TECHNICAL BRIEF

McAfee
Together is power.

Technical Overview: McAfee MVISION Endpoint and MVISION ePO

Evolving threats, shortage of security talent, and proliferation of management tools—these are the driving forces behind the McAfee® Device Security portfolio and, in particular, our newest McAfee® MVISION product innovations. With solutions that span endpoints, servers, mobile, cloud, and IoT devices, McAfee aims to increase the effectiveness of your security team while reducing their frustration. This paper provides a technical overview of two of the McAfee MVISION solutions: McAfee® MVISION ePO™ and McAfee® MVISION Endpoint.

Connect With Us

McAfee MVISION ePolicy Orchestrator (MVISION ePO)

McAfee MVISION ePolicy Orchestrator® (MVISION ePO) is a cloud-based system that deploys rapidly and monitors and manages your entire digital terrain from a single console. Automated workflows and prioritized risk assessment reduce the time and tasks required to triage, investigate, and respond to security incidents.

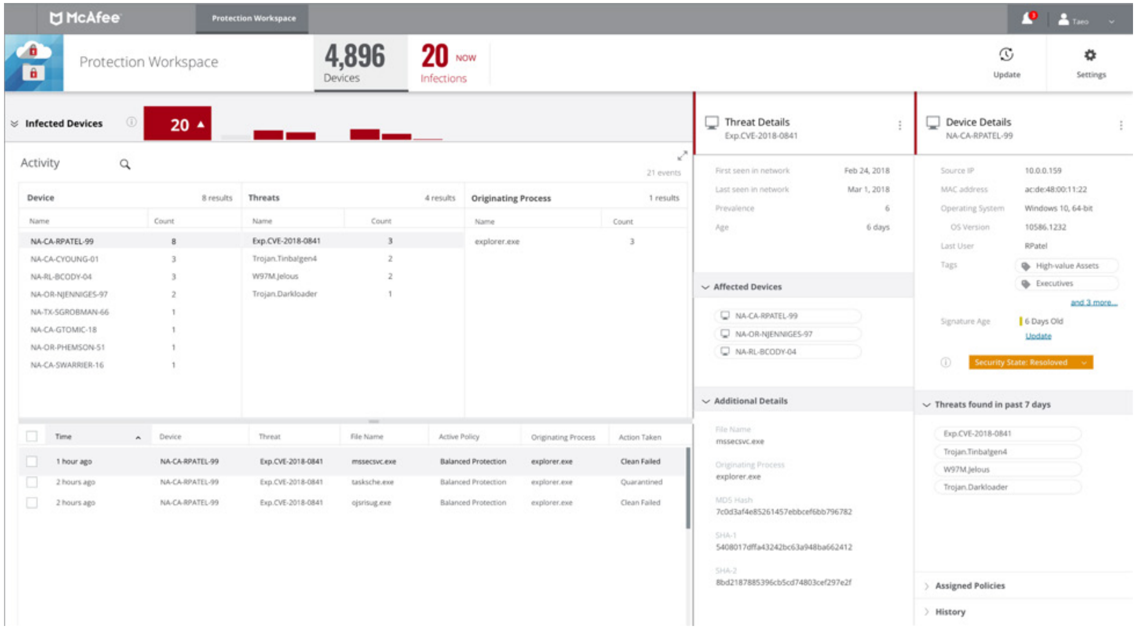
Deployment and setup

MVISION ePO is a Software-as-a-Service (SaaS) management tool hosted by McAfee that is always kept up to date. Setting up the McAfee multitenant hosted version takes only a few minutes. Simply open up a browser to create an account, and configure for your network. There's no need to manage behind-the-scenes infrastructure. All you have to do is focus on security. An extensive set of included scenarios makes it fully functional from the start, while rich customization features enable fine-tuning to fit your environment. The architecture scales to hundreds of thousands of devices and complex environments on a single server.

Customizing dashboards and reports

An easy-to-use dashboard called the Threat Protection Workspace makes processing visualizations much faster than tables of numbers or lists of alerts. You can monitor threats, view compliance information, and manage devices with simplified workflows.

MVISION ePO also includes powerful pre-defined and customizable dashboards and reports to help you keep watch over your environment with your preferred data most prominently displayed. Intuitive color-coded graphs and charts are easy to understand and enable rapid drill downs to investigate and remediate potential threats. You can query your compliance metrics and best practices, such as installed software versions or malware scans. You can also get detailed reports on compliance requirements and historical trends. MVISION ePO allows you to quickly navigate to any group, subnet, or device; review detailed logs; and perform immediate remediation actions.



Device	8 results
Name	Count
NA-CA-RPATEL-99	8
NA-CA-CYOUNG-01	3
NA-RL-BCODY-04	3
NA-OR-NJENNIGES-97	2
NA-TX-SGROBMAN-66	1
NA-CA-GTOMIC-18	1
NA-OR-PHEMSON-51	1
NA-CA-SWARRIER-16	1

Threats	4 results
Name	Count
Exp.CVE-2018-0841	3
Trojan.Tinbalgen4	2
W97M.Jelous	2
Trojan.Darkloader	1

Originating Process	1 results
Name	Count
explorer.exe	3

□	Time	Device	Threat	File Name	Active Policy	Originating Process	Action Taken
□	1 hour ago	NA-CA-RPATEL-99	Exp.CVE-2018-0841	mssecsvc.exe	Balanced Protection	explorer.exe	Clean Failed
□	2 hours ago	NA-CA-RPATEL-99	Exp.CVE-2018-0841	tasksche.exe	Balanced Protection	explorer.exe	Quarantined
□	2 hours ago	NA-CA-RPATEL-99	Exp.CVE-2018-0841	ojsrisug.exe	Balanced Protection	explorer.exe	Clean Failed

Threat Details
Exp.CVE-2018-0841

First seen in network	Feb 24, 2018
Last seen in network	Mar 1, 2018
Prevalence	6
Age	6 days

Affected Devices
NA-CA-RPATEL-99
NA-OR-NJENNIGES-97
NA-RL-BCODY-04

Additional Details
File Name
mssecsvc.exe
Originating Process
explorer.exe
MD5 Hash
7c0d3af4e85261457ebbcef6bb796782
SHA-1
5408017dffa43242bc63a948ba662412
SHA-2
8bd2187885396cb5cd74803cef297e2f

Device Details
NA-CA-RPATEL-99

Source IP	10.0.0.159
MAC address	ac:de:48:00:11:22
Operating System	Windows 10, 64-bit
OS Version	10586.1232
Last User	RPatel
Tags	High-value Assets Executives and 3 more...
Signature Age	6 Days Old Update

Security State: Resoloved

Threats found in past 7 days
Exp.CVE-2018-0841
Trojan.Tinbalgen4
W97M.Jelous
Trojan.Darkloader

Figure 1. MVISION ePO includes pre-defined and customizable dashboards a consolidated view, and prioritization of threat data.

MVISION Endpoint

Advanced defenses for Microsoft Windows 10

McAfee MVISION Endpoint works with the native security in Windows 10 systems by adding local and cloud-based technologies to analyze and combat advanced, zero-day threats. A lightweight agent is used to manage McAfee technologies alongside Microsoft Windows Defender Antivirus, Defender Exploit Guard, and Microsoft Windows Firewall settings. McAfee machine learning analysis detects threats that bypass Windows 10, Server 2016, and Server 2019's basic malware detection capabilities. File-based, fileless, and zero-day threats that otherwise might be missed are prevented from compromising your endpoints.

Data theft and system rollback

Unfortunately, you can't guarantee that your users won't fall victim to a phishing or socially engineered attack. MVISION Endpoint includes credential theft monitoring and rollback remediation to help prevent breaches, keep users productive, and help eliminate support tickets or time spent on re-imaging infected machines. Files that otherwise may have been lost to a ransomware infection can also be recovered.

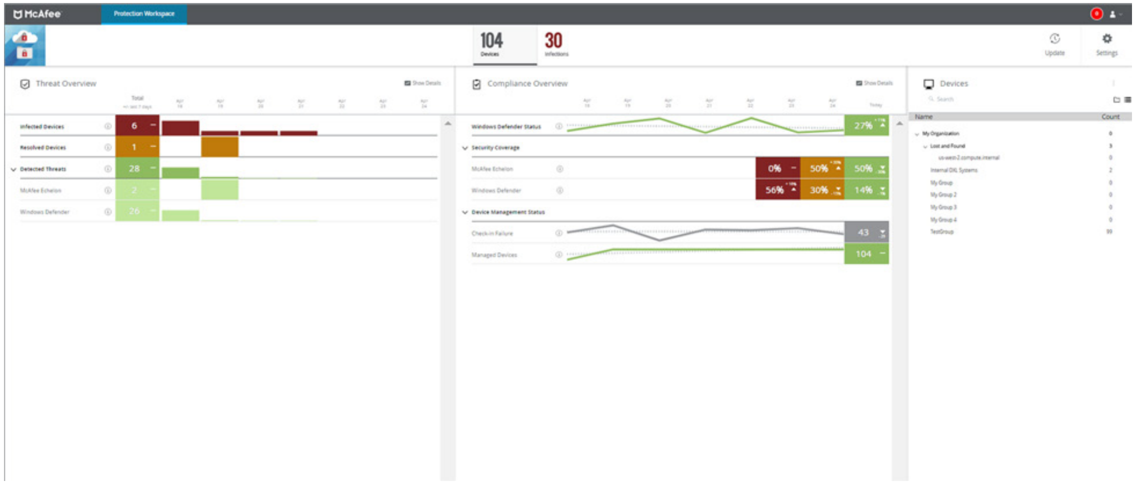
Unified policies and management

Avoid duplicating work by defining policies for Windows Defender Antivirus, Defender Exploit Guard, Windows Firewall, and MVISION Endpoint in one area. Out of the box best-practice rules make it easier to apply and manage the best Windows Firewall rules for your environment. You can also get visibility into the number of blocked events in the last 24 hours from Windows Defender Firewall rules and the compliance data from your endpoints in MVISION ePO.

The Story Graph feature is another way to quickly visualize and get insight into threats and the actions taken against them. It provides trace information about the actions that led up to the detection of a threat event, allows users to review those actions, and better determine the cause of the threat.

Deployment options

MVISION Endpoint is deployed and managed using locally installed, SaaS (MVISION ePO) or an Amazon Web Services (AWS) deployment of McAfee ePolicy Orchestrator software. Automated tasks deploy endpoint software to either individually selected systems or groups of systems. Auto-update functions keep the software clients current with zero user intervention or administrative overhead.



Name	Count
My Organization	0
Lost and Found	3
us-west-2.compute.internal	0
Internal DXL Systems	2
My Group	0
My Group 2	0
My Group 3	0
My Group 4	0
TestGroup	99

Figure 2. See threats and your compliance status across McAfee and Microsoft technologies in one area.

MVISION and McAfee Device Security Offering

Just because threats are complicated doesn't mean your security has to be

Adversaries use a range of attack techniques and target multiple device types. They launch organized campaigns utilizing a breadth of tactics across the entire digital terrain to establish a foothold, maintain persistence, and move laterally in order to take advantage of any unsecured assets. McAfee Device Security provides the unified management, visibility, and layered countermeasures required to mount an effective defense against these campaigns while avoiding the complexity of patchworked point products and fragmented consoles delivering:

- Reduced operational overhead with the simplicity of a single console through McAfee ePO software (with SaaS, cloud and on-premises options)
- Better protection against blended threats through smart, layered countermeasures that stop both fileless and malware-based attacks
- A single solution to secure both modern and legacy devices with the flexibility to deploy full stack defense or an advanced countermeasure overlay to native controls on endpoints
- Simplified management through the unification of both McAfee and native controls and policies
- Comprehensive coverage for multiple device types—traditional endpoints, mobile, and fixed-function systems

Learn more about McAfee MVISION products by visiting **www.mcafee.com/MVISION**.

McAfee
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com