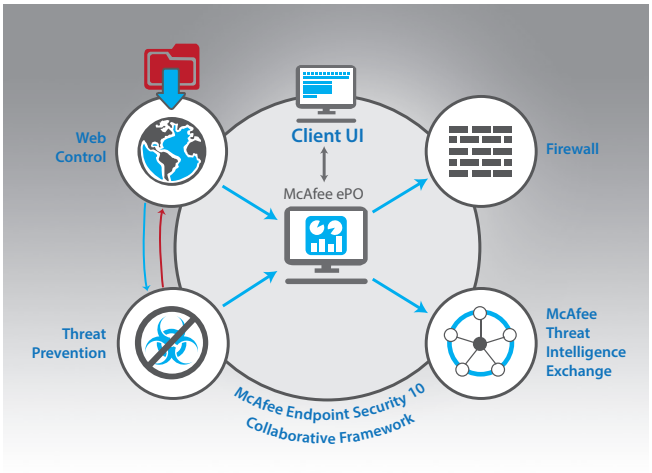
Endpoint Security 10

McAfee Blacklisting Technology



Features

- Endpoint protection for targeted attacks
- Intelligent, adaptive scanning
- Advanced anti-malware protection
- Proactive web security
- Blocks hostile network attacks
- Actionable threat forensics
- Centralized management
- Open, extensible endpoint security framework

Introduction

McAfee Endpoint Security 10 is the newest, best-performing, most effective, collaborative protection for McAfee Endpoint Protection Suites customers. It introduces a new framework that allows multiple endpoint defense technologies to communicate in real time and analyze and collaborate against new and advanced threats.

Endpoint Security modules

Along with a new endpoint security platform with common services architecture, there are three modules included.

- Threat Prevention — Checks for viruses, spyware, unwanted programs, and other threats, either by scanning items automatically when users access them, or scanning on demand at any time.
  This is the a replacement for McAfee VirusScan Enterprise.
- Firewall — Monitors communication between the computer and resources on the network and the Internet. Intercepts suspicious communications. Stops malicious inbound and outbound network traffic and replaces the host intrusion prevention firewall feature of McAfee Host Intrusion Prevention.
- Web Control — Displays safety ratings and reports for websites during online browsing and searching. Web Control enables the site administrator to block access to websites based on safety rating or content. Prevents users from browsing to malicious or unauthorized websites and serves as a replacement for McAfee Site Advisor Enterprise.

Feature Details

Feature	Why You Need It
Endpoint protection for targeted attacks	Closes the gap from encounter to containment from days to milliseconds. McAfee Threat Intelligence Exchange collects intelligence from multiple sources, enabling security components to instantly communicate with each other about emerging and multiphase advanced attacks.
Intelligent, adaptive scanning	Improves performance and productivity by bypassing scanning of trusted processes and prioritizing suspicious processes and applications. Adaptive behavioral scanning monitors, targets, and escalates as warranted by suspicious activity.
Advanced anti-malware protection	Ensures safe browsing with web protection and filtering for endpoints.
Proactive web security	Ensures safe browsing with web protection and filtering for endpoints.
Blocks hostile network attacks	Integrated firewall uses reputation scores based on McAfee GTI to protect endpoints from botnets, DDoS, APTs, and suspicious web connections. Firewall protection allows only outbound traffic during system startup, protecting endpoints when they are not on the corporate network.
Actionable threat forensics	Administrators can quickly see where infections are, why they are occurring, and the length of exposure. Threats are understood fast; reactions are fast.
Centralized management (McAfee ePO platform) with multiple deployment choices	True centralized management offers greater visibility, simplifies operations, boosts IT productivity, unifies security, and reduces costs.
Open, extensible endpoint security framework	Integrated architecture allows endpoint defenses to collaborate and communicate for a stronger defense. Results in lower operating costs by eliminating redundancies and optimizing processes. Seamlessly integrates with other Intel Security and third-party products to reduce protection gaps.

Supported Operating Systems

Client OS	Server OS
Windows 10	Windows Server 2012 R2/R2 update 1
Windows 8/8.1	Windows Server 2008/2008R2
Windows Embedded 8/8.1: Pro, Standard, and Industry	Windows Storage Server 2008 and 2008 R2
Windows 7	Windows Small Business Server 2011
Windows Embedded Standard 7	Windows Small Business Server 2008
Windows XP SP3 Professional x86	Windows Server 2003/2003R2

Ordering Information

Part No.	Description
968ELMESN1	Intel® Security Endpoint Security 10