White Paper

Unmask Evasive Threats

Intel® Security Real Protect and Dynamic Application Containment
Stop Zero-Day Malware in its Tracks

intel Security

Table of Contents

Modern malware now masks itself to evade detection. It hides by piggybacking or misusing legitimate applications. It recognizes when it's being analyzed in a sandbox and delays execution, waiting days, weeks, even months for an opportunity to strike. Smarter malware demands smarter defenses. With state-of-the-art threat detection and containment tools from Intel Security, organizations can unmask the most sophisticated hidden threats. They can stop evasive zero-day malware in its tracks—before an outbreak—and radically reduce the time and resources needed to protect the business.

Combating the Zero-Day Malware Threat

Modern organizations employ an arsenal of powerful defense systems: signature-based anti-malware engines, host intrusion prevention systems (HIPS), sandbox analysis, reputation filters, and many other tools. All of these provide important capabilities to detect, correct, and protect against a broad range of threats. Unfortunately, cyberattackers are not sitting idly by. Well aware of these advances, they're creating a new generation of malware designed to seek out the gaps in these defenses and exploit them.

The savviest cybercriminals now mask their attacks—through packing, encryption, and polymorphism—to hammer away at organizations with previously unseen "zero-day" malware that signature-based mechanisms are too slow to catch. They craft sophisticated executables that can recognize when they're being sandbox-analyzed and delay execution until they've slipped past sandbox-analysis. They weaponize legitimate files and applications that check out as clean but have malicious code buried deep within the file system to wreak havoc on endpoints and systems.

For security teams, it all adds up to three big problems:

- **Too many threats get through to endpoints:** As more malware finds its way past frontline defenses, security teams grapple with constant network infections and a looming threat of serious damage to the organization.
- **Detection and remediation are too slow:** Too many "patient zero" endpoints are lost to previously unknown malware, creating frustration for users and a huge remediation effort for IT.
- **Too many resources are needed to stop threats and infections:** Organizations now use multiple point solutions to stop a wide range of attack types and vectors. Too often, that translates to overwhelming noise and complexity as security teams juggle multiple tools and interfaces that don't talk to each other, trying to manually connect the dots.

The result is a nonstop, overwhelming effort as administrators race against the clock to detect, contain, and remediate new malware threats—a race that they're losing far too often. A smarter approach is needed.

Organizations need to be able to take on the most sophisticated, evasive malware without needing a team of highly trained security administrators. They need to stop most threats before they can do damage to an endpoint. A smarter defense strategy would stop the most sophisticated, evasive malware before it can damage an endpoint. This would allow security teams to strike the right balance between security and flexibility for their organization. They should be able to tightly restrict what can happen on an endpoint or give users more freedom to run outside files and applications, depending on what makes sense for the organization. In either case, they should be able to react immediately to threats, without multiple manual steps. Finally, organizations need a way to connect the dots among different security components much more quickly and easily. They need a zero-day malware defense framework that's continually adaptive—gathering and sharing insights into the most suspicious and evasive threats and automatically applying them to protect the rest of the environment.

Unmask and Contain Hidden Threats

Intel Security offers a new generation of security capabilities designed to combat the most evasive modern threats. Drawing on powerful machine learning analysis and application containment tools, organizations can unmask hidden threats and stop them in their tracks—much more quickly and with much less effort.

These capabilities are delivered through two new innovations from Intel Security:

- **Real Protect:*** Real Protect combines pre-execution static analysis and post-execution behavioral analysis to stop more malware than any signature-based or static-only solution, all integrated into the Intel Security ecosystem. It applies state-of-the-art machine learning techniques to identify malicious code based on both an in-depth assessment of its static features (pre-execution analysis) and what it actually does (dynamic behavioral analysis)—all without signatures. It peels away the latest obfuscation techniques to unmask hidden threats so zero-day malware has no place to hide.
- **Dynamic Application Containment:*** Dynamic Application Containment makes it easy to protect "patient zero" endpoints from new zero-day malware infections, without sacrificing productivity. When an endpoint detects a suspicious file, Dynamic Application Containment 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, Dynamic Application Containment lets the suspicious file load into memory without allowing it to make certain changes to the endpoint or infect other systems while it is under suspicion. The endpoint and user can remain fully productive while providing an opportunity for security teams to perform in-depth analysis.

These new capabilities are integrated—with each other, with other security solutions, and with McAfee® Endpoint Security—to provide a multi-layer defense against the most evasive threats. They empower your security team to address all stages of the threat defense lifecycle—detect, correct, and proactively protect—in a fast, automated way. As a result, you can:

- **Unmask the attack:** Stop more attacks by stripping away obfuscation techniques to see more malware threats.
- **Limit the impact:** Contain, shield, and prevent damage to systems, either before an attack occurs or before it can cause irreversible damage or infection.
- **Track and adapt:** Use automated, integrated defenses to perform a wider range of security operations without having to think about them or manually activate them.

Unmask Hidden Threats with Static and Dynamic Analysis

Cyberattackers use savvy techniques to disguise the appearance, or "fingerprint," of their malware. By making minor alterations to their code, they can change the signature or hash value just enough to evade defenses that rely on attack-specific signatures. But while it's relatively easy to make surface-level code changes, it's very difficult to hide all the attributes of malware. And it's nearly impossible to hide how it behaves.

Real Protect strips away the mask by using 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. As a result, it can catch more zero-day threats than any signature-based or static-only solution.

Blocking threats before they execute: Real Protect static analysis

With traditional signature-based defenses, endpoint protection is always a race against the clock. Recognizing that a previously unknown file is malicious, creating a signature for that specific threat, and distributing the .DAT file out to endpoints so that they can block it takes time. Modern malware authors know that if they just modify a few aspects of their code, they can slip past those signature-based defenses. In the time it takes the signatures to catch up, they can do it again and again.

Real Protect breaks the zero-day signature cycle by starting with a different assumption. Malware authors can change all sorts of things around the edges of their code, but at the end of the day, it's still malware. So it's likely to share many attributes with known malicious code—the compiler used, the programming language, the shared and dynamic libraries it references, and many other features.

Real Protect performs a machine learning statistical analysis of all those static binary code features to unmask malware for what it is, in milliseconds, without signatures. By comparing those features against known threats, it peels away the latest obfuscation techniques and detects most zero-day malware before it ever has a chance to execute.

Here's how it works. Intel Security draws on the more than 500 million malware samples collected from millions of endpoints worldwide through McAfee Global Threat Intelligence (McAfee GTI). It combines this with millions of other malware samples from other threat intelligence sources and creates machine learning models of different malware binary types. These are not signatures for each attack seen in the wild—they are profiles of entire classes of malware.

Real Protect can then unmask hidden malware before it has a chance to execute. No one has to manually examine the code, and no one has to create a signature. Most infections never hit users and systems. And security teams avoid a huge amount of remediation and cleanup.

Detecting the most evasive malware: Real Protect dynamic behavior analysis

Static code analysis can catch many zero-day threats, but it doesn't catch all of them. If a cleverly designed exploit is misusing a legitimate application (for example, a phishing attack buried in a macro in a legitimate Word document), even the best static-only defenses can miss it.

Unfortunately, static code analysis is where most "next-generation" endpoint defense systems stop. Intel Security goes farther. We know that even if cleverly designed malware disguises itself in a file system, it can't hide how it behaves. If it's malware, it always performs malicious actions as a process. Real Protect Dynamic takes the same kind of signature-less machine learning used in static code analysis but applies it to actual behavior.

If an unknown "greyware" executable is able to make it past Real Protect Static and other defenses, but the endpoint still views it as suspicious, it can invoke Real Protect Dynamic. The endpoint then lets the code run in a controlled, monitored mode where Real Protect Dynamic closely scans the application's behavior and reports back to the cloud for analysis.

As with Real Protect Static, the system compares the greyware's behavior against profiles generated from hundreds of millions of samples of known malware in McAfee GTI and other sources. If the behavior matches a behavior profile known to be malicious—if it's dropping sub-processes and overwriting files, making registry changes that match with known-malware behaviors—the endpoint is immediately notified and takes action to stop the threat, typically within seconds.

To understand how powerful dynamic behavioral protection can be, consider a typical ransomware attack. These attacks often disguise themselves in legitimate files or applications, and can wreak devastating damage. But to do that damage, they have to perform a distinct series of actions:

- **Step 1:** Evade frontline defenses by hiding in an email attachment or compromised website to reach the endpoint.
- **Step 2:** Once on the endpoint, begin activating processes—communicating with encryption key servers, searching for important user files on the system, copying, moving, renaming, and encrypting those files.
- **Step 3:** Issue ransom demand.

If you're relying on static-only defenses, once the ransomware evades them, there's nothing to stop it from completing its objective. Even if you're able to recognize what's happening and cut that endpoint off from the rest of the network, that endpoint and everything on it is lost. However, if your defenses are watching the greyware's actual behavior, everything it tries to do on the endpoint presents a new opportunity to detect and stop it.

Even if the ransomware starts running, it won't get far. In the few seconds that elapse while it's being analyzed, it might be able to communicate with the encryption key server. It might even be able to encrypt one or two files. But that's as far as the attack gets before it's stopped and remediated.

With Real Protect Dynamic, you've stopped that malware in its tracks on the first endpoint that encountered it. You've prevented it from spreading to other systems and causing serious damage on the endpoint. You've saved "patient zero" from losing everything on that system. And you've done all of this automatically, in seconds, with no manual intervention.

Protect Patient Zero with Dynamic Application Containment

When does it make sense to let an unknown file or application execute, and when is it better to block all behavior that could potentially be malicious to begin with? The answer can be different for every organization—and can even be different for different parts of an organization.

In some cases, users have a legitimate need to run a wide range of 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. In these scenarios, allowing suspicious files to execute and then monitoring them with dynamic behavioral analysis may make sense. In others (especially in heavily regulated organizations in healthcare or financial services), flexibility takes a back seat to endpoint security. These scenarios demand a "block first, ask questions later" philosophy. But security teams still don't want to impede users more than absolutely necessary.

Dynamic Application Containment provides an alternative, behavioral-based approach to greyware that preemptively contains suspicious applications by narrowly limiting what they can do on an endpoint. Here's how it works. If endpoint defenses classify an executable as suspicious, they can invoke application containment. Dynamic Application Containment lets the file load in memory but blocks 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 has an opportunity to perform deeper analysis on the application.

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 also acts as a greyware "flight recorder," tracking all the activities the application attempts. It communicates with McAfee Endpoint Security and the larger defense fabric, so that if the greyware is deemed to be malicious, the rest of the environment can be updated to block it—in near real time, automatically.

Together, these dynamic containment capabilities:

- **Save patient zero:** Dynamic Application Containment reduces or eliminates the ability of the greyware to make malicious changes on the endpoint, without requiring the user to wait around for in-depth code analysis.
- **Help defeat malware that recognizes when it's being analyzed:** With Dynamic Application Containment, process containment happens on the endpoint, which continues to run as normal, so malware is less likely to detect that it's being contained.
- **Dramatically accelerate the threat defense lifecycle from detect to correct to protect:** Dynamic Application Containment blocks changes on the endpoint, so "correction" activities are often unnecessary, since the malware is already contained. At the same time, it feeds information about the greyware back to the larger threat defense fabric to protect other endpoints from infection.

An Integrated, Automated Defense Fabric

Real Protect Static, Real Protect Dynamic, and Dynamic Application Containment all provide powerful capabilities to unmask hidden threats and stop zero-day malware in its tracks. But unlike point solutions that require disparate tools and interfaces, Intel Security solutions are integrated into a unified, adaptive defense fabric.

Real Protect and Dynamic Application Containment work with each other, as well as with Intel Security solutions such as McAfee Endpoint Security, McAfee Threat Intelligence Exchange, McAfee Active Response, McAfee Advanced Threat Defense, and others as a single, integrated system. For example, when Real Protect or Dynamic Application Containment unmask an evasive threat as malware, they immediately communicate that information to McAfee Threat Intelligence Exchange, which provides threat intelligence information for the entire environment. If one of these defenses unmasks zero-day malware on one endpoint, the rest of the environment is updated to protect against it in near real time.

The result is a continually evolving threat model for the organization. Every new threat detected automatically enhances the organization's defenses as a whole. Previously manual steps in the detect, correct, and protect phases of the threat defense lifecycle disappear. And organizations gain the flexibility to mix and match the industry's broadest portfolio of threat defense capabilities through a single interface, knowing that any intelligence gained in one component automatically carries over to the next.

For security teams, the difference is stark. More zero-day malware unmasked and blocked. Threat response radically accelerated. And security operations are much simpler and require much less time and resources.

Learn More

For more information about Real Protect and Dynamic Application Containment, visit:
http://mcafee.com/us/solutions/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.

* The solution includes hosted data centers located in the United States used to check file reputations and store data relevant to suspicious file detection. Although not required, Dynamic Application Containment will perform optimally with a cloud connection. Full 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

OCTOBER 2016