SOLUTION BRIEF

Overcome the Attacker Advantage with McAfee Endpoint Security

Defenders Are Feeling the Pressure to Up Their Game

In digital combat, cybercriminals benefit from the success of others. Successful breaches provide the motivation and resources for further attacks, whether for financial gain, economic disruption, or corporate intelligence. Organizations of all sizes are at risk from nation-states, hacktivists, organized crime, and malicious and accidental insider threats. The knowledge and capabilities gap between attackers and defenders is mandating fundamental changes to endpoint defenses, cybersecurity's frontline.

Security practitioners are under increasing pressure to defend their organizations. To overcome the attacker advantage, endpoint defenses need to collaborate with each other and with other security technologies to quickly detect, analyze, block, and contain attacks in progress. They need to present forensic information quickly and intuitively. Moreover, they need to do all of this without adding to the complexity of the environment for IT teams or impacting the productivity and performance of the users they protect.

McAfee Endpoint Security Tilts the Battlefield in Your Favor

McAfee® Endpoint Security enables customers to respond to and manage the threat defense lifecycle and provides a collaborative, extensible framework to reduce the complexity of conventional multivendor endpoint security environments. It also provides administrators with visibility into advanced threats to speed detection and remediation response times. Global threat intelligence and real-time local event intelligence are shared between endpoints to further aid in rapid detection and response, while management is kept simple through a true centralized console and easy-to-read dashboards and reports.

McAfee Endpoint Security is built for real-time communication between threat defenses. Events and threat insights are shared with multiple technologies to take immediate actions against suspicious applications, downloads, websites, and files. Redundancies caused by multiple point products or defenses can be found and removed, while a common endpoint architecture integrates several layers of protection to allow threat insights to be shared for faster convictions and analysis.

Integrated Advanced Threat Defenses Automate and Speed Response Times

Additional advanced threat defenses, like Dynamic Application Containment (DAC), are also available as part of the integrated McAfee Endpoint Security framework to help organizations defend against the very latest advanced threats.[1] For example, DAC will analyze and take action against greyware and other emerging malware, containing them to prevent infection.

Another available technology for advanced threat is Real Protect, which uses machine-learning behavior classification to detect zero-day malware and improve detection. The signature-less classification is performed in the cloud and maintains a small client footprint while providing near real-time detection. Actionable insights

are delivered and can be used to create indicators of attack and indicators of compromise. This can be particularly useful for lateral movement detection, patient-zero discovery, threat actor attribution, forensic investigations, and remediation. Real Protect also speeds future analysis by automatically evolving behavior classification to identify behaviors and adding rules to identify future attacks that are similar using both static and runtime features. Lastly, to immediately prevent infection and reduce the time required for IT security administrators, the client repairs the endpoint following a conviction to the last known good state.

Intelligent Endpoint Protection Lets You Know What Attackers Are Doing Now

Better intelligence leads to better results. McAfee Endpoint Security shares its observations in real time with the multiple endpoint defense technologies connected to its framework to collaborate and accelerate identification of suspicious behaviors, facilitate better coordination of defenses, and provide better protection against targeted attacks and zero-day threats. Insights like file hash, source URL, and target processes are tracked and shared not only with other defenses, but also with the client and management interfaces to help users understand attacks and provide administrators with actionable threat forensics. In addition, McAfee Threat Intelligence Exchange technology empowers adaptive defenses to collaborate with other McAfee solutions, including gateways, sandboxes, and our security information and event management (SIEM) solution. Gathering and distributing local, community, and global security intelligence shrinks the time between attack, discovery, and containment from weeks or months to milliseconds.

Combined with McAfee Global Threat Intelligence (McAfee GTI), the McAfee Endpoint Security framework leverages the cloud to monitor and act on the full spectrum of new and emerging threats in real time across all vectors—file, web, message, and network. The existing endpoint footprint and management system is enhanced with localized and global threat intelligence to combat unknown and targeted malware instantly. Automatic actions against suspicious applications and processes quickly escalate responses against new and emerging forms of attack while informing other defenses and the global community.

Customers using DAC and Real Protect get insights into more advanced threats and the behaviors they exhibit. For example, DAC provides information on contained applications and the type of access that they attempt to gain, such as registry or memory.

For organizations interested in collecting endpoint process threat insights to hunt malware and equip incident responders, Real Protect provides insights into behaviors that have been deemed malicious and the classification of threats. These insights can be particularly helpful in uncovering how file-based malware attempts to evade detection through techniques like packing, encryption, or misusing legitimate applications.

Strong and Effective Performance Helps You Respond in Time

Intelligent defenses are of little value if they impede users with slow scans, take a long time to install, or are complicated to manage. McAfee Endpoint Security protects the productivity of users with a common service layer and our new anti-malware core engine that helps reduce the amount of resources and power required by a user's system. Endpoint scans won't impact user productivity because they only occur when the device is idle, and they resume seamlessly after a restart or shutdown. An adaptive scanning process also helps reduce CPU demands by learning which processes and sources are trusted in order to focus resources on only those that appear suspicious or that come from unknown sources. McAfee Endpoint Security possesses an integrated firewall that uses McAfee GTI to protect endpoints from botnets, distributed denial-of-service (DDoS) attacks, advanced persistent threats, and risky web connections.

Relieve the Pressure with Reduced Complexity and Increased Sustainability

The rapid growth of security products with overlapping functionality and separate management consoles has made it difficult for many to derive a clear picture of potential attacks. McAfee Endpoint Security delivers strong, long-term protection thanks to its open and extensible framework, which serves as the foundation to centralize current and future endpoint solutions management. This framework leverages the McAfee Data Exchange Layer for cross-technology collaboration with existing security investments. The integrated architecture seamlessly integrates with other products from McAfee, further reducing security gaps, technology silos, and redundancies, while improving productivity by lowering your operating costs and management complexity.

McAfee® ePolicy Orchestrator® (McAfee ePO™) software can further reduce complexity by providing a single pane of glass to monitor, deploy, and manage endpoints. Customizable views and actionable workflows in understandable language provide the tools to quickly assess security posture, locate infections, and mitigate the impact of threats by quarantining systems, stopping malicious processes, or blocking data exfiltration. It also provides a single place to manage every endpoint, other McAfee capabilities, and more than 130 third-party security solutions.

Feature	Why You Need It
Real Protect	▪ Machine-learning behavior classification detects zero-day threats in near real time, enabling actionable threat intelligence. ▪ Automatically evolves behavior classification to identify behaviors and add rules to identify future attacks. ▪ Repairs the endpoint to the last known good state to immediately prevent infection and reduce administrator burdens.
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	Protects, detects, and corrects malware fast with a new anti-malware engine that works efficiently across multiple devices and operating systems.
Proactive web security	Ensures safe browsing with web protection and filtering for endpoints.
Dynamic Application Containment	Defends against ransomware and greyware and secures "patient zero." [2]
Blocks hostile network attacks	▪ Integrated firewall uses reputation scores based on McAfee GTI to protect endpoints from botnets, DDoS, advanced persistent threats, 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 to understand the threat and react more quickly.
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 operational costs by eliminating redundancies and optimizing processes. ▪ Seamlessly integrates with other McAfee and third-party products to reduce protection gaps

Table 1. Key Features and Why You Need Them.

Gain the Advantage Over Cyberthreats

McAfee Endpoint Security provides what today's security practitioners need to overcome the attackers' advantages: intelligent, collaborative defenses and a framework that simplifies complex environments. With strong and effective performance and threat detection effectiveness that is proven in third-party tests, organizations can protect their users, increase productivity, and create peace of mind.

McAfee, the market leader in endpoint security, offers a full range of solutions that produce defense-in-depth by combining powerful protections with efficient management. Accelerated time to protection, improved performance, and effective management empower security teams to resolve more threats faster with fewer resources.

Migration Made Easy

Environments with current versions of McAfee ePO software, McAfee VirusScan® Enterprise, and the McAfee agent can leverage our automatic migration tool to migrate your existing policies to McAfee Endpoint Security in about 20 minutes or less.[3]

You'll also get these benefits from McAfee Endpoint Security:

- Zero-impact user scans for greater user productivity.
- Stronger forensic data to help you harden your policies.
- Performance improvements.
- Fewer agents to manage, along with scan avoidance, to reduce manual entry.
- Collaborative defenses that work together to defeat advanced threats.
- A next-generation framework that is ready to plug into our other advanced threat and endpoint detection

Learn More

To learn more about McAfee Endpoint Security, visit **www.mcafee.com/nextgenendpoint**. To learn more about how McAfee Endpoint Security complements the McAfee product portfolio, visit:

- **McAfee Endpoint Threat Protection**
- **McAfee Complete Endpoint Threat Protection**
- **McAfee Threat Intelligence Exchange**
- **McAfee Endpoint Threat Defense and Response**
- **McAfee ePolicy Orchestrator**

1. Available with McAfee Complete Endpoint Threat Protection.
2. Ibid.
3. The migration time is dependent on your existing policies and environment.

McAfee Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

1829_1016
OCTOBER 2016