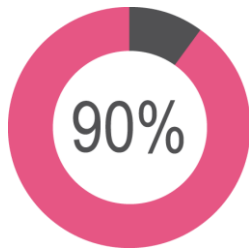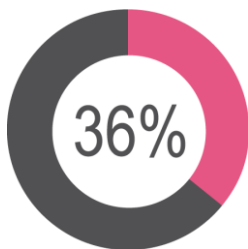# Check Point®
SOFTWARE TECHNOLOGIES LTD.

THE ATTACKER'S TARGET:
THE SMALL BUSINESS

90%

90% OF SMBS DO NOT HAVE PROFESSIONAL IT MANAGERS ON STAFF.

National Cyber Security Alliance, National Small Business Study in 2012

36%

36% OF CYBER ATTACKS ARE AIMED AT SMALL BUSINESSES AND 60% OF SMALL BUSINESSES WILL CLOSE WITHIN 6 MONTHS OF AN ATTACK.

The Cyber Security Alliance

INTRODUCTION

Cybercrime is increasing at epidemic proportions, from consumers, to SMB organizations to large enterprises. According to avtest.org, an independent service provider of anti-virus research, more malware was found in the past two years than in the previous 10 years combined. From 2013 to 2014, new malware jumped just over 71 percent from 83M to 142M new strains being introduced. And it turns out Small to Medium Business (SMB) organizations are becoming the cybercriminal's "sweet spot". Large enterprise organizations have highly valued information that cybercriminals like to go after, however, larger businesses typically have significant budgets and resources to achieve a high level of protection. Consumers on the other hand, have lower value information for attackers, yet they also have a low level of protection.

SMBs represent the best ROI for cyber-criminals
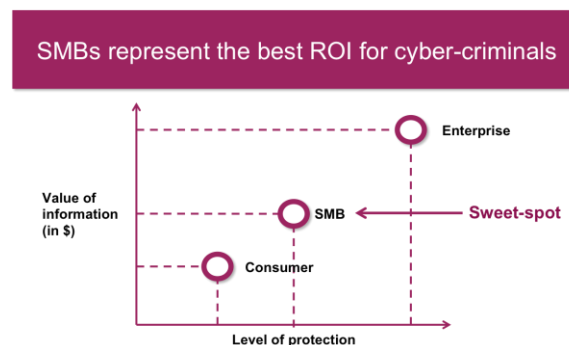
However, it turns out that SMB organizations are a good target for cybercriminals. There is sufficiently valuable information to make it worth an attacker's time and the organization's protection level is typically weaker than that of a larger enterprise. In fact, a recent small business study done by the National Cyber-Security Alliance found that 90% of SMB organizations did not have professional IT managers on staff, much less cyber security specialists.

So why do SMB organizations not do more to achieve higher levels of protection?

According to a 2014 Huffington Post survey of small businesses, 42% of businesses with 1-9 employees are not taking any measures, compared to 28% of businesses with 10-19 employees and 23% of businesses with 20-99 employees. These numbers do make sense, as smaller companies do not believe they have as much sensitive data to protect.

31%
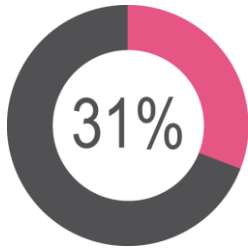
31% OF SURVEYED SMBS ARE NOT DOING ANYTHING TO PROTECT AGAINST SECURITY THREATS.

OF THOSE SURVEYED…

63% ARE WORRIED ABOUT MALWARE

38% ARE WORRIED ABOUT PHISHING ATTACKS

41% ARE WORRIED ABOUT BREACHES DUE TO INTERNAL EMPLOYEE ERROR.

Huffington Post SMB Cyber Security Survey, June 2014

The survey also found that 29% of those companies with less than 10 employees were working with third party vendors to help with security, compared to 45% for companies with 10-99 employees. These small businesses have become a more attractive target for hackers because they typically lack security infrastructure. For those that do get attacked, 60% of small businesses go out of business within 6 months of experiencing a data breach.

ENTERPRISE-GRADE PROTECTION FOR THE SMB ORGANIZATION

Small businesses need enterprise level protection without the complexity, cost and expertise. This means they need security that consolidates the functions to achieve a high level of protection, security that doesn't require a large staff or (deep expertise) and security that just works, right out of the box.

The same protection used by large enterprises and the Fortune 100 is now easily accessible for an SMB organization. Check Point has removed the complexity and need for expertise, the very issue that SMB organizations have faced. 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.

The Check Point 700 Series Appliance simplifies achieving strong protections for any SMB organization

- **Enterprise grade security**—The security technology that protects large organizations is used in the 700 Series Appliances.

- **Easy setup**—Plug it in, follow a simple set-up wizard and start putting protection in place.

- **Out of the box protection**—Policies are included that deliver protection immediately, adjustments can be made to tailor policies for your business.

- **Low price**—Starting at $499, the 700 Series Appliances delivers protection with a modest investment.

- **Easy management**—Ongoing management and upkeep is simple

ENTERPRISE CAPABILITIES IN A SMALL PACKAGE

The 700 series appliances provide all the security functions needed to achieve a high level of protection. The security functions of the 700 appliance enable you to control who accesses your network, prevents attacks and threats, and secures communications with your business from remote employees or additional business locations. Having the tools is important. Knowing how to use them simply and effectively is critical. The number of data loss incidents that were attributed to system administrator errors was a staggering 60%, according to the 2015 Verizon's Data Breach Investigation Report.

60%
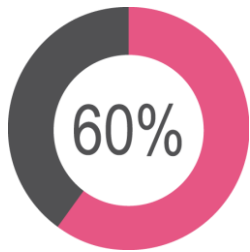
60% OF BREACH INCIDENTS ARE RESULT OF SYSTEM ADMINISTRATOR ERRORS.

Verizon Data Breach Report, 2015

Security Dashboard: Control and monitor Software Blades configurations and status

ACCESS POLICY

Firewall

Applications & URL Filtering

User Awareness

QoS

THREAT PREVENTION

Intrusion Prevention (IPS)

Anti-Virus

Anti-Bot

Anti-Spam

VPN

Remote Access

Site To Site VPN

CONTROL ACCESS TO YOUR NETWORK

Just like enterprises, small businesses need to ensure that only authorized traffic and users are allowed to access the network. They must also ensure that only appropriate websites are accessed by users. Policies span various capabilities that are used to protect the network.

- Firewall—Ensures only the traffic that should be allowed on the network traverses the network. Prohibited traffic is blocked before it ever enters the network.
- **Application Control and URL Filtering**—These capabilities work together to ensure that only allowed applications are used on the network and that only allowed websites can be visited.
- **User Awareness**—Allows an organization to have polices in place that will allow or prohibit what specific people can do, based on their identity or role in the business.
- **QoS**—Quality of Service allows you to give priority to your most important traffic.

47%
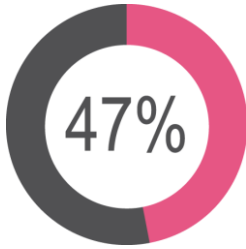
47% OF SMB'S BELIEVE THEY ARE NOT A TARGET FOR CYBER-ATTACKS BECAUSE THEY FEEL THAT THEY ALREADY PROTECT THEMSELVES WELL ENOUGH.

National CyberSecurity Alliance National Small Business Study in 2012

PREVENT ATTACKS AND THREATS

Large enterprises use high levels of protection to defend the business from threats. Small businesses now can leverage these threat prevention technologies to defend their business.

- **IPS**—Intrusion Prevention Systems search traffic for attacks targeting business computers and devices. Computers and devices that do not have the latest patches are protected by the IPS.
- **Anti-Virus**—Malware such as viruses and worms are prevalent and can cause major damage. Anti-Virus blocks malware before it can get into the network.
- **Anti-Spam**—Unwanted email is an issue for any business. Anti-Spam blocks SPAM email messages that can also often deliver malware or lead users to malicious sites.
- **Anti-Bot**—Bots collect information to send to their command and control center for further malicious activity. Anti-Bot will detect and block that communication.

PROTECT BUSINESS DATA

When computers communicate with other computers or remote users, the information can be captured by attackers if it is not encrypted. Virtual Private Networks (VPN) encrypts data traversing the network, allowing only the intended receivers to read the information.

- **Remote Access**—Encrypts traffic from PC's and user devices to the network, whether they are in the office or on the road.
- **Site-to-Site VPN**—If a business has multiple offices, this VPN encrypts all communications between multiple office locations.

SECURITY MANAGEMENT PORTAL

Outsourced security services are one of the fastest growing segments in the security market. Security Management Portal (SMP) introduces a central management and service provisioning platform that answers the needs of a Managed Security Provider (MSP) targeting SMBs and vertical markets. It features an intuitive web-based user interface and uses robust architecture to support the management of up to 10,000 Check Point 600, 700, and 1100 Appliances.
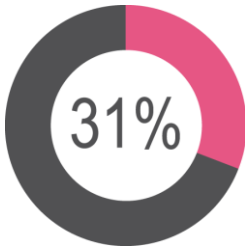
WHY CHECK POINT?

The Fortune 100 relies on Check Point for security. Other providers don't bring the level of expertise and experience delivering high levels of protection. Only Check Point delivers enterprise-grade security in a compact, easy to manage package, designed to meet the needs of a small business.

Network World performs independent tests each year that compare SMB security products. In both 2013 and 2014, Network World concluded that Check Point was the clear choice. "Check Point is our Clear Choice Test winner… It has an appealing user interface, a lot of great security features, is simple to manage and create new security rules".

$36,000. AVERAGE COST OF A DATA BREACH FOR A SMALL BUSINESS.

First Data Market Insight, Small Merchants: The Cost of a Data Breach, 2014

31% OF CUSTOMERS SURVEYED SAY THEY TERMINATED THEIR RELATIONSHIP AFTER BEING NOTIFIED OF A BREACH.

Ponemon Institute on Breach Notification May 2014

NETWORK WORLD SHOOTOUT SCORECARD

Product	Calyptix	Check Point Software	Dell/ Sonicwall	Fortinet	Sophos	WatchGuard
Installation	3.5	5	3.5	3	3	5
Features	3.5	4.5	4	4.5	4	4.5
Value	3.5	5	3	4	4	5
Total	3.5	4.8	3.5	3.8	3.7	4.8

SCORING KEY > 5: Exceptional, 4: Very Good, 3: Average, 2: Below Average, 1: Consistently Subpar

WHAT ARE YOU WAITING FOR?

Security for a small business is too important to ignore. With the Check Point 700 Appliance, small businesses can feel confident that they have the best security available, in a package that doesn't require extensive expertise or time to get high levels of protection.

Contact a Check Point Authorized Reseller today to get started with enterprise-level security that protects the small business.

Visit www.checkpoint.com/smb for more information.

CONTACT US **Worldwide Headquarters** | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com