ESG
Enterprise Strategy Group | **Getting to the bigger truth.™**

Solution Showcase

Operationally Efficient Advanced Endpoint Security with Symantec Endpoint Protection (SEP) Cloud

Date: September 2016 **Author:** Doug Cahill, Senior Analyst; and Leah Matuson, Research Analyst

Abstract: Today's threat landscape is ever constant—but always changing. It's no wonder that security is a top-of-mind concern throughout organizations across all industries. As with enterprises, midmarket organizations are not immune to the realities of today's threat landscape, and must be vigilant in protecting an increasingly mobile workforce, often with limited resources and funds. But how? Small and medium businesses should look to the cloud. As software-as-a-service (SaaS) applications have brought efficiencies to how we live, work, and transact business, the cloud also enables smaller organizations to leverage security-as-a-service for advanced, yet efficient endpoint security. Symantec Endpoint Protection Cloud offers a comprehensive set of features, including advanced threat prevention capabilities delivered efficiently from the cloud, representing a solution that organizations seeking efficacy and efficiency may want to consider.

The Trifecta of Endpoint Security Challenges

In today's dynamic business environment, one thing remains consistent—the ever-evolving threat landscape. Dealing with any number of ongoing threats requires vigilance, along with the use of advanced controls to protect against modern attacks, including ransomware. And while end-user mobility has provided the mobile workforce with the benefits of greater productivity and collaboration, it has also expanded the attack surface, complicating the task at hand for already under-resourced IT and security teams. Many organizations, especially small to medium enterprises, are not staffed with the appropriate security skillsets—in many cases a generalist, or even an office manager, is responsible for overseeing an organization's security needs.

Threat Landscape Spotlight: Ransomware

While a variety of attacks characterize today's threat landscape, the prevalence and insidious nature of ransomware make it a top-of-mind concern for all organizations. In fact, Verizon reports that ransomware incidents saw the largest jump as the malware type employed by cyber-criminals in 2015.[1] This trend continued into 2016 with the FBI reporting that such cyber-criminals generated $209 million in the first quarter alone.[2] As a highly transactional business, bad actors do not discriminate when choosing their targets, with midmarket organizations being regularly targeted with ransomware. The costs to infected organizations are often greater than the paid ransom, and can include impacts to end-user productivity, business operations, and already under-resourced IT and security teams.

[1] Source: *Verizon 2015 Data Breach Investigations Report*, April 2015.
[2] Source: http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/

Ransomware preys on human gullibility via targeted attacks that employ spear phishing and drive-by downloads to infect users' systems. New variants and strains are delivered as malware and exploits evade existing controls, creating a need for advanced preventative measures.

Mobility and an Expanding Attack Surface Area Put Data at Risk

Workplace mobility has given end-users the capability to work anywhere, at any time. And, while burgeoning bring-your-own-device (BYOD) initiatives have been added boons to employee productivity, they also mean that end-users can access corporate assets from outside of the secure confines of the network perimeter—and from multiple devices—putting those assets at risk. While BYOD gets IT out of personal computing device procurement, it still leaves them responsible for securing the matrix of users, applications, and device types that access corporate resources.

Thirty-four percent of ESG research respondents identified proactive threat detection as one of the factors with the greatest influence on their organization's enterprise mobility strategy.

According to ESG research, IT professionals surveyed indicated that, while they believe mobility has increased end-user productivity, they are also concerned about the security implications. In fact, when asked what shaped their organizations' enterprise mobility strategy, the most-cited response was proactive threat detection, at 34%.[3] Mobility also increases the risk of data loss not only from inbound threats but also due to lost or stolen devices that contain corporate data, creating the need for ubiquitous endpoint security controls.

Resource Constraints Inhibit Proactive Threat Defense

Chartered with a "do more with less" imperative, midmarket organizations are constantly seeking operational efficiencies, and research conducted by ESG highlights a problematic shortage of cybersecurity skills. When respondents were asked to identify the areas with the most problematic labor shortages in their IT organizations, the most common response, for the fourth consecutive year and nearly double the percentage reported for the prior year, was cybersecurity.[4]

Modern Endpoint Security Requirements for Midmarket Organizations

Breadth and Depth: Feature Aggregation and Device Coverage

Given the reality of these issues, organizations require a modern endpoint security solution that eliminates the need for multiple point tools and the associated set of disparate agents and management consoles by consolidating essential endpoint security controls into a single solution to reduce complexity and operational overhead. Depth of endpoint functionality in such a solution should include:

- Advanced protection controls.
- Encryption to protect data assets.
- Device/port control policies to protect against both data loss and attacks through this vector.
- Core mobile device management capabilities.

Such depth of functionality needs to protect the multi-device end-user across laptops, desktops, tablets, and smartphones, inclusive of all the associated operating systems.

[3] Source: ESG Research Report, *Security, Productivity and Collaboration: Trends in Workforce Mobility*, May 2016.
[4] Source: ESG Research Report, *2016 IT Spending Intentions Survey*, February 2016.

Beyond Signatures: Advanced Detection Techniques

Highly effective, advanced endpoint security solutions will employ a range of controls to protect against known and unknown threats, including polymorphic malware, and zero-day exploits. Such advanced controls include:

- Machine learning to determine the characteristics of malicious binaries, a particularly important detection technique for disconnected devices that cannot leverage cloud-delivered threat intelligence.

- Software reputation, which will use prevalence to determine whether a file has been seen before and can thus be trusted.

- Host Intrusion Prevention System (HIPS), which will detect and prevent unauthorized system changes and network access that are anomalous and indicative of an attempted compromise.

- Behavioral or dynamic analysis to detect run-time characteristics consistent with malware, such as disabling a backup service, as is the case with many ransomware variants.

- Anti-exploit technologies, including the ability to protect against memory-based attacks, to secure vulnerable applications.

These advanced controls are not mutually exclusive and represent a contemporary set of advanced techniques that, when configured properly, increases efficacy without introducing false positives that adversely impact operational efficiency. Mitigating the incident rate of false positives is an especially important consideration for small and medium businesses given the potential to not only interrupt end-user productivity but also to require IT to spend time investigating a benign event.

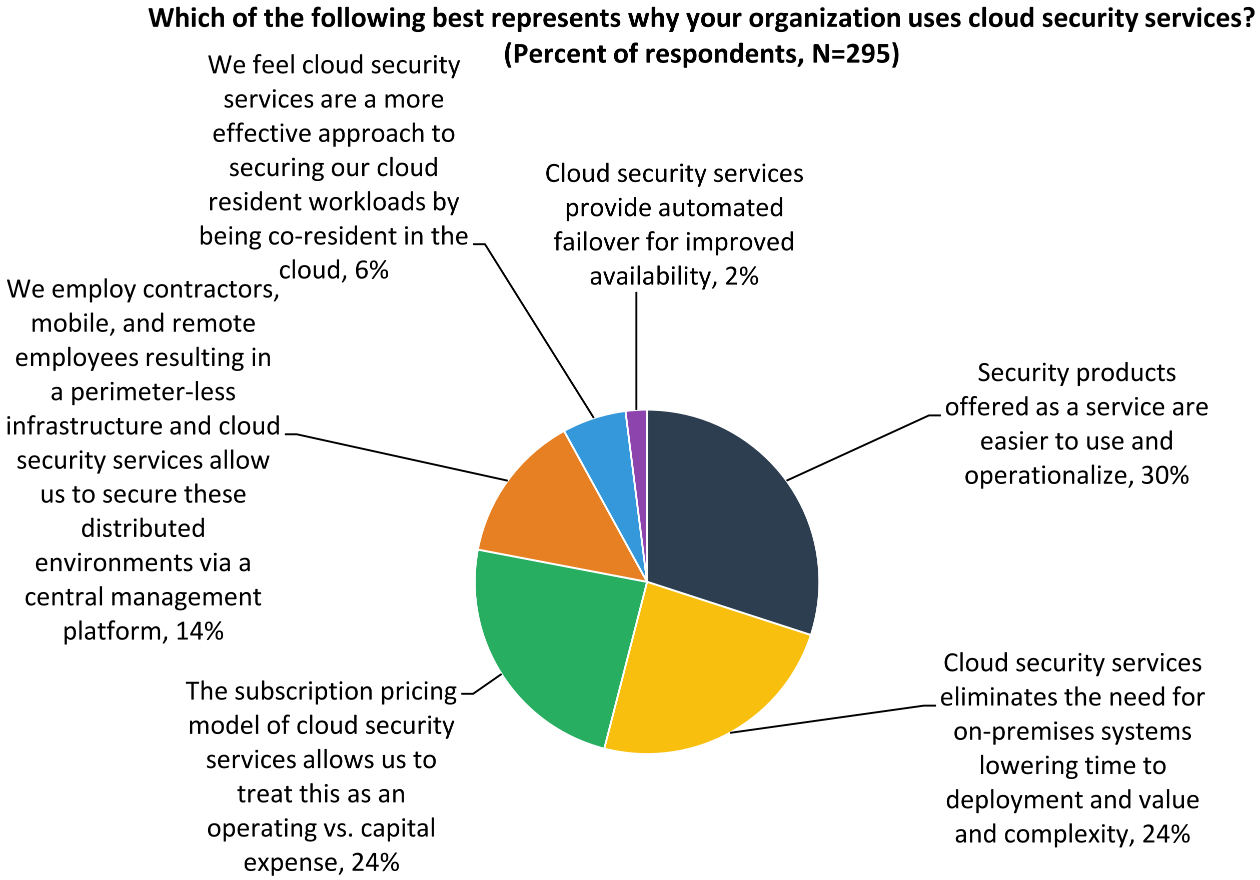
Simplicity via Cloud-delivered Security-as-a-service

The efficacy of these advanced detection techniques can be efficiently operationalized via a cloud-delivered service. The compelling benefits of such security-as-a-service offerings are multi-fold, including expedited onboarding of new employees and devices for shortened time to protection. Ease of use realized via an intuitive user interface, predefined policies, and guided, wizard-based workflows streamlines initial setup, and dashboards and contextual alerts simplify ongoing management, essential considerations for small- to medium-sized businesses.

Research conducted by ESG highlights the multitude of benefits provided by cloud security services (see Figure 1).[5] The ease of use and operational benefits were cited by 30% of survey participants. Nearly one-quarter (24%) of respondents indicated that cloud security services eliminate the need to provision and manage on-premises servers, lowering ongoing cost of ownership, while another 24% indicate the subscription pricing model of cloud security allows them to treat this service as an OpEx versus a CapEx. Another 14% stated security services provide the necessary coverage for remote employees and partners, giving them the ability to secure these distributed environments.

[5] ESG Research Report, *The Visibility and Control Requirements of Cloud Application Security*, May 2016.

Figure 1. Reasons for Using Cloud Security Services



Source: Enterprise Strategy Group, 2016

Protecting Against Advanced Threats Efficiently with Symantec Endpoint Protection Cloud (SEP Cloud)

Symantec's new endpoint protection solution, SEP Cloud, is purpose-built for small- and medium-sized organizations requiring a powerful set of endpoint security controls delivered as an easy-to-use service. SEP Cloud meets those objectives by aligning the requirements of a modern endpoint security solution with the resource constraints of the midmarket by providing consolidated controls, intelligent protection, efficiency, and ease of use.

Consolidated Set of Controls Across a Broad Range of Endpoints

SEP Cloud includes a core set of controls required to protect users, endpoints, and their data from compromise. The solution provides the following:

- Layered threat detection and prevention to protect against known and unknown malware and exploits.
- Encryption to secure data assets at-rest by utilizing the native Windows and OSX controls.
- Device control to keep the good in—and the bad out.
- Mobile device management (MDM) security controls (including remote wipe), reducing the need for smaller organizations to invest in a full-fledged MDM platform.

- **User- and group-centric policies** for the simplified application of appropriate security rules.

Consistent with the aforementioned breadth and depth requirements, SEP Cloud supports a wide range of endpoint devices including laptops, desktops, and mobile devices as well as servers and the associated operating systems for coverage across all of an end-user's devices.

Intelligent Threat Detection and Prevention

SEP Cloud employs an intelligent set of layered detection controls to protect managed endpoints from known and unknown threats for a level of accuracy designed to address false positives.

- **Advanced machine learning** techniques are employed to detect new and unknown threats before such threats execute and infect the targeted endpoint.

- **Symantec's Global Intelligence Network** is a cloud-delivered service providing visibility into web and email attacks, millions of control points and sensors, follow-the-sun threat response centers, and from-the-cloud protection of previously scanned files to prevent known-bad files from executing.

- **Symantec's intelligent threat cloud**, a feature of SEP Cloud, eliminates the need for a full set of endpoint-resident signatures, reducing agent footprint and the use of network bandwidth. This cloud service leverages the variety of detection techniques discussed herein, hosts the corpus of threat intelligence in the cloud, and employs an algorithm to look up such threat information as needed.

- **Symantec Insight**, Symantec's software reputation service, leverages the prevalence of previously unseen software to determine its trustworthiness.

- **SEP Cloud's Memory Exploit Mitigation** protects popular software against memory-based attacks.

- **Symantec Online Network for Advanced Response (SONAR)** performs real-time monitoring and behavioral analysis to ensure the integrity of the system against new and unknown threats.

- SEP Cloud also leverages **host-based intrusion detection and prevention** capabilities by analyzing attempted system changes and inbound and outbound netflow traffic.

These detection and prevention techniques are not mutually exclusive. In fact, such a holistic approach is required to protect against the range of known and unknown threats—whether they are delivered as malware or an exploit.

Cloud-delivered Efficiency and Ease of Use

SEP Cloud is a comprehensive, cost-efficient solution that eliminates the operational overhead of managing the server tier of an on-premises deployment. Its simple user interface provides wizards to guide a user through administration and configuration steps with an objective of setting up the service and seeing the benefits in a matter of minutes. For example, SEP Cloud simplifies the enrollment process of onboarding new users and their endpoints, including remote employees and mobile devices.

In addition, a predefined set of policies allows easy application of suggested best practices, as well as the ability to create custom policies (with feedback on the relative strength of associated policies and controls). Single-click assignment of controls, and a "Fix Now" button helps administrators remediate issues without having to deal with underlying complexities. Delivered as a service, SEP Cloud is offered on a subscription basis with consumption-based pricing.

The Bigger Truth

The incessant targeting of end-users and their vulnerable devices and applications has resulted in endpoint security being constantly on the minds of IT professionals. Employees who use multiple devices to access business applications and information from anywhere at any time are putting corporate data assets at risk. Small and medium businesses are not immune to the realities of today's threat landscape, and need a means to protect a mobile workforce against that harsh reality, often with limited funds and resources.

Efficacy and efficiency do not have to be mutually exclusive. In fact, they are must-have outcomes for modern endpoint security. As is true with other types of highly innovative SaaS applications that have brought efficiencies to how we live, work, and transact business, the cloud enables smaller organizations to realize the benefits of advanced endpoint security controls. Symantec's SEP Cloud brings to bear a rich set of features, including advanced threat prevention capabilities, delivered efficiently from the cloud, representing a solution that organizations seeking efficacy and efficiency may want to consider.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.