Solution Brief

Integrate and Accelerate Endpoint Threat Defense

Today's threat landscape looks very different than it did in the past. Sophisticated cybercriminals are crafting zero-day malware that masks its attributes to evade signature-based defenses. They're creating evasive threats that can recognize when they're being analyzed and delay execution. They're developing sophisticated exploits that burrow deep within legitimate applications and websites to slip past frontline defenses. To combat these threats, security administrators are looking for new methods to keep their endpoints—and data—safe.

Even worse, explosive growth in endpoints and mobility have opened new potential attack vectors for cybercriminals and new places for malware to hide. In attempt to head off every potential point of weakness, many organizations now rely on a patchwork of security point solutions. These disparate defense systems should keep organizations better protected. Instead, they too often generate overwhelming noise and complexity—impeding visibility, stretching already limited IT security expertise, and delaying the time it takes to translate new observations into action.

The end result is that too many threats are making it through to endpoints. Too many "patient zero" infections are creating time-consuming remediation efforts. And security teams are spending too much time and resources trying to manually connect the dots, feeling that the odds are increasingly stacked against them.

Evolve Endpoint Defenses to Automate Multistage Threat Defense

It's time for a more integrated and automated security framework. With McAfee® Dynamic Endpoint Threat Defense from Intel® Security, organizations can combat emerging threats, defeat the unknown, and radically simplify security operations.

McAfee Dynamic Endpoint Threat Defense integrates multiple layers of endpoint defenses into a unified, adaptive defense fabric. It provides capabilities across the threat defense lifecycle—protection, correction, and detection—with tools that share information and coordinate threat response in near real time, without manual intervention. By automatically sharing intelligence across every stage of threat defense, security teams can streamline protection for even the most complex environments. They can shorten the time between detecting and correcting a threat from days to milliseconds. And they can gain the insight to outsmart the savviest cybercriminals and stop advanced threats in their tracks.

intel Security

- **Unmask evasive threats by combining reputation analysis with new machine-learning classification and behavioral modeling:** Stop most greyware, ransomware, and other advanced threats before they infect patient zero or spread to other systems. Strengthen security posture with integrated security technologies that work together to coordinate defenses.
- **Find potential threats in seconds by exposing the unknown and prioritizing suspicious events with the necessary context to quickly convict and then resolve:** Limit exposure by reducing dwell times through real-time visibility, live investigations, and timelines. Use single-click correction to immediately remediate threats across a single endpoint or the entire organization.
- **Understand your security posture at all times through a single-pane-of-glass that provides broad visibility:** Act with precision and speed by executing security policies across the threat defense lifecycle with unified workflows. Close exposure gaps against emerging threats with defenses that share intelligence and automatically adapt to new information.

Inside Dynamic Endpoint Threat Defense

With McAfee Dynamic Endpoint Threat Defense, Intel Security integrates the entire Intel Security endpoint stack, as well as innovative new defense technologies, into a unified, adaptive defense fabric. The solution includes:

- **McAfee Endpoint Security:** Multiple layers of protection share information and collaborate to automatically update your defenses in response to newly discovered threats.
- **Real Protect:*** State-of-the-art machine learning techniques identify malicious code based on both what it looks like it might do (pre-execution analysis) and what it does (dynamic behavioral analysis)—all without signatures.
- **Dynamic Application Containment:*** Prevents "patient zero" infections and stops threats from spreading—without disrupting users—by blocking suspicious files from executing common malicious process actions.
- **McAfee Threat Intelligence Exchange:** Combines threat intelligence from McAfee Global Threat Intelligence (McAfee GTI), third-party intelligence sources, and the organization's own environment to provide organization-wide context and visibility. McAfee Threat Intelligence Exchange empowers security teams to pinpoint where threats are attempting to establish a foothold and closes the exposure gap from days to milliseconds.
- **McAfee Active Response:** Provides the ability to hunt and respond to threats on endpoints anywhere in the environment—whether they're actively propagating, lying in wait, or covering their tracks to avoid detection.
- **McAfee Advanced Threat Defense:** Detonates unknown files and applications in a safe environment to expose hidden threats and instantly adapts the environment to protect against them.
- **McAfee Web Protection:** Provides inline file emulation to unmask advanced, previously unknown threats hidden in internet traffic—in milliseconds, without signatures—and prevent them from ever reaching endpoints.
- **McAfee® ePolicy Orchestrator® software:** Breaks down silos between disparate security tools and allows you to operate the entire endpoint threat defense fabric as a unified system from a single pane of glass.

An Integrated, Automated Defense Fabric

All of these defense capabilities work together to create a continuous feedback loop for endpoint security. Instead of juggling multiple siloed tools and interfaces, security teams can maintain a single, unified defense fabric that automatically shares intelligence and streamlines communication across all components.

The moment a new threat or vulnerability is discovered, that knowledge can be applied to inoculate every other endpoint in the environment. The result is a continuously evolving threat model that can detect, resolve and adapt to new attack strategies much faster, with a fraction of the effort and resources currently needed for effective security.

Learn More

To find out more about Dynamic Endpoint Defense, visit:
http://mcafee.com/us/solutions/neutralize-threats/dynamic-endpoint-threat-defense.aspx

* The solution includes hosted data centers located in the United States used to validate customer authentication, check file reputations and store data relevant to suspicious file detection and hunting. Although not required, Dynamic Application Containment will perform optimally with a cloud connection. Full McAfee Active Response, Dynamic Application Containment and Real Protect product capabilities require cloud access, active support and are subject to Cloud Service Terms and Conditions.

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