CUSTOMERONE

Symantec

SYMANTEC ADVANCED THREAT PROTECTION:

WHAT WE LEARNED AS THE FIRST AND BEST CUSTOMER OF SYMANTEC ATP

When we designed Symantec Advanced Threat Protection in 2014, we set out to create more than just a great product for customers—we also had to have a great product for ourselves. After all, we face (at least) the same cyberthreats as anyone else, and our credibility depends on how well we keep our own enterprise and endpoints secure.

That's why we took an unusual step to develop ATP: We included our security-intelligence director as a key member of the design team. That way the product would be shaped not only by security engineers but also by a hardcore security expert who has decades of experience addressing actual needs.

Javier Santoyo runs our threat-investigation program. His team investigates internal and external threats, escalating the most serious ones to our Incident Response Team. After 16 years at Symantec, Javier knows exactly how a security analyst thinks. He knew the limitations of our earlier security strategies, and he knew which tools could make our security analysts more effective.

Javier Santoyo, senior director, Security Intelligence

Today, he and his team are the beneficiaries of his efforts. Since late 2015 they've been part of our internal CustomerONE program, serving as the first and best customers of Symantec Advanced Threat Protection.

This is the story of Symantec ATP. We'll tell you what it is, how we developed it, and, most important, what it does well and where there's room for improvement. This paper is intended to give you a brief, nontechnical overview. If you'd like more information, we'd be happy to arrange an up-close look with a personalized Executive Briefing.

Symantec Advanced Threat Protection secures enterprises by strengthening their cyber-defenses and providing tools to quickly detect and repair malicious events. It is designed for midsize to enterprise businesses (customers with 100,000 endpoints and as many as 300,000 email seats have deployed it successfully), and it can handle bandwidth in the 10GB/sec range.

This paper is intended for CIOs, CTOs, CISOs, and senior managers. We'll explain (1) how Symantec ATP can meet your needs, and (2) what to expect—good and bad—during installation and operation. We'll address these points using our own installation as a case study. We'll tell you what worked and what didn't. We'll tell you which goals we achieved and which ones we're pursuing in future versions. And we'll tell you the lessons we learned the hard way, so your journey will be smoother.

History: The Market Need That Led Us to Create Symantec ATP

It wasn't that long ago that good cyber-defense was defined as having a strong firewall, a powerful antivirus solution, and effective software to protect against data loss. But these solutions are no longer enough. That's because bad actors are growing more sophisticated, and corporate vulnerabilities are stacking up as employees around the world access their network through an increasing breadth of devices.

Companies today need to know when they're being attacked, and they need tools that empower them to react aggressively. No vendor had ever offered such a full-service product—so in 2014 we set out to fill that niche.

We envisioned a single solution that would protect network, email, and endpoints all at once. We also wanted to be able to investigate, isolate, and remediate from a single console. We wanted enterprise-level visibility on the most serious threats, and we didn't want important alerts to get diluted by noise. Finally, we wanted the solution to correlate its intelligence not only locally but across our entire global network.

And that, in simple terms, was the genesis of Symantec Advanced Threat Protection. We already had strong endpoint-protection technology, and we realized we could extend that technology beyond the endpoint to provide visibility across the network and email gateways. We also added tools that allow users to investigate and remediate from a single console. Finally, we plugged ATP in to our Global Intelligence Network, so it could feed into and draw from one of the industry's most comprehensive sources of threat information.

"Symantec ATP is a major advance for our security," says Tim Fitzgerald, Symantec's chief security officer. "The ability to identify and stop threats across multiple control points has changed the way we operate. Until now, we had to stitch this capability together with multiple products—and it didn't work half as well as ATP version 1.0."

We've been using Symantec ATP 2.0 internally since late 2015. In early results our security analysts tell us the product is effective, powerful, and intuitive.

They do have suggestions for improvement that resolve around ease-of-use issues. For example, they'd like better ways to search for prior events. They'd also like the interface to facilitate communication between security analysts and the incident-response team.

Here's What Symantec ATP Delivers:

Symantec Advanced Threat Protection allows you to:

- Uncover advanced threats across all network, endpoint, and email gateways
- Prioritize events so you can address serious threats first and filter out the noise
- Remediate quickly and thoroughly, from a single console

The first point is the most important. No matter how a threat comes into your environment, ATP will see it because it constantly scans every entry point across your network, email, and endpoint.

Our detection capabilities draw upon a number of proven Symantec technologies. There's **Symantec Cynic**, a cloud-based service that detects advanced threats and previously unknown malware. It works by isolating questionable files into a walled-off sandbox environment, where it runs them and analyzes their behavior to determine whether they're malicious.

There's also **Symantec Synapse**. This technology correlates data with information from Symantec Endpoint Protection and Symantec Email Security.cloud. In simple terms, that means you end up with fewer false positives, higher prioritization for urgent incidents, and lower priority for those already resolved.

(For more CustomerONE information on Symantec Endpoint Protection, see "Symantec Endpoint Protection: How Symantec Keeps its Own Endpoints Safe.")

Other industry products only detect threats at the network or endpoint gateway. Symantec ATP is the only product that gives you visibility at all three nodes—network, email, and endpoint—all at once.

The other significant advantage of Symantec ATP is its access to our advanced global telemetry. Our Global Intelligence Network collects information from 175 million endpoints around the globe. By tapping into that information, ATP can quickly determine whether certain files and URLs are suspect or whether enough data has been gathered on them to conclude they're safe.

Our Personal Journey: Getting the Product Up and Running

Symantec has implemented Symantec ATP for several dozen alpha and beta customers. In 90 percent of cases the implementation took less than a day; even better, 75 percent of customers were up and running in one to two hours.

Our own journey took longer—several months, in fact, but that was by design. We were working closely with Javier and his team in a deliberate, iterative manner, starting when the product was in pre-alpha form. Our aim was to capture completely the needs of a Security Operations Center and individual IT security practitioners.

"We engaged with Javier's team from day one," says Adam Glick, chief architect for Symantec ATP. "We sat side-by-side with his team and asked a lot of questions: What do they do, how do they do it, why, what matters to them. That information was key to how we developed the product."

Javier also worked with product managers to define product requirements and represent the customer perspective. He put the product through rigorous testing and provided feedback to help make it more effective.

"Our goal was to help the product teams deliver a product that was operationally useful from the outset," Javier says.

It's not a revolutionary idea to ask internal experts to help shape a product. However, not everyone does it. Product managers are more likely to solicit early feedback from beta customers and external partners, because those are potential sources of revenue.

We certainly do ask beta customers for feedback, but we want to be respectful of their time. We also know they sometimes hold back in their comments.

"It's a different dynamic when the conversation is internal," Tim says. "Your colleagues can give you feedback without worrying how it will be received. They're brutally honest."

Putting Symantec ATP to the Test in Our Own Environment

One reason ATP is so robust is that we built it on top of Symantec Endpoint Protection. SEP already does an effective job of protecting against ransomware, zero-day attacks, and advanced persistent threats. ATP improves this performance by an order of magnitude.

SEP gives you visibility on individual endpoints, but ATP provides a view of the entire network. It collects telemetry not only from individual SEP reports but also from the network and email gateways. For example, if one endpoint browses a compromised site, ATP can show you whether other endpoints browsed the same site. Or if a security administrator is looking for a specific hash or filename, ATP can search all or specifically chosen endpoints.

Without ATP, a system manager has to go through a longer, more circuitous route. An analyst who receives an alert from SEP Manager has to elevate it to an incident responder, ask the endpoint user to run a specific utility, run a separate analysis, and then help the user clean up or reimage the entire system.

"Now we've reduced that entire workload to a few clicks of a button," Javier says. "That's extremely powerful."

Javier's team spent months putting ATP through the paces. He has noticed areas for improvement (which we'll touch on shortly), but his favorite feature is ATP's capability for endpoint detection and remediation.

Because of its multiple control points, ATP provides a level of visibility that didn't exist before. Now if there's an indication of compromise he can query the entire system; if any endpoints register a positive hit he can take appropriate action, all from a remote console.

Without ATP he wouldn't have been able to query endpoints to see if they had encountered the questionable indicator.

"With ATP we can see everything that's happening across the entire network, and we have tools to surgically remove files that shouldn't be there," Javier says. "For my group that's really exciting."

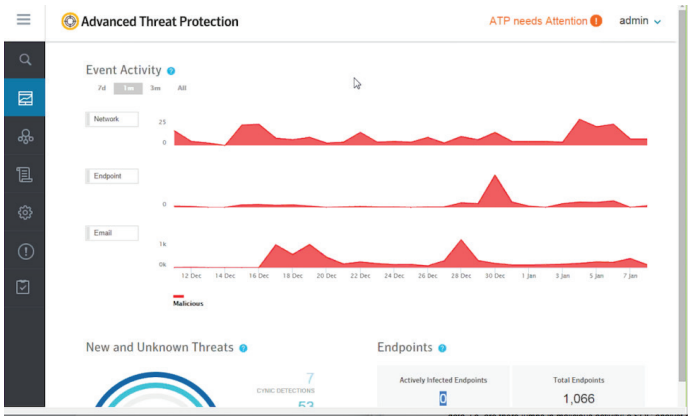

Fig. 1. This screenshot from an actual Symantec console shows how Symantec ATP tracks event activity on the network, endpoint, and email gateways at the same time. Menus (not shown) allow analysts to investigate the peaks by providing information gleaned from our Global Intelligence Network.

Guidance: Finding the ATP "Heartbeat" that Works for You

When we talk about using Symantec ATP to remediate issues, it's important to understand one constraint. SEP currently communicates with ATP through SEPM, or Symantec Endpoint Protection Manager. The tools aren't in constant communication, because trading thousands of messages every second would take up too much bandwidth.

Instead, users set up a default "heartbeat"—a preprogrammed delay that tells the systems how often to reconnect. We use a 30-minute

heartbeat, meaning we get updates at half-hour intervals. There are ways to speed up the interval on demand, but for the most part there's a known lag period.
Our beta customers use 15- to 60-minute heartbeats. That seems to strike an effective balance between security and bandwidth. In theory you could choose an interval of 5 seconds or less, but you'd need top-of-the-line infrastructure to handle that volume of communication.

We're changing our architecture in the summer of 2016 in a way that should make the heartbeat less of an issue. We'll touch on that in the first bullet point below.

Next Steps: Making Symantec ATP Even Better

We're excited about where we are with Symantec ATP. As customers begin migrating to the product, here are some of the features they'll be able to access in future versions.

1. One of the most important will be the ability to bypass SEP Manager and search endpoints directly—even if they're off the network. That's important to our security team because only about a third of Symantec endpoints are on the network at any one time. So instead of depending on an employee to come into the office or log on remotely, our analysts will be able to query that employee's system at any time.

   Once we bypass SEP Manager we'll be able to take remediation actions immediately, and the heartbeat will essentially become a non-issue.

2. You'll also be able to take advantage of upcoming functionality in Symantec Endpoint Protection. We're planning enhancements to SEP that will give you even more detailed information about everything happening on that endpoint. We're upgrading ATP in parallel to take advantage of that information.

3. Finally, we're working to improve how Symantec ATP works with all security ecosystems, including those using third-party products. ATP was initially designed to take advantage of the existing investment that customers have made in SEP and Email Security. cloud. But we also plan to serve customers who've invested in other products. That will include:

   a. Agentless support: Customers won't need any agent on their endpoint machines in order to support investigation and remediation; and

   b. Next-generation firewalls: Even if something is detected by a competitor's product, you'll be able to see it in your ATP console.

What we're trying to do is give customers more control over their security, says Amanda Grady, a senior product manager for ATP network/endpoint. As threats and attackers proliferate, some customers react by buying even more security products—complicating rather than simplifying their security strategy.

"We want to have a single product that lets you do it all: detect, investigate, prioritize, and remediate threats," Amanda says. "There are products that can handle each individual step, but what we're trying to do is make it simpler for customers to manage their environments."

Also on our roadmap: expanding our capabilities for endpoint detection and remediation for Mac and Linux platforms. Our capabilities are currently optimized for a Windows environment, so we'll be looking to extend on that.

Finally, we're collecting feedback from our security analysts as they come up to speed on the product. We're getting praise for ease of use, user interface, and enhanced tools to investigate and remediate threats.

Bryant Binnix, one of our senior information-security analysts, says Symantec ATP makes it easier to determine whether a threat observed in one place has also appeared elsewhere in our worldwide environment. He also likes a number of timesaving shortcuts that give him helpful details to speed up his job.

He does recommend a few improvements to the product.

For example, there were times when he escalated an event but couldn't annotate that an incident ticket had already been made. As a result, more than one team member investigated the same event at the same time.

He'd also like to see one change to the Incident Manager page. Right now it lists incidents by priority, but if it allowed him to filter by date or ID number he says it'd be easier to search for specific incidents.

"These are just minor things I'm passing along to the development team," Bryant says. "Otherwise I can see where this can save a lot of time remediating threats."

Industry Overview: How We Stack Up Against the Competition

EXECUTIVE SUMMARY

Products tested

Product	Detection accuracy	Legitimate accuracy
Symantec Advanced Threat Protection	100%	100%
Palo Alto Networks PA200	90%	97%
Cisco Snort	72%	100%
Fortinet FortiGate60D	69%	100%

Source: Dennis Technology Labs, "Network Threat Detection," December 2015

We have a number of competitors that offer strong network components. But we believe we have two advantages the others can't match.

Besides having the industry's most extensive Global Intelligence Network, only Symantec combines a network solution that includes email and endpoint solutions. The other guys have a presence only on the network, so their customers need additional third-party products to handle the other gateways.

"Symantec has a super-proficient presence on the endpoint already," Tim says. "We've also moved a ton of capability to the cloud, making the agent even more lightweight. There's no denying our competitors have their own strengths, but in the end we think we have the No. 1 efficacy of detection."

But don't take our word for it. See for yourself with an Executive Briefing.

Learn More with an Executive Briefing

This brief was intended to give you a broad look at how we use Symantec Advanced Threat Protection internally. Your Symantec representative can show you how to adapt our blueprint to make your own ATP journey even smoother.

If you'd like even 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.

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.