WHITE PAPER:
THE SYMANTEC APPROACH TO DEFEATING ADVANCED THREATS

The Symantec Approach to Defeating Advanced Threats

Who should read this paper

For security practitioners and decision makers looking to learn more about the technologies that Symantec utilizes to detect advanced threats and prioritize security events.

Symantec

Content

Introduction **1**

The Symantec Approach to Defeating Advanced Threats **1**

Advanced Threat Protection 2

Advanced Threat Detection 2

Advanced Threat Response 4

Unified Advanced Threat Protection, Detection, and Response **6**

Introduction

In 2013, three significant cybercrime trends surfaced. First, targeted attack campaigns increased by 91 percent.[1] When compared to more traditional threats, the advanced and complex nature of targeted threat campaigns makes them much more difficult to detect and respond to. This not only allows them to slip past most traditional security protection layers, but it enables them to probe, scan, and gather information within the corporate network for months before being detected.

In fact, in 2013, such attacks remained hidden on average for 229 days before being discovered.[2] Additionally, when attacks involved credit card data theft, no matter how large or small the organization, in 99 percent of the cases discovery didn't occur until a third-party—often law enforcement, fraud detection agencies, or customers—notified the organization that it had been breached.[3] The longer an advanced threat goes undetected, the greater window of opportunity a cybercriminal has to exploit the organization's intellectual property and customer data and expose the organization to significant financial and reputation damage.

The second significant cybercrime trend indicates a greater persistence and tenacity on the part of cybercriminals in their attempts to breach targeted organizations. In 2013, the time that targeted campaigns were in play more than doubled from the year before, increasing from an average of 3 days to 8.2 days.[4]

The third trend reveals a shift in the types of organizations that cybercriminals target in their attacks. In 2013, 30 percent of attacks targeted businesses with less than 250 employees and 61 percent of attacks targeted businesses with less than 2,500 employees. It's clear that organizations can no longer assume that they're too small to be considered an attractive target for cyber attacks.

These cybercrime trends signal the need for organizations to shift from a focus that primarily seeks to block attacks in order to protect their networks. Regardless of how much an organization invests in network protection, data breaches can and will still occur. To combat the tenacity and growth of advanced threats, organizations need to expand their focus to a more encompassing approach that includes threat protection, detection, and response.

Organizations need to protect, detect and respond to threats faster, with accurate threat prioritization in a way that saves organizations more time, effort and cost, while enhancing their overall security posture.

The Symantec Approach to Defeating Advanced Threats

There is no silver bullet or one size fits all solution when it comes to advanced threats. Point products are ill-equipped in the battle against advanced threats. Even attempts to piece together a variety of different sophisticated solutions or a combination of varying point products leaves an abundance of gaps and holes in security that advanced threats can stealthily work their way through, remain undetected, and wreak havoc.

The Symantec approach to combating advanced threats goes well beyond just trying to block threats. It goes beyond a patchwork of disjointed solutions. Symantec has developed a unified way to combat advanced threats across multiple control points and across all the different stages of an attack. Symantec provides a comprehensive array of solutions that work together to deliver maximum and unified protection, detection, and response against even the most sophisticated and elusive advanced threats.

1- Symantec Internet Security Report 2014
2- Mandiant 2014 Threat Report
3- Verizon 2014 Data Breach Investigations Report
4- Symantec Internet Security Report 2014

Advanced Threat Protection

Symantec has an extensive history of delivering a broad array of superior advanced threat protection technologies that provide much more than just traditional antivirus protection. These solutions derive their powerful protection capabilities by being able to take advantage of a variety of proven Symantec technologies and services, including the following:

- **Symantec Insight™** uses reputation security technology that tracks billions of files from millions of systems to identify new threats as they are created. It utilizes contextual awareness to separate files at-risk from safe files for faster and more accurate malware detection.
- **Symantec SONAR™** uses artificial intelligence and sophisticated behavioral analysis to detect emerging and unknown threats. It monitors over 1,400 file behaviors as they execute in real-time to identify suspicious behavior and remove malicious applications before they can do harm.
- **Symantec Skeptic™** employs a heuristic technology to detect new and emerging threats, as well as variations of existing threats. Its predictive analysis combines with real-time link following to block emails with malicious, shortened links before the emails can even reach users.
- **Symantec Global Intelligence Network (GIN)** is the largest and most sophisticated civilian security intelligence network in the world. Leveraging more than 64.6 million attack sensors across the globe, it fuses the analysis of malicious activity across the entire threat landscape.
- **Symantec Vantage**, previously known as Symantec Intrusion Prevention (IPS), monitors network behavior and traffic to identify malicious activity in real time. It analyzes all inbound and outbound communications for data patterns characteristic of typical attacks.
- **Dynamic IP and URL Blacklist** capabilities inherent to Symantec threat protection solutions are powered by GIN, Symantec DeepSight, and the Symantec STAR research team. DeepSight Intelligence provides timely, relevant, actionable intelligence about emerging threats, threat sources, and vulnerabilities based on deep, proprietary analyses of billions of events from GIN.

Advanced Threat Detection

In addition to superior network protection, organizations need the ability to detect targeted attacks and advanced threat campaigns that somehow manage to infiltrate the network. Effective detection requires the ability to work across all ports and protocols.

To provide the level of advanced threat detection that organizations need, Symantec has developed Cynic™, a cloud-based dynamic malware analysis service that investigates and identifies unknown threats and potentially risky files. Cynic is being integrated into numerous security products in order to extend best-in-class protection with enhanced detection of malicious files. Cynic works to detect, not block content. It doesn't try to stop the entry of any inbound traffic that hasn't been already blocked by protection controls. Rather, it sends a copy of all inbound traffic to a secure cloud-based execution sandbox for analysis where Cynic can determine whether or not the traffic contains any suspicious or malicious content. This allows Cynic to quickly detect advanced threats without hindering user productivity or business operations,

To detect complex malware, the sandbox simulates real technology environments across multiple operating systems using a wide range of applications that malware attacks frequently exploit. Different combinations of operating systems and application versions are used in case the content contains malware that targets specific versions. As part of this content execution, Cynic mimics typical end user behavior within these different environments in an attempt to draw out any potential malicious actions or activity from the content itself.

Initially, Cynic executes the content within a virtualized environment for behavioral analysis. However, to avoid discovery, cybercriminals sometimes program advanced threats to remain inactive if they detect they've been placed in a virtual environment. One of the core benefits of utilizing a cloud platform for malware detection is that if Cynic detects behavior that suggests the content is virtual-machine-aware, it will move the content to a physical machine environment for analysis. Termed "bare metal execution," this physical environment analysis further broadens the investigative scope of Cynic to allow it to detect even the most intelligent malware that has been designed to evade analysis within virtual sandbox environments.

Additionally, even if the content itself remains inactive within the sandbox's physical or virtual environment, Cynic monitors and analyzes any attempts it makes to move within the environment or to communicate with a control server or other machines.

As part of its investigation, Cynic leverages the behavioral analysis capabilities of SONAR, heuristic analysis of Skeptic technology, and the vast real-time security intelligence of GIN. Cynic can observe both user mode and kernel mode convictions, therefore covering a very broad range of suspicious or malicious behaviors.

Using the security intelligence from GIN, Cynic also provides administrators and security experts a detailed report that includes rich contextual information relevant to analyzed content, giving them a broader vision of suspicious activity within their network. Similarities between analyzed files and other emerging threats are examined, providing organizations with the additional data around the behavior, file name and download location. This data can then be used to further help remediating any security event. ,

Since Cynic performs its analyses within the cloud, it can quickly adapt, update, or revise analyses based on the way potential malware behaves or evolves in order to try to avoid detection. An additional significant advantage of being cloud-based, Cynic can leverage Symantec's vast cloud computing resources and services to simulate a much wider range of behaviors, as well as return a verdict significantly faster than competing solutions. In fact, compared to the hours it takes other offerings to return a verdict on potential malware, Cynic guarantees a response time of 15 minutes. In the vast majority of cases, Cynic will return a verdict much faster than even that.

Key differentiators for Cynic advanced threat detection

While other vendors have somewhat similar security offerings that execute suspicious content in virtual sandbox environments in order to detect potential malware, the Cynic technology from Symantec provides four key differentiators:

- **Cloud-based Execution Sandbox** – Operating in the cloud gives Cynic several significant advantages over other offerings, including the processing power to utilize a range of technologies to analyze behavior on a significantly broader array of OS and application configurations to detect suspicious communication activity. Additionally, since Cynic only operates within Symantec's secure cloud environment, cybercriminals are unable to look for ways to elude Cynic through probing and testing their malware against it.
- **Bare-metal Execution** – The ability to automatically move suspicious content to a physical environment for analysis enables Cynic to detect virtual machine-aware advanced threats that have the ability to evade detection in virtual-only sandbox solutions.
- **Smaller Exposure Window** – The cloud processing power of Cynic also enables Symantec to guarantee a 15 minute or less detection verdict, giving potential malware a much small window of opportunity to infect, proliferate and inflict damage.
- **Relevant and Contextual Security Intelligence** – The rich contextual and relevant security intelligence that Cynic delivers via its integration with Symantec GIN gives administrators and security managers greater insight into what is going on inside their network and to be more proactive in acting against legitimate threats.

Advanced Threat Response

One of the major obstacles that prevents organizations from effectively responding to detected threats is the sheer volume of threat alerts that they have to sift through. Administrators and security managers can spend hours analyzing, correlating and prioritizing excessive alerts that might not pose an actual threat. It's not a simple task to determine which events pose an actual threat and which threats need immediate attention or can be put on the back burner.

Even when threats have been properly prioritized, it's often difficult to know the best way to respond to a threat. For example, an administrator might receive a gateway alert about a malicious file heading toward multiple target endpoints. How does the administrator determine which target machines to work on first? Hours can be wasted investigating one set of machines, only to find that those machines' endpoint protection software already remediated the threat. They might later discover that the remaining machines actually were infected and may have already propagated the malware to other vulnerable targets, igniting a chain of significantly damaging and costly activity.

To address these malware response challenges, Symantec has developed Synapse™, a new technology that automatically correlates and coordinates threat intelligence between an organization's gateway, email, and endpoint security systems. Through its integration with Symantec Cynic technology, it receives notifications when an advanced threat has managed to bypass network security and then communicates with the different network control points to determine if they've encountered the threat and if those control points have taken any steps to remediate it. This gives organizations more real-time visibility to what advanced threats are actually doing on their network and the extent of their reach.

As an example, if a file containing a new advanced threat was analyzed by Cynic, it would determine that the file does indeed contain malware and notifies Synapse of the threat. Working at the gateway control point, Synapse first determines the malicious file's destination, which might be a particular user's laptop. Synapse then communicates with the endpoint security solution running on that laptop to determine if it has seen the file and if any action has been taken against it. If the endpoint security solution has already blocked or remediated the threat, no alert is sent to the administrator since no additional action needs to be taken. The event will simply be logged so the administrator can see what happened and how it was resolved.

In that single scenario alone, Synapse can save administrators hours of wasted time investigating an attack that has already been addressed. The cumulative effect of automatically responding to and checking on the status of these types of incidents enables Synapse to dramatically reduce the number of alerts that administrators would otherwise receive, sort through and respond to. This workload reduction can significantly save organizations time and energy.

Even more importantly, through its ability to communicate and coordinate with gateway, endpoint and email control points, Synapse can accurately alert administrators to threats that really do need attention and prioritize those threats in a manner that enables them to respond in the most effective and efficient manner. For example, when Synapse communicates with the different control points about a malicious file that has been detected, it not only can check with the email control point to see if it has seen the file before, but it can ask who sent the file, who received it, and what was the email's subject. That additional information and context can dramatically expand the view of what needs to be done, while enabling more accurate prioritization of events.

As a case in point, consider the situation where the email security solution happens to respond back that it previously saw the malicious file and that it was sent to 10 people and those 10 people don't have Symantec Endpoint Protection installed on their devices. The magnitude of the event significantly escalates from one endpoint almost being infected to potentially 10 endpoints being infected. The prioritization of the

event rises to the top as administrators realize that they might be dealing with an outbreak, as well as a targeted assault. This coordinated communication of threat identification and contextual insight enable organizations to more accurately prioritize events in a manner that allows them to more effectively focus their energy and efforts on events that need attention.

Key differentiators for Synapse advanced threat response

Point product security solutions that try to facilitate threat response often actually complicate and slow down response efforts through their inability to provide comprehensive, coordinated insight into the actual progress and remediation status of advanced threats. Synapse technology from Symantec accelerates, simplifies, and optimizes advanced threat response through the following key differentiators:

- **Coordinated Communication Across Multiple Control Points** – Symantec Synapse technology enables organizations to respond faster to elusive advanced threats through its ability to integrate and correlate security information across gateways, endpoints, and email. It gives administrators and security managers the situational awareness and threat severity they need to quickly analyze security events, and then accurately raise or lower the priority levels of events so they can better maximize and focus their efforts on the most critical, unresolved events for further investigation and response.
- **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 not only determine if they've encountered the threat, but if it has already been remediated. If the threat has already been resolved, it is logged but no alert is generated, reducing the volume of alerts administrators receive to only those that really need attention.
- **Unified View of Security** – Through a unified management interface, 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 at the gateway, email and endpoints, 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 Cynic and Synapse leverage Symantec GIN to provide organizations global context on potential threat activity occurring within their network by giving them access to security intelligence on similar advanced threat activity occurring in other parts of the world.
- **Coordinated Forensic Analysis** – The Symantec Cynic and 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.

Unified Advanced Threat Protection, Detection, and Response

No matter how much an organization invests in trying to keep threats from breaking through their protective security layers, it's only a matter of time before an advanced threat manages to slip past their defenses undetected. To effectively combat advanced threats, organizations need to augment their threat protection with advanced threat detection and advanced threat response. Only Symantec offers a comprehensive, unified approach to advanced threat protection, detection and response that leverages Symantec Cynic and Symantec Synapse technologies to automatically correlate security intelligence and coordinate security efforts across an organization's gateway, email, and endpoint control points.

The Symantec approach enables organizations to investigate and prioritize potential threats more quickly and accurately. It optimizes their ability to analyze, correlate, and prioritize security events, so they know where to focus their efforts. It reduces operating expenses and increases security team effectiveness by eliminating irrelevant and resolved alerts, providing accurate threat prioritization and fostering the situational awareness needed to quickly analyze only those events that need further investigation. It combines analysis of an organization's own local network activity with security intelligence from Symantec's massive global intelligence threat network to deliver the detailed, relevant, and actionable data needed to make smart decisions and respond to the most critical security events in a quick and effective manner.

The Symantec approach to protecting, detecting, and responding to advanced threats provides faster, more reliable security event information and accurate threat prioritization in a way that saves organizations more time, effort, and cost, while enhancing their overall security posture.

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 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenue of $6.7 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

Copyright © 2014 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
11/2014 21341799