Concerned about cybersecurity threats?

Learn more about managed firewall services and how to help protect your business

ADT

Cybersecurity

69%

of data breaches targeted small and medium-sized businesses.*

* 2019 Ponemon Institute report

Cybercriminals shift their target to include small and medium-sized businesses

Forward

Cybercrimes—the size and complexity of the problem continues to grow. Not only are cyberattacks on the rise across the globe, but cybercriminals have shifted their targets to include a growing focus on small and medium-sized businesses. According to the 2019 Global State of Cyber Security in Small and Medium-sized businesses (SMB), conducted by the Ponemon Institute, 76% of U.S. SMB experienced an attack in 2019 – up from 55% in 2018. Furthermore, according to Accenture, 43% of online cyberattacks target small business with fewer than 14% reporting that they are prepared to defend themselves against them. Sadly, as many as 60% of those business will succumb to those attacks and close their doors (source: 2018 research from National Security Alliance). And the problem only continues to grow as larger organizations harden their defenses against these types of attacks. More importantly, the data that cybercriminals now access from SMBs is more valuable than just a few emails with 69% reporting the loss of sensitive customer and employee data (source: Ponemon report).

Some of the weaknesses that make SMBs attractive to criminals, as cited by multiple experts, are:

- 77% of SMBs state that they do not have the personnel or resources to mitigate cyber risks with 55% citing the lack of funding or budgets as a contributing factor (Ponemon).

- 60% of SMB operators state that they do not have a cyberattack prevention plan in place (source: Keeper Security 2019 SMB Cyberthreat Study).

Furthermore:

- Only 9% of SMBs rank cybersecurity as a top business priority. In fact, 18% rank cybersecurity as their lowest priority (Keeper survey).

- 66% believe cyberattacks are unlikely to affect their businesses (Keeper survey).

What is even more alarming is the unprecedented rise in new threats that traditional security solutions often fail to preemptively identify.

Many organizations have reported that these emerging attacks can evade existing preventive measures. The threats have increased in complexity, making prevention, detection and remediation even more difficult for traditional security software.

It is estimated by AV-TEST.org that more than 350,000 new malicious programs (malware) are registered each day. While computer viruses are nothing new and have been around for decades, the methods and motives behind them have changed dramatically.

Gone are the days when a computer virus was created by talented teenagers trying to show off their coding prowess.

Today's cybercriminals are well-funded and highly sophisticated in their approach, netting billions of dollars in profits from unsuspecting or unprotected targets. This new breed of criminals may be just as skilled and versed in security matters as experts working directly in the security industry.

A 2017 report issued by the Center for Strategic and International Studies (CSIS) cites cybercrimes cost the global economy roughly $600 billion every year.

For companies that do not have the resources or expertise to administer a cybersecurity program on their own, a third-party provider of security services may be their best option. However, before selecting a provider of cybersecurity services, companies should consider several factors and choose a partner that can deliver a holistic approach to help secure their business with a single point of contact.

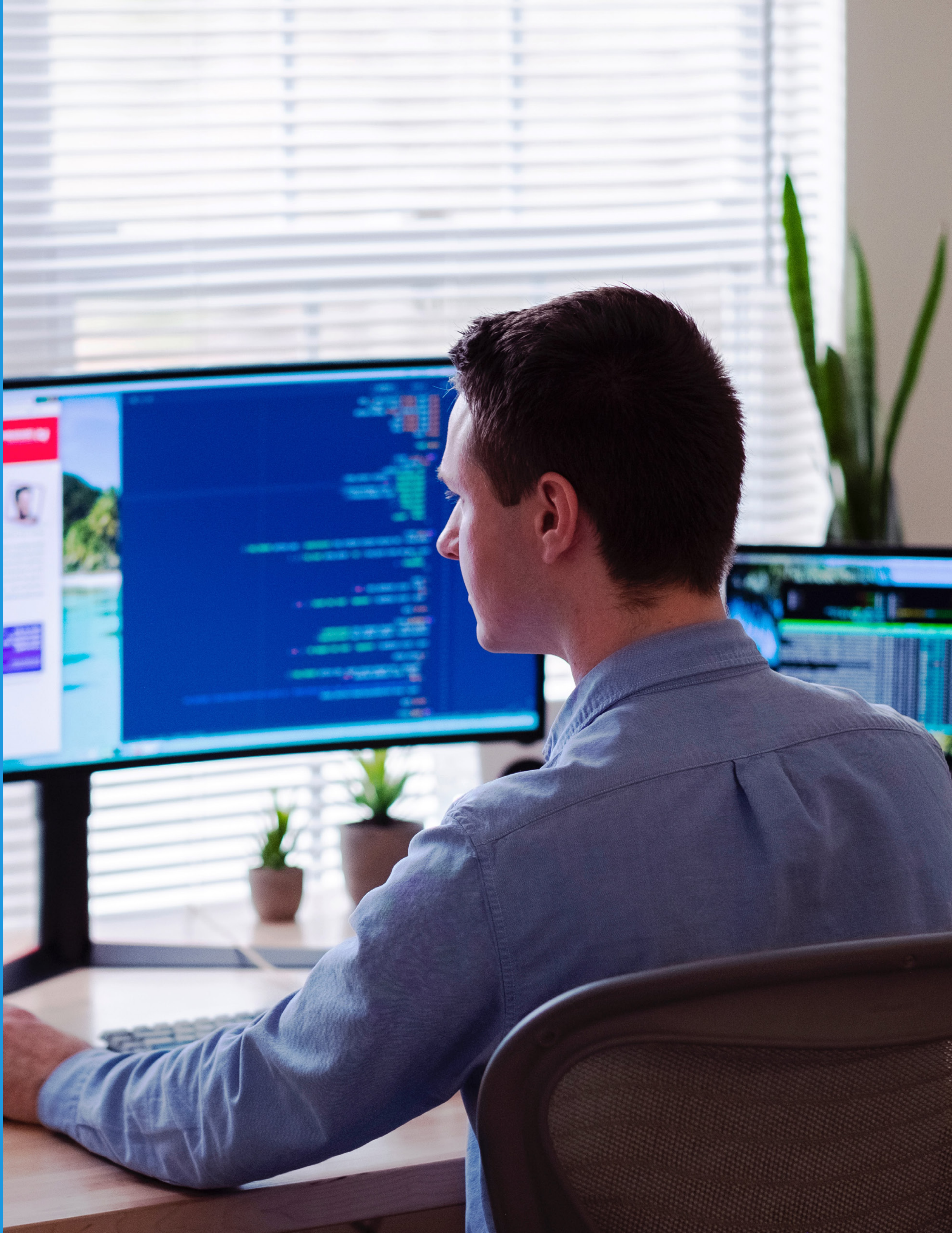
The following white paper outlines some of the factors that should be considered when evaluating the different components of a cybersecurity solution to ensure that the third-party provider is offering the best solution based on world-class organizations.

A multi-pronged problem requires a multi-pronged solution

Cyberattacks come in a variety of forms that can include spam, phishing and social engineering, web-based attacks and general malware such as pump-and-dump schemes, data-stealing Trojans, key loggers and ransomware.

As stated earlier, with more than 350,000 new incidents are registered every day, companies need to look at creating a layered approach to fighting the problem.

At ADT Cybersecurity we believe in partnering with best-in-class organizations that, when combined into a single offering, help to deliver a holistic approach to detecting, preventing and remediating threats to your organization—in real time, 24 hours a day, 7 days a week with a managed and monitored approach.



Network security

For the purposes of this white paper, let's start with how many viruses propagate at the network level. Some of the more common challenges companies face when protecting their networks may include:

Lack of resources to implement a program

Insufficient threat protection software

Lack of visibility into the potential for problems

Commonly referred to as a firewall, this network security application can be either hardware or software-based and controls incoming and outgoing network traffic based on a set of rules.

Many traditional firewall applications may be based on point-in-time controls that are focused on broad prevention only. Often in these scenarios, a file may be scanned just one time to determine if the source contains a virus or other forms of malware.

Given the fact that today's approach to hacking a system is very sophisticated, some viruses may have the ability to "sleep" during the initial review process, possess unknown attack vectors, encrypted executables , or have the ability to polymorph, allowing them to activate the attack at some later point in time. Some write persistent code to the firmware of devices allowing them to survive a factor reset. Some firewall solutions control traffic using a static access list that governs what traffic makes it in and out of the network. This type of firewall fails to protect against threats that have variable or multiple sources on the internet. Modern malicious threats can originate from trusted sources. For this reason adequate network security now requires a solution that employs Deep Packet Inspection to look inside data packets from the internet and inspect them for malicious content, regardless of the source. Some programs will monitor the state of connections to prevent out-of- band-traffic and flag suspicious communications for a protocol. Given the rise in BYOD (bring your own device), many non-controlled devices are being used to access internal networks, so there is now a need to layer your approach to guard against malicious or suspicious activity coming from these sources. Traditional firewalls are often ineffective against new and emerging techniques.

Another important feature of a network security solution is DPI-SSL. In the last 5 years the volume of encrypted website traffic (HTTPS) has risen from around 30% to near 80%.

This change is both good and bad. While HTTPS protects the privacy and security of our personal information it also poses a challenge for cybersecurity. Traditional firewalls do not have the ability to inspect encrypted HTTPS traffic for malicious content. As you can guess, cybercriminals have also turned to HTTPS to encrypt their malware and sneak past firewalls. A modern firewall solution can use DPI-SSL to perform SSL inspection of encrypted traffic. The firewall can then look into this encrypted traffic in order to identify and protect against threats.

When looking for network security, ADT Cybersecurity recommends adopting a solution that provides continuous monitoring for threats and can apply identity-based and device-aware security policies to network traffic to minimize the attack vectors of your network without compromising performance. The solution should embrace an attack continuum that is made up of the following components:

Threat intelligence and analytics for use **before the attack** that will help to:

Discover the threat

Enforce the rules

Harden the defense

Point-in-time detection **during the attack** that can help to:

Detect the threat

Block the threat

Defend against the threat

Retrospective alerting and continuous analysis **after the attack** to help:

Identify the scope of the threat

Contain the threat

Guard against identical attacks in the future

To deliver this type of security, ADT Cybersecurity has chosen SonicWall next generation firewalls. Next generation firewalls:

- Block more attacks with Real-Time Deep Memory.
- Inspection and reassembly-Free deep packet inspection technologies.
- Prevent advanced threats with cloud-based and on-box threat prevention featuring multi-engine sandboxing, anti-malware, intrusion prevention and web filtering.
- Decrypt and inspect TLS/SSL and SSH traffic in real time.
- Gain faster performance through a high-speed multi-core hardware architecture.
- Add high-speed wireless using the built-in wireless controller.

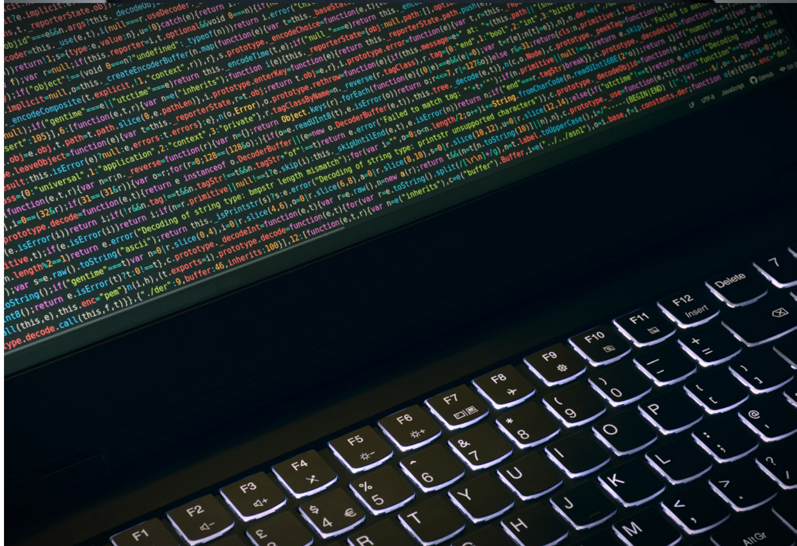
SonicWall also offers virtual firewalls that:

- Help to eliminate breaches for public, private and hybrid cloud environments.
- Help to defend against cross-virtual-machine attacks and side-channel attacks.
- Deploy common network-based intrusion application and protocol protection.
- Help to eliminate unauthorized access to protected virtual data stores.
- Help prevent service disruptions of virtual ecosystems.

Endpoint security

Moving from the network to devices, endpoint security solutions should offer a further layer of security to the overall IT infrastructure. Where network security or firewalls offer the first line of defense against malware, endpoint security refers to security at the device or operating system level, although some applications will overlap. It is imperative, though, that the end user consider several key points when deciding on what approach will work best for them to protect their devices and their data.

- Avoid free software offers. Free anti-virus or endpoint security software typically provides only basic protection and will not protect a company from the variety of threats prevalent today.
- Consider only known and/or trusted brands for your selection criteria. There are many anti- virus software products on the market that are not anti-virus solutions at all but, in fact, could be malware in disguise.
- Choose a product that will protect all your endpoint devices, including mobile, physical, virtual, Windows®, Linux® or Macintosh®. It is important to not only secure your devices but your operating systems as well.
- Insist on a solution that goes beyond traditional signature scanning. Conventional detection software relies on signatures which are code snippets extracted from malware samples and used for pattern-matching. This method takes time to produce the signature and then push that signature to end users, leading to a time lapse where the malware can spread. The complex threats that exists today require behavioral-based and process-monitoring technologies, or heuristics, in order to effectively block the threats. Heuristics do not rely on signatures or binary or code fingerprints to identify a threat but rather on complex algorithms that specify actual patterns and behaviors which may indicate an application is malicious. While the use of heuristics enhance security considerably, it too has some shortcomings.



Virtual private network (VPN) security

With the dramatic increase in remote workers, it is vital to ensure that all employees are using a secure VPN to access the network. A VPN lets you increase the security of your web session, transmitted data, financial transactions and personal information online, from anywhere. New solutions are available that do not require software downloads to employee device and are flexible enough to add licenses and users as needed.

ADT Cybersecurity offers secure VPN connections that protect a wide range of devices, including iOS, Android, Chrome OS, Kindle Fire and Windows.
Secure VPN:

- Offers an easy-to-use solution for secure, encrypted access.
- Maintains the confidentiality of corporate data.
- Establishes IPSec Layr-3 connection between endpoints and corporate networks.
- Provides fast, secure mobile access through an intuitive, easy-to-use app.
- Delivers biometric authentication, per-app VPN and endpoint control enforcement.

Email security

As discussed earlier, phishing and social engineering attacks now account for 53% of incidents followed by web-based attacks at 50% and general malware breaches at 39%. In fact, as many as 90% of cyber attacks start with a successful phishing campaign and 66% of malware is installed via malicious email attachments (source: Verizon Data breach Investigation Report 2018).

To combat these attacks, ADT Cybersecurity deploys secure email filtering with Capture Anti-Phishing technology from Sonicwall. Capture uses a combination of methodologies, including machine learning, heuristics, reputation and content analysis to help stop sophisticated phishing attacks along with spoofing attacks, business email compromise and email fraud.

The solution:

- Helps stop ransomware and zero-day malware from reaching your in-box.
- Helps protect users from clicking on malicious links across any device and from any location with time-of-click URL protection.
- Meets the challenge of new threats less than 24-hours old, with real-time threat intelligence updates.

In conclusion

Cybercriminals will continue to attack businesses of all sizes, with no company or industry being immune. With the number of new or variant threats growing each day at an alarming pace, the cost of just business email compromises alone was projected to be over $5.2 billion a year in 2017.* Add the unknown cost of brand reputation and customer relations looming over a company, the best defense is a layered offense.

No one solution or approach can adequately protect against the barrage of attacks that companies are facing today. Finding a solution provider that can bring it all together for businesses both big and small may offer some relief to a problem that is not going away anytime soon.

Cyberthreats are a cost of doing business these days, so make sure your company isn't the one paying the price.

For more information, visit ADT.com/business/cybersecurity

* Source: Federal Bureau of Investigations

ADT Cybersecurity

This document, materials or presentation, whether offered online or presented in hard copy ("ADT Informational Tools") is for informational purposes only. ADT PROVIDES THESE ADT INFORMATIONAL TOOLS "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

The ADT Informational Tools contain ADT proprietary and confidential materials. No part of the ADT Informational Tools may be modified, altered, reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the prior written permission of ADT, except as otherwise permitted by law. Prior to publication, reasonable effort was made to validate this information. The ADT Information Tools may include technical inaccuracies or typographical errors. Actual savings or results achieved may be different from those outlined in the ADT Informational Tools. The recipient shall not alter or remove any part of this statement.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. ADT Cybersecurity products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective in ensuring network security and regulatory compliance. ADT Cybersecurity does not warrant that its products and services are immune from the malicious or illegal conduct of any party. ADT Cybersecurity products and services are designed to protect your information from the average computer user ©2020 ADT LLC dba ADT Security Services. All rights reserved.