McAfee MVISION Endpoint

Advanced endpoint security for Windows desktops and servers

Organizations looking for simpler, more affordable alternatives to full-featured endpoint security platforms (EPP) are embracing native security like Microsoft Windows Defender. While Windows Defender provides essential base-level protection, it's still necessary to apply advanced countermeasures like machine learning to mount a complete defense against sophisticated fileless and zero-day malware-based threats. The key to success lies within leveraging, strengthening, and managing the security already built into Windows desktop and server environments[1] without introducing the complexity of multiple consoles. McAfee® MVISION Insights[2] delivers proactive endpoint security analytics and actions before the attack hits further strengthening your security posture.

Security or Complexity?

Because these tools are usually managed separately, security teams are faced with the dilemma of whether to get a stronger defense at the cost of adding complexity. Typically, this also means eliminating the financial and operational savings they had hoped to gain.

A better choice: advanced defenses and cohesive management

With McAfee® MVISION Endpoint, you can eliminate the dilemma of effectiveness or efficiency by getting both. You get file, fileless, and behavioral machine learning analysis for advanced threat detection and centralized management for every endpoint in your environment. You can also avoid complex workflows, thanks to a consistent and centralized console for policy management of Windows Defender Antivirus, Defender Exploit Guard, Windows Firewall, McAfee defenses, and Mac or Linux systems. Co-management and unified policies not only remove redundant entry time, it improves your visibility into your endpoint environment.

Maximize your defenses and prevention

MVISION Endpoint delivers enhanced detection and correction capabilities to augment native controls, which are always up to date. Machine learning, credential theft monitoring, and rollback remediation substantially boost the basic security built into the Windows desktop and

Key Advantages

- **Advanced defenses for advanced threats:** Machine-learning, credential theft defense, and rollback remediation complement Windows desktop and server systems' basic security capabilities.
- **No additional complexity:** Manage McAfee technologies, Windows Defender Antivirus policies, Defender Exploit Guard, and Windows Firewall settings using a single policy and console.
- **MVISION Insights:** Respond immediately to potential active campaigns that are prioritized according to whether they are targeting your sector or geographies with a leading actionable security intelligence solution available today. MVISION Insights will predict which endpoints are lacking protection against the campaigns and offer prescriptive guidance on what to do to improve the detection.

Connect With Us

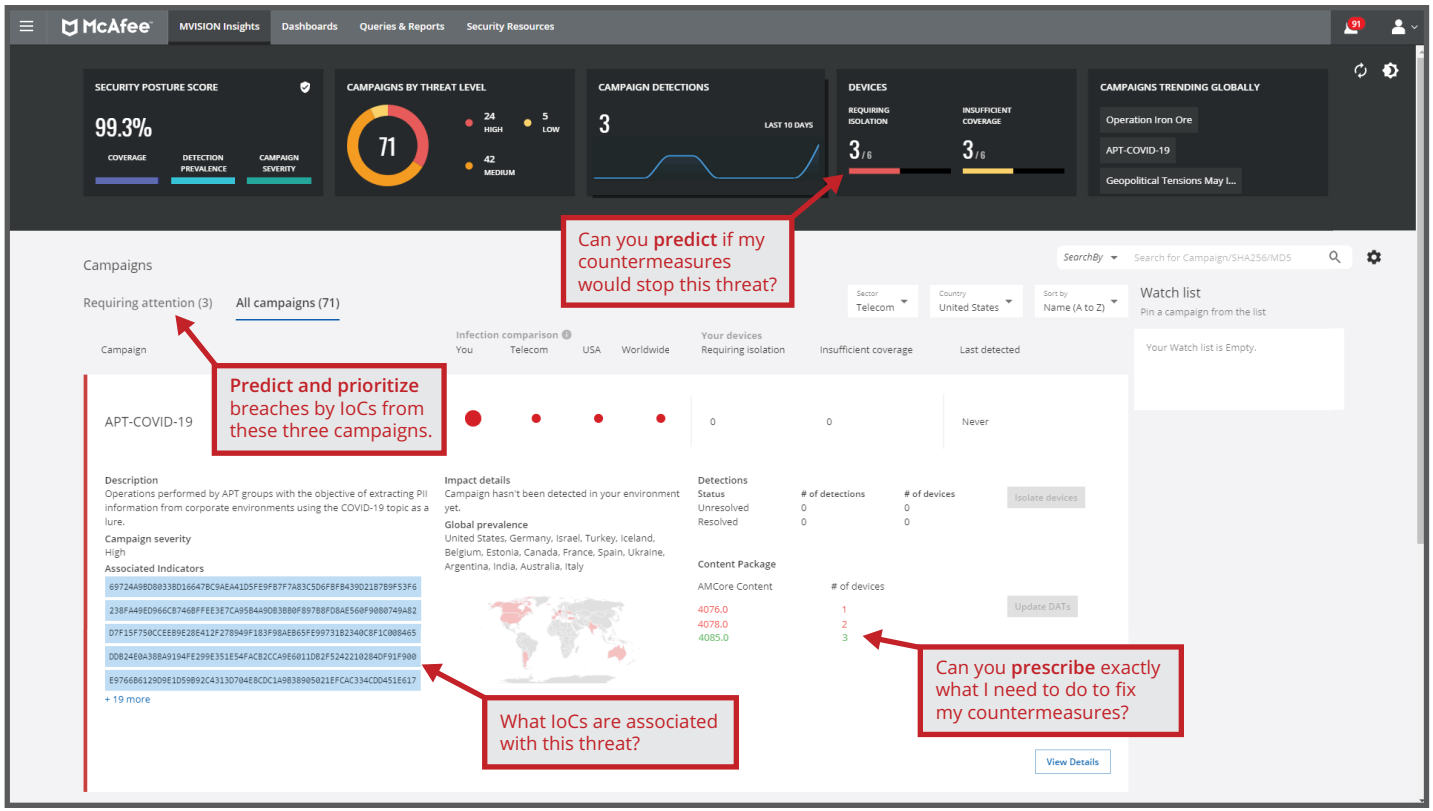

Figure 1. MVISION Insights offers proactive cybersecurity from a unified dashboard that answers key questions.

server operating system (OS) and effectively combat advanced, zero-day threats. This approach lets you avoid the tricky questions of whether to invest in native or third-party technologies by aligning and giving you the best of both. Advance your prevention capabilities by updating your security postures to counter potential high priority threats before they attack.

Recover time

McAfee machine learning technology offers a much higher detection rate than signature-based defenses alone, with fewer false positives than competing solutions. This helps keep administrators focused on the real threats in their environments, rather than on exonerating the non-malicious.

A unified defense that leverages, strengthens, and manages the base security of Windows 10, Windows Server 2016, and Windows Server 2019 systems

Get Started Quickly

- Immediately view and act on the threats that matter to your organization.
- Apply out-of-the-box policies to Windows Defender Antivirus, simplify Defender Exploit Guard management to the most critical rules, and apply best practices rule settings to Windows Firewall.
- Use existing McAfee management or deploy rapidly using a SaaS-based console.
- Use the Story Graph to quickly visualize threats, actions taken against them, and determine how to further harden your endpoints against future attacks.
- A small client size makes downloads light and fast.

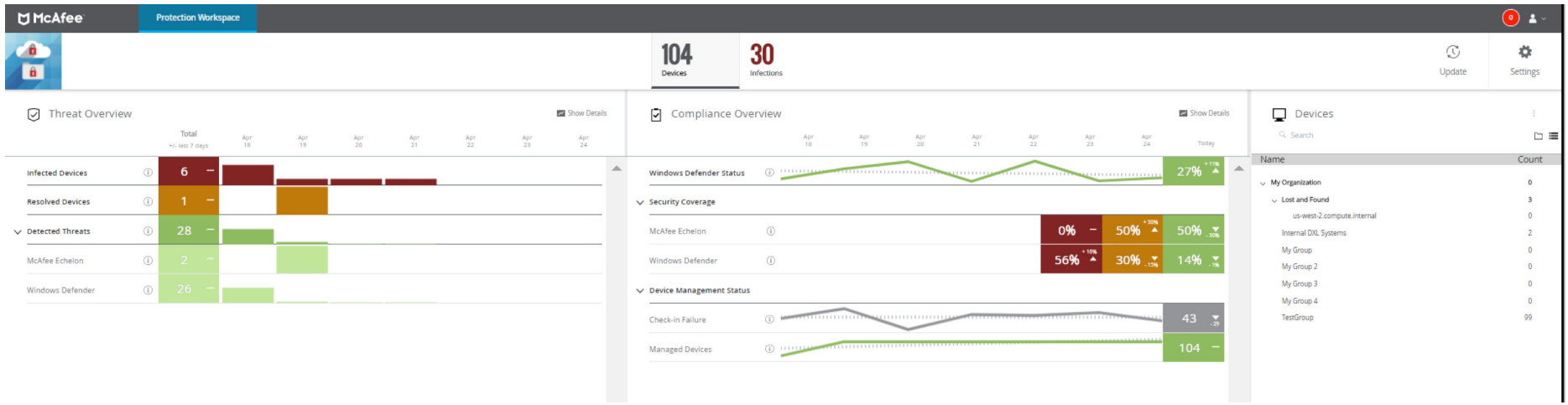

Figure 2. The threat protection workspace allows you to view threats and compliance across McAfee and Microsoft technologies.

MVISION Endpoint is also able to monitor and restore the original versions of files impacted by suspicious processes and to remove other malicious files or processes that may have been introduced. For users, this means they remain productive rather than dealing with downtime during remediation and recovery. For administrators, that means less time spent on re-imaging or recovering compromised endpoints and more time spent on making their organization productive.

Get more visibility

MVISION Endpoint is managed using a single pane of glass that gives visibility into your environment for both threats and compliance, including reporting for BitLocker. Instead of pivoting from one console to another to connect the dots on what, where, and how a threat event happened, an easy-to-use dashboard, and configurable alerts guide you to the data that is most important.

The Story Graph feature is an additional tool to simplify investigations and help administrators harden endpoints from attacks. 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.

Management flexibility

McAfee MVISION Endpoint offers a choice of:

- **Pure SaaS management:** Multitenant, globally scaled, and maintained by McAfee.
  - **Benefits:** Anytime, anywhere access to the management console, automatic updates, and management maintenance for a lower total cost of ownership (TCO).
- **Virtual deployment:** Fully operational in less than an hour with management deployed in an Amazon Web Services (AWS) environment.
  - **Benefits:** Leverage existing investments in virtualized environments to lower your deployment and maintenance costs while retaining customized control.
- **Local deployment:** An onsite, locally installed deployment of the management software on a server.
  - **Benefits:** Customers can use existing deployments and manage multiple McAfee technologies centrally.

Designed for Performance

MVISION Endpoint has an incredibly small and lightweight footprint, as many of its capabilities are delivered through cloud-based services. Getting started can happen rapidly as a result, and the client file size is small, so your download time is short and the impact to your bandwidth is light.

Once installed, no updates are required for your defenses, and any future updates will occur automatically, with no action required by an administrator to install them.

The impact to your endpoint environment and your users is kept minimal through default-balanced performance settings that scale the need for computing power and bandwidth as needed instead of remaining in an always-on state.

A unified platform for your entire environment

With the growth of bring-your-own-device (BYOD), mobile, and Internet of Things (IoT) devices, many organizations need protection for other operating systems and types of devices. To address this growing complexity, McAfee has introduced our innovative MVISION technologies which bring our strategic vision for simplified management, stronger Windows security, mobile, and IoT device security to the McAfee portfolio.

McAfee MVISION technologies use a cloud-first approach to device security that empowers security professionals to manage a comprehensive array of McAfee, third-party, and native operating systems (OS) through a single point of visibility and control.

With the McAfee Device Security portfolio, you get the protection you need across the entire attack surface: desktops, laptops, tablet, mobile, physical/virtual servers, cloud workloads, and IoT.

What can it do for your business?

- Centralized management for all devices
- Advanced, file, fileless, and behavioral machine learning defenses
- Protection for your Mac, Linux, IoT, and mobile devices
- Shift your cybersecurity left before the attack
- Lower your TCO and streamline workflows

Why should you choose McAfee?

- Do more, do it faster, and with fewer clicks
- The industry's only vendor to offer combined management and pre-tuned advanced defense for native controls
- Visibility across your entire device environment
- A large, open ecosystem with multiple integrations
- Distinct proactive endpoint security

Learn More

For more information, visit: **www.mcafee.com/MVISIONEndpoint**.

1. Microsoft Windows 10, Microsoft Server 2016, and Microsoft Server 2019 systems
2. This document contains information on products, services and/or processes in development. The benefits described herein depend on system configuration and require enabled hardware, software, and/or service activation. All information provided here is subject to change without notice at McAfee's sole discretion. Contact your McAfee representative to obtain the latest forecast, schedule, specifications, and roadmaps.

Cost and time reduction scenarios described are intended as examples of how the given McAfee products, with optimized configurations and deployments, may affect future costs and provide cost and time savings. Circumstances and results will vary by configuration and deployment. McAfee does not guarantee any time or cost reduction.

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