White Paper

McAfee Dynamic Endpoint Threat Defense

intel Security

Table of Contents

A new wave of cyberattacks is targeting your organization: Cleverly crafted malware that masks its attributes to avoid signature-based defenses. Evasive threats that can recognize when they're being analyzed and delay execution. Sophisticated exploits that burrow deep into legitimate web and application traffic to slip past frontline defenses.

These advanced threats have a snowball effect on your security organization. Each new attack strategy requires a new kind of defense. Before you know it, you've created a massively complex security infrastructure with multiple point solutions that don't talk to each other. Your security analysts are buried in an avalanche of alerts and false positives. They're struggling to manually connect the dots between siloed defenses, lengthening delays between threat detection, containment, and response.

Savvy cybercriminals, knowing you can't keep up, are happy to exploit these gaps. The result is more "zero-day" malware making it to endpoints. And the risk of outbreaks—as well as the cost to remediate them—only grows.

Smarter Malware Demands Smarter Defenses

McAfee® Dynamic Endpoint Threat Defense offers a new kind of endpoint protection built for a new generation of threats. It integrates industry-leading Intel Security endpoint threat detection capabilities with a suite of next-generation protection tools that use machine learning and aggregated intelligence sources to provide deeper insights and faster, coordinated response. Your security teams can protect "patient zero" and stop outbreaks before they start. And they can continually adapt all points of protection to contain newly discovered threats—instantly and automatically.

With McAfee Dynamic Endpoint Threat Defense, you can:

- **Combat the most evasive threats:** Unmask hidden threats by combining reputation analysis with new machine-learning classification and behavioral modeling. Stop greyware, ransomware, and other advanced threats before they infect "patient zero" or spread to other systems.
- **Quickly hunt, expose, and remediate threats:** Find potential threats in seconds by peeling away obfuscation techniques and prioritizing suspicious events, with the necessary context to quickly convict or exonerate them. Expose threats that are hiding in your environment with real-time investigation tools, and single-click correction. Quickly uncover and stop evasive malware—whether it's actively propagating, lying in wait, or covering its tracks to avoid detection.
- **Operate more quickly and efficiently with simplified network defenses:** Give your teams the tools to understand the organization's security posture at all times with broad visibility, investigation, and action in a single view. Empower them to act with precision and speed by executing security policies across the threat defense lifecycle.

Combat advanced, evasive attacks

By making minor alterations to their code, cybercriminals can now change the hash value of malware just enough to evade defenses that rely on attack-specific signatures. However, it's very difficult to hide all the attributes of malware. And it's nearly impossible to hide how it behaves.

McAfee Dynamic Endpoint Threat Defense includes both static and behavioral analysis capabilities to unmask the most evasive threats. It combines them with both in-line Internet code emulation and tools to block dynamic application processes before they can make changes to an endpoint. As a result, it can catch more zero-day malware than any signature-based or static-only solution.

Next-generation McAfee Dynamic Endpoint capabilities include:

- **Inline file emulation for suspicious web traffic:** Zero-day attacks usually begin when an employee visits a legitimate but compromised website or clicks a malicious link in an email. Most web security solutions are based on filtering known high-risk URLs and scanning traffic with known malware signatures—which means that unique, targeted zero-day attacks can evade them. McAfee Dynamic Endpoint Threat Defense provides in-line file and code emulation that analyzes the actual behavior of Internet code and files to unmask advanced, previously unknown threats hiding in Internet traffic—in milliseconds, without signatures.
- **Pre-execution static code analysis:** If an endpoint detects a suspicious new file or application, it can automatically invoke pre-execution statistical analysis. These scans are based on analysis of hundreds of millions of known malware samples to create profiles of malware features that rarely change—even if the surface-level "fingerprint" does. Using machine-learning models, McAfee Dynamic Endpoint analyzes static attributes of the suspicious file—the compiler used, the programming language, the shared and dynamic libraries it references, and many other features. In less than a second, it identifies similarities with known malware and blocks most threats before they can ever execute.
- **Dynamic behavioral analysis:** The most sophisticated malware may slip past "static-only" defenses by disguising itself as, or misusing, a legitimate application. However, it can't disguise its malicious behavior. When endpoints detect unknown greyware, they can invoke dynamic behavioral analysis to track everything the application attempts to do on the endpoint. This analysis employs the same kind of signature-less machine learning used in static code analysis but applies it to actual behavior, comparing the greyware against profiles generated from 500 million samples of known malware. If the behavior matches anything known to be malicious—if it's dropping sub-processes, overwriting files, making registry changes—the endpoint blocks the malware from taking root on the endpoint or spreading to other systems, typically within seconds.
- **Dynamic application containment:*** When endpoint defense systems detect a suspicious executable but don't have enough information to conclusively classify it as malicious, they can activate application containment to preemptively block process actions that malicious applications commonly use. The file is allowed to load in memory—and the user can remain productive—but the greyware can't make malicious changes on the endpoint. This stops threats in mere milliseconds, saving "patient zero" by shielding the first endpoint to encounter a unique malware binary and effectively isolating the rest of the network from infection.

Shorten the Time Between Detect, Contain, and Correct

Too often when organizations detect new zero-day malware or emerging threats, the damage has already been done. The patient zero endpoint is lost. The threat has spread to other systems. And a major, resource-intensive remediation effort awaits.

Even when organizations use next-generation "signature-less" threat detection tools, the gap between recognizing a previously unknown threat, containing it, and updating the infrastructure to block it is still too long. The problem: in most environments, the disparate security tools handling static analysis, reputation, endpoint protection, and other capabilities can't talk to each other. So human beings have to fill those gaps, which takes a lot more time and resources.

With McAfee Dynamic Endpoint Threat Defense, all of the diverse layers of your defenses—signature-based endpoint defenses, signature-less statistical analysis, sandbox tools, web gateways, and more—collaborate and share what they are seeing in real time. Local intelligence is combined with global and third-party threat intelligence, and communication between components is automated. Endpoints have the context they need to identify newly convicted threats and the ability to block them—before they can enter or leave the environment, and before they can damage endpoints.

The result is an adaptive defense fabric that aggregates insights from the network edge through the endpoint to coordinate threat identification and response. The moment a threat is detected, each layer works with the others to automatically block the execution of suspicious files, websites, and potentially unwanted programs. Effectively, every endpoint and security solution in the environment now operates as one. They exchange and act on shared information instantly. And they shorten the time between detection and containment from days or weeks to milliseconds.

Increase Visibility and Speed Response

Massive growth in cloud-based applications, web traffic, and mobile endpoints that may be operating on or offline has eroded any concept of the traditional security perimeter. The result is an environment that's much harder to visualize and understand from moment to moment, much less protect.

McAfee Dynamic Endpoint Threat Defense gives security teams comprehensive information about the security posture of the organization. At a glance, security analysts can see the sources of threat events, the methods used to detect them, the systems affected, attack duration, targets, and actions taken to mitigate the threat.

With instant, actionable threat forensics, along with real-time endpoint data, analysts can quickly understand the full context of a threat and where deeper scrutiny or action is warranted. And they can use powerful active response tools to quickly hunt for indicators of attack (IoAs), as well as known bad and suspect threats across the entire infrastructure.

Upon recognizing an advanced ransomware attack on an endpoint, for example, they can quickly examine the broader environment to search for other possible infections. They can see where first contact occurred, local prevalence of the malware, its trajectory, and any infection artifacts—all of which simplifies and accelerates investigations. They can also set triggers to search for similar IoAs in the future—in a single action, from the same interface. They can activate continuous monitoring of the IT infrastructure for every newly unmasked zero-day attack in seconds. And they can continually turn new knowledge into proactive global protection.

Filter Through the Noise and Take Action

As organizations bring in new tools and intelligence sources to combat evolving threats, the result is too often overwhelming noise and complexity. Analysts find themselves with the seemingly never-ending task of manually sifting through alerts attempting to understand what's happening, what they can ignore, and what demands immediate action.

With McAfee Dynamic Endpoint Threat Defense, much of that manual effort disappears. Security analysts can see threat forensics and actionable intelligence in understandable language—with full context (attack source, duration, first contact, trajectory)—providing a snapshot of everything they need to know at a glance. With threat "signals" filtered out from the "background noise" of constant endpoint events, they can identify and control suspicious objects much more quickly, and take instant action in response to newly discovered threats. That is, if any manual action is even required.

Using streamlined workflows, McAfee Dynamic Endpoint Threat Defense can automatically resolve previously addressed threats with no action needed at all, escalating only the highest-priority alerts to human analysts. Security teams can see all of this—newly discovered threats, automated actions taken, workflows available to configure, and high-priority events that demand closer scrutiny—from a single interface.

Avoid False Positives, and Bridge Security Gaps

Machine learning and statistical analysis can provide powerful capabilities to stop more zero-day threats than signature-based defenses alone. But the reality is, it's not an either/or proposition. In fact, organizations using only signature-less capabilities often have high rates of false positives, where users are blocked from running legitimate applications and processes. The result is frustrated users, lost productivity, and cumbersome manual remediation processes.

McAfee Dynamic Endpoint Threat Defense combines the best signature-based and next-generation defenses as a unified solution. It aggregates insights from multiple sources, combining malware signatures, real-time reputation scoring, and machine learning to understand the full context of potential threats. Using adaptive scanning, the solution learns which processes and sources are trusted. It can more accurately focus resources on only files and applications that appear suspicious or that come from unknown sources, while substantially reducing CPU demands on the endpoint. As a result, it can deliver unmatched accuracy in detecting emerging threats that have never been seen before, without spiking false positives.

Reduce Complexity, and Lower Costs

With McAfee Dynamic Endpoint Threat Defense, 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.

They gain a single management console that makes it easy to deploy, maintain, and scale with the flexibility to simply activate or deactivate existing and new technologies through policy settings. They can manage the entire endpoint threat defense lifecycle from a single console and synthesize intelligence from multiple security components acting as a single, coordinated system. Effectively, endpoint defenses become a collaborative, tightly integrated ecosystem that strengthens protection, reduces redundancies, and automates threat response across all technologies.

Now, your security teams have the ability to combat practically any type of threat and address the full threat defense lifecycle—protect, detect, and correct—within a single solution. They can take advantage of integration and automated workflows across security technologies to optimize threat defense for the entire environment, while reducing the cost of both security infrastructure and operations. And they gain a continuously evolving defense fabric that can detect, resolve, and adapt to new attack strategies much faster, with a fraction of the effort and resources.

Learn More

For more details on how you can evolve your endpoint security to improve visibility, speed up threat detection and response, and combat the most sophisticated modern threats, visit: **http://mcafee.com/us/solutions/neutralize-threats/dynamic-endpoint-threat-defense.aspx**

About Intel Security

Intel Security, with its McAfee product line, is dedicated to making the digital world safer and more secure for everyone. **www.intelsecurity.com**. Intel Security is a division of Intel.

intel Security

* 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

Intel and the Intel and McAfee logos are trademarks of Intel Corporation or McAfee, Inc. in the US and/or other countries. Other marks and brands may be claimed as the property of others. Copyright © 2016 Intel Corporation. 1957_1016
OCTOBER 2016