SOLUTION BRIEF

A Simpler Approach to Endpoint Security

Developing a unified defense to protect every endpoint—from device to cloud

Cybersecurity is in the midst of a catch-22: As the sheer number, level of sophistication, and financial impact of breaches continues to escalate, the available pool of skilled analysts is smaller than ever.

Now there's a way to solve the complex security issues facing your company, while accomplishing more in less time and with fewer resources. The McAfee® Endpoint Protection Portfolio leverages analytics and machine learning to achieve industry-leading effectiveness, all while offering the flexibility to connect our solutions to products from more 150 other vendors. As we work to unify data and threat defense from device to cloud, we are building a future where security is an integrated system—simpler, smarter, and broader than anything that's ever come before.

Key Benefits

- Defend your endpoints with exploit prevention, firewall, web control, and machine learning.
- Protect iOS and Android devices against phishing, zero-day attacks, and data loss in real time, even when offline.
- Powerful threat detection, investigation, and response—simplified with AI-guided investigations.
- Add machine learning, credential theft defense, and rollback remediation to basic operating system security capabilities.
- Simplify and accelerate your security effectiveness with single-pane-of-glass management. Choose SaaS-based management with MVISION ePO or on-premises management with McAfee® ePO™.

Connect With Us

As the number, type, and complexity of enterprise endpoints continues to grow, companies are finding themselves at a crossroads. Do they continue relying on traditional antivirus solutions alone, knowing that doing so leaves them open to modern threats such as ransomware and botnets? Or should they bolt together a multivendor "solution" that will offer greater threat protection, but also slow processes, bog down machines, and cause significant downtime? Fortunately, with the McAfee Endpoint Protection Portfolio, businesses no longer have to compromise between threat defense and operational agility.

McAfee Endpoint Security

Central management, shared analysis

This integrated, centrally managed endpoint protection platform uses a single agent for multiple technologies, including Threat Protection, Firewall, Web Control, Adaptive Threat Prevention, and more—all designed to simplify complex environments.

Unlike traditional antivirus software, McAfee Endpoint Security leverages connections between local endpoints and McAfee® Global Threat Intelligence in the cloud to detect zero-day threats in near real time. As soon as a threat has been identified anywhere, it can be spotted everywhere. The combination of shared analysis and information with advanced exploit protection capabilities allows McAfee Endpoint Security to achieve a 25% higher protection rate against zero-day threats than McAfee® VirusScan® Enterprise. In independent tests, McAfee Endpoint achieved an effectiveness rate of 99.98% overall—with zero false positives.[1]

Automated maintenance, efficient remediation

With McAfee Endpoint Security, you can leverage enhanced automation and machine learning features. The platform's machine learning behavior classification detects zero-day threats in near-real time, enabling actionable threat intelligence. What's more, it automatically evolves over time to identify new behaviors and add rules to identify future attacks.

During an attack, administrators can quickly see where infections are occurring and how long endpoints have been exposed, allowing them to understand the threat and react more quickly. The Real Protect feature can repair targeted endpoints to the last known good state to immediately prevent infection and reduce administrator burdens. Dynamic Application Containment further defends against ransomware and greyware by allowing you to secure "patient zero."

The combination of the McAfee ePO platform with McAfee Endpoint offers greater visibility, boosts IT productivity, simplifies operations, unifies security, and reduces costs. These and other efficiencies have allowed cybersecurity teams who have migrated to McAfee Endpoint Security to save as much as 40 hours per week on management.[2] Employee productivity is preserved as well: scans take only seconds and only occur when the device is idle, resuming seamlessly after a restart or shutdown. Best of all, McAfee Endpoint Security is lightweight and does not require a cloud connection, so users are defended even when they're offline.

Key Benefits of McAfee Endpoint Security

- Detects zero-day threat in near real time
- Continually updates anti-malware engine
- Enables communication among antivirus, exploit prevention, firewall, and web control
- Repairs the endpoint to the last known good state
- Contains malicious applications and processes on endpoints even when they are offline
- Prioritizes alerts with attack "playback" of events
- Provides integrated, easy-to-use incident hunting and response
- Makes incident response as simple as a single click

McAfee MVISION EDR

The average IT department manages thousands of endpoints—from desktops and servers to mobile phones, smart watches, and IoT devices. Current EDR solutions dump too much information on already stretched security teams, relying on veteran analysts to investigate threats. This approach hasn't proven effective or scalable, especially when compounded by today's bandwidth constraints and skills gaps.

MVISION EDR picks up where antivirus technologies and traditional EDR solutions leave off. The integrated endpoint security solution helps manage a high volume of alerts, monitoring and collecting activity data from endpoints that could indicate a threat and providing the visibility and context needed. By analyzing the data to identify threat patterns, its AI automated response and analysis capabilities can automatically remove or contain threats and notify security personnel, while the forensics and analytics tools research identified threats and search for suspicious activities.

Level up with artificial intelligence (AI)-guided investigation

EDR solutions traditionally "enable" investigation by providing raw data, context, and search functions—but they still require knowledgeable analysts to perform the inquiry and analysis. MVISION EDR, on the other hand, guides the investigation, reducing the expertise and effort needed to perform investigations. It also allows analysts to determine the risk and root cause of the incident more quickly.

AI-guided investigation automatically gathers and processes massive amounts of data from different sources, including the source and target of the attack and what the attack pattern looks like. Then, much like a veteran analyst would steer more junior analyst through an inquiry, it automatically poses one or more hypotheses against alerts and gathers, summarizes, and visualizes evidence from multiple sources as investigations evolve. Based on the evidence, MVISION EDR uses these hypotheses to formulate and help answer pertinent questions that will drive the investigation, as analysts work toward deciding whether to continue with more questions and data gathering, retire the issue, or escalate the issue.

This helps analysts increase their level of expertise, making them more adept at managing a high volume of alerts, reducing time to investigation, and improving fidelity of investigations. With even novice analysts able to analyze threats, more senior analysts are free to apply their skills to the hunt and accelerate response times.

Faster identification equals faster response

Analysts can also use the powerful search and always-on data collection capabilities to expand inquiries and look deeply into and across systems. MVISION EDR can take a snapshot of an endpoint's active processes, network connections, services, and autorun entries, allowing for immediate inspection, real-time search, and historical searches. This data is also streamed to the cloud, enabling rapid adoption of new analytics engines and techniques, while behavior-based detection results

Key Benefits of McAfee MVISION EDR

- High-quality actionable threat detection without the noise
- Faster analysis for a more resilient defense
- AI-guided investigations provide machine-generated insights into the attack
- Ability to maximize impact of existing staff
- Low-maintenance cloud solution
- Leverage industry-acclaimed single console security management, MVISION ePO (SaaS-based) or McAfee ePO (on-premises or IaaS-based)
- Analysts' focus is on strategic incident response without burdensome administration overhead

map to the MITRE ATTACK framework, supporting a more consistent process to determine the phase and risk of a threat and prioritize a response.

MVISION EDR's investigation capabilities and insight are expanded even further through integration with security information and event management (SIEM)solutions, like McAfee® Enterprise Security Manager or third-party products. This allows for the correlation of endpoint artifacts with network information and other data collected by SIEM.

McAfee MVISION Endpoint

MVISION Endpoint delivers enhanced detection and correction capabilities for customers who want to harden their endpoint protection. Designed specifically to augment native operating system (OS) defenses, it amplifies the antivirus firewall and exploit prevention native to Windows 10 and Server 2016 and 2019 environments by detecting sophisticated threats missed by Microsoft Defender.

A smarter endpoint strategy

Unlike alternatives that are limited to one form of machine learning analysis, MVISION Endpoint can perform static, behavioral, and fileless malware analysis for stronger threat protection and lower false positives. It uses behavioral machine learning to identify threats by their actual behavior and convicts a file if it shares features with other malware. It also features enhanced rollback remediation, allowing you to return a system impacted by ransomware back to its last known good state.

Single-console, cloud-based defense

Best of all, MVISION Endpoint provides a unified management experience. Instead of duplicating policy management, it allows Windows Defender Antivirus, Exploit Guard, Windows Firewall settings, and McAfee policies to be managed centrally. By deploying McAfee MVISION Endpoint along with McAfee ePO or MVISION ePO, you'll gain truly integrated defense through a single pane of glass. One tool and data visualization tools show your protection status and compliance, including BitLocker reporting. McAfee ePO and MVISION ePO also offer third-party integration capabilities, bringing additional countermeasures into the console to further strengthen and customize your security.

This extremely lightweight agent is simpler and more robust than traditional security tools. With updates automatically delivered to the client, you'll never wonder whether it's up to date—and with a smaller device footprint and balanced performance considerations, user impact is kept to a minimum to preserve productivity.

Key Benefits of McAfee MVISION Endpoint

- Centralized management for Windows 10 and Windows Server 2016 and 2019
- Advanced file, fileless, and behavioral machine learning defenses
- Lower total cost of ownership (TCO) and streamlining of workflows
- Credential theft defense and rollback remediation
- Single-policy and single-console management of McAfee and Microsoft defense technologies

McAfee MVISION Mobile

McAfee MVISION Mobile detects threats and vulnerabilities on Apple iOS or Android devices, the network they're connected to, and the applications that users download. Its integration with our flagship enterprise central management platform, McAfee ePO software, allows you to manage mobile devices just like you would any other endpoint. As an integrated component of McAfee® Device Security, MVISION Mobile extends visibility and control of your mobile assets from the same single console as all your other McAfee-managed devices.

More intelligent, more vigilant

Unlike cloud-based mobile security solutions that rely on app sandboxing or traffic tunneling, MVISION Mobile sits directly on mobile devices to provide continuous threat detection, no matter how a device is connected: through a corporate network, public access point, cellular carrier, or even no connection at all.

MVISION Mobile uses machine learning algorithms fed by billions of data points from millions of devices to identify current or imminent threats and attacks. These analyze deviations from regular device behavior and make determinations about compromise indicators to accurately identify advanced device-, application-, and network-based attacks—including ones that have never been seen before. Comprehensive application intelligence mitigates security and privacy risks, reducing the chance of data loss. And network protection notifications, designed to let you and your employees know whether their device is connecting to an unsafe or compromised network, focus on stopping attacks before they start.

Key Benefits of McAfee MVISION Mobile

- Provides on-device, real-time protection
- Detects mobile threats and protects against zero-day attacks
- Highlights privacy risks to inform users of the dangers associated with any given application
- Speeds response through enterprise-grade actionable mobile threat intelligence
- Allows employees to work anywhere, any time, and on any device, thanks to compliance controls
- Detects harmful links found in text messages, social media apps, and emails through phishing protection
- Integrates with enterprise mobility management (EMM) solutions, but also works in bring-your-own-device (BYOD) scenarios
- Allows incident response teams to take advantage of deep threat forensics for analysis and action to prevent a compromised device from turning into an outbreak

McAfee MVISION ePO

Industry-acclaimed McAfee MVISION ePO is designed to manage McAfee solutions and enhance native security controls built into operating systems. This global, multitenant enterprise SaaS version of proven and unique McAfee ePO software allows you to manage security, set and automatically enforce policies, streamline and automate compliance processes, and increase visibility. It offers scalability to hundreds of thousands of devices, including those with native controls, with coverage from device to cloud—all without the complexity of maintaining an on-premises architecture.

Security, meet simplicity

MVISION ePO's extensible platform provides a common management experience with shared policies for all devices, including Microsoft Windows 10 devices, across the heterogeneous enterprise to ensure consistency and simplicity. MVISION ePO offers single-pane-of-glass visibility, allowing you to eliminate the complexity of orchestrating multiple products. With agile, automated management capabilities, users can rapidly identify, manage, and respond to vulnerabilities, changes in security posture, and known threats—from anywhere, through their browser. From there, security policies can be deployed and enforced across the entire enterprise in just a few steps.

The protection workspace provides a summary of your entire digital terrain in one graphical view, allowing administrators to prioritize risks and drill down on specific events for greater insight. This summary view reduces the time needed to create reports and rationalize the data at hand and removes the potential for error if manual intervention is needed. By bringing risk management and incident analysis together, it enables your devices to provide critical insights to your SIEM, putting critical information at your analysts' fingertips for improved threat hunting and remediation efforts.

Added efficiency

According to industry analysts, McAfee ePO software is a reason many organizations buy from and stay with McAfee.[3] And with this proven technology now available in a SaaS format, enterprises can benefit further by allowing their security professionals to focus exclusively on monitoring and controlling all devices. In addition to eliminating the setup and maintenance associated with an on-premises security infrastructure, MVISION ePO also automates deployment of device security across the enterprise and provides continuous and transparent updates, offering stability and saving time. And, with advanced capabilities to increase the efficiency of the security operations staff when they mitigate a threat or make a change to restore compliance, even greater time savings can be realized.

To find out of MVISION ePO is right for your business, click here for a free trial.

Key Benefits of McAfee MVISION ePO

- Industry-acclaimed centralized management
- Simple, single point of visibility and control from anywhere
- Removal of the complexity associated with on-premises security platform maintenance
- A common view that brings risk management and incident analysis together
- Comprehensive platform that manages McAfee products and native controls in operating systems
- Automated workflows for efficient administrative duties
- Streamlined incident investigation/remediation
- Common security management for largest share of devices on the market
- Scalability from hundreds to thousands of devices
- Coverage from device to cloud

CASE STUDIES

MGM Resorts International

20,000 nodes across 20 resort entities worldwide

- **Challenges:** Unable to mitigate risks and block zero-day attacks; needed to understand complex attack patterns and provide 24/7 uptime for critical applications; unable to reduce SecOps expenses yet stay current
- **Solutions:** McAfee® Enterprise Security Manager, McAfee® Investigator, MVISION EDR, McAfee® Web Gateway, McAfee Endpoint Security, McAfee Data Loss Prevention, DXL, McAfee® Professional Services
- **Results:** Reduced time to contain, investigate, and remediate threats and improved skill of SecOps team

Atrius Health

More than 65,000 users on 9,000 endpoints across more than 29 sites

- **Challenges:** Guard against ransomware and phishing; accelerate time to detect and respond; keep the organization secure, while enabling business growth
- **Solution:** McAfee Enterprise Security Manager, McAfee Endpoint Security
- **Results:** Operational savings; avoided hiring several full-time employees; faster time-to-detect and respond; improved security for virtual environment

Florida International University

55,000 students and 15,000 staff members across two main campuses and satellite overseas campuses

- **Challenges:** Needed to allow freedom of BYOD, yet protect the environment from threats; keep students from accidentally introducing malware into environment; maintain widespread visibility
- **Solution:** McAfee Enterprise Security Manager and McAfee Endpoint Security
- **Results:** Faster containment of suspicious files or attacks; stronger overall security posture without having to augment staff; more robust endpoint protection with minimal impact on users; ease of management and enterprise-wide visibility

Banco Delta

400 endpoints

- **Challenges:** Reduce security management burden; build a strong defense to protect against sophisticated attacks; plan security strategy for the future, including cloud migration
- **Solution:** McAfee ePO platform, McAfee Enterprise Security Manager, and McAfee Endpoint Security
- **Results:** Noticeable reduction in infections and potentially compromising user behavior

US Insurance Company

6,000 desktops and 2.000 servers across 12 locations

- **Challenges:** Unable to secure customers' sensitive personal data; wanted to provide top security without compromising customer experience
- **Solution:** McAfee Endpoint Security, McAfee Data Loss Prevention, and McAfee Web Gateway
- **Results:** CPU utilization spikes reduced from 95% to 30/35% and multiday scans to hours; numerous hours saved weekly by cybersecurity engineers; increased productivity of both end users and SecOps; improved security posture

Large Multinational Bank (EMEA)

45,000 endpoints across more than 40 countries and two data centers

- **Challenges:** Unable to protect the organization from ransomware and zero-day threats or block threats caused by user behavior; wanted to improve security management efficiency
- **Solution:** McAfee Endpoint Security, McAfee ePO platform, McAfee Web Gateway
- **Results:** Improved endpoint protection that catches more malware and defends better against zero-day threats; accelerated time to protection using integrated security solutions that share threat information in near real time; operational time savings from easier security administration and fewer incidents

Case study results are the reported experiences of our customers. They should not be interpreted as a guaranteed outcome.

Big Wins

McAfee Endpoint Security

- Silver Winner for the 2019 Cybersecurity Excellence Awards' Endpoint Security Category
- AV-Comparatives Approved Business Product Award
- AV-TEST: McAfee had a perfect usability score

MVISION Endpoint

- Silver Winner for the 2019 Cybersecurity Excellence Awards' Endpoint Security Category
- 2018 Tech Innovator Award for Endpoint Security

MVISION Mobile

- Silver Winner for the 2019 Cybersecurity Excellence Awards' Mobile Security Category

The McAfee Endpoint Footprint

- 622 million total endpoints
- 97 million enterprise endpoints
- 525 million consumer endpoints
- 69,000 enterprise customers
- 7,000 employees
- 189 countries
- 80% of Fortune 100 firms
- 75% of Fortune 500 firms
- 64% of Global 2000 firms
- 87% of the world's largest banks
- 54% of the top 50 retailers
- 1,550+ security patents worldwide

> "McAfee ePO is one of the forefathers of integrated security automation and orchestration... today's security professionals require the power of traditional [McAfee] ePO, but delivered as a simplified experience, making them both efficient and effective... as a SaaS-delivered workspace, MVISION combines analytics, policy management, and events in a manner that enterprise and midmarket can appropriate."
>
> —Frank Dickinson, Research Vice President, Security Products, IDC

1. AV Comparatives study, 2017—NSS Labs AEP Report
2. SC Magazine, July 5, 2017
3. Gartner Magic Quadrant for Endpoint Protection Platforms, January 24, 2018

McAfee™
Together is power.

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