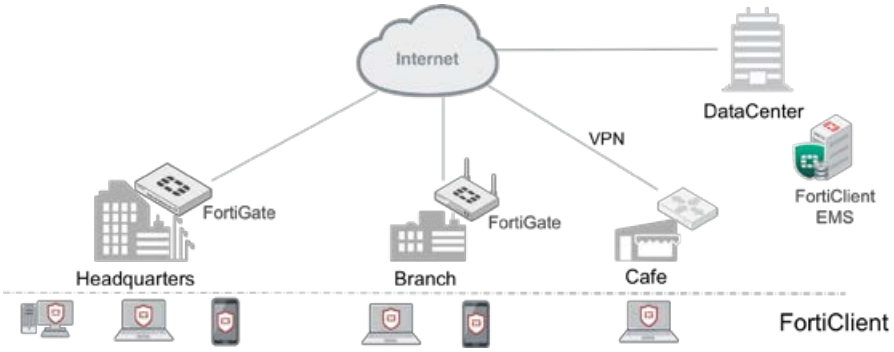
FortiClient
Advanced Endpoint Protection

FortiClient

FortiClient and Enterprise Management Server

With a multitude of devices jumping on to the network each day ranging from corporate laptops to BYOD and even IoT, organizations often struggle to identify and secure these devices that are either internal or external to the organization, increasing the risk of a potential data breach. Exacerbating this even further is the lack of security talent to manage the ever increasing number of daily alerts and the cumbersome task of responding to alerts individually often missing the one that matters the most.



Unified Endpoint Protection Platform

More than just a traditional endpoint protection, FortiClient is an endpoint protection platform that secures a multitude of different devices through a combination of endpoint visibility and control, protection and authorized access. FortiClient integrates with Fortinet's Security Fabric[1] to provide endpoint awareness, compliance and enforcement by sharing endpoint telemetry irregardless of device location e.g. corporate headquarters or a café. At its core, FortiClient automates prevention of known and unknown threats through its built-in host-based security stack and integration with FortiSandbox. FortiClient also provides secure remote access to corporate assets via VPN with native Two-Factor Authentication coupled with Single Sign On.

1. Fortinet Security Fabric: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/WP-Fortinet-Security-Fabric.pdf

Key Highlights

- Fortinet Security Fabric Ready
- Top-rated Threat Prevention
- Enterprise-scale
- Simplified Endpoint Management
- Small footprint, Lightweight Security Agent
- Customizable Feature Installation
- Broad platform coverage including Windows, Mac OS X, Chromebook, Linux, iOS and Android

HIGHLIGHTS

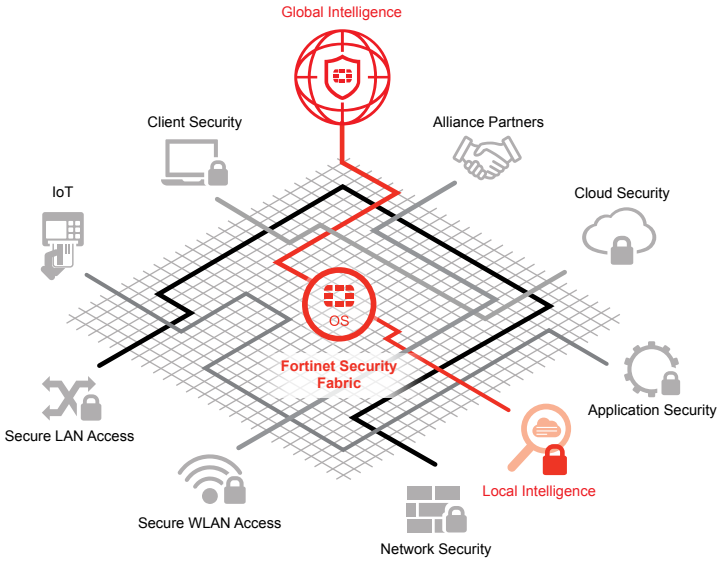
Security Fabric Integration

Unlike other disparate point solutions within a security architecture that fail to communicate with one another, FortiClient works cooperatively with Fortinet's Security Fabric. This is done by extending it down to the endpoints to secure them via security profiles, by sharing endpoint telemetry to increase awareness of where systems, users and data reside within an organization and by enabling the implementation of proper segmentation to protect these endpoints.

At regular intervals, FortiClient sends telemetry data to the nearest associated FortiGate. This visibility coupled with built-in controls from FortiGate allows the security administrator to construct a policy to deny access for example, endpoints with known vulnerabilities, or to quarantine compromised endpoints with a single click.

Endpoint Telemetry

- User detection and identification
- Device details e.g. OS details, IP address, MAC address
- Security information e.g. vulnerabilities, malware detection
- Hardware and software inventory
- Real-time visibility and monitoring



Advanced Threat Protection

Today's advanced endpoint offering still requires manual effort to assess and fully respond to unknown threats identified.

FortiClient is built on the foundational aspect of automating prevent-detect-mitigate in the threat protection lifecycle. It accomplishes this objective in two ways.

Protection against known threats

FortiClient's built-in security stack includes dynamic AV engine, Application Firewall, Vulnerability Scanner with auto-patching and Web Filter working in concert to reduce the attack surface, to prevent polymorphic and common malware, and known exploits from various attack vectors at the endpoint.

Protection against unknown threats

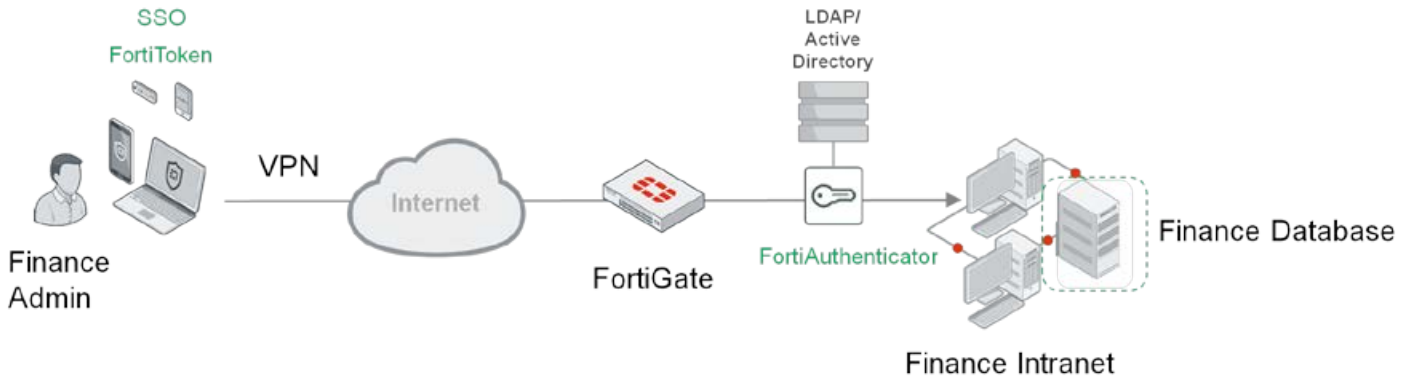
FortiClient automates the submission of unknown objects to the highly-rated FortiSandbox that provides detection through validation of an unknown file's hash, or performs dynamic analysis to determine malicious behavior. Advanced malware or Zero-day is mitigated through the sharing of intelligence with FortiClient to automatically quarantine that object as well as immunize all other endpoints, and with FortiGuard Labs to extend protection to the global community.

HIGHLIGHTS

Secure Remote Access & Mobility

Virtual Private Network (VPN) is necessary and ubiquitous to almost all organizations that offer secure remote access to corporate assets. However, it is usually considered a cumbersome and time consuming task to manage another separate product that may not be the most secure in light of today's targeted attacks. This forces organizations to explore a third party authentication mechanism and integrate into their existing VPN solution. Compounding this issue is scaling with the organization to manage user authentication and complexity of network requirements associated with this.

FortiClient solves these shortcomings by enabling users to roam freely with an always connected VPN client that supports both SSL and IPSec, native two-factor authentication (hardware- or software-based) and Single Sign On (SSO).



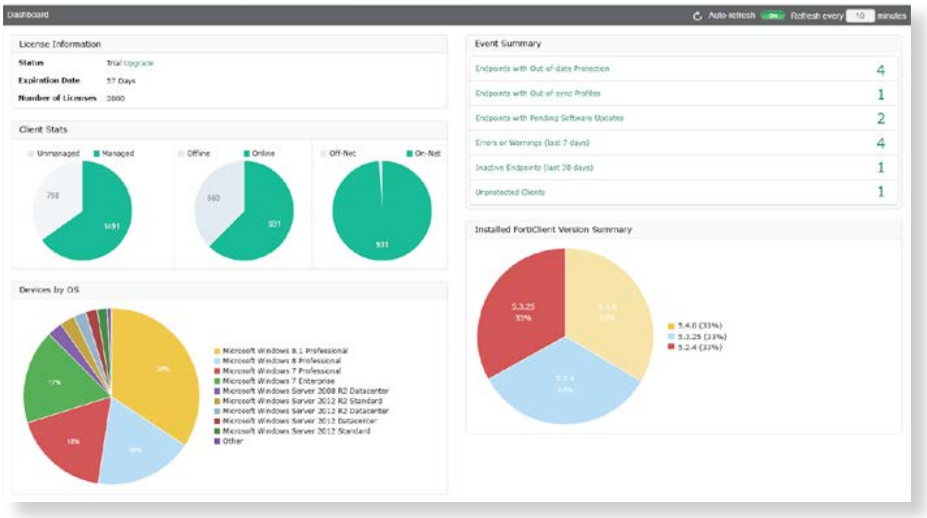
DEPLOYMENT

Simplify Management: Enterprise Management Server (EMS)

The FortiClient Enterprise Management Server (EMS) provides end-to-end endpoint deployment, registration, management and monitoring. You can centrally administer endpoint Antivirus, Web Security, Remote Access (IPsec and SSL VPN), Application Firewall, Vulnerability Scan and related advanced features. You can also remotely trigger AV scans and quarantine infected endpoints.

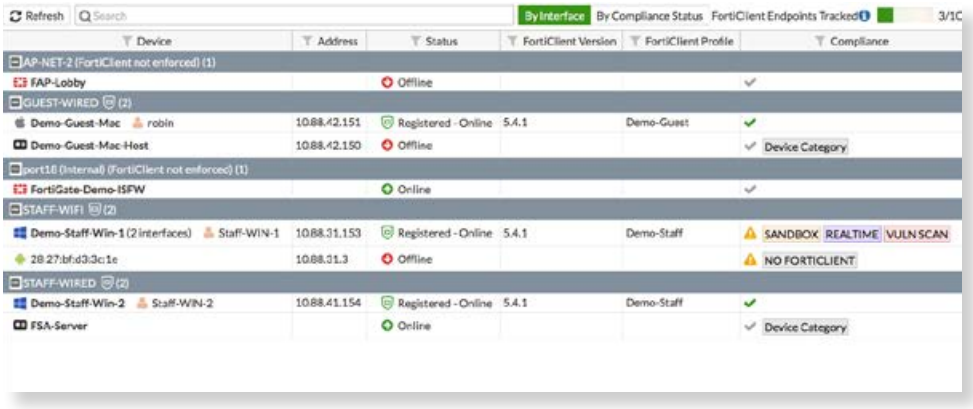
Key benefits:

- Scalable solution to centrally manage up to 100,000 endpoints
- All-in-one management — deploy, manage and monitor FortiClients on- or off-premise
- Integrate and sync with Active Directory (AD) to deploy FortiClient to all endpoints
- Easily create FortiClient security profiles with customizable features such as Application Firewall, applied to specific set of users/devices or for all users/devices
- Enforce endpoint compliance with FortiGate integration
- Centrally log and report on endpoint activity with FortiAnalyzer



Simplify Enforcement: FortiGate

In FortiOS 5.4.1 or later, FortiGate provides compliance enforcement and remediation. When a FortiClient is registered with FortiGate, settings and status can be matched against assigned profile that includes AV settings, system vulnerabilities detected, and more. FortiGate provides remediation e.g. perform an auto-update of the client, or initiate other actions to enforce endpoint compliance. In addition, FortiGate can quarantine an endpoint to allow security analyst to investigate the compromised endpoint.



FEATURES

FortiClient

	Windows	Mac OS X	Linux	Android	iOS	Windows Mobile	Chromebook
Security Fabric Components							
Endpoint Telemetry[1]	•	•		•	•		
Compliance Enforcement[1]	•	•		• (Limited)	• (Limited)		
Endpoint Audit and Remediation with Vulnerbility Scanning[1]	•						
Advanced Threat Protection Components							
File Analysis with FortiSandbox	•						
Host Quarantine Enforcement[1]	•						
Host Security and VPN Components							
Antivirus	•	•					
Web Filtering	•	•		•	•		•
Application Firewall[1]	•	•					
IPSec VPN	•	•		•	•		
SSL VPN	•	•	•	•	•	•	
Others							
Windows AD SSO Agent	•	•					
WAN Optimization	•						

[1] Requires FortiGate Endpoint License

The list above is based on the latest OS for each platform.

FortiClient EMS and FortiGate Endpoint Licenses

	FortiClient EMS License	FortiGate Endpoint Compliance License
Provisioning		
Custom Install/Rebranding Tool	•	•
Centralized Client Provisioning	•	
Client Software Updates	•	
Windows AD Integration	•	
FortiTelemetry Gateway IP List	•	
Compliance Enforcement & Security Fabric Integration		
Fortinet Security Fabric Integration		•
Security Posture Check		•
Vulnerability Compliance Check		•
Minimum System Compliance		•
Authorized Device Detection		•
Remote Control		
On Demand Antivirus Scan	•	
On Demand Vulnerability Scan	•	
Host Quarantine	•	•
Telemetry and Monitoring		
Client Information (client version, OS IP/MAC address, profile assigned, user avatar)	•	•
Client Status	•	Limited, compliance and online status
Reporting	•[2]	•[2]

[2] To FortiAnalyzer

SPECIFICATIONS

FortiClient	
Operating System Supported	▪ Microsoft Windows 10 (32-bit, 64-bit), Windows 8.1 (32-bit, 64-bit), Windows 8 (32-bit, 64-bit), Windows 7 (32-bit, 64-bit), Windows Vista (32-bit, 64-bit), Windows XP (32-bit) ▪ Windows Server 2008 R2 and Windows Server 2012, 2012 R2 ▪ Mac OS X v10.11 El Capitan, OS X v10.10 Yosemite, OS X v10.9 Mavericks and OS X v10.8 Mountain Lion ▪ iOS 5.1 or later (iPhone, iPad, iPod Touch) ▪ Android OS 4.0.4 or later (phone and tablet) ▪ Google Chromebook and Chrome Browser
Encryption	AES 128/192/256, DES/3DES
Deployment Options	Manual Interactive, Manual Silent, Active Directory GPO, Third Party Distribution Tools
Authentication Options	RADIUS, LDAP, Local Database, xAuth, TACACS+, Digital Certificate (X509 format), FortiToken
VPN Protocols	SSL (Tunnel Mode), IPsec
WAN Optimization	CIFS, FTP, HTTP, MAPI, General TCP traffiic
Connection Options	Auto Connect VPN before Windows logon, IKE Mode config for FortiClient VPN IPsec tunnel

Note: All specifcations are based on FortiClient 5.0.

FortiClient Enterprise Management Server	
Operating System Supported	▪ Microsoft Windows Server 2012, 2012 R2 ▪ Microsoft Windows Server 2008 R2
Endpoint Requirement	FortiClient version 5.2.4 or newer, FortiClient for Microsoft Windows and Mac OS X, FortiClient Chrome Extension
System Requirements	▪ 2.0 GHz 64-bit processor, dual core (or two virtual CPUs) ▪ 2 GB RAM ▪ 5 GB free hard disk ▪ Gigabit (10/100/1000BaseT) Ethernet adapter ▪ Internet access

ORDER INFORMATION

Product	SKU	Description
FortiGate FortiClient License Subscription	FC-10-C0102-151-02-12	1 Year Endpoint Telemetry & Compliance License Subscription for up to 200 clients. Includes 24x7 support and ability to download the license file, preconfigure Client, create a custom installer and rebrand.
	FC-10-C0106-151-02-12	1 Year Endpoint Telemetry & Compliance License Subscription for up to 600 clients. Includes 24x7 support and ability to download the license file, preconfigure Client, create a custom installer and rebrand.
	FC-10-C0103-151-02-12	1 Year Endpoint Telemetry & Compliance License Subscription for up to 2,000 clients. Includes 24x7 support and ability to download the license file, preconfigure the client, create a custom installer and rebrand. (Note: In 5.2 only supported for FG-500 through FG-800 and VM01-VM02 series).
	FC-10-C0104-151-02-12	1 Year Endpoint Telemetry & Compliance License Subscription for up to 8,000 clients. Includes 24x7 support and ability to download the license file, preconfigure the client, create a custom installer and rebrand. (Note: In 5.2 only supported for FG-1000 series and VM04).
	FC-10-C0105-151-02-12	1 Year Endpoint Telemetry & Compliance License Subscription for up to 20,000 clients. Includes 24x7 support and ability to download the license file, preconfigure the client, create a custom installer and rebrand.
FortiClient Enterprise Management Server License	FC-15-EMS01-158-02-12	FortiClient Enterprise Management Server Endpoint License for 1 client. Includes 24x7 support and ability to provision all FortiClient features (including VPN settings), deploy FortiClient installer, create custom installer, rebrand and monitor endpoints. One license will be issued good for the amount of units requested on PO. Minimum order quantity 100. License stacking for multi-year license for the exact same number of clients is supported.

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