4 Reasons to Upgrade to Symantec Intelligent Endpoint Solution

Take a Smarter Approach to Stopping Advanced Attacks

Get Ahead of Advanced Attacks

The majority of advanced attacks, and the threats they deliver, are coming faster and with more complexity. They enter stealthily, using highly customized tools and intrusion techniques (ransomware, watering hole, and zero-day attacks) to deliver malware. In 2015, Symantec™ discovered more than 430 million new pieces of malware—or roughly one million new pieces of malware each day. This is why your endpoint protection is a crucial component of your security program. Relying solely on antivirus or any single protection technology is shortsighted; it's just too easy for determined attackers to breach. At some point, attackers will make their way in. To get ahead of advanced attacks, you must go beyond threat prevention to include threat detection and response.

Start With a Solid Foundation

Your Symantec™ Endpoint Protection, proven to be the most effective way to block the majority of threats, is a solid threat-prevention foundation. And blocking advanced threats **before** they infect your endpoints is vital to your security. Make sure you're taking full advantage of your Symantec Endpoint Protection by activating **all** of its protection layers, like reputation analysis, real-time behavior monitoring, Intrusion Prevention System (IPS), firewall, and application control. By properly configuring your Endpoint Protection product, you can neutralize zero-day and unknown threats with 99.99 percent accuracy.

Although your Endpoint Protection might be doing a great job, blocking threats is simply not enough. Attackers are getting smarter and moving faster. If a stealthy threat slips by, don't become a crime statistic. Upgrade to the Symantec Intelligent Endpoint solution so your modern endpoint security can:

1

Detect anomalies across all control points

The potential cost of a data breach can reach nearly $4 million dollars according to a 2016 study. Therefore, when a threat slips past your endpoint security, you must quickly detect and remediate it. Most of the time, threats that hit your endpoints are the stealthiest type of malware and are often part of a long-term attack campaign. That's why it's important to know the origins of the attack with as many details as possible.

Symantec Advanced Threat Protection is the most effective solution of its kind for uncovering threats across key attack vectors—endpoint, network, and email. When threats are detected, an event alert helps you identify high-risk users and actively infected systems; who is downloading malware or suspicious files; the origins of the attack; which assets have been impacted; and the spread across all control points. Symantec uses a robust cloud-based sandboxing and payload detonation service to arrest suspicious files in real time, covering the most popular file types used in targeted attacks and executing them in physical and virtual sandboxes. This is a crucial step for advanced threats that may exhibit different behaviors in different environments.

Using a single console, you cut through thousands of instances of noise, easily prioritize critical events, and focus on threats that matter most to you. We provide a full body of evidence on the attack with our unique Synapse™ correlation technology. You can also investigate and search for attack artifacts—by file hash, registry key, or the source IP address and URL—across your entire infrastructure.

2

Remediate threats from complex attacks with just one click

When threats are detected in your IT environment, you can quickly remediate them—even those from a complex attack. Symantec Advanced Threat Protection rapidly restores normal operations after targeted attacks by containing and remediating all traces of threats in minutes. Our Endpoint Detection and Response (EDR) technology helps you see all data in one place, including files used in a particular attack, originating email addresses, and IP addresses where employees downloaded the file. Quickly remediate any of these artifacts with just one click, decreasing exposure to potential risks and controlling damage from spreading attacks. And because Advanced Threat Protection is integrated with your Endpoint Protection product, you can achieve all of this without deploying new endpoint agents.

3

Preempt future attacks with smarter risk assessment

Symantec helps prepare you for attacks **before** they happen. Symantec Risk Insight provides a comprehensive view of your internal risk posture and your extended enterprise, including your customers, benchmarked against peers in your industry. With an executive dashboard, you can quantify the effectiveness of your security program, track improvements over time, and justify future investments. The drill-down capabilities and advanced analytics help you pinpoint specific weaknesses, such as high-risk users and endpoints, suspicious applications, and unpatched vulnerabilities, and develop plans to close your vulnerabilities.

Integrated with Symantec Endpoint Protection, Risk Insight provides actionable insights to help you make smarter security investments without requiring additional agents, software, or hardware provisioning. It streamlines complex manual assessments with an automated cloud-based service, making risk assessment a simpler process. With Symantec Risk Insight, you can be more proactive in protecting against advanced attacks.

4

Stop data breaches from lost or stolen endpoints

The Symantec Intelligent Endpoint solution stops cyber threats **and** “physical” threats of endpoints. If your devices are physically lost or stolen, Endpoint Encryption is essential. It’s the best way to protect the data on laptops, desktops, and removable media because even if an endpoint goes missing, the data remains safe.

Symantec Endpoint Encryption uses a preboot passphrase to protect a machine and prevent it from booting up until the correct phrase is entered. Without the passphrase, the information on the device remains scrambled, preventing outsiders from accessing data. With an intuitive central management platform, Symantec helps administrators deploy and manage encryption on every end-user device or prove a device was encrypted should it go missing.

Maximize Your Endpoint Protection Solution

Neither traditional antivirus security, nor any single protection technology, can keep pace with advanced attackers, which puts organizations of all sizes and industries at risk. To stay ahead of advanced attacks, blocking them is not enough. The most effective strategy is to maximize your Symantec investment with our Intelligent Endpoint solution. Symantec Intelligent Endpoint is a dynamic, multilayered approach designed to block the majority of threats before your endpoints are infected; detect the stealthiest threats across all control points and remediate them within minutes; provide an automated risk assessment to help you understand your risk exposure; and deflect critical attacks. Working together, these technologies provide multiple layers of protection to secure your organization and keep your sensitive information safe.

It’s time to stop putting out fires and start putting up better defenses. With Intelligent Endpoint from Symantec, you can focus on what matters most to you.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

Symantec Corporation World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934

www.symantec.com

For specific country offices and contact numbers, please visit our website. For product information in the U.S., call toll-free 1 (800) 745 6054.

07/16 21367206