WHITE PAPER

McAfee
Together is power.

Busting the Myth of the Malware "Silver Bullet"

Layer Real Protect, Dynamic Application Containment, and McAfee Advanced Threat Defense for the most effective defense

Table of Contents

Busting the Myth of the Malware "Silver Bullet"

Layer Real Protect, Dynamic Application Containment, and McAfee Advanced Threat Defense for the most effective defense

When it comes to fighting modern malware, there is no "silver bullet" that can guard against every threat every time. That's why McAfee takes a different approach. We combine multiple layers of advanced malware protection, detection, and correction technologies into a single endpoint defense fabric. To keep up with cyberthreat innovation, effective detection and analysis requires new state-of-the-art anti-malware technologies: Real Protect and Dynamic Application Containment, complemented by the McAfee® Advanced Threat Defense sandbox. Find out how these tools work together to systematically protect against the most dangerous malware threats.

The Security Snowball Effect

As malware grows more sophisticated and harder to combat, it's tempting to believe that there is a breakthrough technology that will solve the problem. But the reality is, modern adversaries are far too clever for that. There are great solutions out there for combating a particular kind of malware that infects your endpoints in a particular way. But the minute you rely on a single technology to protect your business, adversaries find a way to fool it. All of a sudden, you need another solution. And then another. Soon, you're dealing with the security snowball effect: you're juggling a dozen different security tools, each with its own separate console, each requiring specialized processes and expertise. Who stitches all of those tools together so that your security team isn't buried in complexity and delays? In most cases, you do—if they can be brought together at all. All of that effort adds critical seconds (and hours, and days) at a time when you can least afford it—when you're responding to a potential threat. At the same time, it takes up valuable time and strains your scarcest resource: your people.

Malware represents a special challenge: you need tools for opportunistic, evasive, zero-day, targeted, and weaponized malware, as well as defenses against the inevitable "patient zero," when malware gets past defenses and works to compromise a system. If you omit or unplug

any of these capabilities, you can be sure that route will be the avenue your attacker uses. And, realistically, the malware itself is just part of the attack chain. The content and actions associated with malware bring value to security analysts in the security operations center, as well as guide improvements to all of the enterprise's preventative controls, including web gateways and network intrusion prevention systems.

For these reasons, businesses don't need one amazing technology to fight the modern malware threat. They need multiple technologies, not just co-located, but working together in an integrated, automated way to ensure that even if a threat makes it past one layer of your defenses, it won't make it past all of them. McAfee is the only anti-malware vendor that uses a truly integrated and coordinated endpoint defense fabric—with connected components working with each other. With this design, your defenses can combine the capabilities they need moment by moment to protect better than any technology working in isolation.

The End of Uncoordinated Security

The new generation of McAfee anti-malware and endpoint security technologies coordinates multiple layers of state-of-the-art defenses to combat the most sophisticated, well-hidden threats. Unlike security strategies based on isolated products, these complementary defenses operate as a system to identify malware. Then, they go beyond that to integrate detections with blocking, containment, and investigation to make threat management simpler, faster, and more effective. They make the most effective use of the latest dynamic, static, machine learning, reputation, and sandbox technologies and enable enterprises to tailor actions to their own situation.

- **Pre- and post-execution machine learning analysis**: Real Protect, available in the new generation of McAfee Endpoint Security, peels away the latest obfuscation techniques to unmask hidden threats, so zero-day malware has no place to hide. It ushers in a new age in endpoint security by introducing machine learning techniques that perform both pre-execution static analysis (What are the features of the file?) and post-execution behavioral analysis (What does it actually do?)—all without signatures. It stops more malware than any signature-based or static-only solution—blocking most malware at the endpoint before it ever has a chance to execute.
- **Suspicious process containment**: Dynamic Application Containment, another available component of McAfee Endpoint Security, protects patient zero endpoints from previously unknown "zero-day" malware infections by immediately blocking process actions that malware often uses. Designed to halt malicious changes to endpoints and available only from McAfee, Dynamic Application Containment doesn't hold up the endpoint (and the user) for minutes at a time while an unknown file is analyzed. Dynamic Application Containment lets the suspicious file load into memory without allowing it to make changes to the endpoint (such as changing the registry or deleting files) or to infect other systems while under suspicion. The endpoint and user can remain fully productive while providing an opportunity for more in-depth analysis.

- **Threat sandboxing**: The McAfee Advanced Threat Defense sandbox solution provides powerful capabilities to detect the most advanced targeted malware and convert newly discovered threat information into immediate action. It detonates suspicious files in a safe environment and performs in-depth static code analysis on the entire code base to gain the granular insight needed to conclusively convict or exonerate a threat. When a new malware threat is uncovered, McAfee Advanced Threat Defense links with McAfee Threat Intelligence Exchange to inform other security systems—from endpoints to the network edge—about the new threat and inoculate the broader environment, thus shortening the gap between threat detection, correction, and proactive protection.

Individually, each of these technologies provides important anti-malware capabilities. Together, they are part of a multilayered defense environment that stops most threats before they infect patient zero and then coordinates threat response in near real time, without manual intervention.

Organizations can coordinate Real Protect, Dynamic Application Containment, and McAfee Advanced Threat Defense capabilities, turning different layers up and down for different organizational needs, or even different areas of the business.

Flexibility for Different Organizational Needs

All three McAfee solutions provide important malware defense capabilities, but different organizations will use them in different ways. Here's what that might look like in practice.

- **Organizations that tightly control and limit endpoint activities**: Some organizations, such as financial and healthcare institutions, prioritize endpoint security above all else, using a "block first, ask questions later" philosophy. They want to halt anything that is unauthorized from continuing to execute on endpoints, and they limit web browsing to whitelisted sites. These types of organizations can use Dynamic Application Containment as the centerpiece of their endpoint protection, tightly restricting what can happen on an endpoint. They can use McAfee Advanced Threat Defense to support their whitelisting efforts—detonating unknown files out of band to determine if they should be allowed in the environment, even at the expense of making users wait while they do it. And they can use Real Protect static scanning on endpoints to block most threats before they ever execute.
- **Organizations that prioritize endpoint and user flexibility**: In some organizations, employees need the flexibility to surf the web, programs they need to get work done, and install them without waiting for IT approval. For these types of organizations, Real Protect static scanning provides critical frontline security while allowing users to remain fully productive. And with Real Protect behavioral scanning, even if malware is allowed to execute, it will be identified and remediated before it can cause a wholesale infection. These organizations can back up this protection with Dynamic Application Containment, tuned to prevent the most egregious malicious process actions. And, they can use McAfee Advanced

Threat Defense to support forensic analysis and advanced threat hunting and response.

- **Organizations looking to balance security and flexibility**: Many organizations collaborate with outside vendors and customers, and constantly receive files from external sources. They want to keep malware out of their network and save patient zero, but they don't want to block every executable or ask users to wait while every file is analyzed. These organizations can use Dynamic Application Containment in conjunction with McAfee Advanced Threat Defense to block malicious activity on endpoints and later examine them safely using McAfee Advanced Threat Defense's sandbox techniques to understand and adapt to threats. At the same time, they can allow users to continue working productively while suspicious files are sent out-of-band for deeper analysis. Meanwhile, Real Protect static scanning blocks most malware from ever making it through to endpoints.

Inside McAfee Multilayered Malware Defenses

Let's take a closer look at the ways these three technologies work together to stop the vast majority of malware threats, save patient zero, and quickly turn new endpoint insights into broad-based action.

Layer 1: Strengthening Endpoint Defenses Against Unknown Threats

Previous-generation endpoint defenses can stop malware effectively—as long as it's a known threat. But many modern cyberattacks are designed to evade traditional signature-based defenses. They use packing, encryption, and polymorphism to mask a file's attributes. They piggyback on or misuse legitimate applications. They recognize that they're being analyzed in a test environment and delay execution.

Real Protect uses the power of machine learning and statistical analysis to detect evasive threats. And, unlike other solutions, it applies these techniques to both static and behavioral analysis.

- **Real Protect Static** performs machine learning statistical analysis of static binary code features (the compiler used, the programming language, shared and dynamic libraries referenced, and more) to unmask malware for what it is—in milliseconds, without signatures. By comparing those features against those of known threats, it peels away the latest obfuscation techniques and detects most zero-day malware before it ever has a chance to execute.
- **Real Protect Dynamic** starts with the premise that even if malware hides the way it looks, it can't hide how it behaves. If an unknown "greyware" executable makes it past Real Protect Static but still seems suspicious, the endpoint can invoke Real Protect Dynamic. The endpoint then lets the code run while closely scanning the application's behavior and reporting back to the cloud to compare that behavior against known threats. In this way, it can detect cleverly disguised malware—even threats that have carefully disguised the file's static attributes, and even those designed to recognize they're being analyzed in a sandbox or virtual machine (VM). If the file is convicted, the endpoint immediately remediates the threat.

The moment a threat is convicted by Real Protect static or dynamic analysis, the endpoint immediately remediates it—automatically, without intervention by users or security teams.

Together, these Real Protect capabilities:

- **Accelerate zero-day threat detection**: Most malware is unmasked in milliseconds while requiring minimal resources on endpoints
- **Prevent patient zero infections**: The vast majority of malware is detected and stopped before it ever has a chance to execute
- **Block more malware**: This occurs by combining both static and behavioral analysis, and analyzing many types of malware (PDFs, Javascript, and other non-executable files) that other solutions miss
- **Provide ongoing protection against the newest threats**: This is accomplished by analyzing threats against machine learning models that are updated continuously—not just once or twice a year like other solutions
- **Automate endpoint cleanup**: Convicted threats are immediately remediated.

Layer 2: Blocking Malicious Behavior on Endpoints

Even with the best frontline defenses, some zero-day threats can occasionally make it through to endpoints or require more time to convict. Dynamic Application Containment provides another layer of defense to ensure that, even if a zero-day threat executes, it can do little or no damage to the endpoint. Dynamic Application Containment preemptively contains suspicious applications, letting the file load in memory but blocking process actions that malicious applications commonly use. This immediately prevents the greyware from making any changes on the endpoint, spreading to other systems, or exposing the user to malicious behavior. The system and user can continue working as normal, while the security team uses other tools, such as McAfee Advanced Threat Defense, to perform deeper analysis on the application.

Dynamic Application Containment is typically triggered through reputation scoring—based on information from both the local environment and McAfee Global Threat Intelligence (McAfee GTI). Organizations can customize the triggers that invoke Dynamic Application Containment, as well as the specific actions that are blocked to protect against different types of threats or tailor containment for specific targets and activities. Additionally, Dynamic Application Containment is lightweight enough to run on the endpoint, so it can protect users and systems even when they're offline.

Dynamic Application Containment is the first host-based containment method that immediately stops malicious behavior while allowing the endpoint and user to remain productive. It's the only solution available that can block malware at the process level, instead of having to isolate (and often sacrifice) the entire endpoint.

Layer 3: Performing In-Depth Analysis and Inoculating the Environment

While Dynamic Application Containment is blocking malicious process actions on an unknown executable (and while that endpoint and user are still working productively), the suspicious file can be sent to McAfee Advanced Threat Defense for in-depth analysis. This state-of-the-art advanced analysis tool functions as its own multilayered threat detection system within the larger endpoint defense fabric. It combines low-touch antivirus signatures, reputation, and real-time emulation defenses with in-depth static code scanning and dynamic behavioral analysis to expose the most evasive, camouflaged malware. Unlike solutions that look only at high-level file attributes, McAfee Advanced Threat Defense uses sophisticated unpacking capabilities to analyze all of a file's attributes and instruction sets. It combines this with behavioral analysis to learn everything there is to know about a threat.

If a file is convicted as malicious, McAfee Advanced Threat Defense reports that information back to McAfee Threat Intelligence Exchange, which then inoculates the rest of the environment against that threat. Now, when any endpoint across the environment encounters that malware and tries to run it, the malware is blocked from even initializing. McAfee Advanced Threat Defense also publishes conviction information to McAfee Data Exchange Layer, so that other McAfee solutions and third-party security solutions outside the McAfee ecosystem that subscribe to McAfee Data Exchange Layer can incorporate information about the threat into their own defenses. And, McAfee Advanced Threat Defense produces in-depth indicator of compromise (IoC) information, which security information and event management (SIEM) systems, endpoint detection and response (EDR), and security teams can use to hunt for evidence of similar attacks across the organization—even if they are dormant or entered the environment months ago and then deleted themselves. Additionally, as an out-of-band sandbox, McAfee Advanced Threat Defense can receive and analyze files from sources other than endpoints, including servers, web gateways, intrusion prevention systems (IPS), and more.

Layered Defenses at a Glance

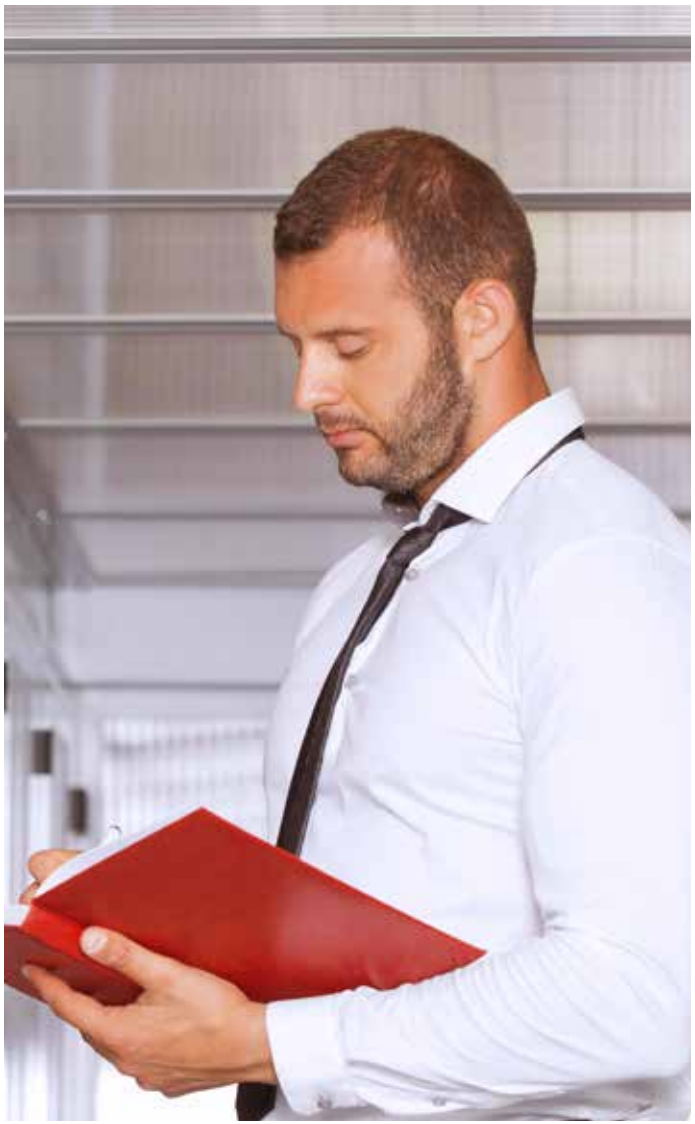
The following table highlights the role of each layer in the next-generation McAfee anti-malware fabric.

	Real Protect	Dynamic Application Containment	McAfee Advanced Threat Defense
What does it do?	Uses machine learning to detect advanced, evasive malware without signatures, and immediately remediates convicted threats.	Limits or eliminates the ability of greyware to make changes on the endpoint by blocking process actions.	Provides deeper static and dynamic analysis. Allows greyware to run on a sacrificial VM to observe its behavior, convict it, harvest IoCs, and inoculate the rest of the environment.
How does it protect "patient zero"?	Blocks most zero-day threats before they can execute.	Prevents greyware from making changes on the endpoint.	Shares IoCs with the forwarding product, McAfee Threat Intelligence Exchange, and McAfee Data Exchange Layer-connected solutions for immediate protection against similar threats.
Where does it live?	Real Protect Static (pre-execution scanning): Analysis and remediation performed directly on endpoint. Real Protect Dynamic (behavioral scanning): File executes on endpoint; behavior analyzed in cloud; remediation on endpoint.	Directly on the endpoint.	Out-of-band solution; analyzes files detected by endpoint on separate server/cluster.
How long does it take to work?	Real Protect Static: Milliseconds. RP Dynamic: Seconds up to about a minute.	Contains suspicious objects immediately.	From seconds to minutes or longer, depending on the type of analysis being run.
How does it reduce the time and resources needed to protect the environment?	Stops more threats and reduces or eliminates the need for endpoint cleanup. Automatically remediates convicted threats with no additional action needed.	Shields the first endpoint to encounter a new malware threat from damage and isolates the rest of the network from infection by that malware.	Automatically updates other security solutions about newly discovered threats through McAfee Threat Intelligence Exchange and McAfee Data Exchange Layer. Gives security teams detailed IoCs to find threats in the broader environment more quickly.
Can it protect endpoints that are offline?	Real Protect Static: Yes, analysis runs directly on the endpoint. Real Protect Dynamic: Requires connection to cloud.	Yes, containment is handled locally on the endpoint. (Note: Dynamic Application Containment can use local file reputation analysis to trigger containment but will have more reputation intelligence available when connected.)	File must be forwarded to McAfee Advanced Threat Defense for analysis.
Which part of the Threat Defense Lifecycle does it address?	Protect, detect, and correct.	Protect.	Detect.

Next-Generation Malware Demands Next-Level Defenses

The malware threat will continue to evolve. As quickly as the industry develops strategies to detect new attack types and vectors, savvy cybercriminals are hard at work on the next generation of advanced zero-day malware threats. No single "silver bullet" solution exists to protect against all of them. And juggling multiple solutions that operate in silos means more time, resources, and complexity for already strained security teams. The smarter approach is to use multiple layers of advanced defenses that are all coordinating their actions to detect more threats and stop them more quickly.

McAfee provides the industry's most comprehensive anti-malware portfolio, and the only one that's integrated into a single, multilayered endpoint security fabric. We help you break down the security silos that burden your operations with extra steps and effort, and cost you critical time in the race to detect and respond to emerging threats. With multiple layers of next-generation McAfee technologies working together, you can continually adapt defenses against the latest malware threats.



Learn More

For more information on Real Protect and Dynamic Application Containment, visit: **www.mcafee.com/dynamic-endpoint**

To find out more about McAfee Advanced Threat Defense, visit: **www.mcafee.com/atd**

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

McAfee™
Together is power.

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