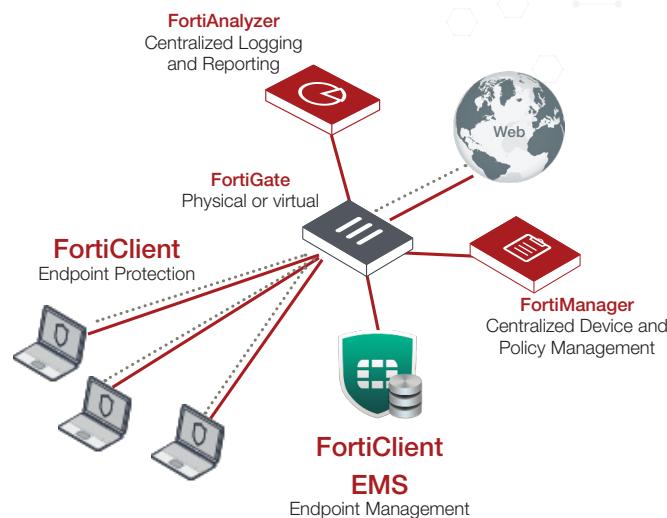


# FortiClient

Lock down visibility and control of your software and hardware inventory across the entire security fabric. Identify vulnerable or compromised hosts and track all details of systems and user profiles across your attack surface.

**FortiClient's Security Fabric Integration**, ensures that all fabric components – FortiGate, FortiAnalyzer, EMS, Managed AP, Managed Switches, Sandbox – have a unified view of endpoints in order to provide tracking & awareness, compliance enforcement and reporting.

**Advanced Threat Protection** automates prevention of known and unknown threats through built-in host-based security stack and integration with FortiSandbox. Easy to use **Secure Remote Access & Mobility** via SSL and IPsec VPN. **FortiClient** connects every endpoint to form a cohesive security fabric.



Icon	6 Devices Total	2 Devices Out of Sync	3 Devices Not Compliant	4 Devices Security Risk																						
Scan	6 Devices Total	2 Devices Out of Sync	3 Devices Not Compliant	4 Devices Security Risk																						
Endpoint Details	<table border="1"> <thead> <tr> <th>Device</th> <th>User</th> <th>IP</th> <th>Endpoint Connection</th> <th>Endpoint Profile</th> </tr> </thead> <tbody> <tr> <td>acac03cb.upt.aol</td> <td>Wendy</td> <td>172.172.3.203</td> <td>FortiTelemetry to FGT (FGT3445456765) Managed by EMS</td> <td>Installer Config Gateway IP List</td> </tr> <tr> <td>JeffC-Laptop</td> <td>Jeff</td> <td>172.28.1.108</td> <td>FortiTelemetry to FGT (FGT1345653678) Managed by EMS</td> <td>Installer Config Gateway IP List</td> </tr> <tr> <td>Andrew's PC</td> <td>Andrew</td> <td>172.18.72.40</td> <td>FortiTelemetry to FGT (FGT3762288377) Managed by EMS</td> <td>Installer Config Gateway IP List</td> </tr> </tbody> </table>				Device	User	IP	Endpoint Connection	Endpoint Profile	acac03cb.upt.aol	Wendy	172.172.3.203	FortiTelemetry to FGT (FGT3445456765) Managed by EMS	Installer Config Gateway IP List	JeffC-Laptop	Jeff	172.28.1.108	FortiTelemetry to FGT (FGT1345653678) Managed by EMS	Installer Config Gateway IP List	Andrew's PC	Andrew	172.18.72.40	FortiTelemetry to FGT (FGT3762288377) Managed by EMS	Installer Config Gateway IP List		
Device	User	IP	Endpoint Connection	Endpoint Profile																						
acac03cb.upt.aol	Wendy	172.172.3.203	FortiTelemetry to FGT (FGT3445456765) Managed by EMS	Installer Config Gateway IP List																						
JeffC-Laptop	Jeff	172.28.1.108	FortiTelemetry to FGT (FGT1345653678) Managed by EMS	Installer Config Gateway IP List																						
Andrew's PC	Andrew	172.18.72.40	FortiTelemetry to FGT (FGT3762288377) Managed by EMS	Installer Config Gateway IP List																						
Endpoint Summary	<table border="1"> <thead> <tr> <th>Anti-Virus Events</th> <th>Vulnerability Events</th> <th>Web Filter Events</th> <th>System Events</th> </tr> </thead> <tbody> <tr> <td colspan="4"> <table border="1"> <thead> <tr> <th>Device</th> <th>Endpoint Connection</th> </tr> </thead> <tbody> <tr> <td>Andrew</td> <td>FortiTelemetry to FGT3762288377</td> </tr> <tr> <td>Device: Andrew's PC</td> <td>Managed by EMS</td> </tr> <tr> <td>Mac Address: 00:21:15:B1:S2</td> <td></td> </tr> <tr> <td>OS: Windows 10</td> <td></td> </tr> <tr> <td>Last Seen: 09-19-2016 19:23:11</td> <td></td> </tr> <tr> <td>Location: On Net</td> <td></td> </tr> </tbody> </table> </td> </tr> </tbody> </table>				Anti-Virus Events	Vulnerability Events	Web Filter Events	System Events	<table border="1"> <thead> <tr> <th>Device</th> <th>Endpoint Connection</th> </tr> </thead> <tbody> <tr> <td>Andrew</td> <td>FortiTelemetry to FGT3762288377</td> </tr> <tr> <td>Device: Andrew's PC</td> <td>Managed by EMS</td> </tr> <tr> <td>Mac Address: 00:21:15:B1:S2</td> <td></td> </tr> <tr> <td>OS: Windows 10</td> <td></td> </tr> <tr> <td>Last Seen: 09-19-2016 19:23:11</td> <td></td> </tr> <tr> <td>Location: On Net</td> <td></td> </tr> </tbody> </table>				Device	Endpoint Connection	Andrew	FortiTelemetry to FGT3762288377	Device: Andrew's PC	Managed by EMS	Mac Address: 00:21:15:B1:S2		OS: Windows 10		Last Seen: 09-19-2016 19:23:11		Location: On Net	
Anti-Virus Events	Vulnerability Events	Web Filter Events	System Events																							
<table border="1"> <thead> <tr> <th>Device</th> <th>Endpoint Connection</th> </tr> </thead> <tbody> <tr> <td>Andrew</td> <td>FortiTelemetry to FGT3762288377</td> </tr> <tr> <td>Device: Andrew's PC</td> <td>Managed by EMS</td> </tr> <tr> <td>Mac Address: 00:21:15:B1:S2</td> <td></td> </tr> <tr> <td>OS: Windows 10</td> <td></td> </tr> <tr> <td>Last Seen: 09-19-2016 19:23:11</td> <td></td> </tr> <tr> <td>Location: On Net</td> <td></td> </tr> </tbody> </table>				Device	Endpoint Connection	Andrew	FortiTelemetry to FGT3762288377	Device: Andrew's PC	Managed by EMS	Mac Address: 00:21:15:B1:S2		OS: Windows 10		Last Seen: 09-19-2016 19:23:11		Location: On Net										
Device	Endpoint Connection																									
Andrew	FortiTelemetry to FGT3762288377																									
Device: Andrew's PC	Managed by EMS																									
Mac Address: 00:21:15:B1:S2																										
OS: Windows 10																										
Last Seen: 09-19-2016 19:23:11																										
Location: On Net																										



## EMS for Central Management

- Simple & User Friendly UI
- Remote FortiClient Deployment
- Realtime Dashboard
- Software Inventory Management
- Active Directory Integration
- Central Quarantine Management
- Automatic Group Assignment
- Automatic Email Alerts
- Supports Custom Groups
- Remote Triggers

## FortiClient Benefits:

**Unified** endpoint features including compliance, protection, and secure access into a single, modular lightweight client.

**End-to-end** threat visibility and control by natively integrating endpoint into the Security Fabric architecture.

**Advanced** threat protection against exploits and advanced malware, powered by FortiGuard along with FortiSandbox integration.

**Integrated** patch management and vulnerability shielding to harden all endpoints.

**Simplified** management and policy enforcement with Enterprise Management Server (EMS) and FortiGate, respectively.

## Advanced Threat Protection

As a next-generation endpoint protection solution, FortiClient helps connect endpoints to FortiSandbox, which uses **behavior-based analysis** to automatically analyze in real-time all files downloaded to FortiClient endpoints. Millions of FortiClient and FortiSandbox users worldwide share information about known and unknown, malware with cloud-based **FortiGuard**. FortiGuard automatically shares the intelligence with other FortiSandbox units and FortiClient endpoints to **prevent attacks** from known and unknown malware.

## Security Fabric Integration

As a key piece of the **Fortinet Security Fabric**, FortiClient integrates the endpoints into the Fabric for early detection and prevention of advanced threats and delivers endpoint visibility, compliance control, vulnerability management and automation. With 6.0, FortiOS & FortiAnalyzer leverages **FortiClient endpoint telemetry** intelligence to identify Indicator of Compromise (IoC). With the **Automation** capability, admins can investigate real-time and set policies to automate responses including quarantining suspicious or compromised endpoints to contain incidents and stem outbreaks. Fortinet's endpoint compliance & vulnerability management features **simplifies the enforcement** of enterprise security policies preventing endpoints from becoming easy attack targets.

## Secure Remote Access & Mobility

FortiClient uses SSL and IPSec VPN to provide **secure, reliable access** to corporate networks and applications from virtually any internet connected remote location.

FortiClient simplifies remote user experience with built-in **auto-connect and always-up** VPN features. Two-Factor authentication can also be used to provide additional layer of security. Feature like, VPN auto-connect, Always up, Dynamic VPN Gateway Selection and split-tunneling ensures smooth user experience on all device types connecting from home or public places.

## Anti-Exploit

This behavioral-based detection technology **protects against zero-day attacks** that target applications with zero-day or unpatched vulnerabilities.



**Protects against zero-day** attacks targeting undiscovered or unpatched application vulnerabilities

**Detects various memory techniques** used in an exploit, such as ROP, HeapSpray, bufferoverflow

**File-less Attacks** powershell & other scripted attacks

**Shields web browsers**, Java/Flash plug-ins, Microsoft Office applications, and PDF Reader

**Identifies and Blocks** exploit kits, prevents drive-by downloads

## Signature-less solution



## Feature Highlights

EMS provides ability to centrally manage Windows, Mac, Linux, Chrome, iOS and Android endpoints



FortiGate provides awareness and control over all your endpoints



### Remote FortiClient Deployment

that allows administrators to remotely deploy endpoint software and perform controlled upgrades.

**Centralized Client Provisioning** makes deploying FortiClient configuration to thousands of clients an effortless task with a click of a button.

**Software Inventory Management** provides visibility into installed software applications and licence management to improve security hygiene. You can use inventory information to detect and remove unnecessary or outdated applications that might have vulnerabilities to reduce your attack surface.

**Windows AD Integration** helps sync organisations AD structure into EMS so same OUs can be used for endpoint management.

**Realtime Endpoint Status** always provides current information on endpoint activity & security events.

**Vulnerability Dashboard** helps manage organizations attack surface. All vulnerable endpoints are easily identified for administrative action.

**Telemetry** provides real-time endpoint visibility (including user avatar) on FortiGate console so administrators can get a comprehensive view of the whole network. Telemetry also ensures that all fabric components have a unified view of the endpoints.

**Compliance Enforcement** can be used to enforce organisations security policies. Only authorized and compliant endpoints with no security risks are granted access.

### Endpoint Quarantine

helps to quickly disconnect a compromised endpoint from the network and stop it from infecting other assets.

### Automated Response

helps detect and isolate suspicious or compromised endpoints without manual intervention

## FortiClient EMS and FortiGate Endpoint Licenses

	FORTICLIENT EMS LICENSE	FORTIGATE ENDPOINT TELEMETRY & COMPLIANCE LICENSE
<b>PROVISIONING</b>		
Centralized Client Provisioning	✓	
Client Software Updates	✓	
Windows AD Integration	✓	
FortiTelemetry Gateway IP List	✓	
Software Inventory	✓	
Automatic Group Assignment	✓	
<b>COMPLIANCE ENFORCEMENT AND SECURITY FABRIC INTEGRATION</b>		
Fortinet Security Fabric Integration		✓
Security Posture Check		✓
Vulnerability Compliance Check		✓
Minimum System Compliance		✓
Authorized Device Detection		✓
Automated Endpoint Quarantine	✓	✓
<b>REMOTE CONTROL</b>		
On-demand Antivirus Scan	✓	
On-demand Vulnerability Scan	✓	
Host Quarantine	✓	✓
<b>TELEMETRY AND MONITORING</b>		
Client Information (client version, OS IP/MAC address, profile assigned, user avatar)	✓	✓
Client Status	✓	✓
Reporting	✓ (To FortiAnalyzer)	✓ (To FortiAnalyzer)

**PLUS** - THE FORTICLIENT CUSTOM INSTALLER TOOL IS AVAILABLE FOR FREE ON FNDN. REBRANDING TOOL REQUIRES AN FNDN SUBSCRIPTION

**SECURITY FABRIC COMPONENTS**

	WINDOWS	MAC OS X	ANDROID	iOS	ChromeBook	Linux
Endpoint Telemetry <sup>1</sup>	✓	✓	✓	✓	✓	✓
Compliance Enforcement <sup>1</sup>	✓	✓	✓	✓	✓	✓
Endpoint Audit and Remediation with Vulnerability Scanning <sup>1</sup>	✓	✓	✓			✓
Automated Endpoint Quarantine	✓	✓				

**HOST SECURITY AND VPN COMPONENTS**

	WINDOWS	MAC OS X	ANDROID	iOS	ChromeBook	Linux
Antivirus	✓	✓			✓	
Anti-Exploit	✓					
Sandbox Detection	✓				✓	
Web Filtering <sup>2</sup>	✓	✓	✓	✓	✓	
Application Firewall <sup>1</sup>	✓	✓				
IPSec VPN	✓	✓	✓	✓		
SSL VPN <sup>3</sup>	✓	✓	✓	✓		✓

**OTHERS**

	WINDOWS	MAC OS X	ANDROID	iOS	ChromeBook	Linux
Remote Logging and Reporting <sup>4</sup>	✓	✓		✓	✓	
Windows AD SSO Agent	✓	✓				
USB Device Control	✓	✓				✓

**PLUS - ADVANCED THREAT PROTECTION COMPONENTS FOR WINDOWS: File Analysis with FortiSandbox and Host Quarantine Enforcement<sup>1</sup>**<sup>1</sup> Requires FortiClient to be managed by EMS <sup>2</sup> Also compatible in Chrome OS <sup>3</sup> Also compatible in Windows Mobile.

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

<sup>4</sup> Requires FortiAnalyzer

\* No file submission

**Specifications****FORTICLIENT****Operating System Supported:**

Microsoft Windows 7 (32-bit and 64-bit)  
 Microsoft Windows 8, 8.1 (32-bit and 64-bit)  
 Microsoft Windows 10 (32-bit and 64-bit)  
 FortiClient 6.0.0 does not support Windows XP or Windows Vista

Windows Server 2008 or newer

Mac OS X v10.12, v10.11, v10.10, v10.9, v10.8

iOS 5.1 or later (iPhone, iPad, iPod Touch)

Android OS 4.4.4 or later (phone and tablet)  
 Linux OS, Ubuntu 16.04 and later, Red Hat 7.4 and later, CentOS 7.4 and later with KDE or GNOME**Authentication Options**

RADIUS, LDAP, Local Database, xAuth, TACACS+, Digital Certificate (X509 format), FortiToken

**Connection Options**

Auto Connect VPN before Windows logon, IKE Mode config for FortiClient VPN IPsec tunnel

Note: All specifications are based on FortiClient 6.0.

**FORTICLIENT EMS****Operating System Supported**

Microsoft Windows Server 2008 or newer

**Endpoint Requirement**

FortiClient version 5.6 or newer, FortiClient for Microsoft Windows and Mac OS X, 5.4 for iOS and Android

**System Requirements**

2.0 GHz 64-bit processor, dual core (or two virtual CPUs), 4 GB RAM, 40 GB free hard disk, Gigabit (10/100/1000BaseT) Ethernet adapter, Internet access

**Order Information**

PRODUCT	SKU	DESCRIPTION
Enterprise Management Server Endpoint License for 100 clients	FC1-15-EMS01-158-02-DD	FortiClient Enterprise Management Server License subscription for 100 clients. Includes 24x7 support.
FortiClient Chromebook Enterprise Management Server License for 100 users	FC1-15-EMS02-158-02-DD	Chromebook Enterprise Management Server License subscription for 100 ChromeOS users. Includes 24x7 support
FortiClient Telemetry License for 100 Clients	FC1-10-C1100-151-02-DD	Endpoint Telemetry & Compliance License subscription for 100 clients. Includes 24x7 support.  Note1: Compatible with FortiOS 5.6 and above only; Note2: Refer to the FortiOS admin guide for specific platform restrictions and maximum license limit.

FortiGuard Security Services  
[www.fortiguard.com](http://www.fortiguard.com)FortiCare Worldwide  
 24/7 support  
[support.fortinet.com](http://support.fortinet.com)**GLOBAL HEADQUARTERS**

Fortinet Inc.  
 899 Kifer Road  
 Sunnyvale, CA 94086  
 United States  
 Tel: +1.408.235.7700  
[www.fortinet.com/sales](http://www.fortinet.com/sales)

**EMEA SALES OFFICE**

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

**APAC SALES OFFICE**

8 Temasek Boulevard  
 # 12-01 Suntec Tower Three  
 Singapore 038988  
 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

Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

FST-PROD-DS-FCT

FCT-DAT-R19-201810