CUSTOMERONE

Symantec

How Symantec Keeps Its Own Endpoints Safe

One morning in late 2014, several Symantec employees made an alarming discovery: Their laptops had been infected with malware that had encrypted their files, making it impossible for them to access their work. A popup message demanded several hundred dollars apiece for a digital key to un-encrypt their files.

The malware spread to 14 Symantec users, in the U.S., India, and Australia. But then we activated Download Insight, a feature in our endpoint-protection product–and the spread of infections stopped immediately.

"That did the trick," says Gary Van Horn, the administrator who manages Symantec Endpoint Protection. "Once we turned on Download Insight, the malware was stopped in its tracks."

This experience highlights one of the strengths of our endpoint-protection technology (and a weakness in our early planning). Antivirus protection is becoming a commodity, but we've engineered other features that go beyond the industry standard. Symantec Endpoint Protection can guard against specific threats, but more important, it can leverage our Global Intelligence Network to watch for suspicious behaviors. It also uses reputation-based detection and behavior-monitoring technologies that block rapidly mutating malware quickly and surgically.

Symantec Endpoint Protection is a crucial part of our own internal security strategy. We use it to guard against ransomware and zero-day threats, and to guard the entry points that bad actors are most likely to target.

In this paper we'll discuss how we use Endpoint Protection internally, and which features we use most often. We'll also explain our product roadmap, and touch on some of the common questions we get from customers. We'll close by previewing how we're designing Symantec Advanced Threat Protection to enhance Endpoint Protection by at least an order of magnitude.

If you'd like to learn more about how Symantec Endpoint Protection fits into our overall security strategy, consider visiting one of our two Executive Briefing Centers. We'll walk you through our own blueprint for corporate security, and help you understand how you can adapt our model to keep your own enterprise secure.

With thousands of employees around the world, Symantec had to be sure that our method for keeping our endpoints safe was as robust as possible. We spent 10 years developing products and refining strategies to achieve just that–and having done so, we're now able to share our best practices with you. Protecting endpoints is an ever-evolving cat-and-mouse game with the bad guys, but what we've developed represents to date a best-in-class solution that can work for any medium-size to enterprise company.

This paper gives CIOs, CTOs, CISOs and other senior managers a transparent look into how we keep our endpoints safe. We describe the challenges we faced, the solutions we tested, and the best practices we fine-tuned over the past decade. We also explain how we configured our own products for maximum protection, and how that effort fits into our overall mission: (1) to provide elite levels of security for ourselves and (2) to pass that knowledge and experience on to our customers.

Our IT Staff's Favorite Features of Endpoint Protection

Protecting your company's computers means striking a balance—you want high barriers against external threats, but not so high that they impede productivity.

At Symantec we have the same concerns. That's why we've made endpoint protection one of our top priorities, leveraging our own products and testing them on our own staff as our first and best customers.

Naturally, our strategy involves a heavy dose of Symantec Endpoint Protection, powered by the wealth of information we gather in our Global Intelligence Network.

Before we get into strategy, let's start by looking at what makes Symantec Endpoint Protection different from other security products. Here's a summary of our IT staff's favorite features:

- Intrusion Prevention System (IPS) protects against ransomware, drive-by downloads, and bots
- Symantec Insight identifies a file's reputation and blocks malicious files based on risk
- SONAR (Symantec Online Network for Advanced Response) blocks unknown threats by monitoring file behavior for malicious activity
- Power Eraser finds and removes tenacious malware and hard-to-remove infections

Our security technology is strengthened by telemetry we gather from around the world. Millions of endpoints share anonymous user data with us, which enables us to spot malware quickly in any corner of the globe. We can then use that knowledge to inform customers and begin creating solutions.

We're not the only security company that uses telemetry, but we gather more than anyone else can. That allows us to triangulate threats wherever they arise and respond swiftly. We can also feed that information into powerful protection technologies such as Symantec Insight and SONAR.

Stopping Threats, Creating Confidence, and Scanning Faster

Gary Van Horn is one of Symantec's top Endpoint Protection experts. He's spent almost eight years as a product administrator, making sure Symantec Endpoint Protection is running seamlessly on our 10,000 or so Symantec endpoints.

He recalls the day when our colleagues' 14 laptops got infected with crypto-malware. The problem began with our third-party administrators who were managing the product. They had received a number of false positives, but rather than fine-tune the security rules as they should have they simply turned off Download Insight, the feature that specifically guards against such infections.

As soon as Gary and the incident-response team learned of the infections they reactivated Download Insight. With that one move, the infections were contained and the spread immediately halted.

"It was a great feeling," he recalls. "We didn't have time to do a lot of testing or poking around—we just turned it on to its defaults. And that's all it took."

Another popular feature that makes life easier for our IT staff is Intrusion Prevention System. Instead of watching the network stream for specific threats it looks for particular behaviors. For example, just like a storeowner would grow suspicious of a customer who keeps eyeing the cash register or casing the place for security cameras, Intrusion Prevention System looks for and blocks files that seem to be targeting certain entry points.

"It's great because it stops things before they even get on a machine," Gary says. "Sometimes our teams are concerned about a particular vulnerability in mission-critical software. But as soon as we tell them we have an IPS signature everyone calms down because they know we're protected."

We also rely heavily on Symantec Insight and SONAR.

Symantec Insight uses reputation-based technology to assess files based on their age, location, frequency of occurrence, and more. If a file is too new to have earned a safe reputation, Insight will block it, a tactic that's especially effective against new or rapidly mutating threats. (A user who knows the file is safe can ask our team to evaluate and whitelist it.)

Even though Symantec Insight is popular with customers, some turn it off because they don't understand it. When you first install Symantec Endpoint Protection it will scan and catalog every file on that computer. Naturally, the first scan will be thorough, which can bog down the system to the point where some customers disable the feature.

What they don't realize is, Endpoint Protection is designed to scan only new files. Once it catalogs a file, it ignores that file on subsequent scans unless the file has changed. So ensuing scans run faster and use fewer resources.

"That little bit of slowdown initially is totally worth the hit," Gary says. "After all, having all those features in place, that's what's keeping you safe."

We use SONAR to target malware activity. Instead of evaluating what a file looks like, SONAR watches what a file does and uses artificial

intelligence and behavior signatures to determine whether its behaviors are good or bad. If an executable is identified as malicious, SONAR blocks it in real time.

Integrating with Symantec Advanced Threat Protection

As a standalone product, Symantec Endpoint Protection does an effective job of protecting against ransomware; targeted and zero-day attacks; and advanced persistent threats. But the product got a serious boost in late 2015 with our release of Symantec Advanced Threat Protection. Symantec ATP is designed to keep enterprises secure by strengthening their threat protection and providing tools that detect and remediate malicious events.

It also enhances our Endpoint Protection solution because it collects telemetry not only from individual Endpoint Protection reports but also from network and email modules, thus producing the broadest possible view. Now if one endpoint browses a compromised site, Symantec ATP will be able to show whether other endpoints browsed the same site. Or if a security administrator is looking for a specific hash or filename, Symantec ATP will be able to search all or specifically chosen endpoints.

In addition, Symantec ATP simplifies how affected endpoints are remediated. "You're now able, via one console, to investigate, isolate, and remediate," says Javier Santoyo, our senior director of security intelligence.

Without Symantec ATP, a system manager has to go through a longer, more circuitous route. A manager who receives an Endpoint Protection alert has to elevate it to an incident responder; ask the endpoint user to run a utility to interrogate the system; pull back any suspicious files; run an analysis; and then help the user clean up or re-image the entire system.

"Now I've reduced that entire workload to a few clicks of a button," Javier says. "That's extremely powerful." (For more information, please see the CustomerONE paper "Symantec Advanced Threat Protection: What We Learned as the First and Best Customer of Symantec ATP.")

Next Version Makes Mac Updates Easier

There's one aspect of Endpoint Protection that used to frustrate our IT administrators (and is the focus of an upcoming update).

Once Endpoint Protection is set up, an administrator's main responsibility is to keep it current with the latest updates, as part of the never-ending game to stay ahead of the bad guys.

Rolling out updates is easy—at least in a Windows environment.

"I'm so confident in the product I always expect zero problems at each rollout," Gary says. "Sometimes you have bad machines or bad network connectivity, but otherwise I achieve success rates of 98 percent without even trying."

However, the story with Macs isn't quite as clean. That's because we originally optimized Endpoint Protection to work with Windows, the dominant operating system when we acquired the product in 2005. We've been improving Endpoint Protection for Macs, but rolling out updates on Mac products has tended to be slower.

For example, in rare cases the team can't run the update remotely, so someone has to go physically to the server and run the necessary update package. We can still get the job done, but the effort is more labor-intensive and involves more people.

Fortunately, Version 12.2, which is due out in the first half of 2016, is specifically designed to simplify the process of pushing updates to Mac clients.

Why Upgrade to Symantec Endpoint Protection

Some companies, intentionally or not, install several endpoint-protection solutions at the same time. In some cases it happens because a company has multiple corporate sites, and each buys a different solution. Or sometimes IT managers in different departments choose different endpoint solutions based on their own personal preference or familiarity. Or a company might believe it's diversifying its risk by doubling (or tripling) up on security vendors.

Regardless of the reason, it makes a lot more sense to standardize, says Kari Ann Sewell, a Symantec product marketing manager. A single trusted solution saves money, improves efficiency and eliminates incompatibilities.

"The best way to mitigate risk is by standardizing on the fastest, most effective protection available, " Kari Ann says. "It's not by chopping up your infrastructure into puzzle pieces that don't work well together."

We believe we have the best solution on the market, and we speak from personal experience. In the 10 years we've used Symantec Endpoint Protection, we've seen it deliver lockdown security that has caught countless instances of known and unknown threats—malware, ransomware, zero-day threats and more. And it works on all 10,000 of our endpoints without compromising productivity.

For proprietary reasons we're limited in the level of detail we can discuss in this paper. If you want to learn more, join us for an exclusive executive briefing.

Learn More with an Executive Briefing

This brief was intended to give you a broad look at how we keep our endpoints secure. Your Symantec representative can show you how to adapt our blueprint to protect your own environment.

For a more in-depth experience, visit our Executive Briefing Centers at our U.S. headquarters in Mountain View, California, or in Reading, U.K.

Executive briefings provide you an exclusive opportunity to learn how Symantec solutions can protect your business and network environments. We'll customize the briefing to meet your specific goals, and we'll also give you a sneak peek at new technologies and challenges on the horizon.

Contact Symantec today.

SYMANTEC SOLUTIONS AND PRODUCTS IN THIS PAPER

Symantec Endpoint Protection: SEP provides layered protection and intelligent security to guard against targeted attacks and advanced persistent threats on all endpoints

Symantec Advanced Threat Protection: ATP uncovers advanced threats across endpoints, networks and email gateways, and then prioritizes events to facilitate faster remediation of the most dangerous threats

customer_one@symantec.com

CustomerONE Team
350 Ellis Street
Mountain View, CA 94043
800-745-6054

Symantec's CustomerONE team can facilitate discussions between you and our IT security practitioners to help you address your security questions and concerns. Please contact us directly or through your Symantec sales team.