THE NEXT CYBER ATTACK CAN BE PREVENTED
INTRODUCTION

Organizations are increasingly worried about their business vulnerability to cyber threats in the wake of the outbreaks of WannaCry and Petya, large breaches such as the HBO leak and Equifax, and targeted attacks on cities like Atlanta, Charlotte, and Baltimore. This is for good reason. These incidents illustrate the global impact and devastation that can be caused by modern cyber-attacks. Today’s threat actors have increasingly more powerful and destructive tools at their disposal than ever before.

This document discusses the growing threats and potential damages posed by cyber attacks, and provides guidelines to the approaches organizations should take and technologies they should use in order to prevent the next attack.
A WAKEUP CALL

The future is here. In today’s world, everything and everyone is constantly connected, and people’s information and transactions are digitized. Our era of technology offers huge opportunities for mankind, but at the same time, it means organizations are more vulnerable and more exposed than ever before.

In May and June of 2017, the world witnessed two massive cyberattacks, demonstrating the fragility of the our digital world. The WannaCry and Petya outbreaks, rapidly propagated by exploiting Windows vulnerabilities and caused tremendous damage worldwide.

The Petya attack (or NotPetya) reportedly spread through updates of a compromised Ukrainian accounting software. Once a system was infected, the attack moved laterally, exploiting vulnerabilities in the Windows operating system to infect other hosts on the network. Ukrainian banks, ministries, media, and energy companies were shut down. The Ukrainian infrastructure was crippled. Although seemingly focused on Ukrainian targets, Petya generated global damage, paralyzing companies across the world and causing huge financial losses.

HOW THESE ATTACKS MAY HAVE BEEN AVOIDED

SandBlast™ prevented both the WannaCry and the Petya outbreaks from the moment they started.

Several SandBlast technologies were key in preventing these outbreaks:

- **THREAT EMULATION**
  Threat Emulation blocked the infectious payloads of both Petya and WannaCry.

- **IPS**
  Check Point IPS had protections for the exploit used by WannaCry and Petya long before the attacks erupted, effectively preventing both the initial infection and the lateral movement of these attacks. The IPS protection covered also Windows XP systems for which a security patch did not exist at the time.

- **ANTI-RANSOMWARE**
  As the last line of defense on the endpoint, SandBlast Anti-Ransomware effectively prevented both the attacks. See videos of how SandBlast technologies helped prevent WannaCry and for Petya.
The WannaCry outbreak from a month earlier was even larger in scale and impact. Within a day it infected more than 230,000 computers across 150 countries. Similar to Petya, WannaCry severely impacted many companies globally. Among its victims were hospitals in the UK, carmakers Honda and Renault, Russian and German Railways, Telefónica, O2, Hitachi, LATAM Airlines and FedEx. Estimates of the total damage range from hundreds of millions of dollars to up to $4 billion.

These attacks, along with others targeting health care institutions, media (HBO leak) and financial services (Equifax breach), send a clear message – cyber attacks are a growing threat to people’s daily lives around the globe.

Cyber attacks continue to grow at an alarming rate – in volume, sophistication, and impact. In this age of super-powered cybercrime, the need to protect organizations from advanced attacks is more essential than ever before. Companies must use cutting-edge technologies in order to remain protected.
HOW TO PREVENT THE NEXT ATTACK

The impacts of mega cyberattacks like Petya and WannaCry were not inevitable. With the correct measures and technologies in place, many organizations could have avoided these attacks.

In order to truly combat the next threats, organizations must take a proactive approach, using advanced technologies that can prevent even the most evasive zero-day attacks.

The next attack can be prevented if companies change their view on security, and follow a few principles.

1. MAINTAIN SECURITY HYGIENE

- **Patching:** All too often, attacks penetrate by leveraging known vulnerabilities for which a patch exists but has not been applied. Organizations should strive to make sure up-to-date security patches are maintained across all systems and software.

- **Segmentation:** Networks should be segmented, applying strong firewall and IPS safeguards between the network segments in order to contain infections from propagating across the entire network.

- **Review:** Security products’ policies must be carefully reviewed, and incident logs and alerts should be continuously monitored.

- **Audit:** Routine audits and penetration testing should be conducted across all systems.

- **Principle of Least Privilege:** User and software privileges should be kept to a minimum – is there really a need for all users to have local admin rights on their PCs?
2. CHOOSING PREVENTION OVER DETECTION

Traditional cybersecurity vendors often claim that attacks will happen, and there’s no way to avoid them, and therefore the only thing left to do is to invest in technologies that detect the attack once it has already breached the network, and mitigate the damages as soon as possible.

This is untrue. Not only can attacks be blocked, but they can be prevented, including zero-day attacks and unknown malware. With the right technologies in place, the majority of attacks, even the most advanced ones can be prevented without disrupting the normal business flow.

3. LEVERAGING A COMPLETE UNIFIED ARCHITECTURE

Many companies attempt to build their security using a patchwork of single-purpose products from multiple vendors. This approach usually fails: it results in disjointed technologies that don’t collaborate – creating security gaps. Plus, it introduces a huge overhead of working with multiple systems and vendors. As a result of this inefficient approach, many attacks are not prevented, forcing organizations to invest more on post-infection and breach mitigation.

In order to achieve comprehensive security, companies should adopt a unified multi-layer approach that protects all IT elements – networks, endpoint, cloud, and mobile, all sharing the same prevention architecture and the same threat intelligence.

THE AGE OF SUPER-POWERED CYBERCRIME IS UPON US

The WannaCry and Petya attacks both encrypted victims’ files and demanded a ransom. However, these two attacks have something much more fundamental in common. Both leveraged cyber-weapons which were developed by the National Security Agency of the United States and leaked to the public in April 2017.

The US is hardly the only country developing sophisticated offensive cyberwarfare capabilities. Nation-states across the globe are investing billions and employing top talent to create advanced hacking tools and cyber weaponry.

Was the NSA leak from April the last of its kind? It would be naïve to believe so. In all likelihood, we will see more military-grade cyber tools exposed in the future. The WannaCry and Petya attacks illustrate how leaked tools and knowledge from powerful threat actors put incredible firepower in the hands of common cyber criminals.
4. COVERING ALL ATTACK VECTORS

**Mail or Message:** Send a mail or text message with a malicious attachment or a malicious link.

**Web Browsing:** Compromise the user’s browser (typically through exploit kits) or trick a user to download and open a malicious file.

**Server and Systems Exploitation:** Infect by exploiting unpatched vulnerabilities in any online host.

**Mobile Apps:** One of the most common sources for compromising mobile devices is through mobile apps.

**External Storage:** Physically mounted drives allow malicious files to enter without even traversing the network.

**Phishing:** A fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy person.

To achieve effective coverage, organizations should seek a single solution that can cover all attack surfaces and vectors. One solution that provides broad prevention across all attack surfaces, including mail, web browsing, systems exploitation, external storage, mobile apps and more.

5. IMPLEMENTING THE MOST ADVANCED TECHNOLOGIES

Attack techniques are diverse and constantly evolving. IT systems are complex. There is no single silver-bullet technology that can protect from all threats and all threat vectors. However, there are many great technologies and ideas available – machine learning, sandboxing, anomaly detection, content disarmament, and numerous more. Each of these technologies can be highly effective in specific scenarios, covering specific file types or attack vectors. Strong solutions integrate a wide range of technologies and innovations in order to effectively combat modern attacks in IT environments.
6. KEEP YOUR THREAT INTELLIGENCE UP TO DATE

In the constant fight against malware, threat intelligence and rapid response, capabilities are vital. Keeping your business up and running with comprehensive intelligence to proactively stop threats, manage security services to monitor your network and incident response to quickly respond to and resolve attacks.

Malware is constantly evolving, making threat intelligence an essential tool for almost every company to consider. When an organization has financial, personal, intellectual, or national assets, a more comprehensive approach to security is the only way to protect against today’s attackers. And one of the most effective proactive security solutions available today is threat intelligence.

THE BOTTOM LINE

Even with numerous daily cyber attacks, the WannaCry and Petya outbreaks stand out due to their rapid spread, their devastating impact, and above all their use of leaked superpower cyber weapons. Many look upon these attacks as a wakeup signal, a call to reduce business vulnerability to cyber attacks and to the disastrous potential they pose to day-to-day business operations.

Relying on post-infection breach detection and mitigation as the sole security strategy is a risky and dangerous paradigm.

In order to truly combat the next threats, organizations must take a proactive approach, utilizing advanced technologies that can prevent even the most evasive zero-day attacks. Companies should seek to adopt a proven unified solution, which offers a broad multi-layered cyber protection architecture, implemented across their entire IT infrastructure and covering all attack vectors.

SandBlast, Check Point’s zero-day protection suite and part of the Infinity architecture, protects thousands of businesses today. Built to block advanced and unknown attacks, SandBlast is designed to effectively prevent the cyber-attacks that the world has yet to see.
PREVENT THE NEXT ATTACK WITH CHECK POINT INFINITY

Check Point Infinity is the only unified cyber security architecture that future-proofs your business and IT infrastructure across all networks, cloud and mobile. The architecture is designed to resolve the complexities of growing connectivity and inefficient security. It provides complete threat prevention, sealing security gaps, enabling automatic, immediate threat intelligence sharing across all security environments, and consolidating security management for an efficient security operation.

At the forefront of Check Point Infinity’s focused threat-prevention, stands SandBlast – a family of products incorporating the most advanced zero-day prevention technologies, all sharing the same threat intelligence – based on Check Point ThreatCloud. With over 30 different innovative technologies, SandBlast focuses on prevention rather than detection, addresses all common attack vectors, and covers all IT elements – network, mobile endpoint and cloud.
SANDBLAST TECHNOLOGIES

SandBlast’s technology portfolio includes:

**Threat Emulation** (Sandboxing) is a unique evasion-resistant sandbox technology. Threat Emulation detects and blocks unknown and zero-day malware in files and objects entering a network – through mail and web, or delivered directly to endpoints. It blends a dozens of underlying innovative technologies to facilitate the best detection rates and fastest verdict speeds in the industry.

**Threat Extraction** delivers sanitized threat-free files to users – in real-time, providing a high security posture while maintaining business flow. Email attachments and web downloads are sanitized on the fly, delivering safe content to users without exposing them to risks that may lurk in the original file. The original files are sent in parallel to the Threat Emulation sandbox, and can easily be retrieved by the user – if they aren’t malicious.

**Zero Phishing** protects user credentials using signature-less identification of unknown phishing sites. The technology further protects company credentials by alerting when users reuse their corporate credentials on personal internet accounts.

**Mobile Threat Defense** delivers a comprehensive protection against cyberattacks for Android and IOS. The technology identifies and blocks malicious apps, and prevents network and OS attacks from compromising mobile devices.

**Anti-Ransomware** is an endpoint protection designed specifically to combat ransomware. Its signature-less technology is designed to detect unknown and zero-day ransomware attacks through advanced behavioral analysis and by detecting attempts to illegitimately encrypt files. Moreover, ransomware infections are automatically quarantined and if any data was encrypted then it is automatically restored.

**Forensic Analysis and Incident Quarantine** provides automated attack quarantine and instant actionable insight to attacks. Taking a unique approach, SandBlast’s Forensic analysis makes attack information useful to any security administrator – not just forensics experts. Based on the automated forensic analysis, SandBlast automatically quarantines infections.

**Intrusion Prevention (IPS)** blocks attacks and exploitation attempts on networks and systems. Check Point IPS leads the industry in terms of vulnerability coverage and in the timeliness of delivering protections for new vulnerabilities – as they surface.

**Anti-Bot** using the unique Multi-Tier ThreatSpect™ engine, Check Point Anti-Bot technology identifies infected hosts and blocks command-and control communications, thus containing the infection and preventing data exfiltration.
THE SANDBLAST PRODUCT FAMILY

The SandBlast solution is built upon a unified family of products, providing comprehensive multilayer protection from all attack vectors and covering all IT assets.

SandBlast Network

SandBlast Network offers complete protection with a unique combination of advanced threat prevention technologies – starting with the baseline IPS and AV and adding SandBlast’s unique combination of Threat Emulation and Threat Extraction for proactive prevention of unknown and zero-day attacks. The solution is tuned to provide maximum security without disrupting the business flow while leveraging unique innovative developments in the Artificial Intelligence space.

Check Point customers can add SandBlast protection to their existing security gateways, thus leveraging their investment in Check Point security gateways, as well as the skill-set of their existing staff.
Flexible deployment options allow for inline or SPAN-port deployment. Mail integration can be achieved via MTA and web browsing can be protected either inline or through integration with an HTTP proxy integration using the ICAP protocol.

The SandBlast network solution is fully integrated with Check Point’s SSL inspection and Identity Awareness technologies providing maximum visibility and attack coverage.

**SandBlast Agent**

SandBlast Agent offers advanced protections to the endpoint layer, covering Web Downloads, the File System, applications and the operating systems. SandBlast Agent uses a fleet of threat engine technologies to help defend against the full scope of known and unknown zero-day malware. The direct endpoint protection adds an additional defense layer over network protections, and additional coverage for roaming users and files entering through external storage.

SandBlast Agent implements a comprehensive set of SandBlast’s advanced technologies including Threat Emulation, Threat Extraction, Zero Phishing and Anti-ransomware. Incident analysis and remediation are automated through SandBlast’s advanced forensics capabilities.

**SandBlast Mobile**

SandBlast Mobile protects organizations’ iOS and Android devices, utilizing a wide range of unique technologies to protect against advanced mobile threats.

The solution provides enterprise mobile security that protects against threats to the OS, apps, and network. It offers the industry’s highest threat catch rate without impacting performance or user experience.
Cloud Security Solutions

SaaS applications deliver many benefits to businesses of all sizes, but also expose them to risks from advanced threats largely due to unauthorized access to corporate SaaS accounts. Check Point CloudGuard SaaS is the only cyber security solution that prevents cyber criminals from hacking SaaS applications. While most SaaS security solutions offer only visibility and control over application policies, CloudGuard SaaS provides complete protections against even the most sophisticated malware and zero-day threats while easily preventing account breaches. With Check Point CloudGuard, SaaS security is just one click away.

Process efficiencies and increased network agility are driving IaaS and SDN technology adoption at a rapid pace. But these new infrastructures also present businesses with a unique set of security challenges. Check Point CloudGuard IaaS protects assets in the cloud from the most sophisticated Gen V cyberthreats with dynamic scalability, intelligent provisioning and consistent control across physical and virtual networks, ensuring you can embrace the cloud with confidence.

CloudGuard with Dome9 is a comprehensive platform for security and compliance automation in the public cloud, offering visibility, continuous compliance, active protection and threat detection. CloudGuard Dome9 is an API based SaaS platform that integrates natively with Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP). It provides guardrails to minimize your attack surface and ensures you meet compliance and governance standards in the public cloud.