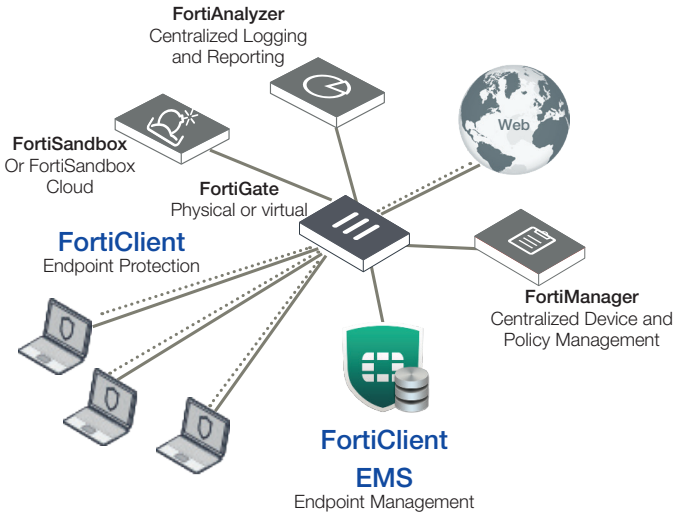
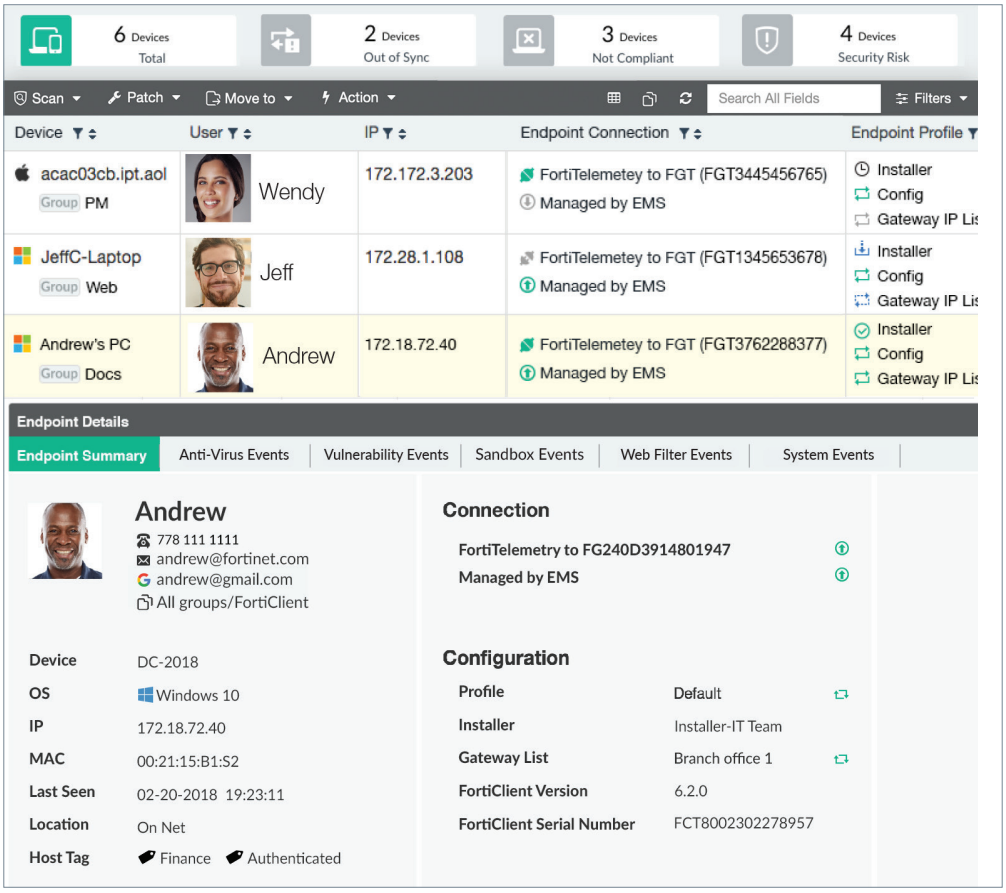
DATA SHEET

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 and FortiSandbox Cloud. Easy to use **Secure Remote Access & Mobility** via SSL and IPsec VPN. FortiClient connects every endpoint to form a cohesive security fabric.





EMS for Central Management

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

FortiGuard Security Services
www.fortiguard.com

FortiCare Worldwide 24/7 support
support.fortinet.com

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 Dashboard for Ease of Management

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 p**rotects against zero-day file-less attacks** that target applications with zero-day or un-patched vulnerabilities.

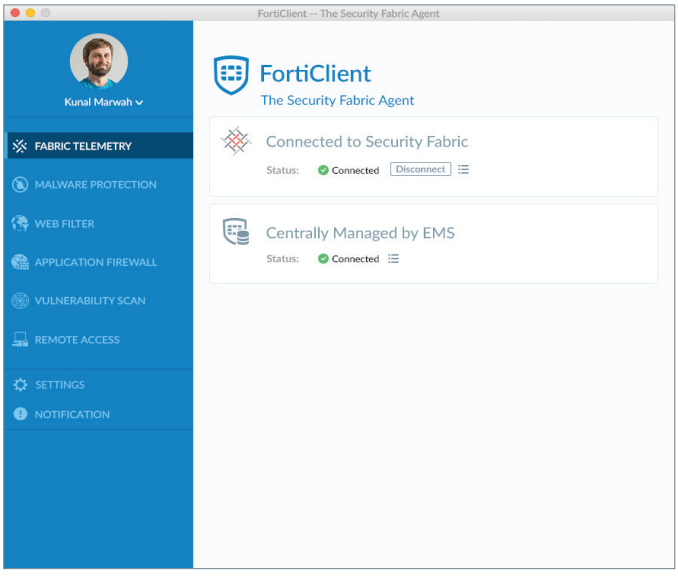
Protects against zero-day attacks targeting undiscovered or un-patched application vulnerabilities

Detects various memory techniques used in an exploit, such as ROP, HeapSpray, buffer overflow

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

Cloud-Based Threat Detection

Protects against emerging threats with real-time threat intelligence powered by FortiGuard.



Feature Highlights

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

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 organizations AD structure into EMS so same OUs can be used for endpoint management.

Real-time 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.

Centralized FortiClient Deployment & Provisioning that allows administrators to remotely deploy endpoint software and perform controlled upgrades. Makes deploying FortiClient configuration to thousands of clients an effortless task with a click of a button.

Sandbox settings are automatically synchronized with EMS and detailed analysis of FortiClient submitted files for behavior based detection is accessible in EMS. Administrators can see all behavior activity of a file including graphic visualization of full process tree.

FortiGate provides awareness and control over all your endpoints

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.

Dynamic Access Control for Compliance Enforcement requires EMS to create virtual groups based on endpoint security posture. These virtual groups are then retrieved by FortiGate and used in firewall policy for dynamic access control. Dynamic groups help automate & simplify compliance to security policies.

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

	SECURITY FABRIC AGENT
Provisioning	
Centralized Client Provisioning	✓
Client Software Updates	✓
Windows AD Integration	✓
FortiTelemetry Gateway IP List	✓
Software Inventory	✓
Automatic Group Assignment	✓
Compliance Enforcement and Security Fabric Integration	
Fortinet Security Fabric Integration	✓
Security Posture Check	✓
Vulnerability Compliance Check	✓
Dynamic Access Control	✓
Authorized Device Detection	✓
Automated Endpoint Quarantine	✓
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	✓
Reporting (to FortiAnalyzer)	✓

PLUS - Add Sandbox Cloud Subscription for Proactive Advanced Threat Detection as well as other upcoming add-ons in the future.

	WINDOWS	MAC OS X	ANDROID	iOS	CHROMEBOOK	LINUX
Security Fabric Components						
Endpoint Telemetry[1]	✓	✓	✓	✓	✓	✓
Compliance Enforcement using Dynamic Access Control[1]	✓	✓	✓	✓		✓
Endpoint Audit and Remediation with Vulnerability Scanning[1]	✓	✓				✓
Automated Endpoint Quarantine	✓	✓				
Host Security and VPN Components						
Antivirus	✓	✓				✓
Cloud-based Threat Detection	✓					
Anti-Exploit	✓					
Sandbox Detection (on-prem)	✓	✓				✓*
Sandbox Cloud Detection	✓					
Web Filtering[2]	✓	✓	✓	✓	✓	
Application Firewall[1]	✓	✓				
IPsec VPN	✓	✓	✓			
SSL VPN[3]	✓	✓	✓	✓		✓
Others						
Remote Logging and Reporting[4]	✓	✓		✓	✓	✓
Windows AD SSO Agent	✓	✓				
USB Device Control	✓	✓				✓

PLUS - Add Sandbox Cloud Subscription for Proactive Advanced Threat Detection

[1] Requires FortiClient to be managed by EMS
[2] Also compatible in Chrome OS
[3] Also compatible in Windows Mobile.
The list above is based on the latest OS for each platform.
[4] Requires FortiAnalyzer
* No file submission

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 6.2.0 does not support Windows XP or Windows Vista
Windows Server 2008 or newer
Mac OS X v10.13 , v10.12, v10.11,
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 specifcations are based on FortiClient 6.2.

FORTICLIENT EMS

Operating System Supported
Microsoft Windows Server 2008 or newer

Endpoint Requirement
FortiClient version 6.0 or newer, FortiClient for Microsoft Windows and Mac OS X, 6.0 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
FortiClient Security Fabric Agent with FortiSandbox Cloud	FC1-15-EMS01-299-02-DD	Security Fabric Agent with EPP license subscription for 25 endpoints. Includes Fabric Agent, Anti-Malware, Remote Access, Web Filter, Vulnerability Scan, Software Inventory, Application Firewall, SSOMA, Threat Outbreak Detection, Sandbox Agent with Cloud Sandbox subscription, Central Management and 24x7 Support
FortiClient Security Fabric Agent for 25 Clients	FC1-15-EMS01-297-02-DD	Security Fabric Agent with EPP license subscription for 25 endpoints. Includes Fabric Agent, Anti-Malware, Remote Access, Web Filter, Vulnerability Scan, Software Inventory, Application Firewall, SSOMA, Threat Outbreak Detection, Sandbox Agent (On-Prem), Central Management and 24x7 Support
FortiClient Chromebook for 25 Clients	FC1-15-EMS01-403-02-DD	FortiClient Chromebook license subscription for 25 Chrome OS users. Includes Web Filter, Central Management and 24x7 Support.

CERTIFIED

www.fortinet.com