COMODO
CYBERSECURITY

Everything you wanted to know about endpoint protection but were afraid to ask

Selecting the right endpoint protection platform for your business

Issue 2

Gartner

Importance of Endpoint Protection, Taking a Holistic Approach to Avoid a Breach

Business IT has come to embrace the term "endpoint," which has become the moniker for any device that can connect to the network, including desktops, laptops, tablets, smartphones, and more recently, IoT (Internet of Things) devices. Many businesses are discovering that as the number of endpoints increase, firewalls and antivirus software is no longer adequate protection. The fact is, malware will get into your system. Endpoints are now subject to a much broader swath of malicious activity, including ransomware, phishing, malvertising, drive-by-downloads, cryptojacking, software subversion, as well as other backchannel attacks. What's more, attackers are leveraging zero-day attacks, where previously undetected vulnerabilities are used to deliver malicious payloads into endpoints.

Therefore, to avoid a breach, today's businesses need to take a more holistic approach to protecting their organizations from harm caused by an exposure to outside threats. Security providers cannot prevent 100% of new malware from coming into the network and causing damage to critical systems. Therefore, organizations need to be protected from malware inflicting damage to their network.

Protecting endpoints from today's ever evolving threat vectors requires endpoint protection solutions to use more than detection technology and white lists to identify good and bad files. Endpoint protection solutions must evolve into a platform approach, where multiple cybersecurity technologies, capabilities, and techniques are integrated into an advanced automated umbrella of protection, which stops both known and unknown threats. EPP solutions must include capabilities which can identify and prevent malicious activity. Comodo's Threat Research Lab indicates your EPP solution "must have" these features:

- Capability to prevent known and unknown malware from causing damage, without the need for daily signature distribution
- Behavioral detection that identifies suspicious
- Native protection for application vulnerabilities and memory exploits
- Integrated on-demand malware detection scans of folders, drives or devices such as USB drives
- Logging of suspicious event data, stored in a centralized location for retrospective IOC and indicator of attack (IOA) searching and analysis, that can be searched in real-time
- Support remote quarantines and restricts network access to only the EPP management server
- Automatically distributes policies, controls and new agent/engine versions without connecting directly to the corporate network
- Collect suspicious event data, even when not attached to the corporate network
- Offer severity and confidence indicators for detections and alerts
- Provide risk-prioritized views based on confidence of the verdict and severity of the incident
- Display full process tree to identify how processes were spawned, for root cause analysis
- Automatically quarantines malicious files
- Identify changes made by malware, and provides the recommended remediation steps
- Detect, block and report attempts to disable or remove the EPP agent

Those core capabilities are only a starting point for full endpoint protection. Comodo Cybersecurity also recommends that an EPP solution include

- A unified management console that is cloud based and fully supported by the vendor as a multitenant solution and malicious activity associated with a process
- Supports virtual patching which shields both the OS and applications from known vulnerabilities

- Incorporates zero trust whitelisting, which is further supported by a vendor-maintained "app store"
- Provides application isolation to separate untrusted applications from the rest of the system
- Includes access to a cloud- or network-based sandbox that is VM-evasion-aware
- Incorporates technologies, such as deception and honey pots to expose an attacker
- Vendor itself offers managed detection services, alerting customers to suspicious activity
- Vendor itself offers managed threat hunting, or managed IOC/IOA searching, for detecting the existence of threats
- Supports advanced natural-language queries with operators and thresholds
- Provides guided analysis and remediation based on intelligence gathered by the vendor
- Provides attribution information and potential motivations behind attacks
- Can utilize third-party, community and intelligence feeds
- Allows remote remediation via the management console
- Includes APIs for integration with security orchestration, automation and response (SOAR)/orchestration for automation

Source: Comodo

Verdicting Systems, Battle the Growth of Cybercriminals Creating Unknown Threats

Dealing with new or unknown files is one of the most critical capabilities of any EPP. According to Comodo Cybersecurity, the rise of Unknown files has skyrocketed in the last 5 years. Comodo reports that there are currently more than 300K new malicious files detected every day, which adds up as 100MIL yearly.

Simply put, an unknown file is a unrecognized executable that could be potentially malicious. Without any way to identify and classify unknown files, endpoints can be infected with malicious code. Most EPP products use assumptive based trust (or a Default Allow posture) when dealing with new or unknown files. The default allow posture allows all files, other than the known bad files, to have unfettered access to system files. That method assumes that files that are not identified as bad, must be good or safe. One of the major problems with a Default Allow posture is that cybercriminals are constantly building new variants of existing malware designed to avoid detection from anti-malware solutions. Cybercriminals will put a great deal of effort into disguising the new variants of malware, aiming to keep the files in the realm of the unknown, instead of quickly identified as bad. That allows those redesigned pieces of malware to infect systems as an unknown file, until other methods are used to detect the infection. What's more, those new pieces of malware can go undetected for days, weeks, or even months, if the code is not analyzed then a new signature will be created for the signature database. Even if the vendor has many other detection techniques, such as heuristic based, dynamic behavioral analysis, machine learning, artificial intelligence, reputation-based detection, network-based detection... these all depend on a previously seen behaviors of malware activity. They would eventually fail to detect a malware specifically crafted for that organization, or newly created and never seen before malware, called zero-day malware.

And the question for enterprises is not whether they will be target of a zero-day attack (previously undetected or unknown vulnerability) or not, but the real question is what their endpoint security solution could do after one of the imprudent employees execute a zero-day malware thinking it's a safe attachment from a phishing email or a file downloaded from a fake website. That's where the zero-day will bypass all detection methods and Default Allow would put the enterprise under risk.

There are numerous reasons why many EPP vendors use a Default Allow methodology. Productivity is the key reason for not preventing an endpoint from running a "good" unknown file. Unfortunately, new types of malicious software, such as ransomware, are able to spread using the Default Allow ideology.

One solution is to use a Zero Trust environment, where any unknown files are blocked from executing. Consider perhaps that unknown file is a legitimate process or program that may have been created internally or by a known vendor? A Zero Trust environment will prevent good unknowns from running potentially hampering productivity.

For a Zero Trust environment to work effectively, new or unknown files must be examined when first encountered and classified as malicious or good. The process that accomplishes that is called verdicting. Comodo Cybersecurity uses a multifaceted approach to deliver verdicts on unknown files quickly. The key differentiator here is how quickly a verdict can be derived, without any interaction from the end user, IT administrator, or other support individual. Verdicting must be both accurate and fast to deliver true business and make a Zero Trust environment a reality.

Comodo Cybersecurity deals with "unknown files" by automatically isolating them in a sophisticated secure container until the final verdict is provided. Those unknown files are kept in a secure container until Valkyrie, Comodo Cybersecurity's advanced cloud file analysis platform, analyze the file to determine if it is malicious code. Comodo has built its Automated Containerization Technology on its Zero Trust environment. The container is a combination of a virtualization of COM interfaces, disk, registry, and memory.

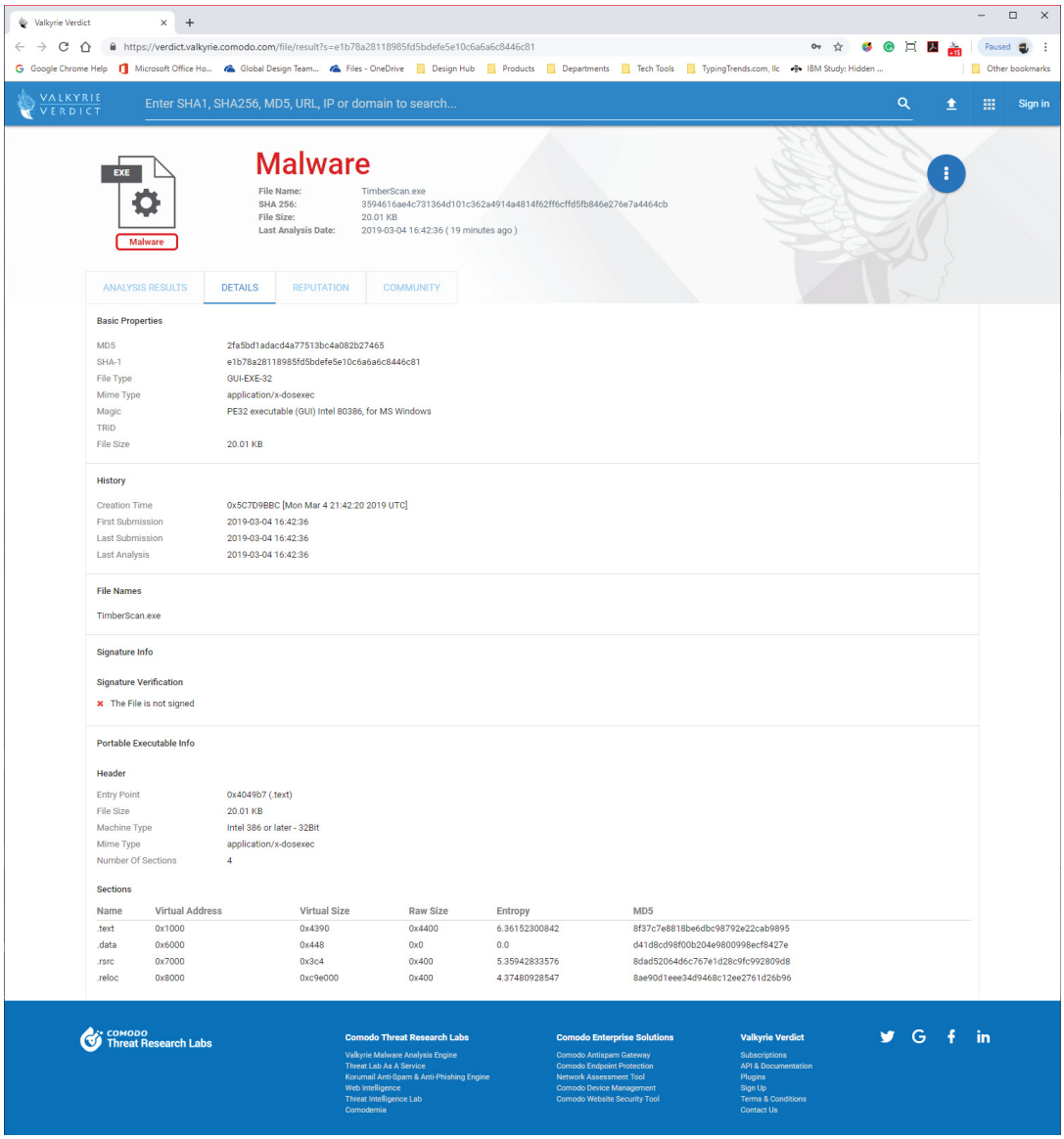
The unknown file enacts its malicious activity and makes changes to the system; however, it is making changes only to the virtual system while the real system remains unaffected.

Comodo Cybersecurity's EPP product, which is called Advanced Endpoint Protection (AEP), submits the unknowns to Valkyrie in order to observe the activity and behavior of the unknown file, and then obtains a verdict to determine if the unknown file is good or malicious. Comodo Valkyrie uses many techniques used to obtain an accelerated verdict. Static and dynamic analysis and expert human analysis is used to obtain the verdict, with results offered within 4 hours, if not instantly.

Verdicting systems used by other EPP vendors usually require that the file be submitted manually, and a verdict may take days or weeks to be determined. Fast verdicting ensures that whitelists are updated quickly and that only files with a "known safe state" can run unfettered in the system. Comodo AEP leverages Comodo Valkyrie, which is a verdict-driven platform that provides static, dynamic and as needed, expert human analysis for submitted files of unknown and zero-day files. The Valkyrie verdict system analyzes over 200 million file queries per day and more than 300 million unknown files each year through tightly integrated Comodo solutions and Comodo's active global community of threat researchers.

Comodo Cybersecurity's combination of fast verdicting via Valkyrie and instantaneous file behaviour analysis via VirusScope, ensures that a default deny posture is possible across any network, while at the same time, not hampering productivity and protecting endpoints from zero-day threats.

Source: Comodo



Beyond the Sandbox, Preventing Damage from Undetected Malware that Enters your Network

A sandbox is an isolated virtualized environment that mimics an endpoint operating environment to safely execute unknown files, without risking harm to the host device or network. Many cybersecurity vendors have integrated sandbox technology into their EPP products to combat malicious software and have met with some success in the ever-evolving battle against cybercriminals.

However, sandboxes are beginning to lose their effectiveness against the latest threats. Malware is constantly evolving, and cybercriminals are now creating malware that can detect when a sandbox is being used and automatically take steps to avoid detection. Cybercriminals are using numerous techniques to evade sandbox technology. For example:

- Sandbox Detection and Evasion: Malware is being designed to detect whether the file is in a sandbox or in the target host environment before it executes. If the malware detects a sandbox environment, it quickly terminates without doing anything malicious, or executes phony benign operations, causing the sandbox to judge the file harmless, allowing it to run on the target system.

- Delayed Malware Execution: Cybercriminals are designing malware to delay execution of malicious behavior; or trigger execution only after an event such as a system reboot. That can prevent a sandbox from detecting malicious activity, allowing the malicious code to slip by and execute later.

As threats evolve, sandboxes will become less effective and malware will slip past the security controls offered by sandboxes. What's more, sandboxes are becoming more resource intensive and more complex, slowing down their ability to process threats without hindering productivity.

Comodo Cybersecurity uses a different approach that eliminates the need for a locally executed sandbox. Comodo Advanced Endpoint Protection incorporates intelligence Auto-Containment technology to prevent damage from undetected malware that enters your network. Comodo Cybersecurity's patented solution "contains" unknown files in run time, automatically. The containment system is intelligent enough to weed out good and bad and contain only the unknown, creating a very efficient "Containment" technology.

AEP classifies an executable file into three states, good, bad and unknown. Only unknown files are executed within a container, offering zero friction for the end user. That means the user who is executing the application continues to use the program with no indication that this application is running in a container. With containment, all untrusted processes and applications are automatically contained in a secure environment, allowing potentially safe applications the freedom to run with the real environment experience. If the unknown turns out to be malicious code and attempts to exploit the machine, that action will occur entirely within the container, and affect only the shadow resources provided and NOT the native machine.

Source: Comodo

Implementing a "Zero Trust" Environment without Hampering Productivity

Today, most EPP vendors are using a Default Allow approach, meaning that only applications or executables deemed malicious are blocked from executing on an endpoint. Cybercriminals are using that Default Allow approach to their benefit; creating new attacks that are only slightly different from the previously detected malware variants. Once easily identified malicious files are appearing as unknown files never encountered before.

What's more, those same attackers are further modifying those "brand new" unknown variants to bypass sandboxes and other detection methods allowing malicious payloads to slip by undetected and ready to strike. Simply put, signature files, black lists, sandboxes, firewalls, and other antimalware technologies are ill equipped to deal with unknown files in a Default Allow environment.

The obvious answer here is to switch to a Zero Trust posture, where only known good files can be executed and all other files are deemed suspicious and are prevented from being executed. Until recently, a Default Deny posture proved impractical to implement and created numerous productivity problems for end users, as well as increasing the workload of IT departments charged with determining if a new, unknown file was a legitimate application. Those application technologies mean that "unknown" applications could multiply exponentially across networks as new variants and changes were slipstreamed in.

Comodo Cybersecurity offers the solution in the form of the company's Intelligent Automatic Containment™ technology. Used within Comodo AEP, auto-containment's turnkey technology enables three emerging endpoint protection techniques. Identified by Gartner analysts to come together into a new combination that re-defines the category and offers full support for a Zero Trust environment.

One important advantage offered by the Comodo approach is that containers require fewer computing resources than traditional virtualization. so Instead, malware containment can be efficiently implemented at the endpoint without negatively impacting user experience, productivity, CPU resources or IT budget.

Comodo Auto Containment™ technology also makes it possible to safely jail unknown executables at the process level instead of at the entire application level. For example, the endpoint can run a trusted Web browser outside of containment, but if suddenly an unknown plugin tries to launch a file or command via interpreter, 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 can run normally.

Taken together, these advanced techniques make it possible to evolve from today's Default Allow posture that leaves endpoints vulnerable, to a Zero Trust environment that isolates unknown threats in containment. With Comodo's Zero Trust environment 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.

Comodo AEP offers highly efficient virtualization at two layers, the OS and the CPU. However, AEP focuses on the OS as the constant, since virtualization is not always supported by the CPU. That dual layer approach provides 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.

Comodo Auto Containment™ provides full endpoint protection by creating a secure container (sandbox) where all unknown files or applications can be used and analyzed. The containment environment is highly integrated into host systems where whole host environment is visible to sandboxed application, in contrast to OS virtualization where the virtualized machine sees only its own environment. One important aspect of this feature is to gain good compatibility and seamless user experience. Moreover, with this feature, virtualization of any kind of application including

most popular applications including browsers, email clients, office, games and various other applications is possible with Comodo Containment technology. What's more, Comodo's containment technology makes startup performance very fast, in stark contrast to almost all CPU-draining, system-slowing VM systems in use by other vendors.

Comodo Auto Containment™ technology is extremely lightweight, has no CPU dependencies and is completely application agnostic. Malware or any other unknown process entering Comodo's virtualization environment cannot modify the hard disk, registry, or COM interface, preventing malware infections.

AEP focuses on the OS as the constant, since virtualization is not always supported by the CPU. That dual layer approach provides 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.

Comodo Auto Containment™ provides full endpoint protection by creating a secure container (sandbox) where all unknown files or applications can be used and analyzed. The containment environment is highly integrated into host systems where whole host environment is visible to sandboxed application, in contrast to OS virtualization where the virtualized machine sees only its own environment. One important aspect of this feature is to gain good compatibility and seamless user experience. Moreover, with this feature, virtualization of any kind of application including most popular applications including browsers, email clients, office, games and various other applications is possible with Comodo Containment technology. What's more, Comodo's containment technology makes startup performance very fast, in stark contrast to almost all CPU-draining, system-slowing VM systems in use by other vendors.

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

Source: Comodo

Best Practices for Evaluating Endpoint Protection

Protecting endpoints from malicious software, intrusions and cyber-attacks is one of the most crucial aspects of securing an organization's IT resources. Endpoint protection should be part of a holistic IT security approach where network perimeter security solutions secure the boundaries between internal networks and service provider's network, and endpoint protection further reduces the risk of malware or malicious activity impacting IT operations. In other words, EPP solutions should work as another layer of security, backed by other technologies that operate at the network edge or in the cloud.

The first step in picking an EPP solution is evaluating the needs of the business, which should include:

- **Capacity and Scalability:** IT managers should determine the number of endpoints to be protected, the number of users that must be managed, the dispersion of those endpoints, and the potential for growth. The product selected should readily support numerous endpoints, OSes, and be able to address rapid growth, all from a centrally managed console.
- **Compliance:** Many businesses are bound by regulatory requirements, it is critical to determine if there are any compliance regulations that impact IT operations, privacy, and data stewardship. Examples include PCI-DSS, HiPPA, and GDPR. The product selected should support regulations and surpass the minimum regulatory requirements.
- **Budget:** Many organizations have limited budgets and it is critical that the necessary funds are secured to deploy the best solution for each business. EPP can offer a very quick return on investment when deployed properly and managed effectively.
- **Policies:** Organizations seeking to deploy EPP solutions should carefully evaluate the cybersecurity policies in place and make sure that the selected product can support those policies. Examples include whether or not employees can work remotely, if employees can use their own devices to access organizational resources, if employees can install their own software, and so forth.

Once the needs of the business are defined, the next step is to look at the capabilities of the products under consideration An EPP solution should include:

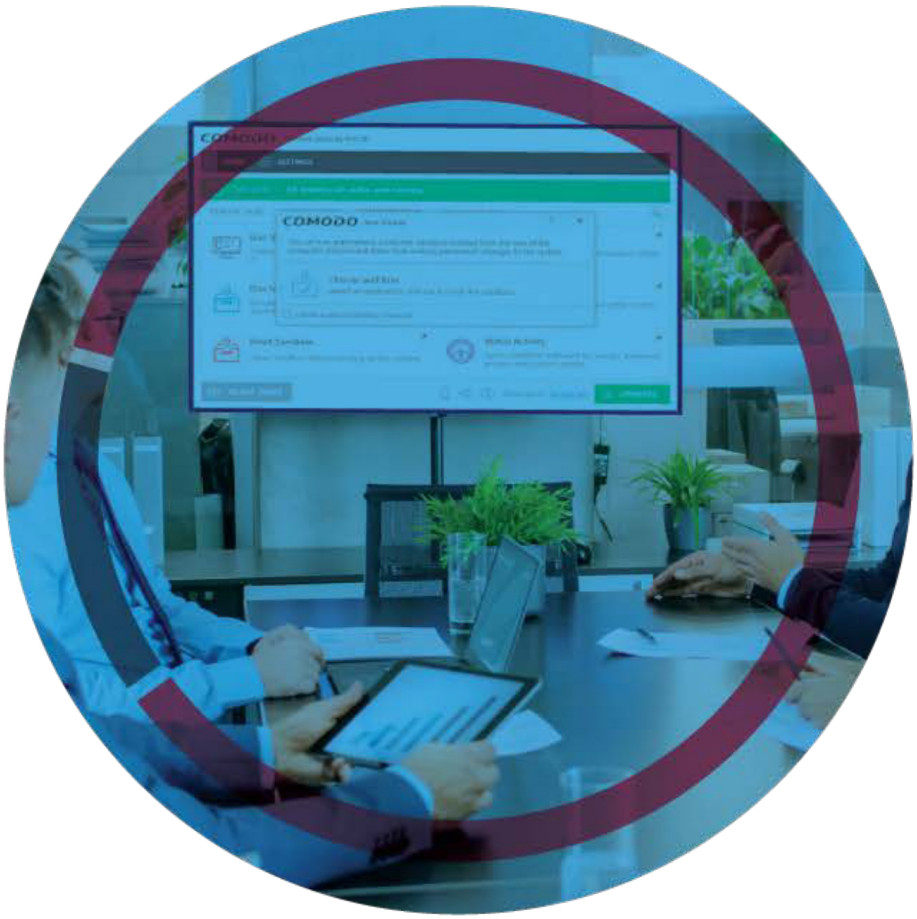
- **Centralized management:** All functionality should report into a centralized management system that unifies the deployment, management, and operation of the EPP system. The management console should support customized views/dashboards/reports, and role-based access control.
- **Malware detection & blocking:** Layered endpoint security technologies (AV signatures, heuristics, IoC comparisons, etc.) and machine learning algorithms that can detects and blocks malicious code, zero-day/unknown files and fileless malware.
- **Remediation capabilities:** Administrators should be able to perform the operations needed to quarantine systems, delete registry keys, or terminate malicious processes. There should also be automated and guided remediation options that lesson the administrative load.
- **Anti-exploit technologies:** Capability to block in-memory and common application- layer attacks, such as ransomware and crypto-mining exploits.
- **EDR Option:** Administrators should be able to add Endpoint Detection and Response capabilities, which incorporate the tools to detect, investigate, contain, and remediate security incidents
- **Unknown File Handling:** The EPP solution should be able to evaluate new, previously unseen files, to determine if those files are potentially malicious, and then remediate or block those files and prevent zero-day threats.
- **Application Control:** The EPP solution should offer control over applications using technologies such as verdicting, whitelisting, and blacklisting functions. Application control tools protect endpoints by restricting or preventing unauthorized and compromised

applications from executing in a way that puts the network or company data at risk.

- **Browser Security and Isolation:** Web browsers are among the most prevalent attack vectors for drive-by downloads, zero-day attacks, ransomware, crypto jacking malware, and other malicious browser-executable code. The EPP solution should be able to protect endpoints from malicious code delivered by a browser session, prevent malicious plugin operation, and isolate suspicious code execution.
- **File reputation scoring and verdicting:** All accessed files should have a reputation score and unknown files should go through analysis to determine if they are malicious.
- **A single endpoint agent:** The EPP solution should be easy to deploy and only require a single agent for the endpoints being provisioned.
- **Support for a Zero Trust environment:** The EPP solution should support the ability to block unknown or previously unseen files, denying execution of those files until they are validated as not malicious.
- **Host Intrusion Prevention System:** The EPP solution should include the ability to detect and block attempts to breach an endpoint via network traffic. HIPS scans network traffic for suspicious patterns in the data and can block the data stream or notify an administrator.

While the above list includes the major features that any leading EPP solution should have, there are other less tangible capabilities, such as vendor support, renewal discounts, the ability to add additional features, and integration with other products that should also be part of the selection criteria.

Source: Comodo



Research from Gartner:

Select the Right Endpoint Protection Platform by Running an Effective Proof of Concept

Although a request for proposal process can result in a strong shortlist of candidate products, security and risk management leaders must run a thorough proof of concept to accurately determine which endpoint protection platform product is most suitable.

Key Challenges

- There is no "one size fits all" security strategy or product.
- Security and risk management leaders that are removed from day-to-day operations regularly give too much weight to vendors' marketing claims and industry hype when assessing new controls and capabilities to improve their security posture.
- Selecting any security product based purely on feature checklists can be very ineffective. Vendors and products have similar-sounding capabilities with varying levels of accuracy, effectiveness and usefulness.
- Overuse of marketing buzzwords like "next generation" and "machine learning" regularly distracts from key decisions that have to be made when selecting a new endpoint protection platform (EPP) product.
- Without testing the management interface and user experience, and without understanding how a new product will change established workflows, it is almost impossible to predict the additional staffing requirements that advanced capabilities require for detection, investigation and response.

Recommendations

Security and risk management leaders responsible for endpoint and mobile security should:

- Use a proof of concept (POC) to determine how a new EPP product will improved their organization's security posture.
- Ensure the POC covers a set of users and devices that is representative of the overall organization, not just the IT or security department.
- For a replacement product, ensure its protection and security capabilities offer more than just a feature-by-feature match for the existing product. If augmenting existing capabilities, verify that there is a benefit to introducing the complexity of multiple vendors and products. In other words, think strategically, not tactically.

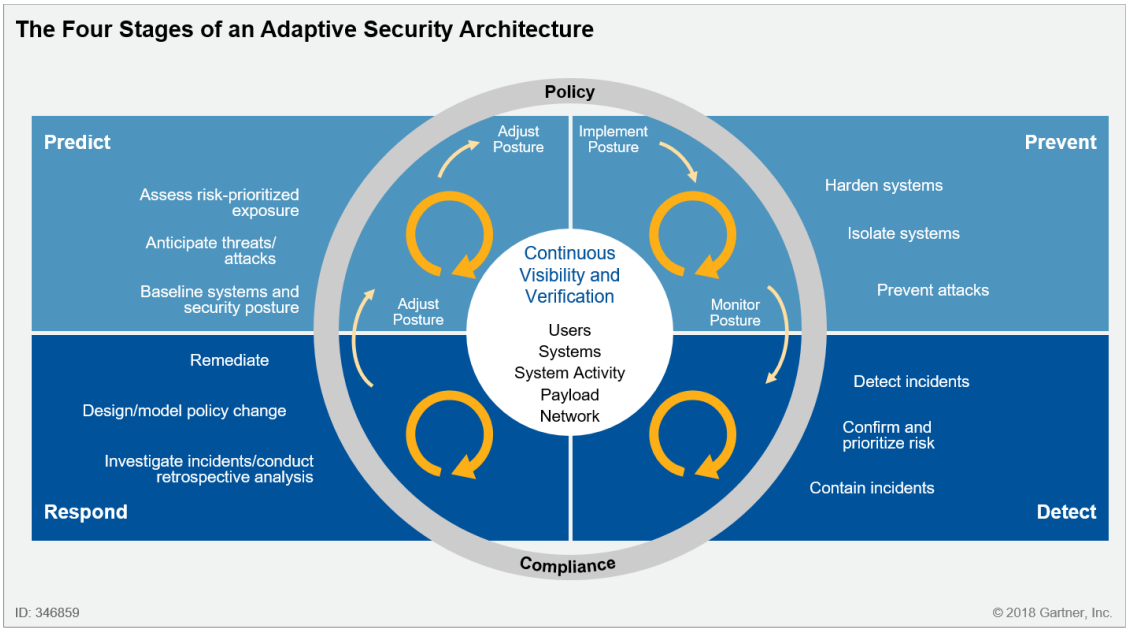
Introduction

Choosing an EPP can be a complex decision, due to the broad functionality within EPP products and the pace of innovation, which is fueled by new vendors in the endpoint security market. Every organization will find itself considering a new EPP product, even if it is just to check the relevancy of the incumbent vendor at the time of renewal. A thorough investigation of the market should be undertaken well in advance of the renewal time (ideally 12 months before). It should include discussions with Gartner analysts, vendor RFPs, and testing or implementing a POC to fully assess the benefits of the incumbent versus a replacement vendor.

Organizations should use Gartner's Adaptive Security Architecture model to assess their capabilities in four quadrants. Note that this is not limited to an EPP, and this assessment is far more valuable when it covers the entire scope of security controls, rather than just an isolated set of security products. There are many security practices outside the EPP market — for example, privileged account management, network isolation and vulnerability management — that can have a direct impact on the controls required from an EPP.

Focusing initially on strong prevention — the ability to harden systems, use network controls to isolate business-critical assets from the general endpoint populace, and block the most common and commodity attacks — this framework can serve to identify areas for improvement (see Figure 1).

Figure 1. Assess the Current State and Identify Areas for Improvement



Source: Gartner (June 2018)

As organizations move from purely preventative controls to a modern incident investigation model that includes detection and response, organizations must be able to track the effectiveness and impact of security investments. There are four metrics that can be monitored, and organizations should strive to improve them with every process/workflow change, new talent hire, and deployment of new security products and controls:

- **Average time to detection** — The time it takes for an incident to be noticed and documented, the first step in an investigation process. This may be taken automatically with security controls (for example, detecting suspicious connections to a command and control server) or manually by a user calling the help desk to report a slow-running device.

- **Average time to containment** — The amount of time it takes, after an incident has been detected, to fully contain an incident and prevent it from spreading to other users, devices or locations. This may include, but is not limited to, isolating specific endpoint or server devices that are exhibiting suspicious behavior, resetting user passwords, enforcing stricter access controls (such as multifactor authentication for every log-in), and, in extreme circumstances, temporarily severing network connections. Containment is not the same as remediation or resolution.

- **Average time to remediation** — The amount of time it takes, after an incident has been detected, to remediate impacted devices and restore service. This may include, but is not limited to, reimaging a device, rolling back changes made by malicious or suspicious processes, or simply removing containment controls in the event of a false positive. Remediation is not the same as resolution.

- **Average time to resolution** — The amount of time it takes, after an incident has been detected, to fully resolve the root cause of an incident. This can include, but is not limited to, deploying software updates and reconfiguring access controls and policies.

When considering a new product or vendor, it is imperative to remain agnostic about the marketing hype around products and capabilities, and focus on assessing the capabilities that provide solid and meaningful improvements to an organization's security posture. The POC process can help to establish how a new product will impact these metrics.

Analysis

Use a POC to Determine the Real Benefit of Switching to Another EPP

Gartner clients often inquire about switching EPP products following large industry conferences, or due to concerns about high-profile 2017 outbreaks such as WannaCry and NotPetya. In many cases, security and risk management leaders driving the appetite for change (and occasionally the IT and security teams) are unaware of the capabilities of their incumbent solution and are letting the marketing lead their thought process.

The rip-and-replace approach to switching to a new EPP can take many months to complete, even in small organizations. Poor decision making in the purchasing cycle can result in wasted deployment time and effort, and organizations can find themselves stuck in two contracts with two vendors, increasing the overall cost. Some organizations find themselves replacing the incumbent product with a product that doesn't meet their needs or abilities, so they must start the process of product selection all over again.

A well-run POC phase will help ensure that a new EPP actually provides the required enhancements to the protection, detection and response capabilities assessed against the Adaptive Security Architecture model.

Request for proposal (RFPs) are an important part of the process of creating an initial shortlist of vendors and products that fit basic feature-by-feature requirements, but organizations often rely too heavily on vendor marketing and vendor-led demonstrations. Vendor demonstrations showcase products in the best light, often with vendor-provided malware samples or attack tools, and regularly include the full suite of capabilities that a vendor can offer. Many organizations overvalue product demonstrations when making their selection, and neglect to understand how the product will function within the complications of their own environment.

The shortlist of vendors invited to the POC is generated by the response to the RFP, so ideally the requirements listed within the RFP should reflect the desired capabilities of the new EPP. RFPs are often line after line of specific features or functions. Organizations should use the POC to validate that the products deliver those features. They should also use it to check that those features are actually important in the real-world, day-to-day operations of their business, and that they will bring meaningful change and improvement to the existing controls.

Before beginning any part of a product selection process, organizations would be wise to ensure that the incumbent solution is correctly configured and functioning in the best possible way. Almost all vendors are happy to perform a "health check" of a product deployment, so they can make recommendations and ensure the product is deployed correctly. Performing this level-setting should be a regular task — annual at least — to make sure the full benefit of the product is being realized. It is critical that this takes place before embarking on a POC as it enables the organization to truly assess whether a new product provides improved tools and capabilities.

Organizations should treat the POC with the same priority and workflow that any existing solution is given, and it is important to run the POC phase in the production environment. This helps the operational teams who will work with the product assesses the functionality, workflow and ease of operation. The response time and support experience delivered by vendor technical support can also be properly evaluated, and these can help decide which service levels the organization requires.

Ensure the POC Is Representative of the Organization

Almost all organizations are wary of making changes that impact their ability to continue doing business. Using the IT team for an initial short-term test is encouraged, as it gives an organization insight into any potential changes that will affect a wider pilot group. However, the scope of a full and proper POC must be expanded and the following aspects must be considered and evaluated:

1. **The mix of people and devices:** In order to achieve as much coverage as possible in the POC, the test group must include users and devices representative of every department. Identify the hardware configurations of endpoints deployed across the enterprise and ensure that they are included in the scope. Including one or two users from every department or business unit ensures that business can continue in the event of a software (or hardware) problem linked to the POC. It also provides greater confidence in the overall deployment. Time should be taken to

identify important business milestones that occur infrequently. For example, some tasks or applications may only be used once a month.

2 **The appropriate duration:** As a rule of thumb, a strong POC will run for at least one month across a representative number of endpoints and users (as described above). The ideal duration of a POC can depend on:

1. The time to deploy to the representative group — organizations with a distributed installed base may need longer to fully deploy.
2. Business processes — functional groups may have irregular tasks that do not occur on a monthly basis. Organizations should strive to include users and endpoints that have infrequent activities, and, where possible, extend the duration to include those events.

Many Gartner clients report increased levels of detection and increased workload on the operational teams, often due to improved detection technology and false positives generated by "normal" activity. The duration of a POC is often extended as these issues are discovered and managed. Organizations should ensure that the vendor has provided a license key to keep the product active for long enough.

3 **Measuring success or failure:** Identify what will be measured during the POC. A POC is incomplete without a consistent metrics and list of parameters to evaluate the EPP. Having a common, consistent set of parameters for all POC participants ensures a like-for-like comparison is made.

Gartner recommends that the following metrics are used when evaluating an EPP:

1. Time to detection
2. Time to containment
3. Time to remediation
4. Time to resolution

Testing for accuracy and efficacy at the prevention stage is hard to do. Vendors may offer the use of test samples to use with their product (which, of course, will detect all of them) and with other products competing in the POC (hoping that they won't detect them as malicious). There are few organizations that can effectively measure malware detection themselves; most organizations rely on third-party testing from NSS Labs, AV-Comparatives or AV-TEST. Gartner advises against using test results and any vendor's claims in isolation. The most effective and accurate product for an organization is one that can be deployed and utilized fully and one which provides meaningful improvement over existing metrics (see above). For more information, see "Understand the Relative Importance of AV Testing in EPP Product Selection."

4 **Assess integration capabilities:** An EPP no longer works in isolation and will often benefit from integration with other security tools, threat intelligence feeds and operational tools (see "How to Decide Whether Endpoint and Network Security Integration Is a Feature or a Fad"). This is another area that will have been enriched by a thorough and inclusive assessment of existing security controls (see Figure 1). Understanding where integration capabilities can improve operations and threat response capabilities will help identify process and workflow enhancements, and can surface requirements or outcomes that were not part of the initial RFP scope but provide a large improvement. Particular notice should be given to integration with security orchestration, automation and response (SOAR) or (security information and event management [SIEM]) tools that may already exist or be under consideration.

5 **Assess user experience, workflow and ease of use:** Running the POC in production will provide valuable insight into the user experience for the operational team involved with the day-to-day use. Some vendors have different consoles (or even products) that provide capabilities found in a single product or UI from other vendors. The ease of use and the workflow-driven user experience will play a major role in the perception of value and improvement.

6 **Assess vendor support:** Consideration should be given to the service levels that vendors offer, including technical support, managed services, and the overall operational SLAs of any cloud-driven capabilities.

7 **Assess deployment efforts:** This topic addresses the deployment of the EPP in the organization's architecture, and the integration with existing security controls and operational tools.

When conducting a POC, it is recommended to keep it as close as possible to the real environment. The defenders (the "blue team") can then understand whether they are getting the tools and information that they rely on prevent, detect or respond to an attack.

The Outcome: Four Important Questions Answered by a POC

What Effort Will the Deployment Involve?

Deploying a new EPP usually requires multiple steps — updating the endpoint itself to a supported patch or OS level, removing the existing EPP agent, and deploying the new agent. Although many EPP products can automate these tasks as part of the new agent installation, they often require a reboot of the device. Additionally, user interaction can reduce the likelihood of success. In a worst-case scenario, the endpoint may be left without any EPP agent at all.

The POC should capture the success and failure rate of any automated steps, as well as the required remediation steps — for example, could it be resolved remotely, or did it require the intervention of a local resource? These data points will help assess and predict the amount of effort required to roll out to the entire organization. For example, should remote employees be required to attend a specific site, rather than upgrade remotely? Are there particular hardware configurations or user privileges that have a high likelihood of failure?

This deployment scoping will also help determine the likelihood of completing the migration before the incumbent product contract expires, or whether an extension to the existing vendor contract will be required.

Is the Product Fit for Purpose?

Most organizations are concerned about malware protection efficacy and accuracy. Of course, malware prevention is an important capability of an EPP, but it is one that is tough to test and is not the only important consideration. Organizations should also be concerned with how the product handles false positives, and how feedback on false positives is fed back to the system to improve the effectiveness. Most importantly, organizations must be convinced that the replacement product can be used successfully in their environment, and that it will improve their security posture. Consider the not-uncommon scenario of an organization discovering six months into an expensive deployment, that staff levels are too low or not skilled enough to use the product effectively.

What Existing Processes Need to Be Changed and What Additional Processes Need to Be Implemented?

Every organization will have its own way of managing applications, reporting security metrics, and investigating and responding to incidents. Changing EPP vendors will certainly have an impact on the existing processes and workflow, and the changes should be captured during the POC. Include new types of data that are made available, how alerts will be triaged and investigated, how case management features fit current escalation steps, and how endpoint incidents can be quickly contained in the event of an outbreak or attack.

Configuration management reporting may need to be updated to include reporting on protected and unprotected devices, failed installations or out-of-date agents.

Is There a Real Benefit to Moving to a New Product?

As organizations notice capabilities or process changes that conflict with their current implementation, they should not ignore these changes purely because "It's how it's always worked." Many organizations have policies and processes that are decades old, written for a time when threats were different and mitigations did not exist. As part of the POC process, discuss changes and concerns with Gartner analysts and with vendors (including your existing one), and ask for their best-practice recommendations.

On many occasions, Gartner clients discover that the benefits of switching to a new EPP vendor are not as big as marketing would have them believe. They realize that investing in other areas of basic IT hygiene will give them a stronger security posture in the long term.

Source: Gartner Research Note G00346859, Prateek Bhajanka, Ian McShane, 27 June 2018

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity provides active breach protection with its cloud-delivered Cybersecurity platform. The Comodo Cybersecurity platform provides a zero trust security environment that verdicts 100% of unknown files. The platform renders an almost immediate verdict on the status of any unknown file, so it can be handled accordingly by either software or human analysts. This shift from reactive to proactive is what makes Comodo Cybersecurity unique and gives us the capacity to protect your business – from network to web to cloud – with confidence and efficacy.

Comodo has experts and analysts in 185 countries, protecting 100 million endpoints and serving 200,000 customers globally. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers worldwide.

COMODO CYBERSECURITY

200K secured customers

Delivering reliable, centralized, and fully scalable security solutions for today's business.

85 million endpoints installed

With tens of billions of OS-VMs created in over 85 million endpoint installations, not a single infection!

193 countries worldwide

Over 850 cybersecurity scientists and engineers analyzing 100,000 threats per day and reaching definitive verdicts around the world.

For demo, pricing and other customer requests:
sales@comodo.com

US and Canada
+1-888-551-1531
+1-877-712-1309

For ISV and referral partners:
channeloperations@comodo.com

Headquarters
+1-973-859-4000

For help and support inquiries:
c1-support@comodo.com

Fax Line
+1-973-777-4394