SIZE DOESN'T MATTER IN CYBERSECURITY
SIZE DOESN’T MATTER IN CYBERSECURITY
SIZE DOESN’T MATTER IN CYBERSPACE

03 SUMMARY
05 TOP REASONS WHY SMBs MUST INVEST IN CYBERSECURITY
09 RECOMMENDATIONS
10 FIVE BEST PRACTICES TO HELP INCREASE THE SECURITY OF YOUR BUSINESS
11 CONSIDER CHECK POINT
12 THE CHECK POINT 600 APPLIANCE
13 THE TIME IS NOW
While the internet has brought great opportunities and benefits, it has also brought tremendous risk. As we have seen in the news recently, security breaches are becoming more disturbing and increasingly expensive to clean up. Every day there are data breaches at all kinds of companies, attempting to steal important financial and customer information or disrupt business continuity. Limited financial resources and technical skills have driven many small and medium-sized businesses (SMBs) to compromise on their IT security and settle for rudimentary protection like anti-virus software. However, SMBs have become much more reliant on the internet for their businesses. With growing adoption of cloud services and an increase in e-commerce, the internet has become the lifeline of SMBs. And, recent developments in cybercrime have demonstrated that SMBs require a new security strategy to stay ahead of new threats.

Cybercrime has greatly evolved and doesn’t only target large companies. Over the decades, it has become extremely destructive to both large and small companies around the world. Attackers hide malware inside documents, websites, hosts and networks. Typically, they focus on stealing data, sabotaging business continuity, or damaging a company’s reputation.

There is a general misconception that SMBs are not vulnerable to cyberthreats, or that they don’t need robust security like large enterprises. This is simply not true. Often times, small business owners do not realize just how vulnerable they are to cyberthreats.
This is not a statistical anomaly. Hackers target SMBs for specific reasons. Yet, despite these numbers, many small business owners believe that hackers will simply not waste their time targeting them, especially when there are much bigger organizations with more important information to lose. This couldn’t be farther from the truth.

The purpose of this document is to provide you with perspective and solutions, to deepen your understanding of the threat landscape, and to help you better protect your customers, employees and business assets.

1 National Cybersecurity Alliance
A successful business works on the basis of revenue growth and loss prevention. Small businesses can suffer the same kinds of cyberthreats that have plagued large enterprises over the past year. In fact, the small enterprise is becoming more attractive to cybercriminals for many reasons. For that reason, small businesses have a host of modern threats that they have to manage.

Just because a business is small, it doesn’t mean it’s immune to threats. Security challenges facing small and medium-sized businesses globally are on the rise. For businesses of all sizes, viruses, hacker intrusions, spyware, ransomware and spam can lead to lost or stolen data, computer downtime, decreased productivity, compliance issues, lost sales and even loss of reputation resulting in substantial financial damages.
UNIQUE NEEDS AND CHALLENGES
Small businesses need the same levels of protection as large enterprises, but without the complexity, cost and expertise. This means they need security that consolidates functions to achieve powerful defenses but doesn’t require a dedicated staff or deep expertise. They need security that just works, right out of the box.

THE IDEAL TARGET
Large corporations have highly valued information that hackers like to steal. However, they typically have extensive resources to achieve a high level of protection. But small-to-medium-sized businesses are a cybercriminal’s ideal target because they are, typically, the path of least resistance. SMBs have sufficiently valuable information to make it worth an attacker’s time, yet the organization’s protection level is typically weaker than that of larger enterprises.

SOCIAL ENGINEERING
Social engineering is perhaps one of the biggest issues for small businesses. The fact is, people are the easiest way in. Taking advantage of human nature is a given for hackers targeting small enterprises. Social engineering tricks people into revealing personal information such as login details, or into performing actions like downloading malware disguised as an attachment or link.

WATERING-HOLE ATTACKS
If you have large companies as customers, you’re an even bigger target. Watering-hole attacks refer to using the services of one organization (typically a small business) in order to gain access to even the largest, most secure and sophisticated companies and government agencies. Because it’s difficult to get malware onto major, high-traffic websites like major news sources or large corporations, cybercriminals target smaller, less-secure sites (i.e. watering-holes) that are frequented by employees. This means that SMBs are used as a channel to access other corporations.
HERE ARE A FEW EXAMPLES OF HOW SMALL BUSINESSES ARE USED TO ACCESS LARGE COMPANIES:

- Target’s point-of-sale system was compromised through the network of a small HVAC contractor.

- CNN, Washington Post, and Time were compromised by ‘hacktivists’ through Outbrain, a content syndication provider.

- LoyaltyBuild caused a 500,000+ card breach in Europe, heavily affecting the grocery company SuperValu, which has over 200 stores in Ireland.

- Patient data from a Florida hospital was breached through a small billing company.

- Hackers wrote malware into the online menu of a Chinese restaurant that was popular with employees of a large oil company. When employees browsed the restaurant’s website, they inadvertently downloaded malicious code that gave hackers traction into the company’s computer network.

These events show that small enterprises are not only vulnerable to being directly hacked, but also hacked to gain access to larger businesses and those companies’ customers.
DAMAGED REPUTATION
When a large enterprise suffers a costly data breach, it will suffer financial losses and damage to its reputation. As embarrassing and expensive as that can be, most likely, the enterprise will eventually recover. Small businesses are not so lucky.

It takes years to build a solid reputation and a data breach can destroy that reputation in seconds. Small enterprises can thrive or fail, depending on their reputation and customer service. If your business suffers a breach and sensitive information is stolen, your reputation can be jeopardized. And because small businesses don’t usually have the same robust security and resources as large enterprises, the chance of recovering from a devastating data breach is low.

PARALYZING FINANCIAL LOSSES
Security might cost money, but a breach could put you out of business. Data breaches are costly, and small businesses just can’t afford to suffer that level of financial loss. It can immediately and negatively impact sales, and expose the company to litigation expenses, lawsuits, damages, fines and penalties, as well as the costs associated with experiencing business interruption.

SECURITY MIGHT COST MONEY, BUT A BREACH COULD PUT YOU OUT OF BUSINESS.
RECOMMENDATIONS

Be proactive. It’s far less costly to prevent an attack than it is to recover from one. So, how do we protect ourselves in the digital age? Small companies must possess intelligent technology that will identify and block the attacks—offering complete protection of the network and the data.
FIVE BEST PRACTICES TO HELP INCREASE THE SECURITY OF YOUR BUSINESS

1. **HAVE A SOLID NEXT-GENERATION FIREWALL**
   Firewalls are a company’s first line of defense. They are a fundamental part of any network security strategy, serving as a type of gatekeeper. Inspecting all data passing in or out of the network, firewalls ensure that the traffic is safe.

2. **INSTALL ANTI-MALWARE/ANTI-VIRUS PROTECTION**
   All computers and internet users, regardless of the reasons that they are online, need to have the latest anti-virus software programs installed on their computers. It can protect your vital documents and files from becoming damaged or lost forever.

3. **BE MINDFUL OF SOCIAL MEDIA (APPLICATION CONTROL)**
   Social media sites are a treasure trove for cybercriminals looking to obtain information about people, to improve their success rates for attacks. Educating employees to be cautious with sharing on social media sites, even in their personal accounts, can go a long way in keeping your organization secure.

4. **PROTECT AGAINST EMAIL SPAM**
   Email can create a host of problems for companies. Most spear phishing and social engineering attacks begin with email. This is precisely why strong spam filtering is necessary for small enterprises.

   If your email is hosted off site, you can prevent most email spam from ever reaching your company’s internal network by implementing spam filtering.

5. **SSL INSPECTION**
   More than 30 percent of internet traffic is encrypted with SSL, and it’s important that your business have the ability to inspect this traffic. SSL inspection can halt attacks, but also track if employees send data outside of your company. For example, employees that use SSL-encrypted Gmail may accidentally leak passwords and other personal information. SSL Inspection can safely eliminate threats that originate from internet traffic.
CONSIDER CHECK POINT

For decades, Check Point has been the leader in protecting some of the biggest security-conscious companies from the worst cyberthreats in existence. That same level of security is available to small enterprises through specialized products and services that effectively defend against the vast array of cybercrimes.
Many small and mid-sized businesses are challenged by their reliance on point solutions that each provides a piece of the security puzzle. The reality is, these different systems that are brought together are not meant to work together, and as time goes on, these solutions cause more complexity and problems. With Check Point, this is not the case.

The same protection used by large enterprises and Fortune 100 companies is now easily accessible for an SMB organization. Check Point has removed the complexity, one of the chief challenges for SMB organizations. The same next-generation firewall (NGFW) deployed to deliver the highest levels of protection for large enterprises, is now available in a simpler, easy-to-use, easy-to-manage small business package.

COMPREHENSIVE SECURITY PROTECTIONS
Small businesses need multi-layered security in a simple, affordable solution. The Check Point 600 is an all-in-one network security solution featuring an industry-leading firewall, VPN, URL filtering, anti-virus, anti-spam and next-generation threat prevention—specifically designed to meet the needs of small businesses.

Whether you use Macs, PCs, laptops, tablets or mobile devices, the Check Point 600 is a total security solution. The Check Point 600 protects your data on site and remotely via VPN, so you can stay securely connected anywhere and anytime. This is a one-stop, robust security solution for your business.

Features:
• Next-generation enterprise security is designed for SMBs that require maximum protection against modern hackers and malware.
• Comprehensive software blade architecture optimized for SMBs protects all network vectors and delivers complete security coverage.
• Single device consolidates security with cloud-based management on a single high-performance hardware platform.

Check Point’s customers include tens of thousands of organizations of all sizes ranging from small businesses to the largest of Fortune and Global 100 companies. The Check Point 600 Security Gateway lets every business access enterprise-grade cybersecurity.
Security has to be taken seriously all the time, not just when it is convenient. Small businesses are being targeted more than ever before, and the risk of hackers gaining access to vital customer data is real. It’s no longer an option to secure your business. It’s a requirement. Your business is important and requires a solution that delivers the best security on the market, in a package that is cost effective and easy to use. Check Point’s 600 Security Gateway appliances are the best way to protect your business from the different cyberthreats in existence today, in one integrated solution.

By understanding potential threats and vulnerabilities; creating a solid plan that aligns with your business; and ensuring protections are integrated into your IT infrastructure, you can turn security into an enabler. And in doing so, you’re able to foster an environment for high performance and productivity.

Don’t risk the integrity of your business. If you’d like to get a cybersecurity assessment, sign up for a free Check Point Security Check Up at [www.checkpoint.com/resources/securitycheckup](http://www.checkpoint.com/resources/securitycheckup). Or, to learn more about Check Point and how we can help secure your small business, please visit [www.checkpoint.com](http://www.checkpoint.com).
To learn more about how to secure your organization, please visit www.checkpoint.com