Symantec Advanced Threat Protection 2.3: Platform

Advanced Threat Protection

The Problem

Today's advanced persistent threats leverage endpoint systems in order to infiltrate their target organizations, whether by exploiting vulnerabilities, through social engineering, via phishing websites, or some combination of all of these. And once inside the victim's infrastructure, targeted attacks use endpoint systems to traverse the network, steal credentials, and connect with command-and-control servers, all with the goal of compromising the organizations' most critical systems and data.

This problem is only growing. Over 430[1] million new pieces of malware were found in 2015. In addition, Symantec saw a 125% increase in zero-day vulnerability and 55% increase in targeted attacks from 2015. Today, preventing threats is simply not enough. Attackers are moving faster. At some point, they will find their way through. A recent report[2] shows that it can take organizations 120 days on average to remediate found vulnerabilities. Undetected threats and slow remediation can leave customers' organization exposed and result in significant cost, including but not limited to the loss of intellectual property and sensitive data, financial losses, reputation damage. On top of that, significant amount of alerts and the user impact from infection could raise IT overhead and disrupt customers' business.

Solution Overview

Symantec Advanced Threat Protection Platform

Symantec Advanced Threat Protection (ATP) solution is a unified platform that **Uncovers, Prioritizes, Investigates, and Remediates** advanced threats across multiple control points from a single console. Each control point represents a vector which attackers can take advantage of to invade an organization. There are four ATP modules today- ATP: Endpoint, ATP: Network, ATP: Email, and ATP: Roaming. Each of these modules sends event information from different control points to the ATP platform that correlates and prioritizes all the malicious events, allowing security analysts to focus on what matters the most.

Symantec ATP uncovers stealthy threats that others miss by leveraging one of the world's largest civilian threat intelligence networks combined with local customer context. Incident responders are notified as soon as an organization has been identified as a target of an active attack campaign. Symantec ATP also provides customers with granular attack details and allows them to remediate all instances of threats in minutes. It is the first solution in the market that can detect, prioritize, and remediate advanced threats across multiple control points, through a single console with no new endpoint agent to deploy.

Symantec

Key Features and Benefits

- Detect, prioritize, investigate, and remediate threats across multiple control points in a single console
- Uncover stealthy threats across endpoint, network, email, and web traffic
- Prioritize what matters the most by correlating across events from all Symantec-protected control points for complete visibility and faster remediation
- Contain and remediate any attack artifact in minutes, with a single click
- Customize incident response flow with public APIs and third-party SIEM integration

Uncover Advanced Threats across Multiple Control Points

See all threat data in one place

As a unified platform, Symantec Advanced Threat Protection (ATP) solution provides a consolidated view of all malicious activities across multiple control points. Today, email and web continue to be the most common vectors of malicious attacks with all attacks destined for the endpoint. Symantec has four ATP modules to provide advanced protection and complete threat visibility into IT environment:

1. ATP: Endpoint

Provides Endpoint Detection and Response (EDR) capability without adding new endpoint agent; leverages the best-of-breed threat prevention product, Symantec Endpoint Protection. Customers can hunt for any Indicators-of-Compromise (IoC) across their endpoints and remediate all instances of threats in minutes, with one click.

2. ATP: Network

Uncovers stealthy threats with multiple technologies, including file reputation analysis, IPS, and a cloud hosted sandboxing and detonation. Customers can search for IoC across network; blacklist or whitelist any files or URLs once identified as malicious.

3. ATP: Email

Protects against targeted attacks and advanced threats via email, such as spear-phishing. Leverages cloud-hosted sandbox and detonation, and Symantec Email Security.cloud to expose granular threat data from malicious emails. Tightly integrated with third party SIEM, so that customers can quickly respond to attacks.

4. ATP: Roaming

Protects users from advanced threats when they are browsing the internet outside of corporate network. It detects and remediates advanced threats even in encrypted traffic by leveraging cloud hosted sandbox. Get deep threat visibility into web traffic, no matter where the users are.

Sandbox with both physical and virtual execution

Symantec uncovers today's most complex targeted attacks with our Cynic™ technology, a cloud-based sandboxing and payload detonation capability built from the ground up. Cynic leverages advanced machine learning combined with global threat intelligence to uncover even the stealthiest and the most persistent threats. It provides a detailed detonation report consisting of process and stack trace as well as any network trace, including command and control call traffic information, so that all relevant information is available to the incident responder from a single pane of glass and attack components can be quickly remediated. Today, 28 percent of advanced attacks are "virtual machine-aware", that is, they don't reveal their suspicious behaviors when run in typical sandboxing systems. To combat this, Cynic has built-in anti-evasion technology that can mimic human behavior. It can also execute suspicious files on physical hardware to uncover those attacks that would evade detection by traditional sandboxing technologies.

Quick search for Indicators-of-Compromise

A new feature, Dynamic Adversary Intelligence, is also included in Symantec Advanced Threat Protection. It is a high-value feed of actionable intelligence data extracted from comprehensive investigations into targeted attacks. It can quickly identify whether

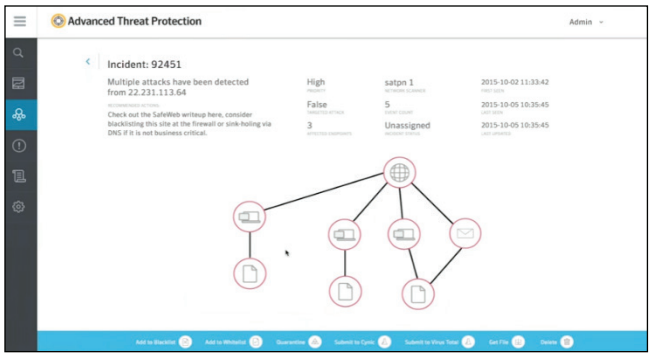
customers' organizations are being targeted by threat actors, so that they can respond to targeted attacks more appropriately. The new Dynamic Adversary Intelligence feed automatically searches for known Indicators-of-Compromise across the entire environment, reducing the time for customers to uncover targeted attacks.

Automatically Prioritize Critical Events

One of the challenges that incident responders are facing today is that they are overwhelmed with too many alerts, resulting in huge incident response ques. Symantec Advanced Threat Protection solution leverages our exclusive Synapse correlation technology that aggregates suspicious activities across all installed control points. Synapse automatically prioritizes threats based on various attributes, including the type, scope, complexity of a threat and more. It cuts through the noise of random alerts, allowing customers to focus on what matters the most and "zero in" on just those specific events of importance. Customers will also be immediately alerted if there are systems that remain compromised and require immediate actions.

Remediate Complex Attacks in Minutes

Once an event has been identified as malicious, Symantec Advanced Threat Protection allows customers to remediate all instances of the threat in minutes. With a single click of a button, customers can quickly delete a file, whitelist or blacklist a file or a domain, or isolate an endpoint from communicating to the rest of the organization and the internet. Symantec ATP platform also provides unique visualization of related Indicators-of-Compromise of an attack, including a complete graphical view of how all Indicators-of-Compromise are connected to each other. An analyst can easily find out the impact of an incident and see all files used in a particular attack, all IP addresses and URLs where the file was downloaded from, and all affected registry keys with the graphical view. He can then remediate any of these attack artifacts, with one single click, effectively containing the spread of an attack.



Leverage Existing Investments

Maximize your Symantec investments

Symantec Advanced Threat Protection (ATP) solution leverages Symantec Endpoint Protection and Symantec Email Security. cloud to gather threat events detected from these two market-leading products. If customers are currently on Symantec Endpoint Protection, the Symantec ATP Endpoint module would provide the Endpoint Detection and Response (EDR) capability without the need for them to deploy any new endpoint agent. And if customers are currently on Symantec Email Security.cloud, they can get Symantec ATP Email module to protect against targeted attacks and spear-phishing campaign without deploying new agent.

Leverage existing Non-Symantec investments

Customers often have existing security products for incident response and security monitoring. Symantec Advanced Threat Protection exports rich intelligence into third-party Security Incident and Event Management Systems (SIEMs). With public API, customers can leverage the products they have already invested in to conduct investigations. Symantec Advanced Threat Protection is also now integrated with Splunk and ServiceNow, the two popular SIEM and workflow products, to facilitate out-of-the-box use of our APIs. Hence, customers can optimize and customize their own incident response flow, maximizing their existing investment.

Optimize Security, Minimize Risk, Maximize Return with Symantec Services

Access security experts who can provide training on Symantec Advanced Threat Protection, proactive planning and risk management as well as deployment, configuration and assessment solutions for your enterprise.

To learn more, visit go.symantec.com/services

Footnotes

1. Symantec Internet Threat Report, Volume 21, April, 2016

2. Dennis Technology Lab, December 2015

About Symantec

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