ANALYST CONNECTION

Robert Westervelt
Research Director, Security Products

SMBs Adopt Modern Endpoint Security to Address Sophisticated Threats and Reinforce Customer, Business Partner Trust

August 2018

Security is now a top IT spending priority for small and medium-sized businesses (SMBs), which have historically struggled to adopt modern security products that work cohesively to support business operations with a comprehensive line of defense against sophisticated attacks. A recent IDC survey of U.S. small businesses (fewer than 100 employees) and medium-sized businesses (100–999 employees) found that SMBs are increasingly trying to establish ways to coordinate security across their security infrastructure to support threat detection, incident response, containment, and remediation to prevent a reoccurrence of similar attacks.

The following questions were posed by Carbon Black to Robert Westervelt, research director of IDC's Security Products service, on behalf of Carbon Black customers.

Q. Even though SMBs may be small in size, are they still targets for advanced attacks?

A. Forensics investigators consistently report that attackers often target small businesses, using them as pawns to gain access to highly coveted business partner resources. Part of the problem is that SMBs have consistently lacked financial resources to support skilled IT staff and rely on technology alone to detect and prevent threats.

IDC research finds most data breaches involving midmarket organizations stem from stolen account credentials and the use of outdated antivirus software, and investigators often uncover signs that reconnaissance work had been done against the victim organization. Financially motivated attackers are getting especially savvy at identifying individuals within the organization, such as a payroll clerk, the CFO's support staff, and HR, to get what they need.

IDC's survey of 900 technology decision makers in companies with fewer than 5,000 employees found that advanced attacks and ransomware, which has had a particularly disruptive impact on small businesses in the past several years, are among the key drivers of increased security spending among small and medium-sized businesses. Nearly one-third of small businesses and half of firms with more than 50 employees cited network security improvements and adding "next generation" security as an IT spending priority.

Q. Can existing antivirus solutions owned by SMBs keep pace with the rapidly evolving threat landscape?

A. Signature-based security products are generally designed to be triggered by malware that has already been seen and documented on other corporate networks. These traditional antivirus solutions do little, if anything, to defeat newly developed malware or to detect targeted, nonmalware attacks that leverage compromised credentials or system vulnerabilities. In addition, attackers now use legitimate administrative tools to avoid being detected by standard antivirus software. Small businesses must elevate their security postures to defeat these advanced attacks by choosing modern endpoint security solutions.

Modern threat detection and prevention solutions collect massive amounts of endpoint activity data and change the paradigm by strengthening defenses using cloud-based, big data analytics to prevent and predict advanced attacks. Using advanced analysis, these solutions examine the data to uncover new threats and potential avenues of attack. This approach is easy to deploy and manage, and it addresses both malware and file-less attacks.

By leveraging the cloud, organizations of all sizes can use sophisticated analytics once reserved for larger enterprises that could afford to staff data scientists to probe the data. Modern solutions should incorporate non-signature-based methods and continuously monitor and apply the right algorithms to identify potential threats from subtle system changes. These solutions tend to utilize threat intelligence from a variety of resources to identify real-time threats as they develop.

Q. How can SMBs better integrate security into standard IT practices?

A. The sad truth is that one product alone won't solve the security problems challenging small businesses. Modern endpoint security products, designed to augment or replace traditional antivirus, should ease security coordination and management, a key challenge cited by IDC survey respondents. Buyers of security products for small businesses should identify solutions with a strong technology partner ecosystem. This typically is a sign that the product is designed to integrate, and often interoperate, with a broad spectrum of security solutions. Modern security products often provide open APIs to simplify integration using automated, plug-and-play connectors to existing security infrastructure, such as SIEM, security analytics, threat intelligence, and network security products.

Small businesses that put into practice the idea of "defense in depth" should be reminded that it isn't about the number of security products protecting the organization; rather, it's about how the products fit into the combination of people, process, and technologies. Businesses of all sizes are increasingly finding that support is needed to combine these three critical areas. Their options include choosing to outsource management of security and incident response to a managed security services provider or choosing a proactive management service from a product manufacturer.

Q. Can SMBs create a comprehensive security program supported by an incident response team with limited resources?

A. Continuous monitoring and coordinated response processes are required but often not realized, which is detrimental to many organizations. Even large organizations often lack the resources to staff and manage a security operations center and dedicated incident response team with "eyes on screen" watching, analyzing, and acting on behalf of the enterprise. False positives and false negatives will continue to be problematic for businesses of all sizes. False positives suggest that a threat was investigated and determined to be harmless. False negatives suggest that a verifiable threat was dismissed due to a lack of visibility. Today's most effective threat analysis and mitigation strategies require the correlation of data across disparate networks throughout the enterprise and beyond.

There are cost-effective solutions that can help small businesses bolster their security posture and gain the benefits of continuous monitoring and coordinated incident response. Security buyers should identify the modern products that are supported with an in-house team of analysts — real people who research alerts, combined with big data analytics and threat intelligence — to identify true potential threats that require the most immediate attention. These security analysts are trained to connect the dots by using a variety of data sources as opposed to guessing about the significance of a single event from a monitored system and then attempting to recreate relatable events from unmonitored systems. This eases the burden of investigating alerts and identifying the root cause of a threat, another critical activity that, if overlooked, can result in a costly data breach and losses from business disruption.

Q. How should SMBs approach the decision to move endpoint security to the cloud?

A. IDC is already seeing organizations adopting security products either fully delivered from the cloud or supported by cloud-based resources. SaaS-delivered endpoint security software is generally easy to implement and can run side by side with traditional antivirus. IDC research suggests that this software can provide profound benefits to the organization's security posture.

Now is the time to address advanced threats by finding solutions that can bolster detection capabilities and support rapid response. Cloud-based endpoint security is a great place to start modernizing your security infrastructure. These security products can be a cost-effective way to achieve compliance with both internal policies and industry regulations and to protect data from unauthorized access stemming from a security breach or an inadvertent disclosure.

These modern products are generally believed to perform better than traditional on-premises solutions because the existing endpoint agent collects endpoint sensory telemetry and is combined with threat indicators collected from other customers in real time and analyzed using scalable, cloud-based analytics.

ABOUT THIS ANALYST

Robert Westervelt is a research director within IDC's Security Products group. He provides insight and thought leadership in the areas of cloud security, mobile security, and security related to the Internet of Things (IoT). Rob is also responsible for research and analysis around a wide range of evolving security markets, including endpoint security, security and vulnerability management (SVM), and identity and access management (IAM).

ABOUT THIS PUBLICATION

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

COPYRIGHT AND RESTRICTIONS

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com