SOLUTION BRIEF:
HARNESSING GLOBAL INTELLIGENCE TO
DETECT AND RESPOND TO THREATS FASTER

Advanced Threat Protection: Harnessing Global Intelligence to Detect and Respond to Threats Faster

Who should read this paper

Strategic IT and Functional IT professionals

Symantec

Content

Overview

Symantec™ Advanced Threat Protection uses real-time threat intelligence to help organizations detect and resolve threats within minutes, not days or weeks—reducing their security operating costs.

Cyber threats are evolving at a dramatic rate and becoming more hostile. Far-reaching vulnerabilities, faster attacks, files held for ransom, and far more malicious code than in previous years are all making it increasingly difficult for security professionals to stay ahead of the threat curve. Savvy cyber attackers are using advanced tools to get inside more networks, faster than most businesses can defend against them. And often, organizations don't even know they're under attack—less than 25% of breaches are discovered by internal security practices[1].

As the threat landscape continues to grow and evolve, organizations of all sizes face increasing vulnerability. Symantec recently revealed in its Internet Security Threat Report[2] (ISTR) that 83% of large companies (2,500+ employees), 63% of medium-sized companies, and 45% of small companies (1-250 employees) were targeted with spear-phishing attacks in 2014. This is a 40% increase from the year before.

Today's attackers hijack companies and use their own networks against them. Once inside the breached network, they leverage existing IT management tools to move stolen intellectual property (IP) around. Others create custom attack software to deploy from their victims' own servers. And many use stolen email accounts to spear-phish the next victim. Cyber attackers exploit critical vulnerabilities much faster than vendors can create and roll out patches. In 2014, the top five zero-day threats left companies without a patch for 295 days[3].

The volume of attacks continues to rise, as does the variety and sophisticated nature of attacks. Nearly one million new pieces of malware are released every single day—and a growing portion uses various tricks to avoid detection in virtual machine environments. Up to 28% of all malware released in 2014 was "virtual machine aware", proving that virtual environments do not provide enough protection[4]. Clearly, organizations must take a more intelligent approach to protecting and securing their infrastructure.

Symantec™ Advanced Threat Protection leverages one of the world's largest civilian threat intelligence networks to correlate real-time security data across endpoint, email, and network—to detect more malware and prioritize threats faster.

Symantec Global Intelligence Network

Symantec delivers the industry's first Unified Advanced Threat Protection solution, combining the analysis of an organization's local network activity with security intelligence from Symantec's massive global intelligence threat network. Symantec Advanced Threat Protection delivers the detailed, relevant, and actionable information needed to correlate security data across their enterprise, make smart decisions, and respond to critical security events quickly and effectively.

The Symantec Global Intelligence Network has the volume and variety of threat data analytics to detect advanced threats, vulnerabilities, and malicious behavior. Symantec Advanced Threat Protection uses threat intelligence delivered from the cloud in real-time to rapidly detect attacks or ongoing breaches.

Based on analysis of downloaded Symantec™ Insight data and other Symantec telemetry, Symantec stops more than 800,000 unknown threats every single day.

1- Ponemon 2014 Cost of Data Breach Study
2- Symantec Internet Threat Report, Volume 20, April, 2015
3- Symantec Internet Threat Report, Volume 20, April, 2015
4- Symantec Internet Threat Report, Volume 20, April, 2015

Symantec Cynic™

Cloud-based detonation

Symantec Cynic is a cloud-based malware analysis and sandbox technology that detonates suspicious content in multiple scenarios across virtual and physical infrastructure. Symantec Cynic uses the scalability and power of cloud computing to deliver intelligence in minutes, not hours.

Most sandbox analysis products focus on offering a variety of virtual machines or customer-specific images to detonate and detect malware. Symantec Cynic uses a suite of analysis technologies—coupled with our global intelligence and analytics data—to accurately detect malicious code.

Symantec Cynic mimics human behavior to detect even the most advanced threats in minutes and provides the context and actionable security intelligence to understand what a threat was, why it was detected, what it did, where it came from, and where else it is in your environment.

In 2014, 28% of all malware was virtual machine-aware[5], and with most sandboxing technologies heavily reliant on hypervisors for content execution and analysis, the use of bare metal environments is critical to detecting advanced malware. For this reason, Cynic includes an additional layer of analysis on physical hardware. This layer is employed for malware samples that attempt to check if it is being analyzed in a hypervisor. All environments are highly calibrated to draw out and record VM-aware malware behaviors. Exhibited behaviors are categorized and further analyzed by Symantec™ SONAR and correlated with global security intelligence to determine if the content is malicious.

Details of how analyzed content behaves are available to security administrators through the user interface, enabling a deep understanding of the intent of the content and remediation steps.

Symantec Synapse™

Correlation across control points

Symantec Advanced Threat Protection intelligently correlates security events across endpoint, email, and network in real-time. Working with Symantec Endpoint Protection and Symantec Email Security.cloud, incidents are prioritized for faster response with Symantec Synapse™.

Symantec Synapse can save administrators hours of wasted time investigating an attack that has already been addressed. Synapse automatically responds to and checks the status of these types of incidents, with a cumulative effect of dramatically reducing the number of alerts that administrators would otherwise receive and manage.

Symantec Synapse can accurately alert administrators to threats that really do need attention and prioritize those threats in a manner that enables the most effective and efficient response.

5- Symantec Internet Threat Report, Volume 20, April, 2015

Symantec Advanced Threat Protection Benefits

Advanced Threat Protection from Symantec provides:

Coordinated Communication Across Multiple Control Points – Symantec Synapse technology enables organizations to respond to elusive advanced threats more quickly, through its ability to integrate and correlate security information across endpoint, email, and network. It gives administrators and security managers the situational awareness they need to quickly analyze security events and threat severity, and then accurately raise or lower the priority levels of events so they can focus and maximize their efforts on the most critical, unresolved events.

Intelligent, Trusted Alert System – Symantec Synapse doesn't automatically send out an alert just because a threat has been detected on one control point. First, it checks in with the other control points to determine if they've encountered the threat, and if it has already been remediated. If the threat has already been resolved, it is logged, but no alert is generated. This reduces the volume of alerts administrators receive to only those that really need attention.

Unified View of Security – Through a unified management interface, Symantec Synapse delivers easy to consume threat analysis that includes unresolved incidents, targeted attacks, threat campaigns, recurring infections, on-demand queries and cross-solution data sets for more productive forensics analysis. Powered by its ability to correlate activity across endpoint, email, and network, it presents a rich, contextual view of security events that inform administrators and security managers what the event means to the organization, why it's considered malicious, what it did, how it got in, and what can be done about it.

Global Contextual Insight – Both Symantec Cynic and Symantec Synapse leverage Symantec's Global Intelligence Network to provide organizations global context on potential threat activity occurring within their network. This gives them access to security intelligence on similar advanced threat activity occurring in other parts of the world.

Coordinated Forensic Analysis – Symantec Cynic and Symantec Synapse technologies give administrators full access to Symantec SONAR so they can see everything that a malicious file attempted to do. It allows them to forensically analyze user email and endpoint activity associated with particular files, origins, dates, threat campaigns, malware types, and more.

Summary

Now more than ever, organizations need full lifecycle protection against targeted attacks and advanced persistent threats. Symantec Advanced Threat Protection offers automated threat analysis at the network for rapid detection and accurate prioritization of security events through correlation with endpoints and email, reducing the volume of security alerts and prioritizing the most significant threats.

Symantec provides day-one integration across all three control points—with no additional agent or endpoint update required—identifying when a threat or incident has already been resolved and highlighting and prioritizing the unresolved, high-risk incidents. This provides customers with the tools to respond quickly and with confidence, cuts discovery from months to minutes, and provides containment and remediation with a single click.

For more information visit http://symantec.com/advanced-threat-protection/

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings – anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 19,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2015, it recorded revenues of $6.5 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com