White Paper

Prevention is the Cornerstone in Delivering Value Through Integrated Endpoint Security

Table of Contents

Complexity is the Enemy of Endpoint Security

Attackers target seams—they examine where things come together, looking for imperfections and openings they can use to get into your resources. The more complex your environment, the more likely you are to have seams that expose vulnerabilities that attackers can exploit. This is why managing and securing all your endpoints is both so important and difficult to do.

The average organization has thousands, even hundreds of thousands, of endpoints to protect. They span an ever-increasing number of form factors, device types, and operating systems, many of which are not under the direct control or ownership of the organization. Each is used to access a wide variety of resources, using a wide variety of applications—leading app stores have millions of downloadable apps, and in 2020, total app downloads exceeded 218 billion.[1]

All these moving parts need to be managed and protected to ensure the organization's policies, security, and compliance can be maintained. The tools to manage and protect endpoints should help you bring order to the chaos, but instead they often add to the complexity. Ponemon found that 42% of security teams are not effective in detecting endpoint attacks because of the complexity in managing multiple agents.[2]

Each agent operates independently—loading up, scanning the same files, and hooking into the same processes, which can collectively slow down the endpoint. Each must be deployed, configured, managed, and maintained, with its own console, policies, and upgrade cycles. Each does things slightly differently, requiring you to learn how it works and how it should be integrated into your systems and workflows. It is easy to see why many organizations feel their endpoint security solutions are both ineffective and difficult and costly to manage, as a 2020 Forbes article showed that the average number of endpoint security agents increased to 10.2.[3]

Then there is the reality that each agent delivers specific, yet often overlapping, functions—providing network firewall, endpoint detection and response (EDR), device control, malware prevention, or other capabilities. It's up to you to figure out which features of which agent you ultimately want to use.

Keeping track of which agent is doing what generates a lot of unnecessary complexity, creating a lot of room for error, waste, and vulnerabilities (seams). An alert from one agent may already have been handled by another. Unfortunately, it's usually up to you to follow up on each and verify that an incident has in fact been handled. When something goes wrong, it can be almost impossible to figure out which agent is at fault. It's time things changed. It's time for an integrated approach to endpoint security.

1: "Number of mobile app downloads worldwide in 2020," https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/

2: Ponemon Institute, "The Third Annual Study on the State of Endpoint Security Risk," https://www.morphisec.com/hubfs/2020%20State%20of%20Endpoint%20Security%20Final.pdf

3: Forbes, "Answers to Today's Toughest Endpoint Security Questions in the Enterprise," https://www.forbes.com/sites/louiscolumbus/2020/08/02/answers-to-todays-toughest-endpoint-security-questions-in-the-enterprise/?sh=4c6bbcb11258

Complexity is the Enemy of Endpoint Security (cont.)

An integrated approach to endpoint security can drastically simplify your environment and reduce the seams—eliminating overlap and streamlining workflows and administrative effort. When done right, it can provide robust, cohesive security that can effectively protect your organization from the threats targeting your endpoints. This white paper defines what a truly integrated approach entails and describes how Symantec® technology delivers.

Defining an Integrated Approach to Endpoint Security

Integration doesn't come easily. Just because something says it is integrated, doesn't make it so. To achieve, integration needs to be a design requirement from the start. It must be baked into every level—product, portfolio and ecosystem—to create a single, unified end-to-end solution. Let's look at what this requires:

Product Integration

It's easy to see how integrating capabilities into a single solution will reduce the capital and operational expenses associated with purchasing, deploying, configuring, managing, and maintaining multiple point solutions. However, if those capabilities still operate independently, the benefits will be minimal. A truly integrated solution doesn't just consolidate capabilities onto a single agent, it ensures those capabilities are working together—as a single, cohesive unit, with a single console. All the various functions must be talking to each other, processing information once and sharing the insights to ensure threats are accurately identified, incidents appropriately handled, and policies tuned to harden and protect the environment from similar events in the future. There's no more manual correlation of security events detected by multiple technologies required. Interactions between capabilities are automated, so activities can be streamlined and optimal outcomes ensured.

Portfolio Integration

When vendors say they offer an integrated portfolio, it's important to look under the hood to understand exactly what that means. The solutions shouldn't be held together by superficial branding elements, they should operate as one. It shouldn't require custom "hacks," scripts, or development on your part to exchange threat intelligence and respond to threats. A truly integrated portfolio looks and acts like a single solution, even though it's made up of multiple different products. It automatically processes and shares information amongst the different products, so that everything operates in a singular, efficient way, with no room for fingerpointing if a support issue arises. It also provides a single console to make it easy to manage and tune capabilities. This allows you to minimize the costs of integration and maximize the value of the products you purchased.

Ecosystem Integration

No one vendor can do everything, particularly when it comes to cybersecurity, so it's important to be able to integrate with other solutions from other vendors. Typically, this integration starts and ends with vendors offering application programming interfaces (APIs) that allow other vendors to extract data from their solutions for their own analysis or purpose. But this isn't enough. True, meaningful integration is a two-way street. Vendors need to allow inputs into their systems, as well as data extraction to ensure one plus one really does equal three! To achieve, vendors must offer open APIs that any vendor or in-house developers can consume for their commercial, off-the-shelf, or custom app. These open APIs should allow the following:

- Retrieve security events for threat correlation, prioritization, incident generation, and workflow.
- Upload third-party threat intelligence (e.g. threat feeds or blacklists) for event enrichment, context, threat hunting, and proactive prevention (an example of an open standard that allows this is STIX).
- Manage policies for orchestration, automation, and operations management to further simplify implementations across large environments.
- Respond to threats by taking immediate action, such as blacklisting a file, quarantining a file, quarantining an endpoint, terminating a process, and so on.

Ideally, the vendor will help foster a community of customers and partners who can freely exchange ideas and accelerate innovation. This type of ecosystem integration allows your infrastructure to operate in a more cohesive manner, delivering greater efficiencies and results.

Only when a solution can support all three levels—product, portfolio, and ecosystem—can it truly be called integrated. Only when integration is baked into everything will you be able to streamline your endpoint management and security and minimize any "seams" to establish and maintain a security stance that meets your security and compliance objectives.

The Symantec Integrated Approach

Symantec technology provides the world's most advanced single-agent endpoint security solution featuring breadth of the number of security engines and depth of protections offered in each. Symantec Endpoint Security offers advanced prevention as the foundational core protection and the rest of the endpoint security portfolio delivers additional protections for the most complete security.

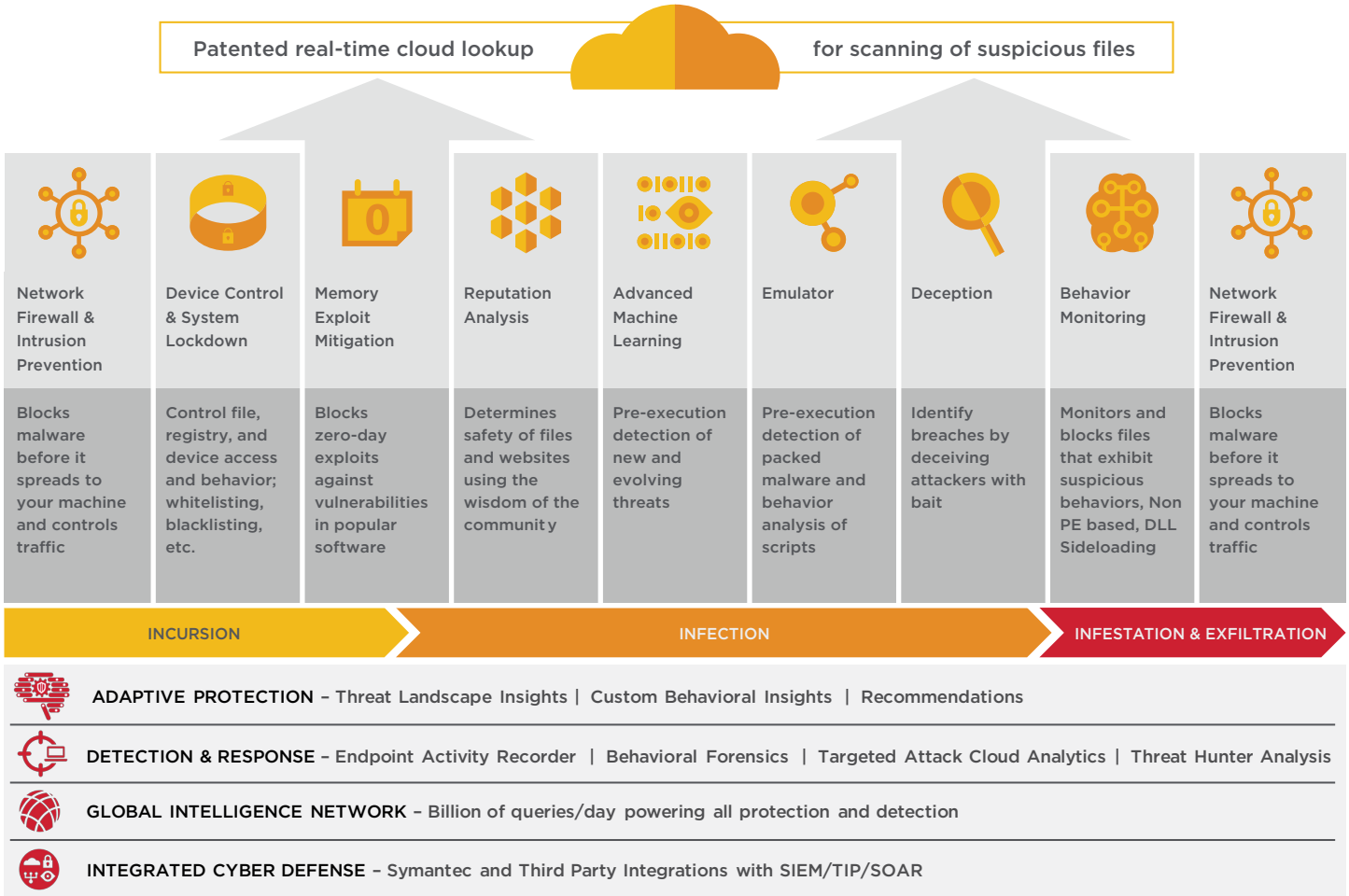
See Figure 1 for endpoint prevention capabilities. The additional protections include endpoint detection and response, adaptive protection, protections for Active Directory, and more. The Symantec commitment to integrating capabilities within the product, across the portfolio, and across the greater endpoint security and management ecosystem, is one reason why Symantec Endpoint Security is able to offer such a complete solution. No other vendor can match Symantec integration—streamlining operations and reducing any "seams" to protect endpoints from all attack vectors.

Symantec Product Integration

Using a single-agent architecture, Symantec technology provides truly integrated and coordinated capabilities, starting with Symantec Endpoint Security's core prevention and adding detection and response, deception and hardening. All the different functions are working in concert—single agent, single console—to automatically identify, process, and address security issues in the most efficient and effective way possible. For example, when a new process is launched on an endpoint, its reputation will automatically be checked. If it's known to be good or malicious, it will be allowed or blocked, respectively. If its reputation is unknown, it can be placed into a high, medium, or low security sandbox, based on its attributes. This gives you a post-execution protection method that allows users to work unimpeded, while mitigating any risks posed by "gray" apps.

If Symantec Endpoint Security's behavior analysis engine identifies a suspicious PowerShell command, it will send it to the other engines for analysis. It can

Figure 1: The Deepest Detection Stack in the Industry—Stop Targeted Attacks and Zero-Day Threats with Layered Protection



4: "Machine Learning: Symantec's Past, Present, and Future," by Joshua Abramson, Symantec, June 27, 2018, https://symantec-enterprise-blogs.security.com/blogs/feature-stories/machine-learning-symantecs-past-present-and-future

also use its sandbox for detonation and deep analysis. The point is the engines work together until it can determine whether the activity is malicious or benign.

The integration is made possible, in part, by Symantec advanced machine learning (AML) algorithms, which allow the security engines to learn from past events and automatically incorporate these learnings into future analysis and actions. Symantec technology is constantly revisiting its work and retraining its algorithms, over and over, to produce newer and better classifiers that can more accurately identify and deal with threats as they emerge.

This is unique to Symantec technology, primarily because it requires vast amounts of data at the level that only the Symantec Global Information Network (GIN) can provide. GIN collects telemetry from 175 million endpoints, 80 million web proxy users, and 63 million email users, generating over 8 billion reputation requests per day and over 20 trillion security events per year.[4]

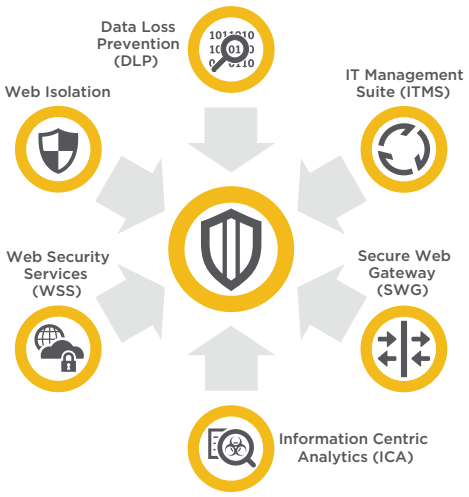
The Symantec AML can use all of this data to run thousands of checks in parallel. It automatically combs trillions of security events to connect the dots and find the paths that are most interesting, and then builds out the entire attack chain to understand exactly what's happening (referred to as spidering). This gives Symantec technology unparalleled visibility into what's going on, in real-time, to determine what's good and what's bad and feed that information back into the automated analysis and responses that are consumed by Symantec solutions.

Symantec Portfolio Integration

Symantec Endpoint Security can be easily integrated with other Symantec solutions to extend its capabilities and value. The integrated solutions look and act like one, with a single management console that can be used to monitor and manage everything (see Figure 2).

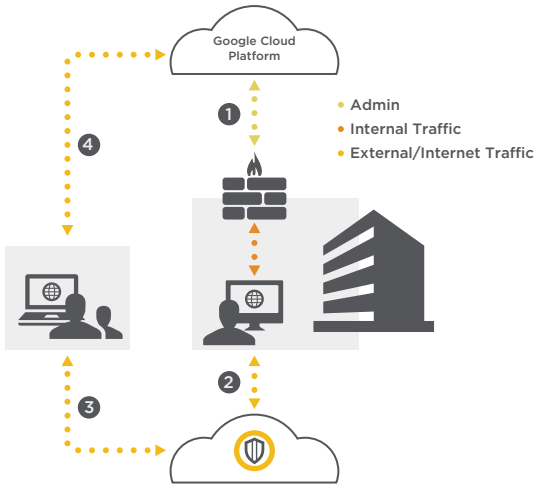
- **Symantec Data Loss Prevention (DLP)** to discover, monitor, and secure confidential content from suspicious processes in support of your security and compliance initiatives. For example, Endpoint Security can prevent suspicious processes from accessing documents classified by DLP as sensitive, regulated information.
- **Symantec Web Isolation** for integrated web and endpoint isolation. It can automatically isolate suspicious web pages in the cloud, while suspicious content found on the endpoint can be isolated using Endpoint Security's hardening capabilities to help protect your organization from malware and phishing threats.

Figure 2: Only Symantec Endpoint Security Can Bring Together All This Functionality



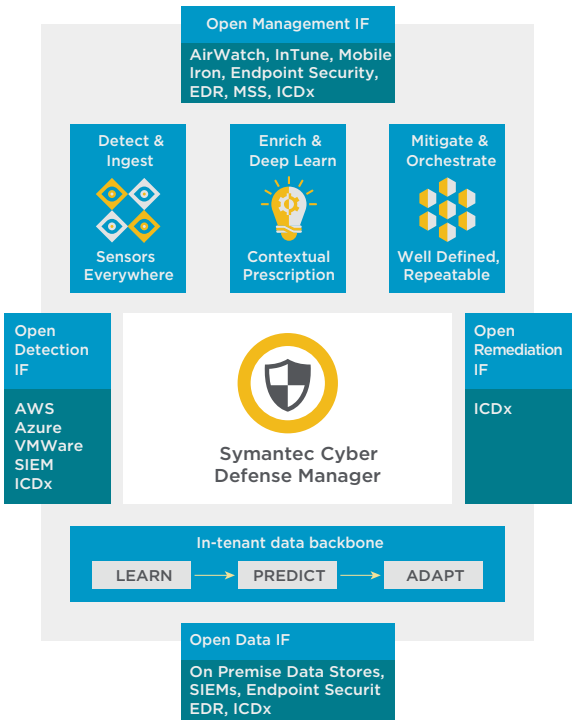
- **Symantec Web Security Services (WSS)** to provide a web use policy and malware threat solution for remote clients. Roaming endpoints can achieve additional network protection, by having Symantec Endpoint Security configure all web traffic to be routed through the WSS cloud proxy. This allows for consistent web policy enforcement throughout your environment, whether users are remote or behind a corporate firewall, and enables you to easily detect, identify, block and remediate threats and other security risks on your devices (see Figure 3 on the following page).
- **Information Centric Analytics (ICA)** to validate and improve intrusion detections. Suspicious or malicious files can be sent to CA (or a third-party engine) for sandbox analysis. When identified as malicious, you can quickly add it to Endpoint Security's blacklist, so that no other end users will be able to run the file, stopping it from propagating on the network. In addition, administrators can have Endpoint Security run a remediation policy to clean up the initial infection on the endpoint.
- **Symantec Secure Web Gateway (SWG)** to support detection at a network level and remediation at the endpoint. For example, when SWG detects a file as malicious, it can query Endpoint Security to determine how many devices have the same file and then trigger Endpoint Security to block or eliminate those files.
- **Symantec IT Management Suite (ITMS)** to simplify patch management and make it easy to close "seams" and keep endpoints up-to-date. ITMS can coordinate with Endpoint Security to automatically quarantine endpoints missing critical security patches, for Windows or other third party applications, until the patches have been installed.

Figure 3: Endpoint Security—WSS Integration



1. The Admin uses the Web Security Service portal to create custom a PAC file—possibly providing custom bypassing of specific servers—and associates it with an Explicit Proxy Location.
2. The Admin accesses the endpoint management console and configures Web Traffic Redirection (WTR), which includes adding the generated PAC file.
3. The endpoint management console distributes the security policy, including the PAC file URL, to the endpoints receives the security policy and configures the proxy settings for system and browsers.
4. The PAC file proxies all internet-bound traffic to the nearest Web Security Service for web use and security policy processing.

Figure 4: Symantec Cyber Defense Manager—Open, Smart, and Cloud-Managed



Symantec Ecosystem Integration

Everything is accessible through open APIs that any vendor or in-house developer can use to extend and enhance the capabilities of Symantec solutions (see Figure 4). Symantec Integrated Cyber Defense Exchange (ICDx) normalizes the incoming event data to attributes in the Integrated Cyber Defense (ICD) Schema. The ICD Schema is an information model that organizes both attributes and the objects that are made up of attributes into event types. The schema is publicly accessible.

The Symantec open framework allows data to be easily extracted to improve the threat intelligence and response of your other solutions. Information can also be uploaded to enhance Symantec technology's ability to identify and respond to incidents within your environment. For example, you can integrate your security incident and event management (SIEM) system, using the syslog feeds or connectors provided by the SIEM, to enrich Endpoint Security's event correlation with other third-party security products and threat intelligence data sources.

You could also integrate your Network Access Control (NAC) products, such as ForeScout, to prevent endpoints that are infected or compromised from connecting to your corporate network. An Extended Module for Endpoint Security uses ForeScout's CounterACT to validate the integrity of the agent, trigger real-time malware scans and help enforce compliance at device connection time. It also provides automated response options to isolate or restrict network access of non-compliant or infected devices and facilitate remediation actions. As a result, you can reduce your attack surface, minimize malware propagation, and limit the impact of data breaches.[5]

This is just one of many examples of Symantec technology integrating with vendors across the endpoint management and security ecosystem. With Symantec technology, you have full flexibility to customize your security deployment to address your unique needs. You can orchestrate policies and workflows to further streamline and optimize your endpoint security enforcement. For example, you could move an endpoint to a different group in the management console automatically via API. Integration with these types of custom scripts or other products is easily facilitated through the use of REST APIs.

5: "ForeScout Extended Module for Symantec Endpoint Protection," https://www.forescout.com/wp-content/uploads/2017/03/ForeScout-Extended-Module-for-Symantec-Endpoint-Protection-Datasheet.pdf

Summary

Your endpoint environment is fraught with complexity, which is bad for security. The many point solutions available to help you gain control and close up any "seams," more often than not, end up exacerbating the problem. What's needed is an integrated approach to endpoint management and security that can effectively protect your data and resources from attacks on the endpoint, while streamlining operations and reducing your total cost of ownership.

Symantec Endpoint Security does just that, protecting your endpoints from all attack vectors at industry-leading efficacy with a single agent architecture. Endpoint Security lays the foundation, with its coordinated threat detection and response, deception and hardening functions, giving you visibility and control over your endpoint environment, with a single agent, single console. Endpoint Security works in conjunction with other Symantec solutions and third-party products, via open APIs, to ensure you have all the capabilities you need to establish and maintain compliance and a strong security stance.

The integrated Symantec approach unifies cloud and on-premises security to protect users, information, messaging, and the web—powered by unparalleled threat intelligence. The integrated Symantec solution shares intelligence and works as one to defend your network together—no other vendor offers a unified solution that can orchestrate a response at the endpoint that was triggered by the detection of threats across web, email, cloud and information gateways. As a result of Symantec product, portfolio and ecosystem integration, you can greatly simplify your endpoint security to achieve better overall protection and greater overall value from your security investments.

For more information, visit the Symantec Endpoint Security website:
broadcom.com/products/cyber-security/endpoint

Symantec™ by Broadcom Software

For more product information: broadcom.com

20B283331 February 8, 2022