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, 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 defenses to quickly 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—part of the Intel® Security product offering—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 protects productivity with fast, effective performance and 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 can be found and removed while multiple defenses are united on a common endpoint architecture that is built with the future in mind.

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

intel Security

the client and management interfaces to help users understand attacks and provide administrators with actionable threat forensics. In addition, the available McAfee Threat Intelligence Exchange technology empowers adaptive defenses to collaborate with other Intel Security solutions, including gateways, sandboxes, and our security information & event management (SIEM) solution. Gathering and distributing local, community, and global security intelligence shortens the time between attack, discovery, and containment from weeks or months to milliseconds.

Combined with McAfee Global Threat Intelligence (McAfee GTI), the 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.

McAfee Active Response, a powerful endpoint detection and response tool, can add even more visibility for administrators with the speed and agility to defeat threats that are actively propagating, lying in wait, or otherwise trying to avoid detection.

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 (AMCore) engine that helps reduce idle CPU utilization by 89%, boot time by 18%, and shrinks the virus definition file by 55%. 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. 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. It's also worth noting that none of these gains come at the expense of detection or protection effectiveness. When evaluated by independent IT-security institute AV-TEST in August 2015[1], Endpoint Security scored a near-perfect 17.5 out of a possible 18, compared to the base value of 9.5.

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 Data Exchange Layer (DXL) for cross-technology collaboration with existing security investments. The integrated architecture seamlessly integrates with other products from Intel Security, further reducing security gaps, technology silos, and redundancies, while improving productivity by lowering your operating costs and management complexity.

McAfee ePolicy Orchestrator (McAfee ePO) can further reduce complexity by providing a single pane of glass to monitor, deploy, and manage endpoints. A cloud-based ePO console can also help administrators protect their productivity with access from any internet-connected location. 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. Available as a local or cloud-based console, it provides a single place to manage every endpoint, other Intel Security capabilities, and more than 130 third-party security solutions.

Feature	Why You Need It
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 is efficient across multiple devices and operating systems.
Proactive web security	Ensures safe browsing with web protection and filtering for endpoints.
Blocks hostile network attacks	Integrated firewall uses reputation scores based on McAfee GTI to protect endpoints from botnets, DDoS, APTs, 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 with a single local or cloud-based console 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 Intel Security and third-party products to reduce protection gaps.

Table 1. Key Features and Why You Need Them.

Gain the Advantage Over Cyber Threats

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 today and tomorrow. With strong and effective performance and threat detection effectiveness that is proven in third-party tests, organizations can protect their users, productivity, and peace of mind.

Intel Security, 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.

Learn More

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

McAfee Complete Endpoint Protection

McAfee Threat Intelligence Exchange

McAfee Active Response

McAfee ePolicy Orchestrator

1. **AV-TEST: McAfee VirusScan Enterprise with EPO**

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com