Personal computer (PC) desktop and laptop devices have empowered today’s business users with the capability to access enterprise applications and mission critical data both in the office and on the road. While expanding productivity, remote access to the secure network perimeter increases security risk. Unfortunately, all devices are exposed to blended threats such as viruses, trojans, worms, spyware, keyloggers, botnets, spam and Internet attack. While utilizing network security architectures that isolate segments from one another can mitigate infection or breach, PCs within the same subnet can still potentially infect one another.

Users may inadvertently circumvent policy by bringing in portable storage devices, failing to keep antivirus signatures up-to-date, or even disabling personal firewall protection. Users accessing inappropriate and dangerous web content jeopardize device integrity, negatively impact productivity and create security and legal exposure. While point product security technology, such as antivirus agents, are available to protect devices from certain threats, such methods fall short from comprehensively protecting against blended threats and do not enforce content access guidelines.

FortiClient offers the full range of Fortinet threat protection to PCs and laptops, even when being used on insecure public networks. This comprehensive, modular protection suite secures desktops against viruses, trojans, worms and more. The FortiClient product is a client-based software solution designed to be used in connection with our FortiGate appliances to provide security features like Endpoint Control and WAN Optimization for enterprise computers. The feature set includes VPN (IPSec and SSL), antivirus/antispyware, personal firewall, Web filtering, and antispam – each with separate modular installs to completely avoid any potential conflicts with other security software. Powered by FortiGuard security services, FortiClient has access to constantly-updated protection on a real-time basis against current and emerging threats.

**Features and Benefits**
- **Endpoint Control**: Ties into your FortiGate appliance to monitor and enforce endpoint security policy at the network firewall, including FortiClient version enforcement, ensuring signatures are up-to-date and personal firewall is enabled.
- **Application Detection**: Extends Endpoint Control to allow admins to detect if endpoints run applications against security policy and automates denial of network access.
- **Endpoint Management**: Ties into your FortiManager appliance to discover, deploy, update and monitor clients on the network. Ties into your FortiAnalyzer appliance for advanced reporting that leverages FortiClient logs.
- **Secure IPSec VPN Client**: Empowers mobile laptops and remote desktops with the capability to access enterprise applications securely with DES / 3DES encryption.
- **SSL VPN Tunnel Client**: Connects securely from anywhere for remote access to web applications behind the firewall, protecting confidential communications.
- **WAN Optimization**: Speeds services like VPN for remote PC connections over the WAN.
- **Antivirus & Antispyware**: Provides comprehensive protection against viruses, spyware, keyloggers, Trojans, adware and grayware on the client, with updates by FortiGuard.
- **Powerful Personal Firewall**: Monitors network traffic and enforces the appropriate application access control in your security policies.
- **Web Filtering**: Provides real-time web content access enforcement to ensure compliance.
- **Advanced Antispam**: Built in antispam that incorporates into MS Outlook to reduce unsolicited emails, email-borne viruses and phishing attempts.

**Blended Threats and Compliance Requirements**
As Internet attack sophistication increases with blended threats, an endpoint security solution that reflects that sophistication makes sense. An integrated protection suite including antispam, Web filtering, antivirus and firewall provides advanced protection against multi-vector attacks that may include email, Web and trojans that attempt to open network connections through a backdoor. With breach incidents affecting the bottom line, government and industry regulators are looking at endpoint security. Payment Card Industry (PCI) requirement 1.4 specifies installation of personal firewall software on mobile and employee-owned computers. HIPAA healthcare EPHI safeguards address protection from malicious software.
Fortinet Security Framework

FortiClient plays an important role in completing most any FortiGate installation. This advanced endpoint protection solution helps close potential security gaps in network architecture, strengthening your security posture by adding an essential layer of protection to PCs and laptops connecting from the LAN or from off-site remote locations. FortiClient provides integration with FortiGate, FortiManager and FortiAnalyzer.

Enhances FortiGate Endpoint Control

FortiGate users benefit from endpoint control, enforcing a policy based approach to FortiClient use.

- Endpoint Control with Application Detection
- VPN (IPSec and SSL)
- WAN Optimization

Eases Deployment with FortiManager

FortiManager users benefit from streamlined FortiClient deployment and centralized management.

- Bulk Deployments of FortiClient Updates
- Auto Discovery of New FortiClients
- Set Management Events and Alerts

Integrates with FortiAnalyzer Reporting

FortiAnalyzer users benefit from FortiClient log capture for integrated endpoint reporting and analysis.

- Endpoint Security Reports
- Automate Report Scheduling
- Vulnerability Analysis
Modular Installation and Targeted Scanning

Avoids Potential Security Conflicts
FortiClient includes a modular installation feature to avoid potential conflicts with other client security. Preserve existing client security investments while leveraging additional client security features. Administrators can pick and choose. FortiClient offers a number of tools to manage multi-client installations with FortiManager.

- Install FortiClient using Active Directory Server
- Create a network installer image
- Install FortiClient as part of a cloned disk image
- Install FortiClient on Citrix Server for web filtering
- Create a Custom Installation Package with FCRepackager (included)

Targeted Scanning
FortiClient also can target scanning for faster scan times, including exclusion of Exchange or SQL Server filesystem files and extensions.

FortiClient Editions
Fortinet offers FortiClient in two editions: a standard edition for small business and consumers, and a premium edition for mid-sized enterprises and other large organizations. Both editions can be used either as a stand-alone product, or in combination with FortiGate and other Fortinet products. The premium edition includes antispam, enables central management with FortiManager, and comes with Enhanced Support.

<table>
<thead>
<tr>
<th>Comparison</th>
<th>FortiClient Standard Edition</th>
<th>FortiClient Premium Edition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus/Antispyware</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Personal Firewall</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>VPN (SSL and IPSec)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Web Content Filter</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>FortiGuard updates</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Endpoint Control w/ Application Detection*</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>WAN Optimization**</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Antispam</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Extended Signature Database Updates</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Logging</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Central Management**</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Enhanced Support</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

* Required FortiGate
** Required FortiManager

Centralized Policy Management
Fortinet’s management system makes deployment, configuration and policy control quick and easy.

Deployment Scalability
FortiClient deployments can scale to an unlimited number of devices and receive security subscription updates from the FortiGuard update service or from the FortiManager system.

Low Total Cost of Ownership
Unlike point product agents that provide a single security feature, FortiClient is a true unified security agent that bundles all the necessary capabilities into a single low cost and easy to manage application.
**GENERAL**
- Endpoint Control with Application Detection
- Anti-Leak Banned Word List
- Desktop Antivirus
- Remote VPN Client
- WAN Optimization Client
- Personal Firewall
- Antivirus Scanning / Cleaning
- Quarantine Infected Files
- Registry Monitoring
- User-Definable File Types for Scanning
- Scans Compressed Files
- Scheduled Scanning
- Antivirus and Spyware Scanning
- Manual and Scheduled Updates
- Antivirus Logs

**CENTRALIZED MANAGEMENT**
- Client Version and Status Monitoring
- Update Server Override
- Central Logging and Reporting
- Configuration Lockdown
- Group Configurations

**USER AUTHENTICATION**
- Extended Authentication (XAUTH)
- Management, Logging, and Monitoring
- Searchable VPN Logs
- VPN Tunnel Diagnostics Test
- VPN Connection Monitor
- Packet Logs

**ANTIVIRUS / ANTISPYWARE**
- Configurable File Types to Scan Including Files with No Extension
- Manual Scan
- Real-time Protection
- Automatic Submission of Suspicious Files to Fortinet
- Notification Virus Signature is Out of Date
- Email Scanning Incoming and Outgoing Including Attachments
- Heuristics Scanning
- Virus File Quarantine

**CRYPTOGRAPHY**
- 3DES And DES
- SHA-1 And MD5
- AES (128, 192, 256-Bit)
- PKI
- PKCS #7 Certificate Chains
- PKCS #12 Certificate Import

**IPSEC VPN**
- Autokey IKE (Preshared) / Autokey IKE Certificate
- ESP and AH
- NAT Traversal
- Main and Aggressive Mode IKE
- Redundant Gateway Support
- DHCP over IPsec
- Manual Virtual IP
- Multiple Remote Networks
- VPN Policy Retrieval from FortiGate® Unit
- Dead Peer Detection
- Simplified Configuration Process
- Split Tunneling

**SSL VPN**
- IKE Negotiation
- Retrieve Dropped Connections
- VPN Monitor
- Policy Compliance Tool

**WEB CONTENT FILTERING**
- Multiple Categories
- HTTPS Site Inspection/Blocking
- Password Protected Config
- Customizable Block Profiles
- Predefined Usage Profiles for Adults and Children
- User Definable Block / Bypass List
- Continuously Updated Database

**SYSTEM REQUIREMENTS**
To install FortiClient you need:
- Pentium processor or equivalent
- Compatible operating system and minimum RAM:
  - Microsoft Windows 2000:
    - 256 MB
  - Microsoft Windows XP:
    - 512 MB
  - Microsoft Windows Server 2000:
    - 512 MB
  - Microsoft Windows Server 2003:
    - 1024 MB
  - Microsoft Windows Vista:
    - 1024 MB

**LANGUAGE SUPPORT**
- English
- French
- Japanese
- Korean
- Simplified Chinese
- Slovak

---

**FortiGuard® Subscription Services**
- Includes:
  - Automatic updates from over 50 redundant high-speed database servers around the globe.
  - Complete Wildlist virus protection for over 30,000 active viruses from FortiGuard’s active database.
  - Real-time signature updates for protection against over 5,100 threats.
  - 77 rated Web categories for more accurate Web content filtering.
  - Web filtering for more than 47 million URLs with more than 70 languages supported.

**FortiCare® Subscription Services**
- 8x5 Enhance Support (Optional)
- Premium Support (Optional)
- 24x7 Comprehensive Support (Optional)
- Professional Services (Optional)
- 90-Day Limited Software Warranty

**About Fortinet**

Fortinet is a leading provider of network security appliances and the market leader in Unified Threat Management or UTM. Fortinet solutions were built from the ground up to integrate multiple levels of security protection -- including firewall, VPN, antivirus, intrusion prevention, Web filtering, spyware prevention and antispy -- designed to help customers protect against network and content level threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified in five programs by ICSA Labs: Firewall, Antivirus, IPSec VPN, Network IPS and Antispy. Fortinet is based in Sunnyvale, California.