Welcome

The Cloud Generation and its need to access data everywhere, on every device, creates more opportunities for attackers to compromise endpoints and infiltrate networks. Organizations are more vulnerable than ever to cyber damage and disruption. Ransomware attacks grow ever-more ominous, as witnessed by WannaCry and Petya. Also, attackers’ expanding use of fileless and stealthy attacks, combined with ‘living off the land’ (exploiting common IT tools for attacks) threatens the confidentiality, integrity, and availability of endpoints.

Security teams must pursue solutions that keep them one step ahead to outpace attackers’ innovation and relentlessness. As endpoints are your critical line of defense, let’s explore Gartner’s new definition of Endpoint Protection Platforms (EPP) so you can make the best-informed choice to secure your company.

Symantec positioned highest in execution and furthest in vision in the leader’s quadrant in the 2018 Endpoint Protection Platforms Magic Quadrant. Read the report.
Redefining Endpoint Protection for 2017 and 2018

Security and risk management leaders should ensure that their endpoint protection vendor is evolving to defend against the rapidly changing threat landscape and the need for more efficient incident and alert response capabilities.

**Key Challenges**

- Malware and attack tools, tactics, and techniques are evolving faster than the protection capabilities delivered by traditional endpoint protection platforms (EPPs).
- Traditional EPPs are focused on preventing the initial infection, but miss the rest of the adaptive security architecture tasks, such as hardening, incident detection and incident response.
- A new generation of endpoint protection vendors and endpoint detection and response (EDR) solutions have entered the market, making product selection difficult for security and risk planners.
- New techniques and tools to detect and prevent incidents require more sophisticated operators than the historical set-and-forget antivirus solutions.

**Recommendations**

Security and risk management leaders responsible for endpoint security:

- Establish a solid security baseline by upgrading to the latest version of the incumbent solution. Later releases include advanced protection modules, and may also include aspects of detection and response.
- Use Gartner’s Adaptive Security Architecture framework to assess your ability to detect, investigate and respond to security incidents. Compare your incumbent EPP vendor capabilities with those of visionary EPP or EDR vendors to determine if and when to switch vendors.
- Prioritize managed services or managed features within EPP as a tactical investment to improve detection and response time, but this will not remove the long-term need for skilled employees. All organizations should plan to invest in training to augment experience or knowledge gaps.

- Simplify the scope of EPP by using OS-embedded security features, such as disk encryption and USB device control, especially when migrating to Windows 10, and by focusing only on Windows and Mac OS devices. Servers and mobile devices are served by their own market.

**Introduction**

Gartner is updating the definition of an EPP:

> A solution deployed on endpoint devices to prevent file-based malware attacks, detect malicious activity, and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts.

This simplification is necessary because the feature set and definition of an endpoint protection platform (EPP) have evolved considerably in the past decade, but to the extent that it includes features and functionality that are of less importance to buyers looking for improved malware prevention.

Many times, the EPP market consumed features and functionality from adjacent markets, as enterprises drove toward a suite solution for all endpoint-based security controls, including data protection, server protection and mobile device management (MDM). With the growth of highly effective ransomware and advanced fileless attacks, security and risk management leaders are now refocusing on building resilience against these attacks, and improving prevention and their ability to rapidly detect, investigate and recover from incidents. Concurrently, buyers have deprecated the value of nonmalware detection areas such as the data protection features delivered within a traditional EPP platform, as well as the mature commoditized features like personal firewalls and basic signature antivirus.
The reduced demand for EPP to have built-in ancillary capabilities like disk encryption and USB device controls means the primary driver for endpoint protection investment once again becomes protecting the enterprise from malicious adversaries.

In the 2017 “Magic Quadrant for Endpoint Protection Platforms,” Gartner stated that the critical capabilities of an EPP had narrowed considerably, with the key elements being malware detection effectiveness, performance impact on host machines and administration overhead. Other capabilities often found within EPP suites or solutions — for example, disk and file encryption, data loss prevention, and device control — are increasingly being provided by the operating system itself.

In 2013, a related market, endpoint threat detection and response, was born by the realization that it is impossible to prevent 100% of attacks. This led to the development of capabilities that documented a greater set of technical operations occurring on an endpoint. This detailed information could then be analyzed for suspicious and malicious activity that had not been prevented or blocked by the EPP. Security operations teams now had a capability to investigate these and other security alerts with more visibility into historical events, and to recover from issues in a more intelligent and prescriptive way than simply reimaging. This drove early adoption of EDR solutions among highly sophisticated security operations centers (SOCs). Over the last two years, the requirements for EDR use cases have become increasingly mainstream. As a result, the core functions of EDR solutions have been increasingly adopted by EPP vendors. Similarly, many of the EDR vendors have incorporated prevention techniques typically associated with EPP solutions, hoping to displace incumbent EPP vendors with their solutions.

Although the majority of the EPP market remains focused on the Windows platform, Mac OS continues to grow in popularity — especially among C-level executives — leading to an increasing demand for cross-platform EPP parity. This is particularly key in the area of visibility and response, where incidents involving credential misuse can span operating systems. Although the traditional EPP suite usually included protection capabilities for servers and various flavors of the Linux operating system, these platforms — along with mobile platforms like iOS and Android, and VDI implementations — are not considered part of the current core EPP market. A locked-down, application whitelisting approach is recommended for servers, as discussed in “Market Guide for Cloud Workload Protection Platforms” and “The Feasibility of Host-Based Controls and the Evolution of Server Security,” and mobile threat defense has its own Market Guide.

The result is a modernization of the EPP that aligns more closely with Gartner’s Adaptive Security Architecture (see Figure 1), albeit with varying levels of maturity and coverage.

---

**FIGURE 1  Adaptive Security Architecture**

Predict

- Risk Assessment
- Anticipate Threats
- Baseline Security Posture

Respond

- Remediate
- Design Policy Change
- Investigate Incidents

Prevent

- Harden Systems
- Isolate Systems
- Prevent Attacks

Detect

- Detect Incidents
- Confirm and Prioritize Risk
- Contain Incidents

Continuous Visibility and Verification

- Users
- Systems
- System Activity
- Payload
- Network

Source: Gartner (September 2017)
Analysis

Acknowledge the Convergence of EPP and EDR

The market for EDR solutions, which has driven a number of innovations into the endpoint security space, covers four primary capabilities:

- Detecting security incidents, rather than just file-based malware
- Containing security incidents
- Investigating security incidents, and threat hunting
- Providing response capabilities to recover from a security incident

These areas are well-defined in Gartner’s Adaptive Security Architecture.

Originally, EDR solutions addressed the requirements of only the large enterprises that possessed a dedicated SOC, along with security staff that were experienced and knowledgeable in the threat hunting and malware analysis realm. However, interest in these capabilities has grown significantly over the past few years and has become more broadly adopted and desired by the mainstream EPP market. Adoption is driven by the growing acceptance that 100% protection is not practical or possible, and that organizations of all sizes need the ability to detect, investigate and respond to incidents. The resulting trend is for EPP solutions to incorporate some of the functionality from EDR solutions, and for EDR solutions to incorporate some of the prevention capabilities from EPP solutions as buyers want to purchase these capabilities in one, integrated package.

All but the most niche of EPP solutions now provide the ability to search across the endpoints for static indicators of compromise (IOC; for example, a file hash, registry keys, and access to IP or URLs), and many vendors provide a detailed analysis behind the root cause of an incident (for example, the chain of events that led to a process being launched).

As these basic EDR use cases are addressed by the mainstream EPP market, the distinguishing features of advanced EDR will be the capability to log all activity from all endpoints to a centralized location, where it can be data mined, analyzed and correlated with other sources of threat intelligence (for example, user entity and behavior analytics [UEBA]) by dedicated security analysts and threat hunting teams. This big data back end will be overlaid with deeply customizable visualization and reporting, orchestration for incident response that can be configured to mirror the roles and escalation steps in large SOC environments, and context-rich APIs to integrate with third-party platforms.

Before investing in a stand-alone EDR in addition to a separate EPP, all but the most security-mature organizations should review their incumbent EPP vendor’s current and roadmap plans for the integration of EDR functionality into the platform to assess applicability.
Detection capabilities will vary, but advanced solutions will use multiple detection techniques, ranging from static IOCs to behavioral analysis. The inclusion of artificial intelligence (AI) and human-driven managed services such as managed threat hunting — lowering the barrier to entry for more advanced capabilities — will increase over the next 18 months. Deception capabilities, intended to trick adversaries into revealing their presence by accessing fake services or planted files, or by using planted credentials, are emerging.

Desirable EPP solutions are primarily cloud-managed, allowing the continuous monitoring and collection of activity data, along with the ability to take remote remediation actions, whether the endpoint is on the corporate network or outside of the office. In addition, these solutions are cloud-data-assisted, meaning the endpoint agent does not have to maintain a local database of all known IOCs, but can check a cloud resource to find the latest verdicts on objects that it is unable to classify. Integration with security orchestration, automation and response (SOAR) tools will become highly desirable for organizations that are planning to invest in, or already are investing in, providers like ServiceNow, Phantom and IBM Resilient.

With agents running on every endpoint, EPP solutions will also begin to bridge the gap between operational IT and security. Initially, this will be by providing risk-based, prioritized security state assessments, illuminating any known vulnerabilities or misconfigurations. These features will allow enterprises not only to improve their security posture and practices, but also to audit and measure the impact of security investments and process changes.

There is no “one size fits all” approach for endpoint protection, and enterprises will each have their own unique requirements, threat models, workflows and staffing. Organizations should pay particular attention to solutions that include managed services (or perhaps more accurately described as “managed features”) like threat hunting or file classification — those that reduce the administrative workload by automation and orchestration, and those that focus on lowering the knowledge and skills barrier through built-in contextualized threat hunting assistants, guided response tools and easy-to-understand-and-use user interfaces.

Overall, organizations should consider the importance of the various capabilities to their specific requirements, rather than the marketed capabilities hype, when evaluating the detection and response elements of EPP solutions.

Integrate Endpoint Protection Buying Decisions With Your Windows 10 Migration Strategy
Windows 10 Enterprise provides an attractive catalyst for change for many organizations, allowing for a clean-slate approach to endpoint security planning. Where many organizations’ security workflows revolve around the functionality afforded by their incumbent EPP vendor, enterprises are evaluating and considering the applicability of the security features available as an integrated part of the operating system itself. For example, a large number of organizations have moved, or are in the process of moving, to Microsoft BitLocker and Apple’s FileVault for disk encryption and taking advantage of centralized key management via Microsoft Active Directory or Microsoft BitLocker Administration and Monitoring (MBAM). For these organizations, removing dependencies on their endpoint security vendors for one or more of the core capabilities allows for a much more flexible and blended approach when it comes to the replacement or augmentation of their endpoint malware detection capabilities. This blended approach of leveraging capabilities built-in to the OS and third-party solutions under a centralized management umbrella will continue to grow.

The advanced security features available in Windows 10 continue to be best-leveraged via a clean install versus an upgrade and, as such, most organizations tie their Windows 10 upgrade from Windows 7 as part of a hardware refresh. This results in a three- to four-year horizon, during which organizations may have multiple endpoint configurations to manage. This reinforces the need for simplicity of new endpoint protection investments, and for the focus on malware prevention and detection. Importantly, Windows Defender can appear as a very attractive baseline of malware protection within the Windows 10 platform. Microsoft continues to make solid improvements in the protection capabilities, as noted in recent public test reports, and its detect and response capabilities will be extended when Windows Defender Advanced Threat Protection (ATP) is made widely available to solve EDR use cases.
However, Windows 7 does not provide many of the safeguards that make Windows Defender a stronger proposition in Windows 10, and the fragmented management approach that includes System Center Configuration Manager, Intune, PowerShell and Group Policy commands continues to turn enterprises away from Windows Defender. Organizations running Windows 7 will find that the protection lacks the coverage of security vendors, and any perceived cost savings prove to be a false economy after factoring in the time spent reimaging infected, corrupted or encrypted devices.

Security and risk management leaders should use Windows 10 as their opportunity to reduce complexity — for example, the number of agents deployed to endpoint devices and the number of management consoles required for endpoint protection — and to rationalize the spend on commodity technology, such as disk encryption. While this type of spend can usually be used more effectively elsewhere in the security stack, using the same approach with Windows Defender is not recommended at this time.

**Include Mac OS Devices in Endpoint Protection Planning**

The presence of Mac OS in the enterprise is not a new phenomenon; however, many organizations are forced to not manage these systems with the same level of scrutiny as their Windows counterparts because of a disparity in the security solution capabilities across the different operating systems. Although Mac OS’s sandbox approach to software distribution is widely accepted as a better security framework than for the Windows operating system, it is important to understand that organizations should strongly consider including these devices in the scope for EDR capabilities. Mac OS can introduce additional threat surfaces, especially if users run unmanaged windows devices in Parallels, VMware Fusion or VirtualBox. If your enhanced visibility is limited to only Windows devices, you do not have a full picture of the activity in your organization. As a further example, compromised user credentials can be just as valuable to an adversary when used on a Mac OS device.

As organizations define their EPP requirements, they should be sure to keep Mac OS support in-scope. Including Mac OS within the threat modeling exercises and documenting the risk mitigation steps can help secure the business case for additional tactical investment budget, or build a strategic business case for a switch to a vendor that can provide a more holistic approach to all endpoints.

**Evidence**

1,625 client and vendor inquiries between 1 September 2016 and 1 September 2017

ETDR named in 2013

Source: Gartner Research, G00337106, Ian McShane, Eric Ouellet, Peter Firstbrook, 29 September 2017
The Security Framework

Your endpoint security must defend against malware, ransomware, and advanced emerging threats. As cyber attacks evolve, so must your endpoint protection. Gartner’s latest definition of an Endpoint Protection Platform (EPP) states:

“An effective solution protects endpoints regardless of where attackers strike on the attack chain. This level of prevention is only possible by combining critical security and signatureless technologies to:

- Stop ransomware with artificial intelligence techniques (including advanced machine learning and behavior analysis), and time-tested technologies like intrusion prevention.
- Use signatureless technology to prevent attackers from exploiting vulnerabilities in popular software, including browsers and productivity tools.
- Gain greater visibility into suspicious files to customize protection on the fly for different needs, by fine-tuning machine learning, behavior analysis, intrusion prevention, and more.

Figure 2 presents an optimal approach to multilayered endpoint security.

SEP delivers all these endpoint security capabilities for both fileless and file-based threat protection. It exceeds the high bar for security requirements, delivering both high performance and an uncompromised user experience.

Detection & Response

A capable EPP solution must include endpoint detection and response (EDR) functionality to prevent attacks from becoming breaches. It should detect, isolate, and quickly eliminate intrusions across all your endpoints by integrating artificial intelligence, automated incident generation, and unparalleled threat intelligence. EDR capabilities should:

- Share one single agent with other security engines (prevention, deception, and hardening) to reduce complexity and costs.
- Correlate and visualize advanced attack activity across critical control points – endpoint, network, and email – identifying the most suspicious incidents.
Utilize advanced threat intelligence to pinpoint-target incidents for investigation.

Record endpoint activity, including flexible policy options to support low-resource endpoints and scheduled transfers of endpoint activity data.

Block suspicious PowerShell and memory exploits with fileless attack detection.

Include pre-built components for popular ITSM and SIEM applications like ServiceNow, Splunk, and Qradar.

Integrate with existing enterprise infrastructure and systems via all-inclusive RESTful APIs.

Symantec’s EPP delivers all the above EDR features via the SEP agent. EDR capabilities are available on premises and in the cloud.
Deception

A complete EPP solution ought to expose hidden adversaries lurking in your ecosystem. Deception technology is designed just for this task and should:

- Use a minefield of lures (decoys) to reveal attacker tactics, techniques, and procedures.
- Sound high-fidelity alerts when adversaries take the bait.
- Share one single agent with other security engines (prevention, detection & response, and hardening) to reduce complexity.

See figure 4 to understand the flow—from deploying baits, to addressing attacker tactics, to adversary intelligence response—creating stronger security.

SEP’s deception includes all the capabilities shown above to expose attackers and enhance security. Joint SEP and Symantec Managed Security Services customers benefit from perpetual SEP (and deception) monitoring and response by our global team of experts. And Symantec is the only endpoint protection vendor offering deception as an integrated feature.

Hardening

Despite your best efforts to engineer a controlled, safe infrastructure, your users will continue to download and use whatever applications they see fit to stay productive. Endpoint hardening is a great way to keep control and reduce the attack surface. A key technology to achieve this goal is application isolation.

To balance your need for safety and still allow users to download and use any app safely, look for easy-to-use, effective application isolation that:

- Automatically discovers apps on endpoints to assess risk levels and vulnerabilities.
- Shields commonly used apps such as browsers, email clients, and productivity tools, preventing hackers from exploiting vulnerabilities to gain a foothold onto the endpoint.
- Isolates suspicious apps so that they cannot execute privileged operations that can harm endpoints and network.
- Shares one single agent with other security engines (prevention, detection & response, and deception) to reduce complexity and costs.

Source: Symantec
Figure 5 shows how application isolation works.

SEP Hardening’s application isolation uses the same SEP agent to discover applications and score the risk levels of apps and vulnerabilities. This intelligence is used to isolate suspicious apps and shield known good apps so that end users can benefit from any app without sacrificing productivity.

**Next Steps**

As you can see, Symantec Endpoint Protection effectively meets the five critical elements that define a complete endpoint security solution.

In fact, Gartner positioned Symantec highest in *ability to execute* and furthest in *completeness of vision* in the 2018 Gartner Magic Quadrant for Endpoint Protection Platforms.

To learn more about Symantec Endpoint Protection, visit [go.symantec.com/sep](go.symantec.com/sep) for videos, white papers, and more.
Customer Validation

Symantec Endpoint Protection wins the 2017 Gold Award for the Gartner Peer Insights, Customer Choice

“After implementing Symantec Endpoint Protection 14, we achieved some stunning results. We have seen a 60 percent drop in malware events.”

- Vicki Gavin, Compliance Director

“SEP 14 is helping to protect us in new and interesting ways. I especially like the application of machine learning, it’s constantly adapting to our environment.”

- Graeme Hackland, CIO

“Consolidating the State of Oklahoma’s spending on IT security solutions and standardizing on Symantec Endpoint Protection will save taxpayers a projected US$2.3 million over 5 years.”

- Mark Gower, CSO

“Full deployment of ATP capabilities was possible within an hour, and we were able to install it ourselves. The simplicity to install and ease of use and speed of integration with our existing environment is one of the product’s strengths.”

- Dor Liniado, Global CIO

Source: Symantec
About Symantec Endpoint Protection

Symantec Endpoint Protection delivers superior, multilayered protection to stop threats regardless of how they attack your endpoints. It combines signatureless protections (e.g., advanced machine learning, memory exploit mitigation, behavior analysis and more) with critical protections like intrusion prevention, firewall, and more. SEP integrates with existing security infrastructure to provide orchestrated responses to address threats quickly. And, the single, lightweight SEP agent offers high performance without compromising end-user productivity, so that you can focus on your business. For more information, please visit go.symantec.com/sep.

Source: Symantec

FIGURE 7 Symantec Endpoint Protection Solution