McAfee™
Together is power.

Defend Against the Unknown

Stay ahead of new threats with McAfee® Endpoint Threat Defense solutions

Targeted exploits. Ransomware. Explosive growth in zero-day malware. Organizations are locked in an ongoing arms race with cybercriminals—and the attackers are gaining the edge. Modern adversaries know the strategies organizations use to try to block their attacks, and they're crafting increasingly sophisticated, targeted malware to evade defenses. They hide attacks within legitimate applications. They delay execution. They exploit the weakest link. And they travel laterally from one endpoint to another, silently collecting information undetected.

Meanwhile, security teams are struggling just to contend with the threats they know about. They're grappling with an expanding attack surface, as more mobile devices create new entry points into the business—even when they're offline. They face overwhelming complexity and noise as they juggle the myriad of alerts coming in from siloed traditional defense systems, slowing down response times and hindering investigations. All the while, they're pressed to deliver critical business services without disruptions or slowdowns—they can't grind productivity to a halt every time an endpoint detects something new.

The result is that more threats are slipping past defenses. They're dwelling inside organizations for a longer period of time, re-infecting systems more frequently, and wreaking more serious damage. A shortage of IT security expertise and resources exacerbates the problem. And many organizations are left playing catch-up, knowing they need to adapt defenses more quickly but feeling as if they're steadily losing the race.

Unmask Evasive Attacks

McAfee® Endpoint Threat Defense solutions help organizations stay ahead of the savviest adversaries. They combine multiple state-of-the-art defense capabilities to detect evasive threats, analyzing suspicious code at multiple stages, and containing malware before it can affect users or systems—whether endpoints are online or offline. They detect more zero-day malware than any signature-based defenses by combining both in-depth static code analysis and advanced behavioral analysis. And they can immediately block malicious behavior to prevent malware from damaging an endpoint or infecting the network, while allowing endpoints to remain productive. All of these endpoint security solutions are linked together into a unified defense fabric that shares insights and automatically adapts to newly discovered threats.

McAfee Endpoint Threat Defense

McAfee Endpoint Threat Defense brings together powerful threat detection and correction tools:

- **Real Protect:*** Real Protect applies state-of-the-art machine learning techniques to 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. It peels away the latest obfuscation techniques to unmask hidden threats so that zero-day malware has no place to hide.
- **Dynamic Application Containment (DAC):*** DAC makes it easy to protect systems from infection without sacrificing productivity. When an endpoint detects a suspicious file, DAC immediately blocks the behaviors that malware often uses (such as changing the registry, writing to a temporary directory, or deleting files). Unlike techniques that would hold up the file and the user for minutes at a time, DAC lets the suspicious file load into memory—it just can't make changes to the endpoint or infect other systems. The endpoint and user can remain fully productive while providing an opportunity for security tools to perform in-depth analysis.

- **McAfee Threat Intelligence Exchange:** This product provides comprehensive threat intelligence—from McAfee Global Threat Intelligence (McAfee GTI), third-party intelligence sources, and an organization's own environment—to accelerate threat detection and response. Security teams gain organization-wide context and visibility to pinpoint where threats are attempting to establish a foothold and close the exposure gap from days to seconds.
- **McAfee Data Exchange Layer:** This advanced technology connects an organization's security components into a unified, adaptive defense fabric. It enables real-time information sharing and coordinated response among endpoints and security components without needing point-to-point application programming interface (API) connections. Security teams can streamline operations—moving from detect to correct to proactively protect in much less time and with much less effort.
- **McAfee® ePolicy Orchestrator® (McAfee ePO™) software:** McAfee ePO software breaks down the silos between disparate security tools. It simplifies management by providing a single dashboard for all endpoint defense components, as well as third-party products from multiple vendors. Security teams can operate the entire endpoint threat defense fabric as a unified system, from a single pane of glass.

McAfee Endpoint Threat Defense and Response

For even more proactive protection against evasive threats, organizations can choose McAfee Endpoint Threat Defense and Response. It combines all of the tools above with McAfee Active Response,* adding advanced malware hunting and response capabilities to the solution's powerful detect and correct tools. McAfee Active Response cuts through the noise generated from siloed traditional defenses, empowering analysts to quickly uncover threats anywhere in the environment—whether they're actively propagating, lying in wait, or covering their tracks to avoid detection.

Block Advanced Malware Designed to Evade Detection

Previous-generation anti-malware strategies relied heavily on signature matching, rules-based intrusion prevention systems (IPS), and access protection strategies to try to detect zero-day malware. But modern cybercriminals, well aware of these techniques, cleverly design their malware to evade them. Real Protect takes threat defense beyond previous-generation techniques by applying deep analytics both pre- and post-execution, whether endpoints are online or offline. It combines unified threat intelligence, pre-execution static analysis, and dynamic behavioral analysis to substantially improve security against zero-day malware, without signatures.

- **Static analysis:** Real Protect examines a massive number of static features to profile the properties of any new file that appears suspicious. In less than a second, it compares an exhaustive list of static attributes of the suspicious file against the latest machine-learning models and blocks most threats before they ever execute. This lightweight analysis uses minimal resources, yet happens directly on the endpoint.
- **Dynamic 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. Real Protect analyzes what suspicious applications are attempting to do on an endpoint. It uses machine learning models in the cloud to match malicious behavior in near real time and prevent malware from taking root on endpoints or spreading to other systems.

By combining both static and dynamic behavioral analysis and evaluating threats across multiple stages, Real Protect blocks more zero-day threats than any signature-based or static-only solutions. In addition, it integrates with an organization's larger defense fabric to automate and accelerate activities across each stage of the threat defense lifecycle: protect, detect, correct, and adapt.

Protect Patient Zero and Prevent Infections from Spreading

In many organizations, users have a legitimate need to run third-party files and applications. Security teams can't block every executable, and they can't ask users to wait around while each and every file is analyzed. Even if they could, the most advanced threats now recognize when they're being launched in a sandbox and delay execution until they've been cleared. DAC works with Real Protect and McAfee Endpoint Security to detect the most evasive threats and contain infections before they begin—without sacrificing flexibility or productivity.

When endpoint defense systems detect a suspicious executable (example: greyware) but don't have enough information to conclusively classify it as malicious, DAC is automatically activated to block the 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 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. Users can remain productive, and security teams have fewer infections they need to remediate. At the same time, DAC buys time to analyze the suspicious object with Real Protect dynamic analysis or the McAfee Advanced Threat Defense sandbox.

Proactively Adapt the Environment

In many organizations, threat correction ends when a single endpoint is remediated. Security teams may be able to detect and clean up an individual infection, but they don't have the visibility or resources to hunt down that infection everywhere it might have spread. The result is frequent re-infections—and a never-ending job for IT.

By adding McAfee Active Response malware hunting and response capabilities, McAfee Endpoint Threat Defense and Response closes the loop of the detect, correct, and protect stages of the threat defense lifecycle. Analysts can proactively search the entire organization to detect similar threats, including attacks that are actively propagating or lying hidden and even malware that entered the system months ago and then deleted itself. And, because McAfee Active Response communicates with McAfee Threat Intelligence Exchange as part of a unified threat defense fabric, the moment a new threat or vulnerability is discovered, that knowledge can be applied to inoculate every other endpoint in the environment. McAfee Active Response provides single-click correction, customizable triggers and reactions and unified workflows to automate security operations across the full threat defense lifecycle: protection, detection, and correction. The result is a continuously evolving threat model that can detect, resolve, and adapt to new attack strategies much faster, with less effort and fewer resources.

Gain Unmatched Visibility and Speed

All of these McAfee Endpoint Threat Defense and Response capabilities work together to create a continuous feedback loop for endpoint defenses. 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.

Through the McAfee Threat Intelligence Exchange, the defense fabric combines local insights with constantly updated information from McAfee Global Threat Intelligence and other third-party sources to drive more accurate threat classification. By combining this intelligence with McAfee Active Response and other McAfee Endpoint Threat Defense capabilities, security teams gain visibility across the entire endpoint environment and have the ability to verify the organization's current security posture at any time. They can continually apply knowledge from newly discovered threats and vulnerabilities to adapt defenses. They can move from detect to correct to proactively protect much faster, often in near real time. And they can do all of this through a single platform with a unified interface.

The results? Faster and more accurate threat detection. Dramatically lower operational overhead. And an evolving threat defense fabric that continually learns cybercriminals' latest tricks and stops them in their tracks.

Learn More

To find out more about McAfee Endpoint Threat Defense and McAfee Endpoint Threat Defense and Response, visit:

- **www.mcafee.com/endpointdefense**
- **www.mcafee.com/ETDR**

* McAfee Endpoint Threat Defense and Response 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, DAC will perform optimally with a cloud connection. Full McAfee Active Response, DAC, and Real Protect product capabilities require cloud access and active support and are subject to Cloud Service Terms and Conditions.

McAfee Together is power.

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

McAfee and the McAfee logo, ePolicy Orchestrator, and McAfee ePO are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2017 McAfee, LLC. 1929_1016 OCTOBER 2016