

Features

Learn about the features and benefits of Microsoft Forefront Client Security, which provides unified virus and spyware protection for business desktops, laptops, and server operating systems that is easier to manage and control.

Forefront Client Security provides:

Unified Protection

Feature	Description
Integrated antivirus and antispyware engine	Single engine enhances client machine performance and detection capabilities by minimizing end-user disruptions. By using “mini-filter” technology with the Windows Filter Manager, Forefront Client Security is able to scan virus and spyware files before they run, providing better security against spyware and blended threats (for example, spyware that infects a PC through backdoor Trojans or other means).
Real-time protection with the Windows Filter Manager	The other benefit to using the Windows Filter Manager is that end-user disruption (system slowdowns) is minimized during real-time scans for both viruses and spyware.
Scheduled and on-demand scans	Quickly scan in-memory processes, targeted directories, and common malware extensibility points to ensure that the client machine is malware-free at all times.
Malware removal and system recovery	The Microsoft anti-malware engine removes malware and runs cleaning scripts to help ensure that the machine is still in a usable state.
Archives and packers scans	Archives and packers are a common way for malware authors to try to hide from anti-malware technologies, but the engine is

able to look inside archives and packers and remove infected files.

Advanced protection mechanisms

The engine includes advanced protection mechanisms to find user-mode rootkits, polymorphic viruses based on behavior analysis, tunneling signatures, and heuristic detection mechanisms that find new malware and variants.

Compatible with Windows Security Center and Windows Vista Network Access Protection (NAP)

Forefront Client Security provides customers the ability to see whether Forefront Client Security is running and up to date. IT administrators are able to configure NAP on Windows Server 2008 servers so that Forefront Client Security–managed machines attempting to connect to the network are checked to ensure that the security agent is up to date and actively protecting clients. If the client machine does not have the Forefront Client Security agent or is not up to date, the user is not allowed to connect to the network and is notified within Windows Security Center. If the user installs the security agent for Forefront Client Security with updated signatures, he or she can then connect to the network.

FCS Virtualization Security

The Forefront Client Security agent is installable on Windows Server 2008 host and virtualized operating systems to protect against malicious threats. The FCS Management Server can also be installed on Hyper-V virtualized machines to consolidate management server roles.

Windows Server Core and Cluster Services Protection

The Forefront Client Security agent as well as the Forefront Client Security Management Console both support Windows Server 2008. The FCS agent also protects Windows Server Core and Microsoft Cluster Services.

[Simplified Administration](#)

Feature	Description
Central Management System	With one console for simplified client security administration, Microsoft Forefront Client Security saves time and reduces complexity.
Single policy to manage client protection settings	Forefront Client Security helps increase your efficiency through a single policy that configures the antispymware, antivirus, and state assessment technologies for one or more protected computers. New policies are created with preconfigured settings that can be easily tailored to the needs of your environment. Policies also include alert level settings that can be easily configured to specify the type and volume of alerts and events generated by different groups of protected machines.
Integration with Active Directory for policy deployment	Integrating with the familiar Microsoft infrastructure saves administrative time and reduces the “learning curve.” Target policy based on Active Directory Organizational Units (OUs) and security groups.
Integration with WSUS/MU for client deployment	Installing client agents throughout the organization can be a time-consuming process for administrators. Deploying client agents using Microsoft Windows Server Update Services (WSUS) reduces administrative workload since these agents are installed automatically through WSUS sync. Administrators do not require additional software or technology, but can leverage their WSUS distribution infrastructure that provides deployment, status, and reporting. Furthermore, as this is an administrative controlled policy, even rogue machines (machines that have removed client agents accidentally or intentionally) receive the client agent automatically when they sync with the WSUS server.
Signature updates for roaming users	Forefront Client Security provides a failover system for mobile users that enables them to connect to Microsoft Update (MU) to download the latest definition updates if they cannot get access to the corporate network. The administrator will have the ability to centrally manage the opt-in process for managed clients using the Forefront Client Security.

Critical Visibility and Control

Feature	Description
Security State Assessment checks	The Security State Assessment (SSA) checks to examine data from the registry, the file system, WMI, IIS metabase, SQL, and more. Those checks allow a security administrator to detect common vulnerabilities in the environment, as well as configuration issues that increase their exposure. These checks are a set of risk criteria defining industry best practices and known vulnerabilities. The reporting functionality that includes the SSA capabilities in Forefront Client Security enables customers to measure their security risk profile based on security best practices. As a result, customers can focus critical IT resources on the right security issues, and spend less time trying to find and then analyze information from disparate sources.
Reports that can be drilled down into for investigation	Expanding the Security Issue tab in the Alerts Summary report, and the top alert underneath, allows the analyst to view the list of computers that were repeatedly infected with malware. After identifying the extent of the infection reported through the total number of machines infected with each type of malware, the analyst can drill into an infected computer to further explore its detailed security status.
Customized alerts based on incidents and assets	After receiving an e-mail/page message about alerts being present in the enterprise, the security analyst logs into the corporate network and opens the Forefront Client Security Summary report. As the top alert shows a number of computers infected with a malware, the analyst decides to start investigating this problem. The analyst follows the Alerts Summary link to get more information on this alert.
Flood protection	Forefront Client Security is designed to prevent machines from generating alerts when it hits the threshold of 5,000 alerts within a specific time, thus preventing the MOM server from getting flooded. The client machine will still be protected from new malware through Forefront Client Security real-time scans. This preventative measure

ensures that during virus outbreaks administrators do not get data dumped, taking up valuable bandwidth.