FROST & SULLIVAN

Gaining a Strategic Endpoint Security Advantage in the Era of Advanced Threats

A Frost & Sullivan White Paper

Jason Reed- Analyst

Commissioned By:
Symantec.

TABLE OF CONTENTS

INTRODUCTION

Following an upward trend that shows no signs of abating, 2018 featured more high-profile data breaches than the year before. While security failures at major financial institutions[1] and social media giants [2] make headlines, large enterprises aren't alone in their vulnerability to cyber threats. Historically, the predominant perception has been that midsized enterprises (companies with 1,000 to 5,000 employees) were targeted less often than large companies. But studies suggest that these smaller enterprises are an increasingly attractive target for cyber attacks—with 61% reporting a breach in 2017, up from 55% in 2016. [3] This number is likely to have increased again in 2018. One reason for this uptick is that businesses of all sizes are experiencing cyber attacks in greater numbers, but cybercriminals often perceive midsized enterprises to be "softer" targets. These organizations often have smaller budgets and fewer resources to dedicate to cybersecurity efforts, which can result in bare-minimum security deployments and more potential for gaps in protection.

STUDIES SUGGEST THAT THESE SMALLER ENTERPRISES ARE AN INCREASINGLY ATTRACTIVE TARGET FOR CYBERATTACKS

Breaches are Potentially Fatal for Midsized Enterprises

Smaller enterprises stand to lose as much or more as their larger counterparts in the event of a breach; in fact, the average cost of a breach for midsized enterprises is in excess of $2 million USD. [4] Many organizations cannot survive such a financial hit, and a recent study [5] found that 60% of small to midsized businesses fold within six months of a breach. This statistic alone makes it clear that cybersecurity cannot be treated as just another "box to tick," but rather must be viewed as fundamental to overall operations. As digital threats become more sophisticated, and the ease with which would-be attackers can access exploit kits or other hacking tools increases, the time to invest in cybersecurity infrastructure to ward off advanced threats is now, no matter the size of the business.

...

*It's not a matter of **if** you will be attacked, it's **when***—this is a common refrain among cybersecurity professionals, and there is ample evidence that many organizations may not be prepared if they are targeted by a criminal using modern hacking tools. Recent studies suggest that while most midsized organizations are confident that their current array of cybersecurity products are sufficient to secure their data, 63% also admit that they are completely unprepared for zero-day threats. [6] Furthermore, in its 2018 State of Endpoint Security Risk study, Ponemon Institute found that 70% of security personnel believe that the threat to endpoint security has increased significantly, and a similar proportion reports that the threat from new or unknown attacks poses a significant and increasing threat to their organizational security posture. [7]

It is not difficult to imagine why security professionals are raising alarm bells about advanced threats. A typical cybersecurity deployment for midsized enterprises likely features a signature-based antivirus and a firewall that blocks or permits traffic based on access control lists. However, the Ponemon study found that only 29%

[1] https://www.nbcnews.com/news/us-news/equifax-breaks-down-just-how-bad-last-year-s-data-n872496
[2] https://www.bbc.co.uk/news/technology-45686890
[3] https://www.prnewswire.com/news-releases/2017-ponemon-institute-study-finds-smbs-are-a-huge-target-for-hackers-300521423.html
[4] https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/
[5] https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html?fbclid=IwAR0wzjghOvqGswcioj5Yn2b9QGpfQkclrGpGDVlI5dI_BD78uIYFePB4Hgo
[6] https://betanews.com/2017/01/26/enterprise-security-confidence/
[7] https://cdn2.hubspot.net/hubfs/468115/whitepapers/state-of-endpoint-security-2018.pdf?t=1540499453247

of security professionals believe that a traditional deployment provides the protection needed to stop serious attacks against their IT environments. This is due to an outdated notion of security as a perimeter defense that is built around the core elements of enterprise IT. This configuration can deemphasize the importance of one of the most vulnerable entry points for attackers: endpoints. Endpoints are among the most common points of entry for an attacker and must be treated as a fully realized attack vector. Too often they are not. Put simply: today's advanced threat landscape has not seen a commensurate response from enterprise.

Customers Take Their Business Elsewhere After a Breach

Midsized organizations must also be aware that the consequences of a lapse in their security can be severe: as threats have become more advanced and sophisticated, consumers have simultaneously become less tolerant of data breaches. In fact, a recent Frost & Sullivan study found that **half** of consumers are likely to discontinue using an online service or website in the wake of a data breach. [8] The same study found that among those organizations that have been breached, half report a strong long-term negative impact not only on consumer trust (50%) but on their business results (47%).

A RECENT FROST & SULLIVAN STUDY FOUND THAT HALF OF CONSUMERS ARE LIKELY TO DISCONTINUE USING AN ONLINE SERVICE OR WEBSITE IN THE WAKE OF A DATA BREACH.

It is critical that organizations adapt to the state of the contemporary threat environment and invest in solutions that will mitigate the risk posed by advanced hacking techniques. In the following pages, we examine four aspects of the modern threat environment that are particularly relevant to midsized enterprises, including the risks associated with them and the measures that should be taken to limit their impact.

FILELESS ATTACKS

Most often, security breaches are associated with a malicious executable program that runs on a user endpoint. This typically occurs when an executable file is disguised as another type of file (for example, a PDF) or is hidden in a zipped folder. When the file is opened, the executable runs and infects the user with its "payload." This traditional approach by malicious actors is generally perceived as a classic hacking technique.

Recently, however, attackers have adopted different tactics. Unlike traditional, executable file-based attacks that can be stopped by most antivirus software, hackers have adopted a more subtle type of attack: fileless attacks. These attacks, as the name suggests, do not copy any files to the hard disk and operate solely in endpoint system memory, thereby evading standard antivirus software and leaving few traces.

One of the most famous security breaches in recent memory, the hack of the US Democratic National Convention email server, was conducted via fileless attack. The hack was comprised of targeted emails from seemingly legitimate sources that contained links to infected web pages, which subsequently allowed hackers to gain access to the DNC network.

While fileless attacks are not necessarily new (they have existed in one form or another for decades), fileless attacks are popular among advanced threat

A 2018 PONEMON INSTITUTE REPORT FOUND THAT CYBERSECURITY PROFESSIONALS WERE MUCH MORE LIKELY TO BELIEVE THAT FILELESS ATTACKS CAN COMPROMISE THEIR SYSTEMS COMPARED TO FILE BASED ATTACKS.

[8] https://www.ca.com/content/dam/ca/us/files/white-paper/the-global-state-of-online-digital-trust.pdf

actors precisely because they are so effective. A 2018 Ponemon Institute report [9] found that cybersecurity professionals were much more likely to believe that fileless attacks can compromise their systems compared to file-based attacks. The success rate of these attacks has resulted in widespread adoption of the technique: the 2018 Penomon study found that in 2017, fileless attacks accounted for approximately 30% of all attacks but by 2018 that number rose to 35% and is expected to rise to 38% in 2019.

How do Fileless Attacks Work?

There are several different types of fileless attacks, and they range from relatively simple to highly sophisticated. While the example of the DNC hack may appear to be far removed from the day-to-day business activities of enterprises, the method employed by hackers should be immediately familiar to anyone in a modern business environment. Emailed phishing web links are a typical starting point for a fileless attack because they load directly into memory as system commands and run immediately without copying a single file to the hard disk. They then continue to run, usually undetected by antivirus programs. The best way to stop a fileless attack is to shut down the infected endpoint(s); however, it is often too late and the malicious code may have spread to other endpoints.

Generally speaking, fileless attacks take one of two forms: either “hit-and-run” techniques or more permanent code. Hit-and-run attacks run on the infected system, typically stealing credentials or running ransomware, and then disappear. These attacks are extremely difficult to analyze as they leave few traces of their presence for forensic analysts to examine. The other common form of fileless attack establishes a presence in the endpoint’s registry and runs on system startup or on another schedule. In both cases, fileless attacks evade normal antivirus software and, as a result, present serious problems for infected environments.

The Repercussions of Fileless Attacks

The risks that fileless attacks present to organizations with traditional security configurations are clear: according to a recent Frost & Sullivan study, **half** of consumers are likely to discontinue using an online service that has been involved in a data breach. [10] The same study found that for **78% of consumers it is *very important or crucial* that their data be well protected online.** Furthermore, 86% indicate that a high level of data protection is a priority when choosing online services.

Fileless attacks are particularly concerning because they often use otherwise legitimate tools (known as “living off the land”) such as PowerShell or Microsoft Office to operate. A single fileless attack and subsequent data breach can cause irreparable damage to midsized organizations.

These attacks are also particularly dangerous because they leverage what is typically the weakest link in an organization’s security posture: non-technical staff that may not recognize a phishing campaign.

FILELESS ATTACKS ARE PARTICULARLY CONCERNING BECAUSE THEY OFTEN USE OTHERWISE LEGITIMATE TOOLS (KNOWN AS “LIVING OFF THE LAND”) SUCH AS POWERSHELL OR MICROSOFT OFFICE TO OPERATE.

[9] https://cdn2.hubspot.net/hubfs/468115/whitepapers/state-of-endpoint-security-2018.pdf?t=1540499453247
[10] https://www.ca.com/content/dam/ca/us/files/white-paper/the-global-state-of-online-digital-trust.pdf

Mitigating the Risks

There are several steps organizations should consider taking to minimize the risks posed by fileless attacks. They include:

- **Embrace a workplace culture of security.** It is essential that **all** personnel complete security training to minimize the risk that human error will cause a security breach.
- **Invest in technology.** Modern endpoint security solutions have moved away from the signature-based model of threat detection and instead monitor and analyze network activity. These newer detection systems, including advanced machine learning, memory exploit mitigation, and advanced endpoint detection and response solutions, can flag anomalous behavior and prevent or contain a fileless attack.
- **Trust the experts.** Finding qualified security personnel can be challenging for organizations given the global shortage of information security workers. [11] Leverage the expertise of your security solution provider, who can provide invaluable insights that will keep your environment secure.

THREATS THAT LINGER

Not all digital threats follow a "hit-and-run" model of breaching an environment—exfiltrating or corrupting data, then exiting the environment while making every effort to eliminate any trace that might be left and analyzed in a post-breach forensics exercise. Often, it is more advantageous for cybercriminals to inhabit the environment they have penetrated for an extended period of time to gain access to more sensitive data. In fact, a recent Ponemon report found that threats were active in their hosts (known as threat "dwell time") for an average duration of **191 days.** [12] The trend toward longer delays from the moment of infection to the moment of detection means that more and more data runs the risk of exposure.

A RECENT REPORT FOUND THAT THREATS WERE ACTIVE IN THEIR HOSTS (KNOWN AS THREAT 'DWELL TIME') FOR AN AVERAGE DURATION OF 191 DAYS.

Threat dwell time is a metric that is underrepresented in most discussions about security; traditional metrics are largely oriented around Time-to-Detect and Time-to-Respond. These measures, however, are meaningless if both commence long after the breach occurs.

The most famous recent example of a lingering threat that caused enormous reputational loss to an organization is the hack of a major online service provider that occurred in 2013 and 2014 but was not revealed until late 2016. [13] The precise moment when this breach, the largest in history, occurred is still unknown.

This breach was among the most consequential in history in terms of its scale and its direct economic impact: it devalued the selling cost of the service by $350 million USD. Had the breach been discovered earlier, or the dwell time minimized, it is extremely unlikely that the consequences would have been so catastrophic. But a breach need not target a technology giant to have a disastrous outcome. Regardless of the size of a business, it is critical to minimize the time between intrusion and detection. Importantly for organizations, attackers follow a broadly predictable pattern when initiating a prolonged attack: [14]

[11] https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage
[12] https://www.hstoday.us/home-posts/report-finds-cybersecurity-dwell-time-is-191-days-and-state-cio-says-it-should-be-zero/
[13] https://eu.usatoday.com/story/tech/2017/10/03/3-billion-yahoo-users-breached-company-says/729155001/
[14] https://www.bulletproof.co.uk/blog/dwell-time

- **Initial exploitation:** In this stage, attackers often use a simple tool such as a Google search designed to test for vulnerabilities. Using this method, attackers identify a worthwhile target and begin gathering preliminary information on the organization. Following this, attackers begin the initial exploitation of the environment. Here, standard perimeter defenses have an opportunity to block the attacker, but advanced threat actors, who comprise an increasingly large proportion of attackers, generally have the tools to circumvent these defenses. Once the attacker has breached perimeter defenses, the weaknesses of older security configurations are exposed.
- **Deposit payload:** There is a wide range of malware or fileless attack techniques that an attacker can execute once they have penetrated an organization's perimeter defenses. This is the stage where attackers establish a foothold in a vulnerable environment.
- **Lateral movement:** When attackers establish a presence that avoids detection in a vulnerable environment, dwell time becomes the most important metric from a defender's standpoint. Attackers will direct their efforts toward stealing credentials to gain access to an organization's most sensitive data. This stage can persist for weeks, months or, in extreme cases, years without an organization noticing.
- **Objective achieved:** This is typically the point where an organization discovers it has been breached, and by this time it is too late: the attackers have successfully accomplished their goal. Whether that is a simple objective such as encrypting organizational data using ransomware and demanding compensation for its safe restoration or has more widespread consequences, such as leaking sensitive customer information into the public domain, organizations must now begin the process of forensic analysis to determine what went wrong.

Implications for Midsized Enterprise

Perhaps the most important measure that an organization can take is to shift its perspective on cybersecurity from one that focuses simply on perimeter defenses to one that also limits the dwell time of an attacker who manages to penetrate its environment. This shift limits the potential damage the attacker can inflict. To accomplish this, organizations cannot rely on outdated security tools and frameworks. Midsized organizations, in particular, are vulnerable to security entropy as they generally have fewer available resources to dedicate to data security. Instead, to meet the demands of an advanced threat landscape, organizations must invest in next-generation security systems with features such as artificial intelligence and machine learning, which can reliably identify attacks as they occur as opposed to weeks or months after the initial incursion. Services such as proactive threat hunting are also an invaluable asset in the fight against lingering threats.

There are a number of opportunities to disrupt the attack lifecycle described above. One of the best ways to deter a would-be attacker is to ensure that your organizational security posture is robust. For enterprises, this means that the basics must be accounted for: keeping operating systems up to date, ensuring that software is patched, providing appropriate training for all personnel, and implementing strong perimeter defenses. This can throw off a substantial number of potential attackers at the recon phase; as a general rule, attackers take the path of least resistance, and if your organization does not seem like an easy mark, it may choose a different target. Unfortunately, too often midsized enterprises have not implemented the measures necessary to deter an attacker. The perceived vulnerability of midsized businesses is the primary reason smaller organizations are more attractive targets to attackers than a large organization with an advanced cybersecurity posture.

MACHINE LEARNING & ARTIFICIAL INTELLIGENCE IN THE FIGHT AGAINST ADVANCED THREATS

It is not uncommon to hear about the perpetual shortage of skilled personnel in the cybersecurity industry. The 2017 Frost & Sullivan/(ISC)2 Global Information Workforce Study concluded that by 2022, the industry would face a 1.8 million worker shortfall. [15] The same study confirmed how widespread knowledge of this shortfall has become: two-thirds (66%) of the nearly 20,000 information security professionals surveyed indicated that they have too few workers on staff to meet their day-to-day needs. Smaller organizations, in particular, may have difficulties competing for or retaining top talent, which can lead to an overtaxed security team.

Widespread issues related to a worker shortage notwithstanding, technological advances can support the work done by both large and small teams of information security professionals by streamlining many processes and tasks, and enhancing security efficiency. In short, there are technological solutions that help information security teams manage and mitigate advanced threats. These advances in technology are invaluable to enterprises, with the most promising examples being the implementation of machine learning and artificial intelligence in current and future-generation security suites.

Cutting Through the Hype: Machine Learning's Applications and Limitations

It is important to note that there is some disagreement among experts as to whether "true" artificial intelligence exists in security products in any measurable capacity. [16] These debates, however, tend to miss the most important point: machine learning, as a subdomain of artificial intelligence, is already used by attackers to stay one step ahead of defenders. It is crucial that the information security industry embraces these systems in the fight against advanced threats.

MACHINE LEARNING, AS A SUBDOMAIN OF ARTIFICIAL INTELLIGENCE, IS ALREADY USED BY ATTACKERS TO STAY ONE STEP AHEAD OF DEFENDERS

As Mike Lynch, contributor to Wired UK aptly noted, **"*2018 will be the year of machine-on-machine attacks.*"** [17] Setting aside the marketing messages and buzzwords, as it currently stands, machine learning is utilized by information security systems to automate the task of analyzing IP traffic flows, DNS logs, and other critical data streams. As a tool for combating advanced threats for resource-strained organizations, machine learning-enabled security products show enormous potential. It is, therefore, worth discussing what machine learning can (and cannot) currently do.

At its core, machine learning is most effective when it is analyzing and categorizing large volumes of data that would overwhelm a human analyst. By learning what normal behavior is and what it is not, machine learning can alert human analysts to anomalous activity on the network and can suggest a course of remediation. Furthermore, machine learning-enabled security services can conduct routine scans of existing endpoints, searching for unpatched vulnerabilities or for protocols that are not in line with the most up-to-date regulations. Because machine learning-enabled security products tend to be updated in real time or near-real time, they can also detect advanced malware and hacking techniques. Finally, these services can assist in predicting and adapting to future threats.

[15] https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage
[16] https://www.csoonline.com/article/3295596/security/ai-in-cybersecurity-what-works-and-what-doesnt.html
[17] https://www.wired.co.uk/article/ai-cyberattack-mike-lynch

Clearly, machine learning has the potential to aid security developments among enterprises. It is not, however, a magic bullet solution. One issue with machine learning as it currently exists is that in some ways it is reactive rather than proactive, and the volume of data required to “train” the machine is extremely large and cumbersome. One recurring flaw in today’s information security deployments is that the solutions tend to analyze IP traffic and data that has ***already entered the environment.*** For the most part, machine learning-enabled solutions do not block suspicious code before it enters the environment. The volume of data required to adequately train a machine learning algorithm and its inherently backward-facing posture are two limitations to machine learning-enabled information security products that every organization must consider.

Augmenting Existing Capabilities

It is best to think of machine learning-enabled cybersecurity suites as augmentations that relieve some of the burden that is placed on the people who are responsible for keeping data secure. As it stands, machine learning-enabled information security products provide insight that would otherwise be impossible for individual humans to compile. Where analysts would previously waste time chasing false positives, machine learning is intuitive enough to cut down the number of false positives returned to human analysts for closer inspection. The training period for machine learning is often the most labor-intensive part of the solution deployment; however, the latest technologies offer machine-learning modules that can self-train autonomously.

Compared to traditional information security configurations that are more or less static between updates, machine learning offers a new dynamic process to keep systems up to date and patched. Furthermore, machine learning-enabled cybersecurity suites offer enhanced network traffic analyses, with advanced pattern recognition that surpasses human capabilities. These advances allow for the flagging of any irregular traffic that appears in the network, any logs that stray from normal procedures, or any users that are behaving in a manner that is inconsistent with established norms.

COMPARED TO TRADITIONAL INFORMATION SECURITY CONFIGURATIONS THAT ARE MORE OR LESS STATIC BETWEEN UPDATES, MACHINE LEARNING OFFERS A NEW DYNAMIC PROCESS TO KEEP SYSTEMS UP-TO-DATE AND PATCHED.

Whether or not one is influenced by the hype surrounding machine learning and AI in cybersecurity, adversaries are already using these technologies to streamline their processes and cover larger attack surfaces in less time. It is, therefore, important for defenders to have access to at least the same level of computing power. Digital security has always been a game of tug of war between cybercriminals and defenders; machine learning and AI accelerate this game and give both parties advantages over less technologically capable players. This is particularly relevant as more and more processes and operations are being moved to clouds or to mobile devices, which is broadening the attack surface for would-be attackers. By leveraging machine learning and AI, smaller organizations can now expend a relatively small portion of their resources to effectively improve their cyber defenses and upgrade their capabilities in a way that is scalable and reduces the burden placed on an overtaxed information security workforce.

MODERN OPERATING SYSTEMS & BROADENING ATTACK SURFACES

As organizations follow their chosen paths toward digital transformation, technological advancement has made it difficult for midsized enterprises to keep pace with the security challenges these changes have ushered in. Recently, security professionals have been tasked with managing a number of contemporaneous changes, including the adoption of mobile computing and bring-your-own-device (BYOD) policies, migration to cloud services, and, most recently, the rise of connected non-personal devices that is the trademark of the Internet of Things (IoT). Many information security teams are attempting to address ongoing threats and update organizational policies while being constrained by outdated threat prevention tools and limited financial and staffing resources. Attackers can leverage these gaps by using advanced hacking tools that bypass legacy defense systems.

MANY INFORMATION SECURITY TEAMS ARE ATTEMPTING TO ADDRESS ONGOING THREATS AND UPDATE ORGANIZATIONAL POLICIES WHILE BEING CONSTRAINED BY OUTDATED THREAT PREVENTION TOOLS AND LIMITED FINANCIAL AND STAFFING RESOURCES.

Each wave of technological change that impacts an organization's IT complexion poses subsequent challenges for the security staff. Mobile computing resulted in a standard arrangement of two or three devices for each employee as opposed to one, with each device running its own set of applications. BYOD further diversified the number and types of devices, operating systems, and applications for security teams to manage. The transition to cloud storage and applications, which virtually all companies have embraced to some extent, saw another expansion of the vulnerable attack surface that is substantively different than securing on-premises environments, while hybrid configurations increased the challenge of harmonized security between cloud and physical systems. And as connected IoT devices become more deeply integrated into business processes, security personnel are now scrambling to ensure that every endpoint meets the high security standards that organizations require to remain competitive.

The rapid expansion of attack surfaces, considered here as targets for potential attackers, is of particular importance to midsized businesses that are under constant pressure to achieve the best results with fewer resources. For security teams, some of the most consequential trends to watch are the broadening attack surface brought on by the proliferation of mobile computing and the latent vulnerabilities of upgrading business processes using IoT-enabled devices.

Mobile Computing and Device Fragmentation

Employees today typically carry multiple connected devices that enable them to be productive in various settings. Whereas security workers once needed to worry only about a single endpoint per user, now they must account for various types of devices—laptops, tablets, smartphones, wearables, and so on—that are accessing sensitive documents using different networks, be it LTE/5G, home Wi-Fi, office network, or public Wi-Fi. This adds layers of complexity to an already challenging threat environment. This creates new surface areas for attackers to penetrate and demands a robust security posture at every level.

Similarly, security teams are challenged by ensuring that all product firmware and operating systems are consistently updated with the latest security patches. This is particularly relevant because different mobile, tablet, laptop, and other devices simultaneously support different versions of operating systems and have a different product lifecycle, meaning new devices are constantly introduced into the environment.

Another danger from mobile computing comes from mobile app stores. Malware packaged inside of seemingly legitimate apps on uncurated app stores can steal data, become part of a malicious mobile botnet, incur data charges on a mobile telecom account, track the location of a user, enable an adversary to turn on device cameras and microphones, and listen in on sensitive business conversations.

Device and operating system fragmentation has led to a considerable broadening of the attack surface for potential intruders to exploit. To combat this, security teams need to be equipped with tools that can compete against these advanced threats.

Security Teams Need New Tools for Today's Threat Environment

Advances in modern OS security powered by machine learning are putting control back into the hands of corporate IT security teams while also protecting end-user privacy. Equipping smartphones and tablets with a solution that detects if a device is compromised or under attack is critical. Just as important is a solution that has a minimal impact on the mobile device battery between charges and maintaining the native OS experience for end users.

It is extremely important that organizations are equipped with the latest security platforms to protect mobile devices. Some best practices for ensuring the safety of mobile devices include:

- Ensuring that each smartphone, tablet, and laptop is equipped with advanced anti-malware endpoint protection. The best solutions on the market today use AI or machine learning algorithms that act in real time to combat today's advanced threats.
- Encrypt all communication. While breaking encryption is technically possible, this is a "security hygiene" that can prevent interception of important communications.
- Choose a mobile threat detection solution that automatically quarantines a device that is displaying behavioral anomalies, which can help mitigate the damage in the event of a breach and stop the spread throughout the environment.

There is little doubt as to the benefits of productivity that the fragmentation and proliferation of devices have brought to today's workforce. However, this simultaneously creates a number of new ways for attackers to access sensitive data and environments. Equipping enterprise security teams with the scalable tools to manage the ever-expanding attack surface will help minimize the risks to the enterprise while retaining the benefits of productivity.

THE FINAL WORD

Today's advanced threat landscape poses serious challenges for enterprises of any size. But the rising trend of attacks directed against midsized enterprises should bring security to the forefront of business planning for these organizations. Security cannot be another "box to tick"; it must be central to operations at every level. The traditional configuration of a firewall with an antivirus is no longer sufficient to protect against advanced threats. Endpoints must be treated as an attack vector and safeguarded accordingly. Fileless attacks, lingering threats, and a broadening attack surface are only some of the concerns that security vendors with the latest technologies are helping to fight against. Tools such as machine learning, already in use by attackers, are also critical in the fight against advanced threats.

With the consequences of a breach being so dire, either in the form of lost customers or the outright loss of the business itself, midsized businesses must ensure that their security teams are equipped with the most robust security tools possible. With attacks predicted to rise in the coming months and years, the time to invest in those tools is now.

FROST & SULLIVAN

Silicon Valley
3211 Scott Blvd
Santa Clara, CA 95054
Tel +1 650.475.4500
Fax +1 650.475.1571

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel +1 210.348.1000
Fax +1 210.348.1003

London
Floor 3 - Building 5,
Chiswick Business Park
566 Chiswick High Road,
London W4 5YF
Tel +44 (0)20 8996 8500
Fax +44 (0)20 8994 1389

877.GoFrost • myfrost@frost.com
http://www.frost.com

NEXT STEPS

- Learn how Symantec helps protect your endpoints against today's advanced threat landscape.
- Schedule a meeting with our global team to experience our thought leadership and to integrate your ideas, opportunities and challenges into the discussion.
- Interested in learning more about the topics covered in this white paper? Call us at 877.GoFrost and reference the paper you're interested in. We'll have an analyst get in touch with you.
- Visit our Digital Transformation web page.
- Attend one of our Growth Innovation & Leadership (GIL) events to unearth hidden growth opportunities.

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?