SYMANTEC™ ADVANCED THREAT PROTECTION

Uncover, prioritize, and remediate today's most advanced attacks

THE PROBLEM

TODAY'S INFORMATION SECURITY PROFESSIONALS FACE A MORE COMPLEX AND RAPIDLY CHANGING THREAT ENVIRONMENT THAN EVER BEFORE.

MORE THAN

28%

OF MALWARE IS VIRTUAL MACHINE AWARE

(able to detect a host hypervisor and stop itself from running and being detected)

IN 2014 THERE WAS A

40%

INCREASE IN ADVANCED ATTACKS

317M

NEW MALWARE CREATED

READ ON >>

SOURCE: SYMANTEC ISTR 20

Cybercriminals have the persistence and the patience to execute their plans over months and years. They employ sophisticated tactics to trick unsuspecting victims or otherwise infiltrate target organizations, and they customize each attack campaign as needed to achieve their goals.

Most of today's security products are not integrated – Security analysts need to examine many distinct sources of security data, or find some way to combine this information manually, and then hope they can "connect the dots" to get visibility into suspicious activity in their environment. As a result, many complex attacks remain undetected for months or even years.

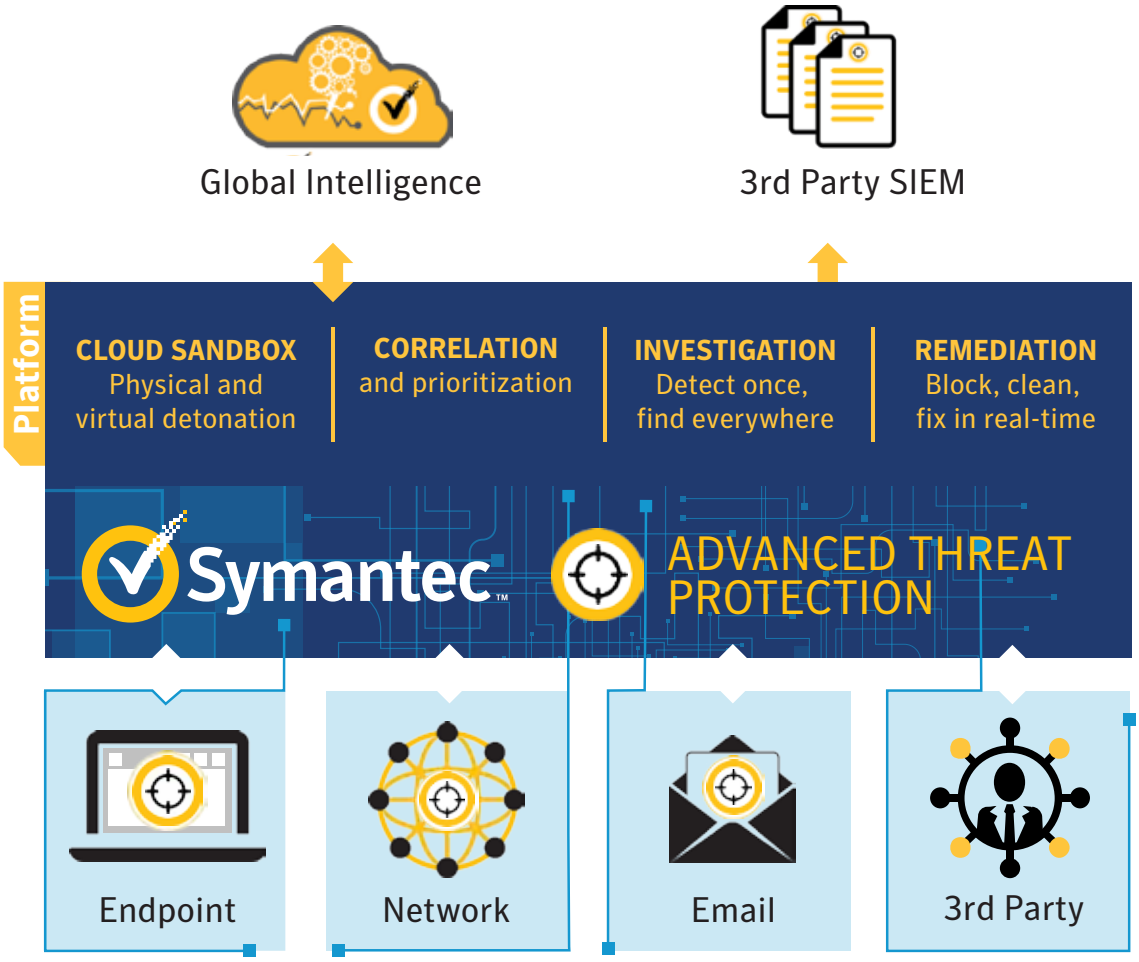
"Given the expanse and diversity of threats and techniques of motivated attackers, Gartner advises clients move away from detect-and-prevent security approaches toward detect-and-respond approaches."

Source: Gartner, Cool Vendors in Security Infrastructure Protection, 2015, Ray Wagner, Joseph Feiman, Avivah Litan, Neil MacDonald, Lawrence Orans, Peter Firstbrook, John Girard, Dionisio Zumerle, 27 April 2015

SYMANTEC™ ADVANCED THREAT PROTECTION

A Unified Solution Across Control Points

Symantec™ Advanced Threat Protection is a new unified solution to help customers uncover, prioritize, and quickly remediate today's most complex advanced attacks, across endpoints, networks and email. It leverages and enhances existing deployments of Symantec™ Endpoint Protection and Symantec™ Email Security.cloud, and does not require any new agents.



Symantec Advanced Threat Protection is a single unified solution that uncovers, prioritizes, and remediates advanced attacks. The product fuses intelligence from endpoint, network, and email control points, as well as Symantec's massive global sensor network, to stop threats that evade individual security products. It leverages your existing Symantec™ Endpoint Protection and Symantec™ Email Security.cloud investments, so it does not require the deployment of any new agents. You can deploy a new installation of Symantec Advanced Threat Protection and start to discover suspicious activity in under an hour.

Using the proven technology in Symantec™ Insight reputation based detection, Symantec™ SONAR behavioral analysis with the new Symantec Cynic™ sandbox and file analysis platform, Symantec Advanced Threat Protection provides better detection and prioritization than other vendors[1], allowing security analysts to "zero in" on just those specific security events of importance.

[1] Miercom, Symantec Advanced Threat Protection: Network, April 2015. http://miercom.com/pdf/reports/20150218.pdf

Symantec Synapse™

Prioritizing and investigating events and attacks is quicker and more effective with the new Symantec Synapse™ correlation technology, providing a single view of all advanced attack activity in your organization, across endpoints, networks, and email, and allows you to quickly search for relevant attack artifacts across all control points. Correlating network and email events with endpoint detections in this way will reduce the number of incidents a typical security analyst needs to examine–all without adding any new agents.

Symantec Cynic™

Uncovering advanced attacks is faster with Symantec Cynic™, an entirely new cloud-based sandboxing and payload detonation service built from the ground up to discover and prioritize today's most complex attacks. It leverages advanced machine learning-based analysis combined with Symantec's global intelligence, to detect even the most stealthy and persistent threats. Cynic sandboxing also executes suspicious files on physical hardware to uncover those attacks that would evade detection by traditional sandboxing technologies

THE MODULES

Symantec™ Advanced Threat Protection: Endpoint

Uncover, prioritize, and remediate advanced attacks across all of your endpoints whether they are inside or outside the network, adding Endpoint Detection and Response (EDR) capabilities to your existing investment in Symantec™ Endpoint Protection. Detect new threats with the Symantec Cynic™ sandbox, and with one click of a button, you can search for, discover, and remediate any attack artifacts in your organization. The Symantec Synapse™ correlation engine automatically matches events with Symantec™ Email Security.cloud and Symantec™ Advanced Threat Protection: Network, reducing the volume of security alerts and prioritizing the most significant threats.

Symantec™ Advanced Threat Protection: Network

Uncover and prioritize advanced attacks coming into the network and detect suspicious activity happening within your organization with file reputation analysis, behavioral analysis and intrusion prevention. The appliance automatically uses the Symantec Cynic™ sandbox for rapid detection of even the most advanced attacks. The Symantec Synapse™ correlation engine automatically matches events with Symantec™ Endpoint Protection and Symantec™ Email Security.cloud, reducing the volume of security alerts and prioritizing the most significant threats.

Symantec™ Advanced Threat Protection: Email

Uncover advanced attacks entering your organization through email, by adding unique targeted attack identification and Symantec Cynic™ sandbox detection capabilities to Symantec™ Email Security.cloud. Get manual analysis of new or unknown malware by Symantec analysts to determine the severity and scope of a targeted attack campaign. The Symantec Synapse™ correlation engine automatically matches events with Symantec™ Endpoint Protection and Symantec™ Advanced Threat Protection: Network, reducing the volume of security alerts and prioritizing the most significant threats.

WHAT MAKES SYMANTEC™ ADVANCED THREAT PROTECTION UNIQUE?

Uncover advanced threats across endpoints, networks, and email

Symantec Advanced Threat Protection provides a single console showing all suspicious events and attacks across the organization, allowing all data and intelligence Symantec Advanced Threat Protection knows about any attack, across endpoint, network, and email, to be shown in one place. Use the single console to search the entire environment for Indicators of Compromise and quickly retrieve any file from any endpoint for further analysis.

Prioritize what matters most

Symantec Advanced Threat Protection identifies suspicious activity, and in one console, prioritizes the security events that pose the most risk to the organization. Symantec Advanced Threat Protection includes our new Synapse cross-control-point correlation capability, and our new Cynic cloud-based sandboxing service, which helps Symantec Advanced Threat Protection to detect more threats faster than competing products. By correlating events from all control points, false positives are suppressed and it significantly reduces the number of incidents that security analysts need to investigate

Remediate fast

Symantec Advanced Threat Protection provides a powerful one-click containment and remediation capability that works with data across endpoint, network, and email control points. Security analysts can instruct Symantec Advanced Threat Protection to remove a specific file from all endpoints and to block any further downloads of that file. If the endpoint needs further analysis, the security analyst can quarantine it to prevent further network activity.

With Symantec Advanced Threat Protection, security analysts can now find and contain even highly complex attacks in minutes, rather than days, weeks or months – all from one console.

Leverages existing Symantec investments

Symantec Advanced Threat Protection enhances the value of our customers' existing Symantec investments, rather than requiring them to deploy and manage an entirely new set of offerings. The Symantec Advanced Threat Protection: Endpoint module leverages and enhances Symantec™ Endpoint Protection to detect new endpoint-based advanced threats – customers do not need to install any new agents on any of their endpoints. Similarly, the Symantec Advanced Threat Protection: Email module enhances the threat detection capabilities of Symantec™ Email Security.cloud.

Customers can purchase our ATP solution for any combination of the three control points that they choose, endpoint, network or email.

Financial Services

Under constant threat of attack, and need rich intelligence to make decisions fast when evidence of comprise has been detected? Use Symantec™ Advanced Threat Protection to uncover complex attacks targeting your data and customer records.

Healthcare

Cybercrime in healthcare has increased at an alarming rate. Security has never been more critical. Symantec™ Advanced Threat Protection will uncover, contain and remediate advanced attacks in minutes, not weeks or months, protecting patient care data from being exposed.

Manufacturing

Manufacturers need to secure critical assets as they move into a new, connected era. Symantec Advanced Threat Protection brings together all suspicious activity across all control points, and prioritizes in one place those events that pose the most risk to an organization before impact to production, safety, and ultimately revenue.

Oil & Gas

As a prime target for attacks, you need advanced security. Leverage an integrated, unified platform to uncover, prioritize and remediate advanced threats and zero-day attacks.

Public Sector

Need advanced security to combat threats from hacktivists? Symantec Advanced Threat Protection leverages and enhances your Symantec™ Endpoint Protection and Symantec™ Email Security.cloud, and does not require any new agents to make sure public sector clients are protected against complex advanced attacks.

Retail

Managing parts of your network remotely and trying to protect against the latest sophisticated attacks? Symantec Advanced Threat Protection provides a single prioritized view of all advanced attack activity in your organization, helping you identify compromised systems and instantly remediate them.

LEARN MORE ABOUT SYMANTEC ADVANCED THREAT PROTECTION AT

symantec.com/advanced-threat-protection

or contact your Symantec Account Representative.

350 Ellis Street | Mountain View, CA 94043 | **symantec.com**