tools for protecting cloud-based data and workloads as well as helping to secure the use of SaaS-based applications such as Salesforce and Microsoft 365. FortiCloud also provides cloud-based management for your Fortinet physical and virtual devices. Components of this use case listed below must be purchased separately.

Securing and Managing Cloud-only Infrastructures

The cloud can help organizations move faster, be more agile, and reduce capital expenses. To maximize these benefits, many
Key Components

**FortiGate Cloud** — A lightweight, cloud-based management platform for your FortiGate Unified Threat Management devices. Use FortiGate Cloud to enable management of SD-WAN functions, UTM features, as well as FortiSwitch and FortiAP deployments to extend functionality. FortiGate Cloud also delivers rich analytics and actionable reports.

**FortiWeb Cloud** — SaaS-based web application firewall

**FortiCASB** — Secure SaaS applications with Shadow IT discovery

**FortiMail Cloud** — SaaS-based, top-rated secure email gateway

Enhance On-premises Security with FortiCloud

While many organizations are moving applications and the security they require into the cloud, most companies still maintain data centers, offices, and branches. FortiCloud augments on-premises security, enhancing them with real-time threat feeds, AI-based threat analysis, cross-platform management, and scalable security offerings.

Key Components

**FortiSandbox Cloud** — Files can be sent from Fortinet devices or other network gear and safely scanned and executed. FortiSandbox uses real-time threat feeds, artificial intelligence, and the MITRE ATT&CK framework to detect threats both known and unknown.

**FortiEDR** — Delivers advanced, real-time threat protection for endpoints both pre- and post-infection. It proactively reduces the attack surface, prevents malware infection, detects and defuses potential threats in real time, and can automate response and remediation procedures with customizable playbooks. FortiEDR features multitenant management in the cloud, receives cloud-based threat feeds, and integrates with FortiSandbox, which can be on-premises or in the cloud.

**FortiCASB** — Secure SaaS applications such as Microsoft 365 and Salesforce and Shadow IT discovery

**FortiMail Cloud** — SaaS-based, top-rated secure email gateway

Solution

FortiCloud delivers Security-as-a-Service from the cloud, augmenting on-premises solutions with up-to-the minute threat feeds, AI-based threat analysis, cross-platform management, and integrated service management.

Conclusion

Traditional security tools are enhanced by cloud-delivered services. And, of course, traditional security devices are ill-suited for securing cloud-based applications and data. The solution is security and threat feeds and management—all delivered from the cloud. The future of security is not only in better detection and remediation but also in new, cloud-native architectures able to weave protection for all devices into a security fabric that can support any application anywhere with the same security everywhere.