ESG Lab
First Look

Enterprise Strategy Group | Getting to the bigger truth.™

Symantec Advanced Threat Protection: Integrated, End-to-end Security

Date: October 2015 **Author:** Tony Palmer, Senior ESG Lab Analyst

Abstract: *This report provides a first look at the key attributes of Symantec's Advanced Threat Protection (ATP) with a focus on how it can enable an organization to prevent, detect, and respond to advanced persistent threats across multiple control points in the ecosystem, in real time.*

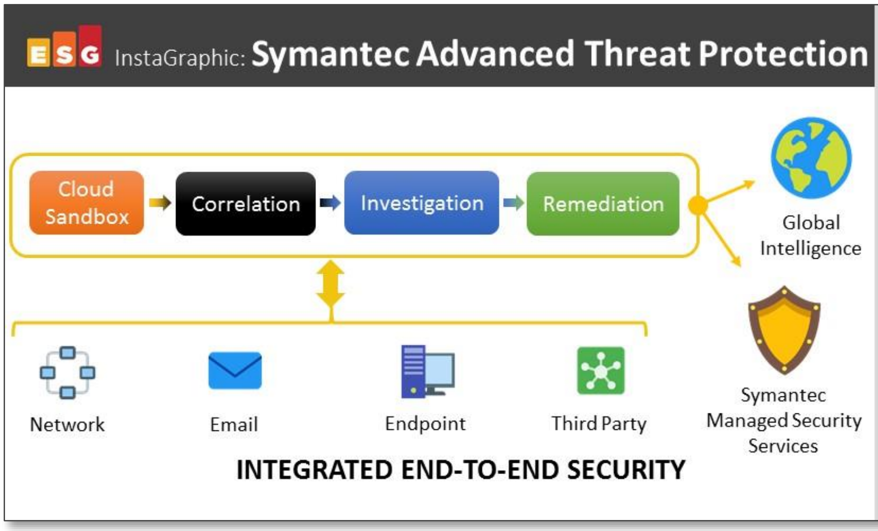
According to ESG Research:[1]

46%	Percentage of respondents who believe *security/risk management initiatives* is one of **the business initiatives** that will drive the most technology spending within their organization in 2015.
34%	Percentage of respondents who consider *information security initiatives* to be one of **the most important IT priorities** within their organization in 2015.

Symantec Advanced Threat Protection

The threat landscape is becoming increasingly dangerous, with targeted attacks on the rise and publicly disclosed data breaches occurring more frequently. Cyber-criminals have become adept at creating new, hard to detect methods of infiltrating data infrastructures. Advanced malware attacks wreak havoc in many ways, from stealing data to shutting down operations. Today's attacks are far more sophisticated and difficult to identify than they have ever been before, and are more than standalone network, endpoint, and e-mail security products can handle on their own. Symantec Advanced Threat Protection (ATP) is designed to help customers uncover, prioritize and remediate advanced attacks across endpoints, networks and email. The solution correlates alerts and intelligence across a range of security technologies with the goal of delivering comprehensive attack prevention.

Symantec's integrated approach offers organizations the benefits of multiple, diverse security technologies working together to simplify the complex fight against advanced threats.


ESG InstaGraphic: Symantec Advanced Threat Protection
Cloud Sandbox
Correlation
Investigation
Remediation
Global Intelligence
Symantec Managed Security Services
Network
Email
Endpoint
Third Party
INTEGRATED END-TO-END SECURITY

Why This Matters

- Cyber-criminals have become adept at creating new, hard to detect hacks and the threat landscape is becoming increasingly dangerous.
- ESG Lab confirmed that Symantec's ATP can halt the spread of malware and initiate immediate damage reparation from a single pane of glass.
- End-to-end solutions like Symantec's can be extremely effective against advanced threats.

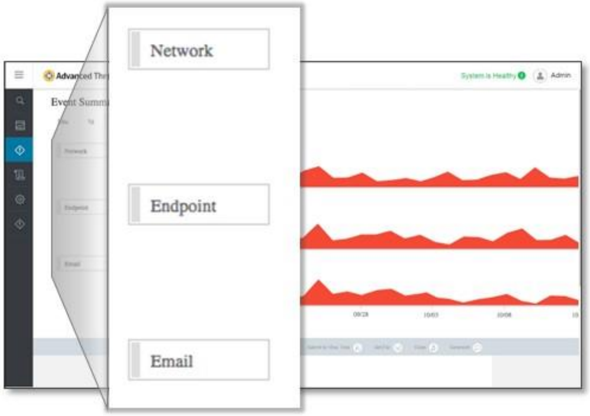
Symantec ATP operates via a single console and works across endpoints, networks, and e-mail, integrating with Symantec Endpoint Protection (SEP) and Symantec Email Security.cloud—which means organizations do not need to deploy any new endpoint agents. Symantec says ATP is the only threat protection appliance that can work with all three sensors without requiring additional endpoint agents. With ATP, Symantec's goal is to deliver end-to-end threat protection—prevention, detection, and response—in a single pane of glass, offering more value to businesses than individual point products can offer. Symantec Advanced Threat Protection combines multiple layers of prevention, detection, and response:

- Symantec Advanced Threat Protection: Endpoint is designed to enhance an organization's deployment of SEP with new investigation and visibility tools. It provides the ability to search across all endpoint devices for files,

[1] Source: ESG Research Report, *2015 IT Spending Intentions Survey*, February 2015.

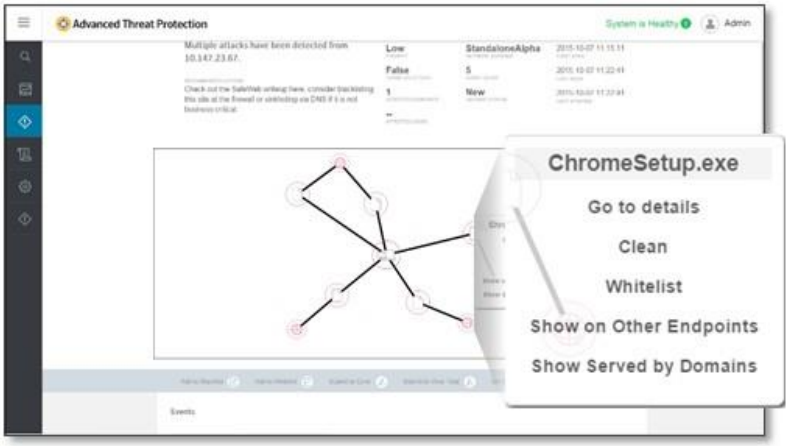
registry keys, or other indicators of compromise. Symantec ATP can search for, discover, and remediate threats with one click in the user interface.

- The Symantec Advanced Threat Protection: Network appliance detects threats as they enter the network. It runs a number of the core prevention technologies that are also included in SEP, including Symantec Insight, Symantec AV and the intrusion prevention system Symantec Vantage. It also utilizes the Symantec Cynic sandboxing technology to detect advanced attacks.
- Symantec Advanced Threat Protection: Email adds new sandbox detection technology and targeted attack identification to the Symantec Email Security.cloud platform. Symantec customers using Email Security.cloud are able to correlate their email security incidents with threat data from Symantec Endpoint Protection and the Symantec Advanced Threat Protection: Network appliance.
- Symantec Cynic is Symantec's new cloud-based sandboxing service which executes suspicious files on both virtual and physical hardware to pick up malware that can be missed by traditional sandboxing technologies.
- Symantec Synapse correlates information between endpoint, network, and e-mail security products which removes false positives and reduces the number of incidents and alerts.



ESG Lab Demo Highlights

ESG Lab had the opportunity to get hands-on experience with Symantec Advanced Threat Protection with a focus on its ability to prevent, detect, and respond to advanced threats and attacks. ESG Lab began with a look at the event summary, which showed events and incidents across network, endpoint, and e-mail control points over time. Selecting a specific incident enabled ESG Lab to drill down into the organism view.



The Organism View is a visual representation of the machines, files, and domains involved in the incident. Clicking on any object in the view brought up a details view with all data known about that object. ESG Lab selected a file and clicked ***Show on Other Endpoints,*** which provided all the locations where the selected file exists in the environment. Remediation is enabled via one-click blacklisting across the platform, endpoint quarantine capabilities, remote file acquisition or deletion from endpoints, all from within the ATP UI. This is extremely valuable as it can take hours to days to correlate and analyze this kind of data across standalone systems manually.

First Impressions

Everywhere you look in the IT infrastructure, there are security breaches. They can occur in smartphones and tablets, Windows desktops, and application servers. The consequences of these attacks can be devastating to operations, reputations, and bank accounts. The costs may include not just resuming operations and addressing security gaps, but legal liability and regulatory fines that can be a tremendous burden as well.

ESG Lab was pleased to find that Symantec Advanced Threat Protection provides a complete solution for detecting, preventing, and responding to advanced malware attacks. Its integrated configuration can offer accurate threat detection, and a key benefit is that it can help to stop malware from spreading and initiate immediate action to repair damage from a single pane of glass. Its integration with other Symantec security solutions without requiring installation of new agents delivers a holistic security platform for advanced protection at a low TCO.