Check Point
SOFTWARE TECHNOLOGIES LTD.

STOPPING
THE NEXT MASSIVE CYBERATTACK

STOPPING THE NEXT
MASSIVE CYBERATTACK

Cybercrime is now a leading menace of 21st century businesses, casting a global shadow that seems both omnipotent and ubiquitous. While the dramatic scope of the recent attack on Sony Pictures Entertainment sent shockwaves through the business world, a high profile string of other breaches in 2014 – many involving major retail brands, as well as government agencies and vendors connected to high profile organizations – has proven that organizations of any size and type can be targeted. Perhaps even more unsettling, many cybercrime victims have been breached despite sizeable security investments and best-of-breed product deployments. For this reason, the sophistication of recent attacks has created a widespread sense of fear and distrust among consumers.

> "THE SOPHISTICATION OF RECENT ATTACKS HAS CREATED A WIDESPREAD SENSE OF FEAR AND DISTRUST AMONG CONSUMERS."

The reality is that organizations can protect themselves against cybercrime by moving from a model of "operations first, security second" to "secure operations" as the primary goal. By partnering a security-driven network architecture and security infrastructure with experienced security staff, organizations can fight malicious actors. The mistaken assumption is that technologies can, on their own, resolve or compensate for foundational flaws. They cannot. But by soundly architecting the network foundation and designing and deploying the best security infrastructure possible, businesses can prevent and mitigate future attacks.

One productive exercise: by analyzing and assessing major attacks and comparing them against one's own infrastructure, operations and incident response readiness, organizations can yield valuable insight into their security vulnerabilities and operational weaknesses. While many details surrounding high visibility attacks have not been publically disclosed, understanding what is known can provide invaluable insight into techniques used by cybercriminals and help identify preventative steps to reduce risk and stop potential future attacks.

The Sony Pictures Entertainment security breach is an especially useful case study. After infiltrating the network, cybercriminals used custom worm malware to quickly gain access and then move across the network to distribute more malware onto user devices. Terabytes of sensitive proprietary data and employee personally identifiable information (PII) were successfully exfiltrated from the network and stolen. Upon completion, the attackers launched destructive malware that erased the hard drives of the internal computers and servers in an attempt to cause damage and destroy evidence to evade forensic analysis activities.

To break the patterns that leave businesses vulnerable and open to attack, organizations must review, re-architect and re-secure their networks from the ground up. In this way, they can turn cybercrime insight into security action, and hold attackers at bay.

FIVE STEPS TO STRONGER SECURITY

STEP 1
ASSESS

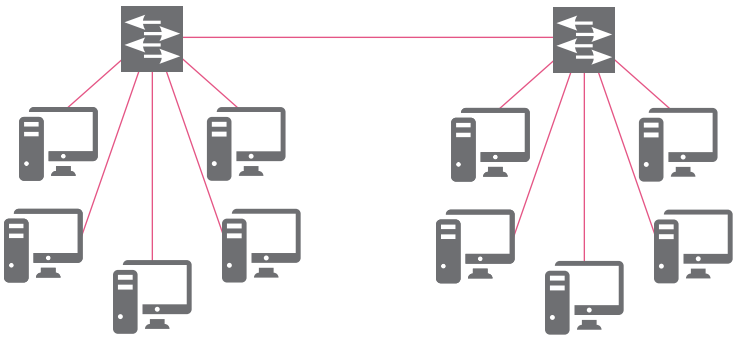
Given the ever-increasing sophistication of cybercrime methods, organizations must employ advanced assessment tools and practices to reduce or eliminate security gaps. Conducting an objective review of the current environment is the first step toward achieving a sound security foundation. A comprehensive assessment should evaluate current posture in all areas, from network architecture and security infrastructure and policy to monitoring capability and incident response readiness. By conducting this evaluation, organizations will generate the input required to design a blueprint for fundamentally secure operations.

ASSESS	CONSIDERATIONS
NETWORK ARCHITECTURE	
Ingress/Egress	How many ingress/egress points are there? Where are they and how are they used? How are they protected, managed and controlled?
Critical Services	What are the critical services required to run day-to-day business operations? Are they properly protected by physical segmentation? What controls are in place to protect their operation?
Critical Data	What are the critical data sources and data stores? Are they properly protected by physical segmentation? What controls are in place to protect access and fidelity? What data should be encrypted at rest and in motion?
Segmentation	Is the network segmented to properly prevent easy access across large portions of the network? Are ingress/egress points similarly segmented? Critical services and data?
SECURITY INFRASTRUCTURE	
Security Controls	What security controls are currently in place... > at ingress/egress points? > to protect critical services? > to protect critical data? Is critical data at rest and in motion encrypted? Do security controls support user identity? Are security controls in detect or prevent mode? Are security controls set to block known, critical attacks? What password policy controls are in place for administration, operations and general users? What advanced threat prevention controls are in place? > Where are they deployed? > Are they in detect or prevent mode? > Are they integrated and supporting the entire security infrastructure or are they standalone?

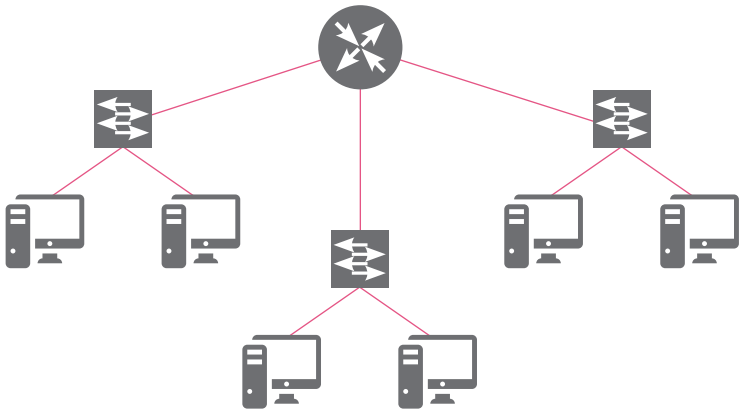
STEP 2
SEGMENT

Following a thorough assessment, the next step is network segmentation. By creating proper controls, organizations can stop high velocity attacks by containing the infection before it escalates across the global network and departmental boundaries. Critical services and data stay protected. Legitimate, credentialed access and business operations proceed unfettered. For example, an attack that successfully penetrates a research and development system would be isolated and unable to access personnel or financial records or order management systems.

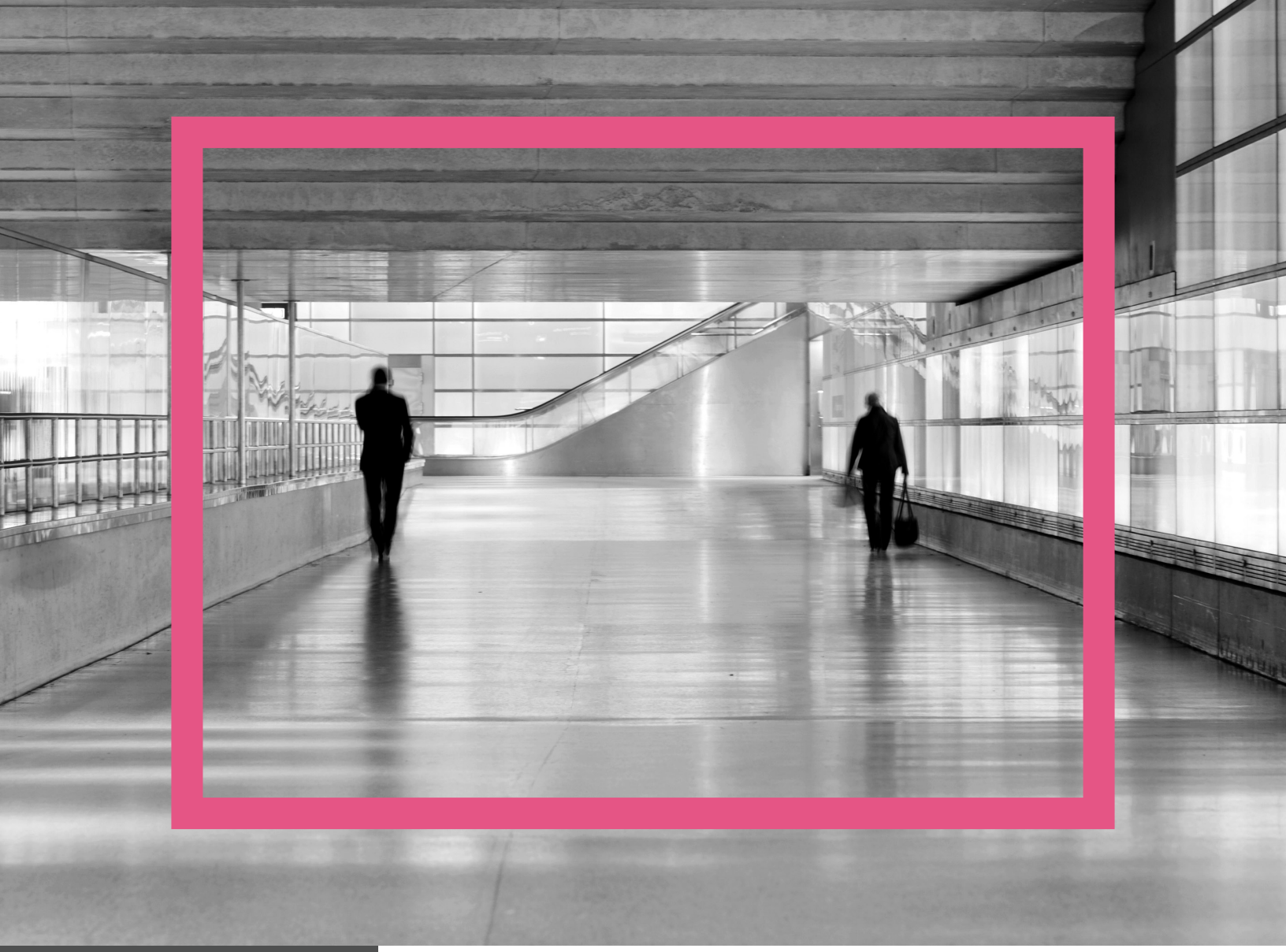
FLAT NETWORK



SEGMENTED NETWORK



To strategize their segmentation approach, organizations often find it helpful to take a defensive approach and work backward from worst-case scenarios. For instance, if an internal workstation is compromised, what other services and machines could that workstation communicate with or contaminate? By reverse-engineering the infection path, teams can identify prime areas for segmentation.



STEP 2
SEGMENT

Key Elements of Segmentation

Limited Access

Critical departments, services and data should be segmented first. Following that, limit network access between internal departments. Third party access must be carefully controlled, including facilities and non-essential service partners that can provide unsuspected back door entry for attackers.

Data Classification

All data should be classified based on its sensitivity and the impact of its disclosure or corruption, with segmentation controls applied accordingly. Every organization will need to define a classification scheme, such as top secret, confidential, restricted, for internal use only or public; it will also need to identify data types such as source code, customer information or human resources data.

STEP 3
ADD SECURITY CONTROLS

With a properly segmented and secure network architecture established, the next step is the implementation of security controls. These controls should be constructed to further protect business assets and operations while enforcing business policy and industry standards.

The security infrastructure protects critical assets and operations by detecting and preventing attacks. As we know, today's advanced threats are designed to compromise specific targets using advanced techniques to monitor and steal information over long periods of time. Thwarting these threats requires an equally sophisticated, comprehensive, multi-layered threat prevention solution. The different layers should work together as one solution that detects, announces and prevents both traditional and advanced attacks. To maintain the latest protections against newly emerging threats, the solution should be supported by dynamic, real-time threat intelligence feeds derived from white hat information and collaboration.

The multiple security layers should offer multiple opportunities to detect an advanced attack as it progresses through its stages and across the network domain.

COMMON PHASES OF AN ATTACK	ATTACK ACTION	SECURITY LAYERS	SECURITY ACTION
Access	Exploit a known vulnerability to gain network access and download malware.	Intrusion Prevention Systems (IPS)	Detects and prevents attacks against known vulnerabilities.
Download Malware	Download the malware to begin the attack.	Anti-Virus (AV) URL Filtering	Detects and prevents known infected files from being downloaded and known bad URLs from being accessed.
Download Unknown Malware	Bypass AV by downloading previously unknown malware for which AV has no signature.	Sandbox	Evaluates files in safe environment to detect and block infection before they contaminate machines or the network.
Command & Control Communications	Establish outbound communications for attack instructions, more malware or export of stolen information.	Bot Protection	Detects and prevents bot communications and prevents bot damages.
Export Stolen Information	Transport stolen information out of the network to the attackers.	Data Leakage Protection	Detects and blocks illegitimate outbound transfers of critical information.

STEP 3 ADD SECURITY CONTROLS

Threat Prevention Policy

Threat prevention policy should be defined to deliver secure operations.

- Configure threat prevention layers to prevent all known critical attacks.
- Create an active process that evaluates and moves new protections to prevent mode.
- Support user identity to facilitate monitoring and incident response effectiveness.
- Advanced threat prevention layers should ideally be integrated with the overall solution, rather than being deployed as an "island solution" that operates without collaboration with the full security infrastructure.

Strong Password Policies

Default and weak passwords are common access points in many attacks, particularly brute force attacks. Mandatory password policies should be implemented for all administration servers, operations staff and general users, with all user levels being required to change passwords regularly. The ideal is every 90 days. Password policy should further require standards such as a minimum of eight characters that include upper case, lower case and numeric characters. In the case of key administration services, a special character should be required as well.

Least Privilege Practices

"Need-to-know" policies define and enforce which team members are allowed to access specific data and company assets. These policies also restrict unnecessary and illicit access and the ability to make unapproved changes, while blocking malicious actions and the access to sensitive information.

Data Encryption

Many past data theft attacks have succeeded only because the critical data was not encrypted. Organizations must encrypt all critical data at rest and in transit to prevent unauthorized disclosure in the event of theft and loss.

STEP 4
MONITOR

Monitoring is a critical security element for sound operations. The increased visibility alerts organizations to the onset of an attack, and exposes security controls and policies that are no longer working. It's clear from several recent high-profile breaches that better monitoring processes would have controlled and possibly prevented the attacks. In some instances, the systems guarding both the perimeter and the network generated alerts but the warning signs were missed or ignored.

Every organization must have trained and designated staff to monitor, review and respond to all high severity events. This is just one example of why even best-of-breed technology must be used in tandem with a knowledgeable team who will look for anomalies, interpret warning signals and respond strategically.

FUNDAMENTALS
OF SOUND SECURITY MONITORING

8 Monitoring Steps to 24/7 Security

1. Monitor logs daily
2. Correlate logs from different technologies
3. Tune detection and analysis rules based on logs
4. Identify potential incidents with anomaly detection tools
5. Stay familiar with network assets
6. Use visualization to assist expert analysis
7. Maintain logs for 90 days or more
8. Retroactively review logs based on new data

STEP 5
INCIDENT RESPONSE PLANS

According to the Check Point 2014 Security report, 88% of organizations experienced at least one data loss incident in the previous year. From invisible malware to company-wide disasters, almost every business will eventually find itself amidst the panic and escalating loss of an active attack.

For this reason, incident response plans are critical as they can make the difference between a contained incident and a brand-destroying catastrophe. From disaster recovery to business continuity, organizations must map out scenarios from the most common to the most severe, and formulate a plan to keep their business running even as they deal with the attack.

Such plans should address every conceivable question, such as:

What should the team do now that the systems are down?	Who should be notified?	What if proprietary source code is disclosed on the Internet?
Is there a plan in place?	How can partners and service providers help?	What if it's an insider threat?
Who is in charge?	Who should the team call if the web server gets compromised?	Is there a LAN with separate connectivity that can be used to maintain business-critical activities?

STEP 5
INCIDENT RESPONSE PLANS

The first step in constructing an incident response plan is establishing a communication plan with a call chain of representatives from all departments, as well as key external partners. The next step: putting together an action plan to keep the business up and running even as the team focuses on stopping the hackers and mitigating any damage. At this point, organizations will need to ask themselves if their teams are fully capable of implementing the necessary actions, or if using service providers with incident response expertise is the wiser strategy. Many providers can handle an attack with greater speed and effectiveness than an organization engaged in the fight to stay functional.

The plan must be tested on a regular basis to make sure it remains relevant and effective. The response plan can be tested live or as a table-top exercise; the lessons learned will help sharpen the organization's incident response capabilities and ultimately reduce exposure and downtime.

On a related note, all relevant teams and contacts must be educated on the proper processes and standards, from their individual roles to working with other involved parties including executive management and law enforcement. This should include media and public relations training. As seen in many recent high visibility breaches, many organizations have suffered a tarnished brand reputation that was due in part to their breaches, but also an inability to control their internal incident response and ultimately their public images in the wake of the attacks.

> "ALL RELEVANT TEAMS AND CONTACTS MUST BE EDUCATED ON THE PROPER PROCESSES AND STANDARDS."

SECURITY SOLUTIONS TODAY
FOR STOPPING TOMORROW'S ATTACKS

The rising wave of cybercrime has taught all businesses that they must proactively and preemptively strengthen their security now, before the next attack. Malicious actors understand quite well how to exploit the security gaps so rampant across industries – but by learning from breaches past, and committing to secure operations through advanced protection and prevention in both their architecture and their solutions, organizations can avoid becoming an attack disaster story and instead become an example of security success.

The unavoidable truth in cybersecurity is that criminals require only a single moment of success to infiltrate a system. Organizations must be vigilant around the clock. Achieving that level of relentless protection requires the right systems, expertise and network architecture to stop and contain attacks.

As the world leader in internet security, Check Point offers innovative threat prevention solutions that go beyond standard cybersecurity tactics. Check Point can assist organizations in addressing all five steps in building stronger network security by providing risk management solutions.

SECURITY SOLUTIONS TODAY
STOPPING TOMORROW'S ATTACKS

The Check Point Security Checkup.

At any given moment, an organization's network can contain stealth malware, data leaks and other security issues. Check Point's Free Security Checkup reveals hidden issues like bot, virus and malware infections, high-risk web applications and exploited vulnerabilities. Organizations can stop and mitigate the problem, while receiving detailed recommendations and guidance from an extensive threat analysis report. Check Point also offers whiteboarding sessions to help organizations identify the most beneficial security architecture, and services to design, deploy, operate and optimize security foundations and infrastructures.

Software Defined Protection.

To stay ahead of fast-moving threats, organizations need an agile security infrastructure designed for today's dynamic networks. Check Point's Software-Defined Protection provides collaborative threat intelligence and a secure, modular infrastructure that delivers enhanced awareness, control and protection. Security administrators get real-time visibility into the network security posture, sharpening incident response; software-defined protections adapt to new threats and changing network configurations while an enforcement layer segments the network, providing modular protection that prevents attacks from proliferating and letting authorized traffic flow unimpeded.

Next Generation Threat Prevention.

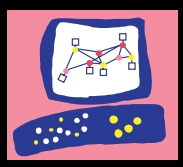
A multi-layered line of defense and extensive security intelligence coverage is essential to combatting today's threats while preventing tomorrow's attacks. Check Point's Advanced Threat Protection solutions, including Antivirus, Anti-Bot, IPS, Threat Extraction and Threat Emulation, defend against known and unknown threats. Using the most advanced tactics available today, Check Point solutions work together to elevate prevention and response aptitude against botnets, targeted attacks, advanced persistent threats and zero-day threats.

Check Point ThreatCloud Managed Security Service.

Handling the quantity and complexity of rising network threats requires expert threat analysis and knowledge around the clock. Check Point's ThreatCloud Intelligence Feeds offer multi-layered defense through a real-time collaborative security intelligence database. Dynamically updated using a worldwide network of threat, the network analyzes over 250 million addresses for Bot discovery, 4.5 million malware signatures, and 300,000 malware-infested websites. The result: proactive threat intelligence that stops threats at security gateways.

Check Point Incident Response (CPIR).

Because attacks and infections are a reality for many organizations, Check Point Incident Response is on hand to contain attacks, stop business disruption and get systems up and running. Experienced first responders instantly respond to any security incident with adaptable solutions that range from complete incident handling to assisting the organization's security operations center. After the attack is contained, CPIR helps reduce future risk with post-incident reports on real-time log capture, digital forensics analysis, malware, virus and data loss incidents and Botnet identification and counteraction, as well as best practices for stronger security.



Check Point®
SOFTWARE TECHNOLOGIES LTD.

WE SECURE THE FUTURE

To learn more about how to secure your organization,
please visit www.checkpoint.com

Take the first step. Schedule your FREE Security Checkup today
and find out if cybercriminals are hiding in your network.

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