



Microsoft® Forefront™ Endpoint Protection 2010

Simplify desktop protection and reduce operational costs

Microsoft® Forefront® Endpoint Protection 2010 helps businesses simplify and improve desktop security while greatly reducing infrastructure costs.

www.microsoft.com/forefront

"The integration of Forefront Endpoint Protection with System Center Configuration Manager lets us break down the silos within our organization and increase efficiency."

—DRAGOSLAV RADIN
Head Division for IT Infrastructure
Services Telekom Slovenije

New Efficiencies: The Convergence of Desktop Security and Management

Desktop management and security have traditionally existed as two separate disciplines, yet both play central roles in keeping users safe and productive. Management ensures proper system configuration, deploys patches against vulnerabilities, and delivers necessary security updates. Security provides critical threat detection, incident response, and remediation of system infection.

Forefront Endpoint Protection 2010 introduces the ability to align these two work streams into a single infrastructure. Built on Microsoft System Center Configuration Manager 2007 R2 and R3, Forefront Endpoint Protection 2010 gives IT:

- Consolidated tools, processes, and infrastructure to create new efficiencies and lower desktop ownership costs.
- A unified view of configuration and security information that makes it easier to identify and remediate vulnerabilities.

Lowers Ownership Costs

With discrete infrastructures for management and security, companies must purchase and maintain separate hardware and software, create and manage two sets of policies, and take two sets of actions when a security incident occurs. Together, Forefront Endpoint Protection and Configuration Manager deliver significant operational efficiencies not available with traditional management and security silos by offering:

- A single server infrastructure to maintain.
- A single mechanism for deploying client software and updates.
- Central implementation of policy.
- A single solution for training administrators regardless of their role.

With the Microsoft Enterprise Client Access License (ECAL), organizations can also purchase all the components they need to manage and secure desktops in one SKU, eliminating the need to buy single-purpose software.

Improves Protection

Most desktop vulnerabilities are a result of poor system configuration, yet security administrators lack ready access to inventory, patch level, and other desktop-specific data.

Forefront Endpoint Protection 2010 and Configuration Manager give organizations industry-leading threat-detection capabilities alongside the world's most widely used tool for remediating desktop security vulnerabilities.

The combination of these technologies in a single infrastructure offers a unique, consolidated view into the health and protection status of user systems. IT can better identify at-risk machines and take action to patch systems, block outbreaks, and initiate clean-up efforts. These combined technologies also consolidate and simplify reporting on the complete desktop environment.

Key Features

Forefront Endpoint Protection 2010 makes it easier to protect critical desktop and server operating systems against viruses, spyware, rootkits, and other threats.

Single Console for Endpoint Management and Security

Configuration Manager 2007 provides a single interface for managing and securing desktops that reduce complexity and improve troubleshooting and reporting insights.

Central Policy Creation

Administrators have a central location for creating and applying all client-related policies.

Enterprise Scalability

Use of the Configuration Manager infrastructure in Forefront Endpoint Protection 2010 makes it possible to efficiently deploy clients and policies in the largest organizations around the globe.

Highly Accurate and Efficient Threat Detection

The new anti-malware engine protects against the latest malware and rootkits with a low false positive rate, and keeps employees productive with scanning that has a low impact on performance.

Behavioral Threat Detection

Forefront Endpoint Protection 2010 uses system behavior and file reputation data to identify and block attacks on client systems from previously unknown threats. Detection methods include behavior monitoring, emulation, and dynamic translation.

Automated Agent Replacement

Forefront Endpoint Protection 2010 automatically detects and removes the most common endpoint security agents, dramatically lowering the time and effort needed to deploy new protection.

Windows Firewall Management

Forefront Endpoint Protection 2010 ensures that Windows® Firewall is active and working properly to protect against network-layer threats. It also enables administrators to more easily manage these protections across the enterprise.

Integration with System Center Operations Manager

The Forefront Endpoint Protection 2010 Security Management Pack enables IT to monitor the security of server operating systems from System Center Operations Manager.

Forefront Endpoint Protection 2010, built on System Center Configuration Manager 2007, gives organizations a single interface for desktop management and security.

SECURING AND STREAMLINING THE WINDOWS OPTIMIZED DESKTOP

Forefront Endpoint Protection 2010 and System Center Configuration Manager are part of the Windows Optimized Desktop, which is built on the Windows 7 Enterprise operating system. The Windows Optimized Desktop also deploys virtualization technologies with integrated management across physical and virtual machines, including Microsoft Virtual Desktop Infrastructure (VDI).

Along with Microsoft Office 2010, Windows Internet Explorer® 8 and the Microsoft Desktop Optimization Pack (MDOP), Forefront Endpoint Protection and Configuration Manager help create a workforce environment that is more productive, manageable, and secure.

For more information on Windows Optimized Desktop, visit www.microsoft.com/windows/enterprise.



Forefront Endpoint Protection 2010 includes a top-ranked anti-malware engine for proactive threat detection.

Forefront Endpoint Protection 2010

Forefront Endpoint Protection allows you to deploy and manage an effective computer protection policy on Configuration Manager managed computers

Dashboard - Updated: 10/20/2010 6:09 AM

Operational Statistics

Clients Deployment Status	Malware Activity Status	Computers
Targeted by FEP: 247 out of 10583	Infected	20
	Restart required	35
	Full scan required	20
	Recent activity (Last 24 hours)	25
	Definition Status	Computers
	Older than 1 week	12
	Up to 7 days old	22
	Up to 3 days old	33
	Up to date	44
	Policy Distribution Status	Computers
	Distribution failed	10
	Distribution in progress	21
	Policy distributed	80

Health Status

Health Status	Computers
Protection inactive	35
Not reporting	25
Healthy	106

Forefront Endpoint Protection Baselines

Baseline	Severity	Assigned	Non-Compliant	Compliant	Failed	Compliance Level
FEP - Laptop	None	0	0	0	0	0.00 %
FEP - Performance-Optimized Desk...	None	0	0	0	0	0.00 %
FEP - High-Security Desktop	None	0	0	0	0	0.00 %
FEP - Standard Desktop	None	0	0	0	0	0.00 %

Links and Resources

Use the following links, reports, and resources to manage Forefront Endpoint Protection.

Navigation Web Reports Resources