COMODO

Issue 1

Default Deny: Preventing Malware & Maintaining User Productivity

Avoiding Infections with Secure Auto-Containment™

Despite sustained and significant investments in IT security solutions the rolling thunder of breach disclosures, nation-state attacks and thriving cybercrime markets are stark reminders that much hard work remains to be done.

Gartner Research Inc. states it bluntly in its latest 2016 research on endpoint protection platforms (EPPs). "When 44% of reference customers for EPP solutions have been successfully compromised, it is clear that the industry is failing in its primary goal: blocking malicious infections."[1]

The hard fact is that most breaches start with endpoints compromised by malware. Like the proverbial crack in the dam from a compromised email, login or social media account – hackers attack relentlessly until the data breach succeeds.

Unfortunately, customers, partners and employees are soft targets. According to the 2016 Verizon Data Breach Investigations Report[2], despite years of education efforts, 30% of recipients open phishing messages and 12% click on unknown attachments. Further, the window to protect users from new threats is extremely short. Verizon's data shows that the median time to click on the attachment is less than four minutes.

Today, most endpoint protection is still based on an increasingly antiquated Default Allow approach, meaning that only applications or executables that are known to be bad are blocked from running. This is easy enough for hackers to overcome by creating new attacks using slight variants of existing malware. These 'brand new' unknown variants, not yet on any blacklist are allowed to infect and compromise their target.

All of these facts help explain why the current endpoint protection approaches are failing. The real solution is twofold: increase detections as much as possible by

Gartner

[1]Firstbrook, Peter and Ouellet, Eric. "Magic Quadrant for Endpoint Protection Platforms." (February 1, 2016): Gartner Research Inc., 28.

[2]"Verizon 2016 Data Breach Investigations Report," (2016) Verizon Inc. Web.

augmenting blacklists with new, non-signature based methods of detection, and change from a default allow to a default deny posture for unknown files. Only one vendor today can meet both these goals, Comodo. Let's look more closely at the details of how this is done with Comodo® Advanced Endpoint Protection solution.

Non-signature based detection products work in a few different ways. For example, application control can be used to monitor and stop suspicious processes that attempt unusual interactions. Memory protections can be used to stop memory-based exploits like buffer overflows. Some solutions even use activity and behavior monitoring in conjunction with machine learning and AI.

Collectively, these techniques catch an array of threats that are missed by signatures alone. However, they are not a complete replacement for signature-based solutions. In other words, they may not catch all the threats that are detected by signatures. Therefore, both types of protection are required.

This is a big strength of Comodo Advanced Endpoint Protection. Most non-signature products in the market today are standalone and require that a traditional endpoint protection product still be used. This makes things more complicated and expensive for the IT security team. With Comodo, these advanced detection techniques are included right alongside traditional, award-winning signature-based protection with only one product to install and manage across all enterprise endpoints.

In addition, Comodo's non-signature defenses are also best of breed in several areas including fileless malware protection and Secure Auto Containment.

A Practical Default Deny Posture

New containment technology makes it not only possible but also practical to implement a Default Deny posture. This is a rare, transformational opportunity for organizations of any size.

In sharp contrast to the Default Allow posture which blocks only known malware and allows everything else unfettered access, a Default Deny posture blocks all known malware and only allows known and trusted applications or executables to run unchecked on the endpoint. A true Default Deny Platform® also prevents infection without impacting usability by automatically wrapping all unknown or untrusted executables in an isolated container. This sustains user productivity while preventing malware from gaining access to the endpoint and network, effectively preventing the damage from zero day threats and APTs.

Achieving a practical Default Deny posture requires innovation in two of the emerging endpoint protection concepts identified by Gartner analysts in its report, "A Buyers Guide to Endpoint Protection Platforms."[3] First, the Gartner analysts identified an emerging malware protection technique called application control and explained how it creates the opportunity for a Default Deny posture:

> "Application control describes the ability to restrict application execution to a list of known and trusted applications. The 'trusted application' list can be as restrictive as the applications already installed (aka lockdown) or as loose as the known universe of cataloged trusted applications – or anything in between. Application control shifts the paradigm from 'default allow' (allowing all applications as long as they are not known malware) to 'default deny' (not allowing any applications to run unfettered unless their providence and reputation are known) thereby automatically blocking new or targeted malware."[4]

Gartner notes that making Default Deny a reality using application control at the endpoint, however, raises many questions. How do security vendors establish what to trust? How are unknown or untrusted applications prevented from executing? And how are unknown applications evaluated automatically?

---

[3]Firstbrook, Peter and Ouellet, Eric. "A Buyer's Guide to Endpoint Protection Platforms." (January 29, 2015): Gartner Research Inc. Copy attached.

[4]Firstbrook and Ouellet, "Buyer's Guide." 5-6.

Early Default Deny attempts tried to achieve isolation by putting entire applications into virtual machines. This approach proved impractical due to the heavy impact on usability and high demands on endpoint resources that reduced performance. Additional attempts to delay the downloading of unknown executables in order to perform file analysis before allowing users access, created usability issues, as the end user must wait for an undisclosed time for access to the file to be granted.

Now, for the first time, a practical Default Deny posture is causing a breakthrough at the endpoint using a new, lightweight filesystem technology "container" explained further in this paper. Using containment at the endpoint is the key breakthrough making it possible to implement a Default Deny Platform without impacting user productivity or taxing endpoint computing resources.

Of course, there is no single silver bullet for any defense and effective endpoint protection requires integration with multiple layers of Specialized Threat Analysis and Protection (STAP). Fortunately, the same Default Deny posture applies to every layer, making the entire security ecosystem exponentially more capable of preventing the damage from unknown malware (zero days) attacks.

The disruptive effect of this advance in security and usability cannot be overstated. We have entered a new era of unprecedented effectiveness in preventing infection from unknown malware at the endpoint.

Containment Breakthrough Leads to Default Deny Protection

From breach disclosures to industry research, it's all too clear that current endpoint protection platforms are failing, and on a large scale.

The reasons why can be summarized into one overarching weakness: most endpoint protection platforms are based on a Default Allow posture that fails to detect unknown applications and executables that contain new malware. Put another way; even though malware begins as an unknown file, malware signatures still rule as the de facto standard for security.

As a result, most enterprise endpoints today rely on an increasingly archaic Default Allow policy, meaning if an application or executable is not known to be bad, it's allowed to execute on the CPU.

Gartner estimates that signature-based malware engines are only 30% accurate at detecting new threats.[5] And with inexpensive and readily available malware toolkits that can spew out unique zero day attacks with unknown signatures in the tens of thousands every day; well, you can understand why we're still seeing so many patient zeros.

Some years ago, malware sandboxing emerged as a new hope. Sandboxing opens every email attachment or executable in an isolated virtual machine to see what happens, and is frequently employed at the gateway. While sandboxing clearly helped, six years later it remains primarily a centralized resource in the gateway or cloud used to reduce the vulnerability window. Every email, attachment and executable coming in a fishing or spam email is sent to a sandbox for evaluation. This is inefficient to say the least, draining much needed CPU resources while achieving dubious ROI.

The problem is that in order to maintain user productivity, this sandboxing evaluation has to be done in parallel to the presentation of the unknown files to end users. This means they may run the files before the sandbox evaluation completes. In essence, this is a default allow approach. The result is that while sandboxing shrinks the gap between malware detection and remediation, it is not eliminated. The zero day threat remains and patient zero keeps occurring.

Meanwhile, hackers are laughing all the way to the bank with profits from ransomware, stolen login credentials sold on the Dark Web and other private information. Their automatic malware tools are creating new unknown malware variants at an overwhelming rate.

Early attempts to evolve sandboxing to provide application control and block execution of everything unknown at the endpoint have met with disappointing results, but for different reasons.

First generation endpoint sandboxing relied on traditional virtualization technology that isolated entire applications in separate virtual machines. In practice, this approach proved far too resource intensive. Traditional virtualization requires that each isolated application run in its own virtual machine, complete with its own full copy of the operating system and its partition of the endpoint hardware. With so much computational overhead, this approach to endpoint sandboxing hurts desktop performance.

There were other basic operational problems with sandboxing too, such as saving files or moving applications out of isolation that impacted usability so significantly that solutions based on traditional virtualization proved unworkable for most companies. Recent advances in virtualization technology in the form of lightweight

[5]Firstbrook and Ouellet, "Buyer's Guide." 3.

containers, however, have created the opportunity to solve these problems and introduce the next generation of endpoint protection.

Containment is the key technology that enables three emerging endpoint protection techniques identified by Gartner analysts to come together into a new combination that re-defines the category. The first is what they call "full software attestation," which involves classifying all running processes as good, bad or unknown. The second is application control and the associated paradigm shift from default allow to default deny. And the third is unknown file containment at the endpoint.

One important advantage is that containers require much less computing resources than traditional virtualization based on virtual machines, so malware containment can be efficiently implemented at the endpoint without negatively impacting user experience, productivity, CPU resources or IT budget.

Even more importantly, container technology makes it possible to safely jail unknown executables at the process level instead of at the entire application level. For example, you can be running a trusted Web browser outside of a container, but if suddenly an unknown plugin tries to execute, it will automatically be isolated in a container until a trust verdict is made. This not only improves performance, it also enables the combination of what Gartner calls full software attestation with application control, so that only trusted executables are allowed to run normally.

Taken together, these advanced techniques make it possible to evolve from today's Default Allow posture that leaves endpoints vulnerable, to a Default Deny posture that isolates unknown threats in containment. With Comodo's Default Deny Platform any process or executable that is not known good or known bad is considered unknown and automatically contained, preventing unknown malware from accessing the resources needed to infect the endpoint and from there, the network.

In their endpoint protection research, Gartner's analysts provide an excellent checklist of points to investigate when evaluating solutions for application control and default deny.[6] For example, keeping users productive also requires that unknown files and executables be quickly evaluated and, if good, are automatically added to the whitelist so they can be moved out of the container as soon as possible, or to the blacklist if bad, and deleted from the entire environment.

A practical Default Deny Platform that prevents infection without hindering usability represents an IT security breakthrough. Using lightweight but robust containment makes it possible to move to a Default Deny posture that for the first time can effectively and practically prevent the damage from all unknown threats such as zero day malware and APTs.

Comodo Advanced Endpoint Protection Blocks Zero day Attacks and Unknown Malware

Comodo Advanced Endpoint Protection represents the vanguard of next generation solutions that mark a major milestone in the fight against endpoint malware.

In Gartner's Endpoint Protection Buyer's Guide, the analysts' top recommendation is, "Give primary consideration to the malware effectiveness of a solution and the breadth and depth of non-signature based techniques used, especially application control, malware sandboxing, vulnerability detection and full software attestation."[7]

Built upon a layered Default Deny Platform, Comodo Advanced Endpoint Protection completely fulfills this recommendation. It uses advanced proprietary Secure Auto Containment™ technology to combine application control, malware sandboxing and full software attestation in a novel approach that effectively isolates zero day attacks, unknown variants of Trojan horses such as Cryptolocker, Cryptowall, SamSam, and TeslaCrypt-style ransomware, as well as newly emerging 'Fileless' malware such as Powerware that is written in Powershell. Secure Auto Containment use OS virtualization to nullify these threats and prevent infection.

A complete endpoint security and management platform, the following components comprise Comodo Advanced Endpoint Protection: Comodo Client which includes antivirus, firewall, Web URL filtering, host intrusion prevention, behavioral analysis, containment and file reputation, and Comodo IT and Security Manager (ITSM). ITSM allows for the configuration of the security policies and visibility into the security infrastructure of enterprise endpoints through solutions such as mobile device management and remote monitoring and management.

Modular, lightweight and supported on virtually all Windows systems and servers, the Comodo Client requires no specialized hardware and also includes a full endpoint protection (EPP) suite with host firewall and IPS while ITSM provides tightly integrated MDM, MAM

[6]Firstbrook and Ouellet, "Buyer's Guide." 6.

[7]Firstbrook and Ouellet, "Buyer's Guide." 1.

and MSM, as well as Remote Monitoring and Management (RMM) and Patch Management.

Gartner says that providing a trust verdict on unknown executables quickly is an essential component of a default deny application control solution.[8] Comodo keeps files in containment for the shortest amount of time of any vendor in the industry. Comodo Advanced Endpoint Protection ensures the highest usability through two layers of Specialized Threat Analysis and Protection (STAP),implementing VirusScope on premises and Comodo Valkyrie in the cloud to verdict all unknown files through static, dynamic and, if needed, human analysis, leading to a verdict, on average, within 45 seconds - much faster than competing solutions. The unknown then becomes known to all Comodo customers with dynamic whitelisting and blacklisting.

Traditional attempts to isolate malware at the endpoint with Default Allow approaches, virtualization or resource-intensive sandboxing technologies are failing. Comodo's approach is completely different optimizing security and usability without impacting performance or productivity. Applying Comodo Advanced Endpoint Protection to the malware problem allows all unknown executables – good or bad – to operate in containment until analysis delvers a trust verdict.

How Comodo Solves the Malware Problem

Comodo's Default Deny Platform, the foundation of Advanced Endpoint Protection, emphasizes allowing known good applications while denying everything else free reign to client's endpoints until a verdict on those unknowns is reached. In order to execute on this strategy, identifying known good and known bad applications becomes critical. As the largest certificate authority in the world[9],

Comodo is uniquely positioned to identify known good signed applications and application publishers (whitelisting) while Comodo's installed base of over 85 million users provides Comodo Threat Research Labs (CTRL) with one of the largest caches of known bad files (blacklisting). Gartner identifies the size and quality of the catalog of known "good" applications and the capability to automatically allow sources of trusted certificates as essential features of application control. All unknown files are automatically run in containment, while an accelerated verdict is reached, both increasing usability and protecting the endpoint from being compromised.

Additionally, Comodo's global product development and malware research team has security professionals working 24x7x365 worldwide to ensure that unknown files are rapidly identified and integrated onto the whitelist if judged good or added to the blacklist if bad, before they are able to cause any damage elsewhere in the ecosystem.

The Engineering Behind Comodo Advanced Endpoint Protection

Secure Auto-Containment via OS Virtualization

IT teams who choose Comodo Advanced Endpoint Protection can be confident knowing that only safe applications will be running on their network with Comodo's Secure Auto Containment technology the key to the company's Default Deny Platform. As endpoint users introduce unknown and possibly malicious applications externally from their devices, those unknown applications are forced to run in containment, never risking infection or compromising corporate data, and never impacting performance or usability.

Comodo Advanced Endpoint Protection offers highly efficient virtualization at two layers – the OS and the CPU – but focuses on the OS as the constant because virtualization is not always supported by the CPU. This gives our customers continuous security at the OS layer with added security at the CPU layer when supported.

Comodo Secure Auto Containment technology uses CPU enforced OS virtualization with a single container (OS virtualization) model, that includes an exact copy of the endpoint machine including the kernel. This is one of the reasons startup performance is so fast in stark contrast to most sandboxes or containers that drain the CPU and slow down the system.

Comodo Secure Auto Containment technology is extremely lightweight, has no CPU dependencies and is completely application agnostic. Malware or any other unknown process entering this virtualization environment cannot modify the hard disk, registry, or COM interface; therefore, preventing infection.

Whenever a process or executable (PE) is run in containment (often referred to as "jailing"), the analysis system sits between the PE and the shadow resources it calls–including CPU, memory, registry, file system and more. If the PE turns out to be malicious code and attempts to exploit the machine, that action is housed entirely within the container where it can affect only the shadow resources provided in the virtualization layers (OS and CPU) and not those of the native machine. This prevents the unknown file from infecting the endpoint when it executes in the container. See the following attributes:

[8]Firstbrook and Ouellet, "Buyer's Guide." 6.

[9] "Market share trends for SSL certificate authorities for websites." W3Techs.com. Feb. 15, 2016. http://w3techs.com/technologies/history_overview/ssl_certificate.

- Two layers of virtualization for better protection: the OS and CPU (when supported)
- Prevents infection from any executable file introduced from the web, email, documents, network or external storage device
- Containment defeats unknown malware such as viruses, trojans and ransomware to zero-day malware and advanced persistent threats on patched or unpatched machines
- Secure Auto Containment of fileless malware to protect system memory with granular security for command line parsers or executors (Windows commands, Python and PERL scripts)
- Extremely lightweight with no performance hits requiring less than 1% CPU and only 20 MB of system resources
- Transparent to end users with no impact on usability; unknown files run safely in containment
- 100% compatible with old or new CPUs
- Broad OS support including Microsoft Windows, Linux and Mac OS

Behavioral Analysis

Through Comodo's technology, unknown software applications quickly move to from unknown to a verdict of known good or known bad with Comodo's Specialized Threat Analysis and Protection (STAP) engine combines local and cloud based analysis. Comodo's local STAP layer, VirusScope, first analyzes application behavior and actions running inside or outside of containment, and then VirusScope leverages multiple techniques to determine any malicious intent. Valkyrie, Comodo's cloud-based STAP layer, correlates the local view of the file activity from VirusScope with the global view and any particularly stubborn unknowns are analyzed by Comodo threat experts for a conclusive verdict. This reduces both false positives and false negatives and provides an accelerated verdict of malware at the endpoint. The result is that unknown files stay in containment for a very short time.

Application Visibility and Control

IT Directors and System Administrators can gain enterprise visibility over the applications that users are installing across Windows-enabled endpoints with device management capabilities built into Comodo ITSM. This allows IT to set mobile application policies based on groups such as productivity apps, utility apps, and gaming apps. Applications can be blocked or allowed to run only inside a secure container and productivity can be increased by allowing non-critical business applications to run only during a specific time. ITSM ensures the security of corporate data through comprehensive application management.

Through application visibility and control, automatic containment, and behavioral analysis, Comodo improves the security posture, keeping endpoints and networks infection free for businesses large and small.

Key Features of Comodo Advanced Endpoint Protection:

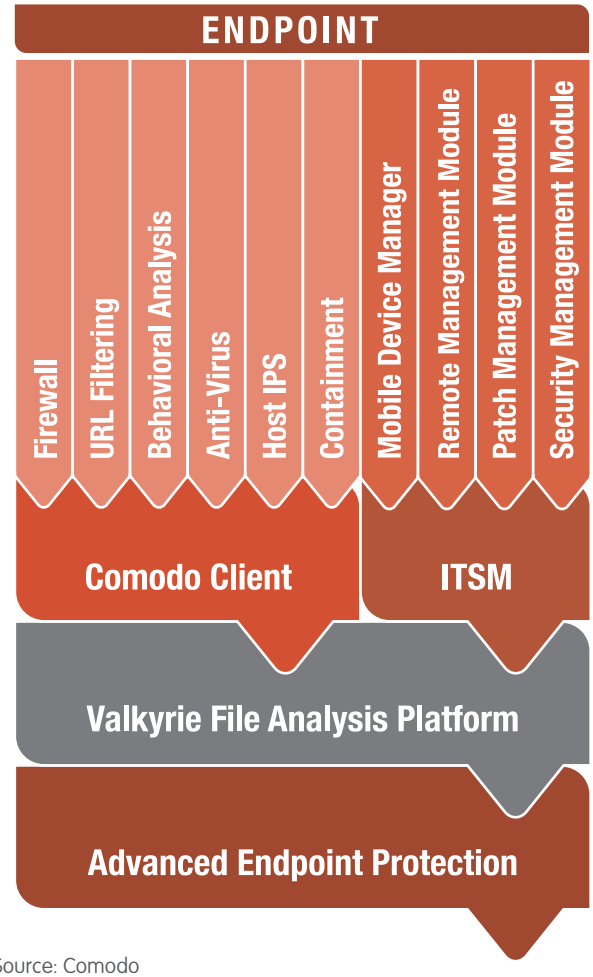
- Patent pending Secure Auto Containment, enabling usability while preventing infection from unknown, zero day and APT malware
- Comodo VirusScope local STAP on premises, employs Artificial Intelligence and Machine Learning to provide a local verdict of unknowns
- Comodo Valkyrie analysis in the cloud , a verdict driven malware analysis platform that provides accelerated verdicts using automatic static and dynamic analysis in seconds, and, if needed expert manual analysis under 2 hours
- Comprehensive Device and Security management for Windows desktops and servers, iOS, Android, OS X and Linux desktops and servers
- Enterprise wide, real-time visibility into all unknowns that have been automatically contained and their status, as well as that of trusted applications

- Tightly integrated device management, application management and device security
- Remote monitoring and management (RMM) with full device takeover capabilities
- Patch management and vulnerability management
- Enterprise wide quick, full and removable media scans for malware
- Cloud-based, unified IT and security management provisioned in about one minute
- Complete suite of endpoint protection (EPP) all-in-one including host firewall, HIPS, web URL filtering, file reputation, certificate-based whitelisting, persistent VPN and BYOD

Comodo Advanced Endpoint Protection is available. Contact **sales@comodo.com** or visit us online for more information at **https://www.enterprise.comodo.com/**

Source: Comodo

FIGURE 1
Comodo Advanced Endpoint Protection



Source: Comodo

Research from Gartner:

Make Sense of Endpoint Malware Protection Technology

The goal of endpoint malware protection is a solution that offers low administrative overhead, low end-user impact and the best available protection. Security and risk management leaders can make educated trade-offs within endpoint protection to achieve two of these three aims.

Key Challenges

- The marketing hype around "next-gen AV" and the IT industry's fascination with machine learning distracts from and creates confusion about the real value provided by different protection techniques.
- Unclear perceptions turn up constantly, as many techniques have similar names or umbrella terms like "application control," which can vary wildly in terms of actual capabilities.
- Blending technologies from multiple vendors risks agent bloat and software conflicts, resulting in disabled protection features and less-than-optimal configurations.
- Not all malware requires an exploit. Users can simply be tricked into downloading and running malware that does not require an exploit.

Recommendations

Security and risk management leaders overseeing endpoint and mobile security should:

- Design an endpoint protection strategy that consists of good security hygiene, layered protection and detection technologies, and end-user education.
- Avoid duplication of security capabilities across multiple solutions; instead, fully deploy existing protection and then begin to identify specific areas to augment.
- Avoid knee-jerk reaction purchases by mapping new purchases to gaps and taking the time to run a useful proof of concept to ensure the technology can fit or enhance existing workflows.
- Use a combination of internal testing and third-party effectiveness tests to verify vendor claims. Vendor-sponsored or -commissioned comparisons can be useful data points, but should not be given the same weight as impartial tests.

Introduction

Endpoint protection is not simple. Security and risk management leaders struggle to find the right balance between threat coverage, administrative overhead and end-user impact. Table 1 illustrates, at a high level, the impact that the most common anti-malware techniques can have for most organizations.

These technologies each carry different capabilities and, importantly, limitations. Although some technologies appear to offer similar functions, they are often marketed as the ideal solution for malware prevention. The hype around artificial intelligence and machine learning is adding more confusion to the matter.

In practice, a combination of technologies will provide the widest protection against malware attacks. Most attacks exploit well-known unpatched vulnerabilities, use social engineering to trick users to install malware, or use interpreted code such as Java to download and install malware. Fileless malware is becoming more and more prevalent in the threat landscape. To address such challenges, security and risk management leaders have a range of options from both established and emerging vendors. Most buyers continue to consider emerging solutions to be complementary, rather than outright endpoint protection platform (EPP) replacements.

The expansion of malware protection technologies in EPPs over the past five years has delivered various advantages, including fewer updates and less administrative overhead, and provided for better protection at specific stages of the kill chain or for specific classes of malware.

It is important to consider education as a key part of the fight against malware. Users remain the weak links — they are impressionable, and subject to deception and coercion. Security awareness programming plays an important part in informing staff and partners of their responsibility in limiting vulnerable behavior.

Signature-based detection is the most well-known approach to malware detection. Because signatures and heuristics use pattern matching to identify malicious files — meaning the vendor must have seen the file to create the signature — it is also the most criticized. Of course, no modern

Table 1. Common Anti-Malware Techniques

Technique	Threat Coverage	Admin. Requirement	End-User Impact
Signatures	Low	Low	Low
Machine Learning	Medium	Low	Low
Application Control	High	High	High
Application Isolation	Medium	High	High
Behavioral Analysis	High	Medium	Low
Exploit Mitigation	Medium	Low	Low
Source: Gartner (April 2017)			

malware protection solution relies solely on malware signatures. Modern endpoint protection platforms will also include one or more of the following technologies:

- **Application control** limits the applications and processes that may execute on an endpoint. The goal is to apply a "default deny" enforcement model, whereby everything that is not known or trusted is not executed.
- **Isolation or containment solutions** allow installed endpoint applications to process potentially malicious files (such as web pages or downloaded documents) safely by isolating the processing of those files from the rest of the system.
- **Behavior analysis** provides rule-based monitoring where applications and processes are observed for particular indicators of intrusions that may be blocked or detected.
- **Endpoint detection and response (EDR) technologies** monitor endpoint activities and aid in the detection, containment, investigation and remediation of malicious behavior.
- **Exploit technique mitigation** prevents software exploits by enforcing in-memory protection. It guards against memory overflow attacks and against other attack methods that take advantage of software vulnerabilities.

By themselves, none of these technologies are a panacea to the intricacies of malware intrusion. Some technologies carry their own weaknesses. Security and risk management leaders should assess new malware protection solutions by discerning what distinguishes these technologies and how the various solutions can combine to form a more formidable malware prevention plan.

Analysis

Include Signature Technology in a Layered Protection and Detection Strategy

The majority of anti-malware solutions, such as EPPs, secure web gateways (SWGs), secure email gateways and unified threat management (UTM) solutions, include some form of signature detection — a fundamental piece of endpoint protection. A purely signature-based detection method has low success rates against sophisticated malware because, by its nature, it can only match to known malware and minor variants. Signature detection is easy to evade and signatures may take a while to develop. They require every endpoint to update frequently or to use cloud-based signature look-ups. For these reasons, it is uncommon to find EPPs that solely rely on signatures.

Most solutions use the cloud to look up the latest reputation information for a previously unseen file; however, the cloud is not available to systems that aren't connected to the internet but are nonetheless vulnerable to malware.

Signature-based detection is strong at blocking common attacks without using more resource-intensive or end-user-impacting technology, but some security vendors incorrectly frame this method of detection as an indicator of outdated technology. Despite some marketing claims to the contrary, signatures and heuristics do have advantages:

- **Proactive protection against known malware.** Scanning a file prior to execution prevents infection, assuming a signature exists for that threat. There is no need to utilize more resource-intensive inspection techniques if a file is known to be bad.
- **Very low false-positive rates (FPRs).** False positives do occur, especially with more aggressive heuristics engines, but most solutions have a very low FPR. Having a low FPR is critical for EPP solutions that are expected to protect endpoints autonomously. Almost every traditional vendor has at one time incorrectly convicted critical Windows files as malicious, rendering operating systems unusable.
- **Prevents false positives in other, more aggressive techniques.** Signatures can be used to help mitigate false positives in more aggressive detection techniques. When used as a method to "protect" known good files instead of purely to detect known bad, signature-based detection is a strong addition to a solution's technology stack.

Use Machine Learning to Reduce the Reliance on the Distribution of Signature Updates

The technology community in general is thrilled by the potential of machine learning, and machine learning has the potential to play an even greater part in the malware prevention space than it does today. Vendors use supervised machine learning engines to process large numbers of malicious files and large numbers of prevalent but known good. The resulting algorithm can be run locally on the endpoint device or in the cloud, and it can test a file for similarities to good or malicious files.

The advantages of this form of detection include:

- **No malicious code is run.** The detection is usually made in the pre-execution phase, before running code.
- **No signatures are used when run on the endpoint.** A mathematical model is used instead of the traditional signature database, removing the dependence on large disk and memory footprint along with the struggles associated with updating endpoint devices.

- New malware can be detected by the same model. Predictive models can use the statistical scoring to detect malware that has not been analyzed before.

- No internet connection is required. All scanning is local, and no cloud-based look-ups are required.

However, security and risk management leaders should also recognize the limitations and current weaknesses of machine learning as a stand-alone anti-malware resource.

The use of packer and encryption technologies limits the inspection model's coverage of the actual malware. Solutions running a purely predictive machine learning model on the endpoints suffer the risk that malware authors will: (1) study the detection behavior of the model on the endpoint, (2) adapt their malware code, and (3) attempt to evade detection.

Solutions should be able to avoid false positives, but it is inevitable that there will be files that are very close to the good and the bad model, resulting in both false positives and false negatives. EPP solutions solely relying on machine-learning-based detection can carry a high false-positive rate. EPP solutions generally combat false positives by adding other techniques, such as whitelisting known good files or cloud lookups for files that are too close to call, or by using signature-based whitelisting. With mathematical models that are infrequently updated, organizations may find themselves building an extremely long and hard-to-manage whitelist.

Recommendations

- Ignore biased claims by endpoint security vendors that signatures are useless.

- Update to the latest version of the incumbent EPP, as newer releases are less dependent on signatures and supplemented by additional protection techniques.

- Ensure the vendor provides a solid workflow to manage false positives and false negatives — be wary of solutions relying on a manual whitelist and blacklist capability.

Improve Visibility With EDR or EPP Tools That Focus on Applications and Processes

Security analysts cannot truly begin to harden systems and infrastructure without a solid understanding of what is running in an environment. EDR and EPP tools that report on applications and processes will provide data points that can be used to strategize a plan to reduce the attack surface.

Application Control/Whitelisting

Application control and application whitelisting apply a default deny enforcement model, where an application or process that is not explicitly whitelisted is deemed to be untrusted. Untrusted processes can be blocked outright or, with solutions that provide for dynamic decision making, can run with extra protection or scrutiny.

As a malware protection technology, application control has various strengths:

- **Provides strong default deny prevention.** If tight policies are used, application control provides strong protection against malware, especially when used in concert with technology that prevents legitimate processes from acting maliciously.

- **Incurs low machine overhead.** Application control solutions do not have a significant impact on endpoint resources.

- **Offers broad platform support.** Application control can be used to keep unsupported and/or unpatched systems secure. Legacy systems that still run on Windows 2000 or Windows XP only, for example, can be locked down by using a restrictive application control policy, typically in combination with some form of memory protection.

- **Requires no signature files/updates.** Application control is independent of malware signature files that require frequent updates. However, more advanced use, such as relying on file reputation in a more dynamic environment, requires access to the latest file reputation databases, typically over the internet.

- **Applies to all potentially unwanted programs.** Application control catches categories of applications that are not technically malware but might compromise security. Such categories include consumer remote access control applications, and file sync and share agents.

There are several considerations that security and risk management leaders must take into account when exploring application control for wide endpoint deployment. There are notable impacts on users and operations.

Application control can be very successful for fixed-function devices such as servers, where their applications and workloads are predictable. Users with well-defined work styles (for example, call center employees) are also ideal candidates for a successful deployment. For other user types, such as mobile workers or developers, the default deny approach may not provide an acceptable experience, unless workflow procedures can minimize approval delays for unknown, untrusted software.

In terms of operations, managing exceptions introduced from untrusted sources can incur substantial overhead. Organizations should plan for such overhead and provide administrators with the proper tooling. Such tooling will allow administrators to streamline the exception management process and to make the right decisions in the least amount of time. Allowing trusted sources of change minimizes the number of exceptions necessary.

Managing fine-grained application control policies in a dynamic endpoint environment is operationally complex. Leading solutions solve this problem by allowing more lenient policies: Trusted publishers, locations, installers and users may be allowed to install new software, automatically updating the application control policy. However, lenient policies may compromise security.

The strength of application control, as a protection technology against malware, greatly depends on the policy and the additional technology deployed on the endpoint. Malware authors have been able to release digitally signed malware using stolen certificates, exploit legitimate applications in memory and launch fileless malware, thus lowering the effectiveness of application control against sophisticated attackers.

Security and risk management leaders should carefully consider vendor claims around application control features. Simply blacklisting executables by name or file path is not considered a strong application control capability.

Application Isolation

Application containment solutions, also known as isolation solutions, implement malware protection using a paradigm best expressed as: Run risky processes and content, but isolate them from the rest of the system.

Security and risk management leaders should consider several strengths of application isolation, beginning with the provision of unrestricted user access. Malware containment does not block users from accessing sites or from downloading and processing potentially harmful content. In the most extreme form of application containment, users, should they choose to do so, may run malware in the isolated environment.

Some solutions discard the isolated environment and reset it to a clean state at launch or at regular intervals. Others do so when malicious behavior is detected in the isolated environment.

Isolation is valuable as a safeguard against a malware author's evasion techniques. The actual suspicious code runs on the endpoint, but in a contained environment. Even though the code runs, its ability to cause damage is limited by the sandbox. Organizations interested in deploying application containment solutions must be aware of the following cautions:

- **User impact.** By design, containment solutions limit interaction between isolated and nonisolated environments, which may impact the user experience.
- **Operational impact.** Administrators must manage trusted sites, applications, file locations and policies for moving files between zones of different trust levels.
- **Lack of application support.** The isolated environment may not support all preferred applications and versions.
- **Hardware support.** Some solutions depend on specific CPUs and chipsets, and the RAM requirements for a successful isolation deployment can be larger than the amount of memory found in typical corporate endpoints.
- **Large differences in implementation.** Solutions differ greatly in terms of policy control options, technologies used to enforce isolation, support for multiple zones, supported applications, management and reporting, and malware behavior analysis in the sandbox.
- **Limited protection.** Applications that run outside of the contained environment are not protected by the containment solution. Some vendors have started to extend their solutions by offering EDR technologies both inside and outside of the contained environment.

Recommendations

- Prepare for increased help desk calls, and put a well-tested and well-documented exception workflow in place, as additional administrative overhead is inevitable with a default deny implementation.
- Enforce default deny only for a subset of devices that have predictable workloads. For other types of users who have a less rigid set of requirements, like developers, use the client in monitoring mode to identify suspicious-looking behavior.
- Verify the hardware requirements can be met with your devices, and that critical applications are fully supported.
- Plan to deploy isolation technology to the group of users that are most at risk, rather than attempting to deploy for every single user.

Reduce the Attack Surface With Technologies That Look for Signs of a Malicious Outcome

While there are a steady stream of new vulnerabilities and attack vectors, the outcome is almost always the same. Consider the case of ransomware, where the

goal is to encrypt the data — if technologies can detect the behavioral intent behind malware, the method of compromise is less important. That said, mitigating known vulnerabilities should be near the top of all organizations' priority lists.

Behavioral Analysis

Behavioral analysis within endpoint protection has several strengths, even when used as an isolated technology. Such analysis can provide runtime protection against attack activity. The solutions not only provide point-in-time detection, but also monitor the behavior of all, or at least all suspicious, processes over time to generate a greater understand of the context of the behavior.

For example, an Outlook.exe process spawning a Word.exe process is typical behavior for an information worker that receives documents by email. However, when the Word.exe process begins to connect to the internet, or to spawn other processes, the behavior becomes more and more suspicious.

EPP solutions using behavior analysis can also detect and block previously unknown malware without the need for resource-intensive scanning or inspection. This detection is not dependent on the malware code, but rather on the behavior, which means that vendors with a focus on this type of detection do not require any signature databases or file scanning. Behavioral analysis can detect multiple stages of the kill chain, such as droppers, network-borne attacks and some exploit techniques.

Some cautions are associated with deploying behavior analysis as a malware protection technology:

- **Potentially high FPR.** There is a fine line between malicious and normal behavior, so any behavior-based blocking technology incurs a risk of false positives. What appears to be malicious behavior is not always malicious. Kernel hooks and OS API calls that seem malicious may be legitimate.

- **Detection instead of prevention.** Sophisticated malware that does not trigger clear malicious-behavior-blocking rules will, at best, be detected after it runs, instead of being prevented before execution.

- **Requires tuning, expertise and updates.** Behavior-based malware protection requires organizations to carefully select rules, specify actions to take after detection, and whitelist trusted applications or digital certificates.

- **May impact users.** Because behavior analysis continuously monitors all activity on the endpoint, it may incur a performance penalty to the endpoint device.

Exploit Technique Mitigation

Exploit technique mitigation aims to stop malicious code from running in memory and, thus, make it more difficult for attackers to exploit software vulnerabilities. It does so by protecting the memory allocated to a process or application. It does not necessarily block the attacker from putting the malicious code into memory; it can also use techniques to prevent the code from being executed. This technology enforces security mechanisms already supported by the operating system, and adds capabilities beyond basic protection.

Security and risk management leaders can expect several benefits for organizations, including low management overhead, as the focus is on a small number of exploit techniques and does not rely on signatures or updates. Solutions generally incur limited performance overhead and operate transparently to the user. Microsoft provides a free Enhanced Mitigation Experience Toolkit (EMET) for free. It is officially supported by Microsoft until mid-2018, can be managed through Group Policy and makes for a good baseline of exploit mitigations.

Recommendations

- Use third-party effectiveness tests to verify vendor claims. Vendor-sponsored or -commissioned comparisons can be useful data points but should not be given the same weight as impartial tests.

- Ensure that incident response tools are adequate, as behavioral analysis is largely a detect-after-execution technology.

Evidence

This research is based on 1,505 client and vendor inquiries on endpoint security across Gartner for IT Leaders and Gartner for Technical Professionals analysts since January 2016.

Source: Gartner Research Note G00320339, Ian McShane, 25 April 2017

About Comodo

Comodo is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Building on its unique position as the world's largest certificate authority, Comodo authenticates, validates and secures networks and infrastructures for individuals, to mid-sized companies, to the world's largest enterprises. Comodo provides complete end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats, both known and unknown. With global headquarters in Clifton, New Jersey and branch offices in Silicon Valley, Comodo has international offices in China, India, the United Kingdom, throughout Europe, as well as Central and East Asia.