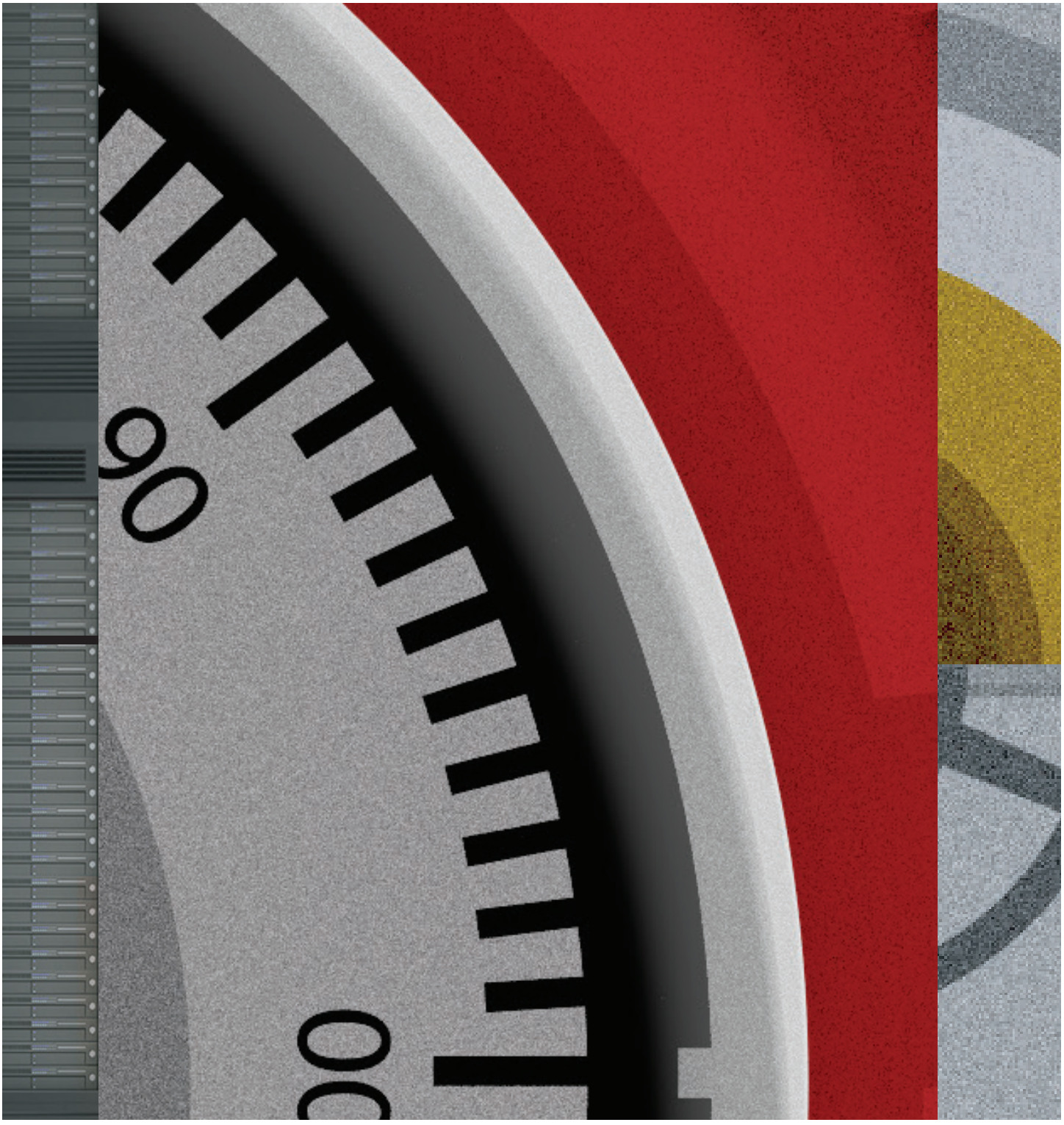
Symantec

TRAVELERS

# The Cyber Siege of SMBs



## Introduction

Cyber security has become a critical issue for governments at all levels and is one of the top risks concerning major global enterprises, which have suffered from cyber incidents costing hundreds of millions of dollars. But cyber security impacts businesses of all sizes, not just governments and major enterprises. Approximately 65% of targeted attacks are directed at small-to-midsized businesses (SMB), up from 50% in 2011.[1] This trend toward attacks on SMBs is even starker for small businesses. The share of attacks targeting companies with fewer than 250 employees has more than doubled in the past five years.[2]

All businesses need to take cyber security seriously, but SMBs face unique challenges. Not only do SMBs lack the budget to deploy the kinds of security tools used by larger enterprises, they typically do not have the personnel to manage such security.

Fortunately, the shift to cloud-based security, or "Security Software as a Service" (SSaaS), is simplifying security for SMBs. This paper outlines some key challenges facing SMBs and four opportunities where the shift to SSaaS can make it easier for SMBs to cost-effectively deploy security across email, endpoints, web traffic, and access management in a way that was not possible before.

*"Leveraging Cloud-Based Security to Protect Small-to-Midsized Businesses"*

## The SMB Challenge

How are SMBs supposed to protect themselves, given all the challenges and limitations they face? They don't have unlimited budgets to spend on expensive cyber security solutions or on hiring in-house experts like larger companies do. Large financial institutions, for example, spend as much as $400 million on cyber security each year.[3] The very smallest businesses may not even have a dedicated IT person, let alone a specialist in information security.

Then there are the staffing limitations most SMBs face. Even if an SMB wanted to hire a qualified cyber security professional, it would be difficult given the industry shortage of qualified individuals. Last year, there were one million job postings in the United States for cyber security professionals, and more than 200,000 of those remained unfilled. [4]

[1] https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

[2] https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

[3] https://www.forbes.com/sites/stevemorgan/2016/01/27/bank-of-americas-unlimited-cybersecurity-budget-sums-up-spending-plans-in-a-war-against-hackers/#981bc6f264cd

[4] https://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#23e23b5827ea

Many SMBs struggle to secure themselves against constantly changing threats from advanced email attacks and advanced endpoint attacks. Many SMBs also have not implemented website traffic filtering or Multi-Factor Authentication (MFA) to help protect their users from inadvertently going to compromised sites or from having their accounts compromised due to weak passwords.

In the past, it was much more difficult to protect SMBs from the critical attack vectors discussed below. The advent of cloud-based technologies, however, has made sophisticated software solutions more cost-effective and easier to implement. These "Software as a Service" (SaaS) solutions are dramatically changing IT strategies and making critical tools and services available to SMBs. More than 94% of SMBs in the U.S. will utilize SaaS solutions by the end of 2017,[5] and globally, 45% of cloud IT budgets will be spent on SaaS.[6]

With these changes has come the evolution of "Security Software as a Service." These services provide critical protection for SMBs in a way that is easily implemented, easily managed, and cost effective, while providing real-time protection that can help prevent SMBs from falling victim to the latest cyber threats.

## Opportunity 1: Email Security

Email threats from malware, spam, and phishing continue to be one of the biggest issues facing SMBs. Many SMBs rely on the spam and malware filtering capabilities built into their email server software or their email provider, only to find out the hard way that those tools have limited capabilities, are difficult to manage and report on, and worse, fail to protect the business from advanced or "zero-day" threats.

In 2016, emails with embedded malware increased to one in every 131 messages, while ransomware exploits such as Locky and TeslaCrypt cost SMBs in the United States approximately $75 billion.[7]

Besides the rise in embedded malware, 2016 saw an increase in "business email compromise" (BEC) scams, a form of financial fraud meant to trick an employee into paying for fraudulent invoices or making a large wire transfer by spoofing a manager's or supervisor's email. More than 400 businesses are attacked each day by BEC scams, with SMBs the most frequently targeted, resulting in losses of more than $3 billion in the past three years.[8] In one reported incident, an aerospace company fell victim to a BEC scam and transferred approximately $50 million to scammers.[9]

A traditional email service or product protects against "known" email malware, i.e., viruses with already-defined signatures. It should also stop known spam and bulk emails, though this often requires a lot of rule tweaking.

An advanced cloud gateway can protect against unknown malware and viruses—even those without signatures.

[5] https://biztechmagazine.com/article/2017/02/small-businesses-are-embracing-saas-cloud-deployments-survey-says

[6] https://biztechmagazine.com/article/2017/02/small-businesses-are-embracing-saas-cloud-deployments-survey-says

[7] http://www.esecurityplanet.com/malware/u.s.-small-businesses-lose-75-billion-a-year-to-ransomware.html

[8] https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

[9] https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

It can block spam and bulk email by leveraging data from global spam trends without requiring the SMB to continually tweak the filtering rules.

The real feature sets that are critical in defense of the SMB are in the advanced and zero-day threat protection capabilities of a cloud-based email gateway service. How well can it stop targeted spear phishing attacks, protect you from malicious embedded links, or stop obfuscated malware from getting through to an employee?

A truly advanced gateway should protect against a host of targeted attacks by leveraging a global intelligence engine fed by millions of endpoints. That intelligence should be constantly updated and combined with technology that scans multiple email attributes to find and block anomalies and obfuscated malware buried deep within a message or attachment.

The service should leverage advanced machine learning and provide the ability to stop targeted BEC campaigns through real-time link following, click-time URL protection, and analysis engines that stop typo squatting of domain names and user spoofing. A cloud-based email service with these features can be the most cost-effective way to keep your SMB safe.

## Opportunity 2: Endpoint Protection

Second on the list of critical SSaaS services is an endpoint product capable of addressing advanced threats. Last year alone, 357 million new malware threats were found.[10] A traditional anti-virus product that updates only virus signatures, or has limited capabilities, will not adequately protect against new and emerging zero-day or advanced threats. Protecting SMB endpoints from the constantly changing landscape presents distinct challenges. Attacks are increasing at a faster rate than ever before. The pressure of a mobile workforce demanding more device choice, budget limitations, and lack of qualified IT support all conspire to complicate the defense of SMBs. Ransomware and mobile device exploits were some of the biggest threats facing organizations in 2016. The average ransom jumped 266%, from $294 to $1,077 in 2016. There were 606 new mobile device vulnerabilities discovered in 2016: 290 for iOS, and 316 for Android.[11]

A cloud endpoint product that truly protects against new malware variants and zero-day threats must be able to protect a wide range of devices and operating systems. It should use intelligence based on big data leveraged from a global intelligence network that is automated and driven by billions of lines of threat telemetry.

Additional advanced features should include the ability to do real-time cloud lookups of all scanned files, as well as a file behavior engine that monitors operating systems and applications for suspicious activity.

Beyond that, the next level of endpoint protection should include artificial intelligence and machine learning in order to pre-execute and detect evolving threats and variants of previously identified malware. Anything less could leave the business vulnerable and exposed.

[10] https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

[11] https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

## Opportunity 3: Web Security

The third major problem facing SMBs is the lack of insight and control over web traffic. End users in many SMBs browse websites that are vulnerable or have been exploited. A user will then inadvertently download some malicious content. Worse, many SMBs have no idea what data is leaving their network via employees, contractors, or third-party vendors. Unfortunately, 76% of websites scanned by Symantec still have vulnerabilities; indeed, 9% of those were critical vulnerabilities. Websites can be subjected to more than 229,000 unique web attacks every day.[12]

So, how can an SMB protect users from ubiquitous threats while managing new devices and mobile users' traffic even when they are remote? How can an SMB protect data in the cloud and comply with required legal regulations?

One way is to use a cloud-based web-filtering service. These services allow SMBs to use URL filtering and categorization to protect a network and enforce usage constraints. They allow an SMB to filter and see all web traffic. Moreover, that web traffic is checked against policy rules, and all traffic to and from blocked or blacklisted sites is stopped. This service gives granular control over web usage by apps, devices, users, and locations, allowing an SMB to exercise greater control over its network and to enforce acceptable use policies while protecting against malicious content.

An advanced cloud-based web-filtering service should also auto-block newly found and zero-day threats before they can impact your network. In particular, malware protection should include sandboxing and behavioral analysis that can detonate a threat in the cloud before it gets to your network. And, because the service is cloud-based, it can protect clients and devices even when they are not in the office or on a company network.

## Opportunity 4: Password and Access Management

The last vulnerability that should concern all SMBs is over-reliance on passwords for authentication. Using passwords as the only protection for user accounts is no longer sufficient to prevent identity theft or data breaches.

Last year, there were 1.1 billion identities exposed because of 1,209 breaches, with 15 of those exposing ten million or more identities.[13] Taking a longer view, over the last eight years, a staggering 7.1 billion identities have been exposed, many repeatedly, in data breaches. Coupled with the fact that 81% of confirmed data breaches involved weak or stolen passwords, the magnitude of this problem becomes clear.[14]

According to research,[15] 90% of employee passwords are crackable within 6 hours and 65% of people use the same password everywhere.

[12] https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

[13] https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

[14] http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

[15] https://www.entrepreneur.com/article/242208

The best way to move past the static password model and all its failings is to implement a dynamic authentication model. Multi-Factor Authentication (MFA) requires users to have a password (something they know), but it also requires a mobile phone or security token (something they have) and/or some form of biometrics like a fingerprint or facial recognition (something they are). A cloud-based MFA service will significantly help protect user accounts from being compromised.

How does MFA keep SMBs safe? To start with, it gives you better control over who and how your data, applications, and devices are accessed. It can help to ensure the identity of the individual accessing your networks and web applications, and to limit which third-party vendors have access. Many cloud apps and services have MFA features, but using different MFA systems for multiple applications and services creates a fragmented and difficult-to-manage process that gives SMBs little or no insight into who is accessing their data and networks. In contrast, a cloud-based MFA architecture gives SMBs centralized control and insight into who has access and when access has taken place.

A robust MFA cloud service should also integrate with your network, allowing for Single Sign-On (SSO) to protect both remote and on-premises access. It should be easily managed from a web portal that allows for reports and alerts that can be used to monitor access and identify attacks before they become breaches.

## Conclusion

Email security, endpoint protection, web security, and access management are the four core SSaaS services that should be the cornerstones for protecting your SMB. Using these services to create a layered and overlapping defensive posture will limit your cyber risk and threat exposure. These fundamental services are four of the biggest entry points and attack vectors for SMBs and larger organizations alike.

What makes these cloud services so attractive to SMBs is the low cost combined with ease of implementation and maintenance. Once they are set up and configured, most of the maintenance and upgrades happen automatically. This is a stark change from the days when complex software installations needed to happen on-premises, often with manual effort required to keep software updated and configured correctly.

And, since they are cloud-based services, advanced threat protection is continuously improving. New capabilities and detection methods are constantly being implemented and deployed by the service provider. As time goes on, more and more SSaaS services will come online and cover a wider array of security functions. Ultimately, the success of these services will come down to which ones give your SMB the best overall protection.

Cyber threats against SMBs continue to grow each year, and no business is completely immune to cyber attacks. However, the shift towards SSaaS is making it easier for SMBs to mitigate the risk of cyber attacks and, when combined with cyber insurance, can help businesses become cyber resilient.

## TRAVELERS AND SYMANTEC: HELPING BUSINESSES BECOME CYBER RESILIENT

Coverage provided by Travelers Casualty and Surety Company of America and its property casualty affiliates. Hartford, CT 06183.

This paper is for general informational purposes only. It is not designed to be comprehensive and it may not apply to your particular facts and circumstances. Consult as needed with your own attorney or other professional adviser. This material does not amend, or otherwise affect, the provisions of any insurance policy issued by Travelers. It is not a representation that coverage does or does not exist for any particular claim or loss under any such policy. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy provisions, and any applicable law. Availability of coverage referenced in this document can depend on underwriting qualifications and state regulations.

Certain services are being provided to you by Symantec and in using them you must agree to Symantec's terms of use and privacy policy. Travelers Casualty and Surety Company of America and its property casualty affiliates ("Travelers") make no warranty, guarantee, or representation as to the accuracy or sufficiency of any such services. The use of the services and the implementation of any product or practices suggested by Symantec or NetDiligence is at your sole discretion. Travelers disclaims all warranties, express or implied. In no event will Travelers be liable in contract or in tort for any loss arising out of the use of the services or Symantec's or any other vendor's products.



Symantec

TRAVELERS