Symantec Advanced Threat Protection 2.3: Roaming

Advanced Threat Protection

The Problem

Today's advanced attacks hide themselves on legitimate websites, leverage new and unknown vulnerabilities, and enter targeted organizations via HTTP or HTTPS. These attacks are designed to evade typical network-based security approaches, allowing them to infiltrate the victim's infrastructure, where they can then compromise critical systems and data. And even in the case where a network security product is aware of such an attack, the specific attack details are often buried in a long list of lower-priority alerts from the product, making it very challenging for an analyst to discover the true problem.

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. A recent study showed that 86% of websites contain at least one serious vulnerability[2]. Today, preventing threats is simply not enough. Attackers are moving faster. At some point, they will find their way through. While organizations are seeking for ways to secure their network, roaming users could be another issue. 70% of organizations support BYOD[3], implying a great chance that advanced threats can infiltrate into endpoints while end users are browsing the internet outside of corporate network. 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: Roaming

Symantec Advanced Threat Protection (ATP) solution **Uncovers, Prioritizes, Investigates, and Remediates** advanced threats across endpoint, network, email, and web traffic in one single console. Symantec Advanced Threat Protection: Roaming is one module of the broader Symantec ATP solution. It's a cloud-based solution that provides full visibility into customers' web traffic, protecting their users wherever they are browsing the internet, even when they are outside of the corporate network. The product uses layered defenses that include Intrusion Prevention, AV, File Reputation, and can automatically send suspicious files to Symantec Cynic™ sandboxing system for rapid detection of the most complex and the stealthiest advanced attacks. It can also decrypt HTTPS traffic to uncover malware in encrypted traffic. And, if customers also have Symantec Advanced Threat Protection: Endpoint module, Email module, or Network module, the threat events detected from these Symantec-protected control points will then be correlated and prioritized, allowing customers to focus on what matters the most and providing a consolidated view of advanced attack activities in one place.

Symantec

Key Features and Benefits

- Protect users from advanced threats when they are browsing the internet outside of corporate network
- Detect and remediate advanced threats in the encrypted traffic and protect against https attacks
- Uncover stealthy threats in real-time with multiple technologies, including reputation analysis, IPS, AV, and our unique cloud-based sandboxing and detonation
- Prioritizes what matters the most by correlating across events from other Symantec-protected control points to greatly reduce the number of incidents that a security analyst needs to examine

Uncover Advanced Attacks

Advanced protection for roaming users

Symantec Advanced Threat Protection: Roaming uncovers and blocks advanced threats that attempt to infiltrate the organization through web traffic. Today's network protection solutions typically rely heavily on sandboxing capabilities to find attacks. By contrast, Symantec Advanced Threat Protection: Roaming includes a complete set of protection technologies in addition to Symantec's innovative sandboxing and detonation capabilities.

Symantec ATP: Roaming leverages reputation-based technology to identify suspicious files based on when they were first seen, their prevalence across the Internet, as well as a number of other sophisticated techniques. The product also detects and blocks advanced threats embedded in the web traffic and helps locate machines outside the network that are communicating with malicious Command-and-Control servers. Powered by one of the world's largest civilian threat intelligence networks, Symantec provides customers with the most up-to-date visibility into new attack sources of both HTTP and HTTPS encrypted traffic.

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. Symantec ATP: Roaming automatically submits suspicious files entering the organization to Cynic, which leverages advanced machine learning-based analysis 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 executes suspicious files on physical hardware to uncover those attacks that would evade detection by traditional sandboxing technologies.

Automatically Prioritize Critical Events

Symantec Advanced Threat Protection: Roaming is part of the full Symantec Advanced Threat Protection (ATP) offering, which also includes endpoint, email, and network modules. With Symantec Synapse correlation technology, Symantec ATP can aggregate suspicious activities across all installed control points by leveraging existing installations of Symantec Endpoint Protection and Symantec Email Security.cloud.

Symantec's correlation technology automatically prioritizes threats based on various attributes, including the type, scope, complexity of a threat and more. For example, a customer's web security product detects that a suspicious file was delivered to an employee's machine. Traditionally, the security analyst would need to manually visit the endpoint machine that received the suspicious file to ensure that it was properly blocked or removed from this computer. In contrast, if Symantec Advanced Threat Protection: Roaming detects the web traffic ingress of a potential threat, the product will leverage correlation technology to automatically determine if that threat was blocked by Symantec Endpoint Protection on the endpoint. If so, the attack will be prioritized much lower on the list for the analyst, drastically reducing the number of security events analysts need to examine.

Leverage Existing Investments

The product also exports rich intelligence into third-party Security Incident and Event Management Systems (SIEMs) via the ATP-Platform. For example, it can export rich data such as “computer A downloaded file B.EXE from website C.COM,” rather than traditional security data such as “virus BAD.EXE detected.”

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

System Requirements

Processor: 2.66 GHz

RAM: 2GB

System Type: 32 Bit

Browser Clients for the UI

Microsoft Internet Explorer 11 or later

Mozilla Firefox 26 or later

Google Chrome 32 or later

Windows OS

Vista, 7, 8.1 and 10

Footnotes

1. Symantec Internet Threat Report, Volume 20, April, 2015
2. SC magazine, 2015
3. Bitglass BYOD Trends Report, 2016

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