DATA SHEET

FortiCloud™

Hosted Wireless and Security Device Provisioning, Management and Analytics

FortiCloud

Hosted Wireless and Security Device Provisioning, Management and Analytics

FortiCloud is a cloud-based provisioning, configuration management and analytics service for FortiGate®, FortiWiFi® and FortiAP® product lines. It gives you the ability to quickly get up and running with Fortinet products while maintaining centralized control and visibility of your network. Since FortiCloud is a hosted solution, there is no additional hardware or software to acquire or deploy at your data center. In addition, FortiCloud is free of charge — optional subscriptions are available for customers who require extended log retention and advanced features.

Industry's first Cloud-managed Secure Wireless Access Point

FortiAP-S Indoor Access Points are cloud-managed access points with enterprise-class capability. The FortiAP-S access point delivers gigabit performance, security and reliability to meet the growing demand of pervasive WiFi in SMBs and distributed enterprises.

A Cloud WiFi service with comprehensive threat protection. With Fortinet's award-winning security technology embedded in the AP, the FortiAP-S series provides the most compact solution for complete content and application security provisioned and managed remotely from the cloud through FortiCloud.

FortiCloud service simplifies ease-of-deployment, operational efficiency and total cost of ownership.

Key Features and Benefits

- One-touch device provisioning with FortiDeploy™
- Centralized configuration management
- Traffic and application visibility
- Filtering and drill-down analytics
- Secure hosted log retention
- Cloud-based APT sandboxing
- Rogue AP detection
- AP device mapping and client usage
- Custom and preconfigured reporting
- Advanced AP configuration capabilities
- Consistent backup and upgrades

How FortiCloud Addresses Key Enterprise Wireless and Security Challenges

Challenge	Solution
Facilitating turnkey **provisioning** of wireless and security devices at remote sites when on-site configuration expertise is unavailable	FortiAPs, FortiWiFis and FortiGates include FortiCloud registration functionality in their firmware that allow individual or multiple devices to provision themselves with minimal on-premise expertise
Keeping initial investment **costs** down and preference for a consumption-based, OPEX model	FortiCloud uses a Software as a Service (SaaS) model that alleviates the need for upfront capital purchases
Maintaining single pane of glass management for overseeing a wireless and security infrastructure	FortiCloud provides control over wireless and security devices while providing granular visibility and reporting at the same time
Protecting the network from advanced threats and allowing granular access controls and application usage policies	Leveraging cloud sandboxing technology from FortiGuard, FortiCloud is able to inspect potentially malicious payloads for zero-day threats
Investing in a **future-proof** wireless and security solution that will scale with your business	As FortiCloud is cloud-based, it can grow as your business grows and accommodate additional event log storage as needed

FEATURES

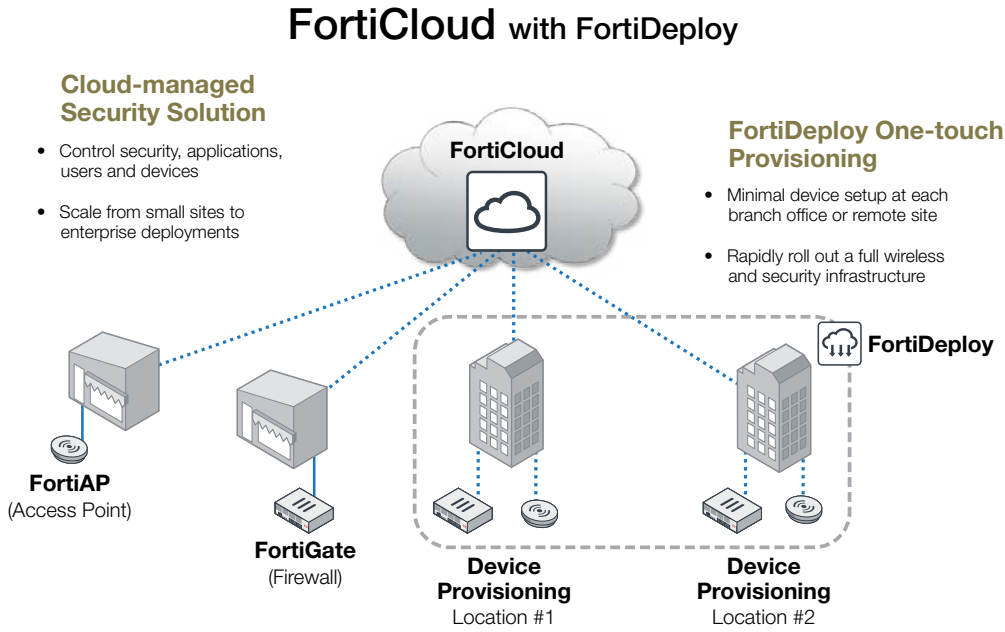
FortiDeploy

Initial configuration of firewalls and access points can be a difficult proposition, often requiring expert staff on site to configure each device individually. FortiDeploy greatly simplifies initial configuration and onboarding by providing one-touch provisioning when devices are deployed, locally or remotely. FortiDeploy provides deployment for FortiAPs into a Cloud AP Network, and automatic connection of FortiGates to be managed by FortiCloud.

Hundreds of FortiGates or FortiAPs can be provisioned by using a bulk key in distributed environments, such as large retail or education networks. Once a communication tunnel is established, FortiCloud leverages provisioning profiles and setup wizards to quickly configure managed devices as required.

Configuration and device management from a single pane of glass

Consistent configuration of the devices within your network is essential to maintaining an optimal performance and security posture. FortiCloud provides a central web-based management console to control Fortinet devices. Device settings such as IP addresses or SSIDs can be centrally configured for individual devices or pushed to multiple devices. Configuration backups are kept in FortiCloud to assist with replacement or recovery efforts. Device firmware updates can also be centrally managed and controlled, thereby ensuring uniformed policy enforcement and allowing you to take advantage of the latest features.



FortiCloud is able to manage FortiAP wireless access points and FortiGate firewalls from a centralized, cloud-based management console.

FEATURES

Hosted log retention and cloud-based storage

Log retention is an integral part of any security and compliance best practice, but administering a separate storage system can be burdensome and costly. FortiCloud takes care of this automatically and stores your valuable log information securely in the cloud. Depending on your device, you can easily store and access different types of logs including traffic, system, web, applications and security events.

Wireless health and oversight at your fingertips

If you're deploying FortiAP wireless access points, you'll want to make sure your WiFi infrastructure stays up and running. FortiCloud provides information about your access point uptime along with performance metrics to ensure your WiFi is operating smoothly. Wireless health statistics are tracked along with client connection data. FortiAP devices can even be rendered on an interactive map to give you a complete view of your wireless infrastructure.

Full control over wireless guest access

Managing wireless guest usage can be cumbersome if administered separately at each remote site, with simple misconfigurations potentially opening up your network to security threats. For organizations in hospitality and retail in particular, centralized guest access management is a must have. FortiCloud allows you to fully control how guests access your wireless network and includes features such as customizable captive portals for authentication.

Built-in protection from APTs with FortiGuard sandboxing technology

If you're deploying FortiGates, you can harness the power and expertise of Fortinet's FortiGuard Labs global threat research team to inspect potentially malicious files. FortiGate firewalls can upload suspicious files to FortiCloud, where it will execute the file in a sandboxed environment and analyze the resulting behavior for risk. If the file exhibits risky behavior or is found to contain a virus, the FortiGuard team creates a new virus signature and adds it to the FortiGuard anti-malware database. You can then review the status of any files you submit from within your FortiCloud console.

Instant security intelligence and analytics with FortiView

In order to place better security controls on your network, you must first know how it is being utilized. FortiCloud's extensive set of dashboards gives you an immediate view of FortiGate usage, including a breakdown of network traffic and bandwidth usage.

FortiCloud analytics provides you with drill-down and filtering functionality to instantly determine how applications, websites, user and threats are impacting your network.

Exceptional network visibility with FortiCloud reporting

Periodic review of network and security activity is essential in order to keep costs down and security breaches at bay. Reporting allows you to be proactive about optimizing your network and satisfying executive staff scrutiny. FortiCloud provides both preconfigured and custom reports to give you the information you need for your specific reporting and compliance requirements. Reports can be either ad-hoc or scheduled and can be either downloaded or emailed to interested parties.

FortiCloud transport security and service availability

FortiCloud encrypts all communication, including log information, between your FortiGate devices and the cloud. Fortinet deploys redundant data centers to give the FortiCloud service its high availability. Fortinet has also used its years of experience in protecting sophisticated networks around the world to implement operational security measures that make sure your data is secure and only you can view or retrieve it.

FortiGuard Indicator of Compromise (IOC)

FortiGuard Indicator of Compromise (IOC) is an automated breach defense system that continuously monitors your network for attacks, vulnerabilities, and persistent threats. It provides protection against legitimate threats, guarding customer data and defending against fraudulent access, malware, and breaches. It also helps businesses detect and prevent fraud from compromised devices or accounts.

With IOC, network security controls are in place to rapidly detect and respond to security events by analyzing your network traffic, evaluating security parameters and using global intelligence.

IOC is a post-infection solution. We detect infected or highly suspicious devices in your network, analyze the risk the infected devices represent and notify you about them. As a result, you can clean up the infected device and minimize your business risk. With the advanced plan, you can instantly see which machines are infected.

IOC improves your security posture and helps safeguard your organization through accurate detection of advanced threats. Fortinet Threat Detection Service is available as an add-on service on FortiCloud.

ORDER INFORMATION AND SYSTEM REQUIREMENTS

Customers with FortiGate model 30 through 900 series receive 7 days of rolling storage (unlimited volume). To order extension for a year of unlimited storage, the following annual subscription SKUs for each device are available:

Product	SKU	Description
FortiCloud Log Retention Service	FC-10-00XXX-131-02-DD	FortiCloud Analysis and 1 Year Log Retention (XXX = model code).
FortiGuard Indicator of Compromise (IOC) FG-20 to FG-90	FC-10-90803-142-02-12	1 year FortiGuard Indicator of Compromise (IOC) for FortiGate 20 Series to FortiGate 90 Series.
FortiGuard Indicator of Compromise (IOC) FG-100 to FG-300	FC-10-90804-142-02-12	1 year FortiGuard Indicator of Compromise (IOC) for FortiGate 100 Series to FortiGate 300 Series.
FortiCloud — Premium Account	FCLE-10-FCLD0-161-02-12	1 year FortiCloud Premium Account service for a Managed Service Provider (MSP) to be able to create and manage multiple SubAccounts (multi-tenancy).

For customers who would like to add bulk provisioning for multiple devices, add the following SKU to the purchase order*:

Product	SKU	Description
FortiDeploy	FDP-SINGLE-USE	Enables zero touch bulk provisioning for your FortiGate, FortiWifi, or FortiAP products with FortiCloud. Must be purchased with every PO.

* This feature is only available on devices running FortiOS 5.2.2 and above.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
Valbonne 06560
Alpes-Maritimes, France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.9990