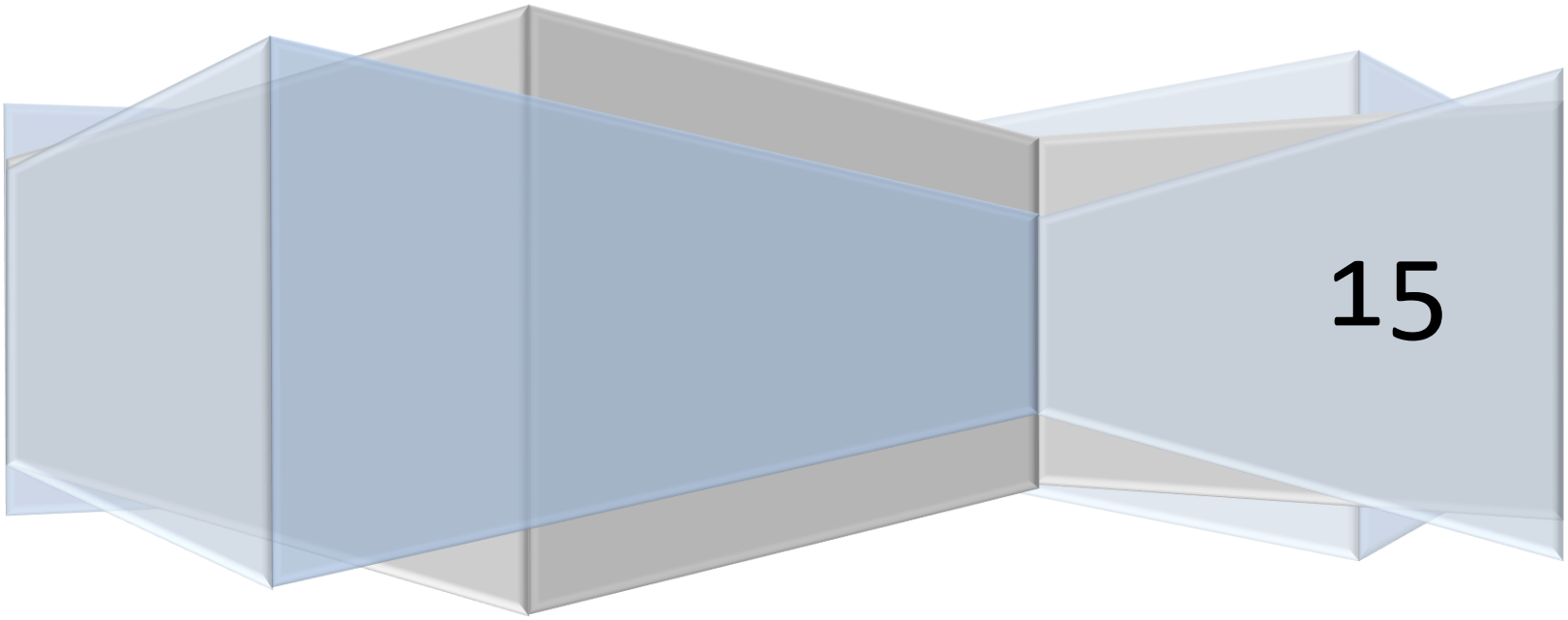
Understanding the Threat Prevention Module

Endpoint Security 10

Intel Security Product Management



Executive Summary

The main audience of this white paper is security administrators who are responsible for managing McAfee VirusScan Enterprise product. The Threat Prevention 10.1 module of McAfee Endpoint Security 10.1 will replace the VirusScan Enterprise 8.8 product. Intel Security has made significant improvements in this new module. The main purpose of this white paper is to familiarize you with new capabilities and provide an understanding of the differences between VirusScan Enterprise 8.8 and Endpoint Security 10.1. This document doesn't replace the Product Guide; instead, it offers a quick, informative read to reduce the learning curve associated with the new product and better prepare you for Endpoint Security 10.1 by answering some questions you might have.

The main topics included in this white paper are:

- New capabilities
- Features, processes and workflows that have changed from VirusScan Enterprise 8.8

What's New in Threat Prevention?

The purpose of this section is to highlight the new capabilities in Threat Prevention module in comparison to VirusScan Enterprise 8.8.

1. Anti-Malware Core (AMCore)

Key Benefit: Better Scanning Performance

AMCore is the next-generation of anti-malware scanning technology that provides enhanced capabilities to counter the newest malware threats with speed and efficacy. The capacity and capabilities of endpoints have increased dramatically and multi-terabyte endpoints are now the norm in the Enterprise. Previous generations of AV, which scanned every individual file, are not optimized for this new environment.

One of the key design goals of the next-generation McAfee Anti-Malware Engine Core (AMCore) is to provide top-tier performance and maintain a high level of protection by introducing an intelligent strategy to scan only items that really need to be scanned, instead of scanning all items equally. AMCore accomplishes this particular efficiency without requiring customers to make any configuration changes in the product. This technology is already running on millions of Consumer endpoints and has been tested extensively in the field. AMCore has also been subjected to numerous efficacy, performance, and false tests by third-party organizations, such as AV-Test.org and AV-Comparatives.org. As with the previous anti-malware engine, each release of AMCore content (V3 DAT) undergoes extensive quality and safety testing.

2. Zero-Impact Scanning

Key Benefits: Increased performance, make scanning invisible to end users

What is Zero-Impact Scanning?

Zero-impact scanning is a new on-demand scan capability that scans a system only when it is idle. As you are aware, scanning, especially on-demand full scans, can be resource-intensive. This new capability enables scanning the system only when end users are not using their computer.

How does Zero-Impact Scanning work?

Endpoint Security 10.1 monitors the system for idle state. The idle-state is determined by monitoring disk utilization, user idle state, and the full screen mode (presentation mode).

- Disk utilization is monitored using WMI (Windows Management Instrumentation). The WMI check is performed at regular intervals to monitor disk usage. If disk usage over that time is less or more than the threshold limit, a notification is sent. Endpoint Security performs further evaluation to determine the idle state.
- The "user idle" state is a derived value based on keyboard events, mouse movement, and full-screen mode.
- Full-screen mode is detected if the current application is run in full screen, for example, PowerPoint presentations and videos playing full screen.

Threat Prevention starts scanning within 3 minutes of determining the idle state. A running scan pauses automatically when end users start using their system or disk utilization increases. At the next idle state, scanning starts again from the point it left off. A system reboot doesn't terminate the scan.

Configuring Zero-Impact Scanning

In McAfee ePO, navigate to the **Policy Catalog | Endpoint Security Threat Prevention | On-Demand Scan**. Under Scheduled Scan Options, you see the **Scan only when the system is idle** option for both full scans and quick scans, which is enabled by default. Please remember that you still have to schedule these scans (frequency, start time etc.) using Client Task assignments.

Traditional On-Demand Scans – Scan anytime option

The Threat Prevention module continues to support traditional scans, which start based on the schedule set by the administrators and continue to run until they finish, without waiting for the idle condition. We have made additional improvements in this type of scans for Threat Prevention 10.1. Administrators will now be able to configure the maximum number of times a user can defer the scan for 1 hour, the user message, and the duration of the message.
Please note that on-demand scans can be configured to run with either **Scan only when the system is idle** or **Scan anytime** option. Both scan types require a schedule and frequency.

However, when **Scan only when the system is idle** is selected, the scan only runs when the system is idle – it continues to pause when the system is no longer idle and resumes when the system is idle again until it finishes.

For example, let's say you have scheduled the weekly full scan to start on Monday at 10 a.m.

- When the **Scan only when the system is idle** option is selected, the full scan starts at 10 a.m. However, if the user is active on the system at 10 a.m., the full scan pauses immediately and waits for the system to become idle before it resumes. The scan continues pausing and resuming until the full scan for that week is complete.
- When the **Scan anytime** option is selected, the full scan starts at 10 a.m. and continues to run until it finishes. This behavior is similar to VirusScan Enterprise 8.8 scans.

We recommend that you use the **Scan only when the system is idle** option for desktops and laptops because these systems are typically idle at some intervals during the day. We recommend that you use **Scan anytime** for servers because they don't typically enter an idle state.

3. Exploit Prevention

Key Benefit: Increased protection

Threat Prevention 10.1 introduces content-based Exploit Prevention capability. This capability replaces the VirusScan Enterprise 8.8 Buffer Overflow Protection and provides broader range of coverage against vulnerabilities and exploits. The Exploit Prevention content is updated monthly, based on research done by our dedicated malware research team. The content is published in line with the Microsoft Black Tuesday vulnerability announcements. This content not only provides protection against zero-day exploits, but also gives you some flexibility in applying Microsoft patches.

Exploit Prevention includes the following technologies:

GBOP

Generic Buffer Overflow Protection (GBOP) provides content-driven protection for a specific list of APIs against one of the most notorious form of attacks from the Internet. Buffer overflow attacks rely on the simple fact that programmers might make mistakes when dealing with memory space for variables.

DEP

Data Execution Prevention (DEP) is a Windows operating system security feature designed to prevent damage from viruses and other security threats by monitoring your programs to ensure that they use system memory safely. Because it is enforced by the operating system, this protection provides an increase in performance and API coverage. Exploit Prevention reports when DEP is triggered.

Kevlar

Kevlar is a kill bit security feature for web browsers and other applications using ActiveX controls. A kill bit specifies the Object Class Identifier (CLSID) of ActiveX controls identified as security vulnerability threats. This protection is also content driven.

Suspicious Caller

Suspicious Caller protection enhances GBOP by detecting code that was injected by an attacker running in memory. These exploits attempt to bypass traditional security protection mechanisms such as GBOP and DEP. This protection also prevents Return-Oriented Programming-based attacks.

Configuring Exploit Prevention

In McAfee ePO, navigate to the **Policy Catalog | Endpoint Security Threat Prevention | Exploit Prevention**. This feature offers two protection levels: Standard and Maximum. Standard is the recommended default option. Increasing the protection level to Maximum requires policy tuning and testing.

4. Enhanced Access Protection

Key Benefits: Flexible configuration and ease of use

Access Protection (AP) capabilities in the Threat Prevention 10.1 module have been enhanced to provide more flexibility to security administrators. These enhancements include the ability to:

- Specify more file and registry operations (such as read, write, create, delete) compared to VirusScan Enterprise 8.8.
- Create a single AP rule that protects files and registry entries, whereas VirusScan Enterprise 8.8 only protects one per rule.
- Include or exclude processes at the rule level, based on file path, MD5, and digital signer. VirusScan Enterprise 8.8 only allows exclusions based on file path.
- Create global exclusions that apply to all AP rules.

In addition, AP now proactively excludes all McAfee-signed processes from being subject to access controls. VirusScan Enterprise 8.8 doesn't support this capability.

5. Integration of Additional Modules

Key Benefit: Reduced overhead of deploying and maintaining multiple products

Endpoint Security 10.1 introduces the concept of an integrated client. In addition to Threat Prevention, the product includes the Firewall module (previously Host Intrusion Prevention Firewall) and the Web Control module (previously SiteAdvisor Enterprise). All three modules are integrated into a single Endpoint Security Client interface. Intel Security has maintained the flexibility for administrators to pick and choose which modules to deploy on endpoint systems. Although each module is designed to work independently, they leverage common components, such as Self Protection, client interface, scheduler, and logging, to provide a better overall user experience when managing these products. If you are not familiar with McAfee Host IPS Firewall and SiteAdvisor Enterprise, refer to the Endpoint Security 10.1 online help to gain an understanding of the capabilities of the Firewall and Web Control modules.

Policy Configurations

Although the McAfee ePO extensions for each module remain separate, we have grouped them into a single package (called McAfee Endpoint Security 10.1) in the McAfee ePO Software Manager. When you check that package into your McAfee ePO server, you see 4 extensions:

- Endpoint Security Threat Prevention
- Endpoint Security Firewall
- Endpoint Security Web Control
- Endpoint Security Platform (also called Common)

While the Threat Prevention, Firewall, and Web Control extensions include their respective configuration options, Common (ESP) includes configuration options that are shared by all modules. These options include Self Protection, Endpoint Security Client interface, scheduler, and logging. Please note that the configuration for McAfee Agent remains separate.

Client Packages for Modules

The client deployment package for each module remains separate. Whether you are using McAfee ePO or a third-party tool to deploy the client package, you can pick and choose the client package to deploy on the endpoints. Each client package uses our new installer, which is shared by all modules, giving you a consistent installation experience.

Integrated Dashboards

You will notice new Endpoint Security dashboards in McAfee ePO. The main objective of these dashboards is to provide an integrated view of the Endpoint Security 10 modules. For example, the new **Endpoint Security: Installation Status** dashboard provides a view of all Endpoint Security modules that are installed on the endpoint systems. Please refer to the online help for information on these new dashboards.

Client User Interface

The new Endpoint Security Client interface is modern, touch-friendly, and designed to address the needs of end users, help desk administrators, and McAfee ePO administrators. The client is also modular – only the modules that are installed on the client appear in the interface.

The client supports three modes of operation:

- **Standard Access**: This mode is the default configuration of the client user interface for McAfee ePO-managed systems. In this mode, end users don't have access to any configurations (policy settings), but they do have the ability to perform basic functions, such as initiating on-demand scans, viewing the quarantine folder, accessing log files, and getting new updates. This mode also supports password-based administrator access. Once you enter the password, the client allows you access to all configuration settings. This ability is useful to helpdesk administrators who might require access to policy settings in troubleshooting scenarios. Please note that any changes made to policy settings locally will be overwritten as soon as the client receives a policy update from McAfee ePO.

- **Full Access**: This mode allows full access to the client interface, including the ability to view and edit policy settings without the need to enter a password. This mode is designed mainly for the standalone (unmanaged or self-managed) systems.

- **Lock Client Interface**: This mode completely hides the client user interface from the end users.

6. Additional improvements

Automatically Scanning Files Downloaded from the Web

The Web Control and Threat Prevention modules work together to provide enhanced protection and visibility of files downloaded from the web. Please note that both Web Control and Threat Prevention must be installed on the endpoint system to use this feature.

Configuring File Download Protection

In McAfee ePO, navigate to the **Policy Catalog | Endpoint Security Web Control |Options**. Under **Action Enforcement**, you see the **Enable file scanning for file downloads** option, which is enabled by default. You can also configure the McAfee GTI sensitivity levels specifically for scanning downloaded files. The McAfee GTI settings for these scans override and are independently of the McAfee GTI sensitivity setting for On-Access Scan (OAS) and On-Demand Scan (ODS). For example, you can set McAfee GTI sensitivity to **Medium** for OAS and ODS and, for files downloaded from the web, you can the sensitivity to **High** to give you an additional level of protection. In addition to protection, you can capture the source URL for these type of events, providing you visibility into Web URLs that are malicious in nature.

On-Demand Scan Configurations

The Threat Prevention module supports 4 different types of On-Demand Scan: Full Scan, Quick Scan, Custom Scan, and Right-Click Scan. All scans can be configured by administrators. Note that configuration of these scans is much more flexible in Threat Prevention when compared to VirusScan Enterprise 8.8:

- Full Scan and Quick Scan are configured through policies instead of the Client Task Catalog.
- Full Scan, Quick Scan, and Custom Scan can be configured to run only when the system idle, as described earlier.
- Right-Click Scan is completely configurable through a policy.

Password Protection for Uninstallation

All modules, including the Threat Prevention module, can be password-protected from being uninstalled. Even local administrators of the system won't be able to uninstall modules unless they know the password for this operation.

Content Rollback in McAfee ePO

The Threat Prevention module allows rollback of AMCore content using a client task in McAfee ePO, giving more flexibility to the administrators.

Enhanced Logging, Threat Events, and Reporting

The Threat Prevention modules provides three distinct type of logs and event reporting. You can access files form the client interface.

- **Activity Logs** are designed to capture information only events. These logs include events, such as when system idle state was determined, when a scan started, paused, or resumed, and which files couldn't be scanned.

- **Threat Events** are more descriptive in the Threat Prevention than in VirusScan Enterprise. We have included new attributes that provide visibility into host name and location, detection feature, file hash, file date and time, if detection occurred through DATs or McAfee GTI lookup, duration of the file on system before it was detected. We also introduce natural language description of threat events. This information is available in the client interface as well as from McAfee ePO.
  Here is an example event:

  Username\name ran C:\Program Files (x86)\Internet Explorer\iexplore.exe, which attempted to access :\Users\username\AppData\Local\Microsoft\Windows\INetCache\IE\1WPY3AJV\jZipSetup-r427-n-bi (1).exe.50l18x8.partial and the threat potentially unwanted program SearchSuite was detected and deleted.

- **Debug Logs** are the standard troubleshooting logs that, when enabled, generate detailed information that can be consumed by McAfee Technical Support to help troubleshoot issues.

Common Policies for Windows and Macintosh Systems

Both Windows and Macintosh systems can now be managed by the same policy configurations in McAfee ePO. Administrators no longer need to manage Threat Prevention policies for Macintosh platform separately.

Migration Assistant

The Threat Prevention 10.1 module supports migration of VirusScan Enterprise 8.8 policies. Please refer to the Migration Guide for details on how existing VirusScan Enterprise 8.8 policies and client configurations can be migrated to Endpoint Security 10.1.

Changes from VirusScan Enterprise 8.8

The purpose of this section is to highlight features, processes, and workflows that have changed in Threat Prevention 10.1 module since VirusScan Enterprise 8.8.

Policy Configurations

- The Threat Prevention module no longer supports the **Workstation Only** and **Server Only** concept that existed in the VirusScan Enterprise 8.8 extension policies. You might have to configure separate policies for workstations and servers based on your needs. Please refer to the Migration Guide to understand how existing VirusScan Enterprise 8.8 configuration related to this aspect will be handled during migration.
- To simplify policy configuration in Threat Prevention, the number of policy categories has been reduced. For example, High-Risk, Low-Risk, and Normal On-Access Scan policies are combined into a single policy category.
- Instead of the VirusScan Enterprise Targeted Scan, we now support out-of-the-box polices for Full Scan and Quick Scan.
- The Access Protection categories concept has been eliminated in the new module. Access Protection rules now exist as a flat list of items. We have also decoupled Self Protection (protection of McAfee resources) from Access Protection. Self Protection is now part of the Endpoint Security Platform in the Options policy.
- The port blocking rules that existed in VirusScan Enterprise have been permanently removed from Threat Prevention. Please leverage the Firewall module for port blocking capabilities.
- Considerations for exclusions:
    - If an administrator wants to exclude files from a scan because there are local or custom applications that could trigger detections, then you must define exclusions.
    - File exclusions were previously used to help improve performance. With the new trust models in AMCore and the use of caching, using file exclusions in this way might be counterproductive.
    - If an administrator needs to exclude files from scanning purely for performance reasons, process exclusion is the most effective approach. Please refer to the AMCore Trust Model document for further details on AMCore scanning mechanism.
- **Let McAfee Decide** – When you let McAfee decide whether a file requires scanning, the on-access scanner uses *trust logic* to optimize scanning. Trust logic improves your security and boosts performance by avoiding unnecessary scans. For example, McAfee analyzes and considers some programs to be trustworthy. If McAfee verifies that these programs haven't been tampered with, the scanner might perform reduced or optimized scanning. Please refer to the AMCore Trust Model document for further details on the AMCore scanning mechanism.

Content

- The traditional VirusScan Enterprise content (signatures or DATs) in the Threat Prevention module are referred to as *V3 DATs* by McAfee Labs. V3 DATs have a different structure, with enhanced capabilities, compared with VirusScan Enterprise DATs. The Endpoint Security Client and McAfee ePO refer to these DATs as “AMCore content”.
- Engine updates in the Threat Prevention module are now bundled with the DATs in the content by Intel Security to ensure the right combination of components. V3 DATs with the new engine are thoroughly tested by McAfee Labs before release and deployment is throttled. This entire process is seamless and handled automatically.
- Exploit Prevention content is a separate content stream and is released monthly. The Endpoint Security Client and McAfee ePO refer to this content as “Exploit Prevention content”. This content doesn’t support the roll back capability available with the V3 DATs.

Endpoint Security Client Interface

- The new Endpoint Security Client interface supports password-based unlocking. When the client interface is unlocked, settings and configuration for all the Endpoint Security modules that are installed on the system are visible. Further granularity of locking and unlocking only certain areas of the client interface is not supported at this time.
- The **About** box displays installed modules, versions, and management mode, as well as AMCore and Exploit Prevention Content versions.
- The client interface can be accessed by right-clicking the McAfee icon in the Windows system tray.