Check Point
SOFTWARE TECHNOLOGIES LTD

STOPPING ZERO DAYS AT THE SPEED OF DIGITAL

THREE MUST-HAVES FOR BLOCKING CYBER ATTACKS WITHOUT COMPROMISING ON BUSINESS PRODUCTIVITY

TABLE OF CONTENTS

INTRODUCTION

Network Threat Prevention: Your first—and sometimes only—line of defense

Can you defend against zero day threats? Most organizations cannot. But with the right technology, organizations can not only detect more zero days, but also stave them off—without having to compromise on business agility or speed. The three must-haves to block zero-day attacks without compromising on business productivity are:

- Pre-emptive user protection
- Fast zero-day verdicts
- Streamlined security management

WHY TRADITIONAL NETWORK PROTECTION METHODS ARE NOT ENOUGH

At best, antivirus software blocks only 43% of the malware strains currently in the wild, meaning most variants can still get into your network. In absolute numbers, that's 8,500 unknown zero-day threats worldwide per day, according to Check Point ThreatCloud which aggregates data from several hundred million sensors globally.

To identify zero-day malware, AV software relies on indicators of compromise (IoCs) such as IP addresses, URLs and file signature or hashes. The zero-day phishing equivalent of these IoCs, used by anti-spam and email security controls, are unknown URL reputation and sender reputation.

With no associated file signatures, sender or website history, AVs, firewalls and other controls cannot identify these as malicious and block them from entering the network. So how do you defend against that which you do not know?

Here are several common network protection approaches and their limitations.

SANDBOXES

Deployed on top of static code analysis, conventional sandboxes examine the behavior of unknown or suspicious files to determine if they are malicious. However, they are susceptible to malware evasion techniques, such as preventing execution in the event that a virtual environment is detected. Also, by default, they are configured to let suspicious files into the network, before analysis is complete and a verdict is reached. Why? Because waiting for eight to 20 minutes is often impractical, especially when it comes to downloading a file from the web (For details, see Check Point's Malware Evasion Encyclopedia.)

ENDPOINT SECURITY

Serving as a last line of defense, solutions such as EPPs and EDRs inspect an exhaustive number of endpoint activities and behaviors and generate alerts in the event of suspicious activity. They are therefore instrumental in threat hunting and threat remediation performed post-infection. However, not all resources can be protected with an endpoint agent. This includes enterprise IoT devices such as surveillance cameras, elevators and HVAC systems for which the network security gateway is usually the first and last line of defense. Similarly, data centers cannot be protected with endpoint solutions, as they consist of dozens—if not hundreds—of servers with specialized OSs (Unix, Linux, Oracle), appliances and other equipment—for which network security serves as the only line of defense.

DETECTION-FIRST APPROACH USING INCIDENT RESPONSE

Giving up on the notion of threat prevention, some organizations place their investments in post-breach incident response, aiming to curtail damages that arise from a breach. This is done using in-house SOC teams, or outsourced MSSP or MDR teams entrusted with monitoring the organization's security and following up on alerts. The problem with relying mainly on this approach is that it's expensive, with an average breach costing $960,000 to remediate. Second, the damage is likely to have already been done at this stage of an attack (for example, with files already encrypted in the event of a ransomware attack).

With such critical limitations, how can you protect your network from zero-days?

CHAPTER 1

PRE-EMPTIVE USER PROTECTION

According to the latest Verizon Data Breach Investigations Report, 94% of attacks whose origin is known were delivered by email. Since humans are the weakest link in the security chain, it makes sense for security to follow them wherever they go—be it browsing or email.

To this end, various pre-emptive technologies can be deployed to eliminate potential threats before they reach users, without affecting their workflows or productivity.

THREAT EXTRACTION

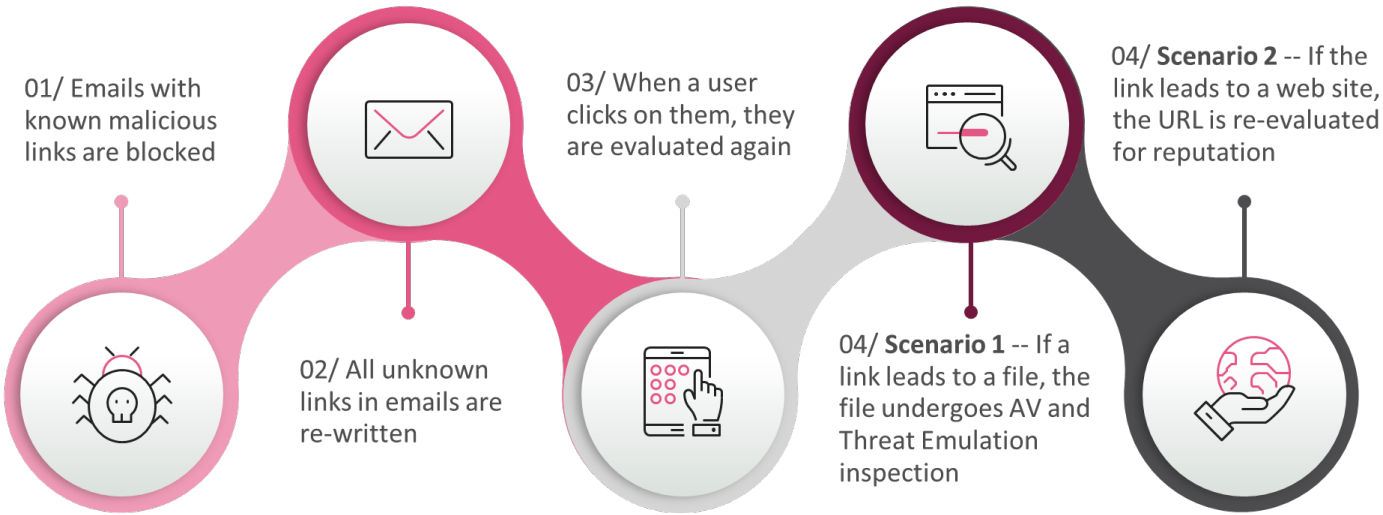
Threat Extraction is also known as content disarm and reconstruction, or CDR—and is employed to remove risky content from web downloads and emails. Threat Extraction cleans PDFs, images and other documents, removing exploitable elements such as active content and embedded objects. Files are then reconstructed, retaining their original format, and delivered to the user. Meanwhile, the original file is emulated in the background, and can be accessed by the user if deemed benign (as shown in this video.)

ADVANCED EMAIL PROTECTIONS

Innovative technologies have emerged to defend against malicious emails, including malicious links, phishing, business email compromise (BEC) and other social engineering attacks. These include revolutionary AI neural network Natural Language Processing (NLP) engines that scrutinize hundreds of email parameters, including the language of the text body, the job title of the purported sender and a host of other variables.

To protect against new zero-day phishing sites, Click-Time URL Protection, or URL rewriting, examines and blocks suspicious links in real time, removing the risk of URLs that are populated with malicious content at the last minute, and for which reputation data does not exist.

PRE-EMPTIVE USER PROTECTION AGAINST RISKY EMAIL LINKS



CHAPTER 2

REACHING ZERO-DAY VERDICTS FAST

For a prevention-first strategy to work, threat emulation verdicts needs to be reached fast. To this end, real time threat intelligence can quickly determine if a file or link has already been deemed malicious. And where no threat intelligence is available, artificial intelligence (AI) comes in to the picture to deliver blazing-speed threat emulation verdicts.

REAL-TIME THREAT INTELLIGENCE

Threat intelligence gleaned from hundreds of millions of sensors deployed on various assets, such as endpoints, devices and networks can be shared in real time to block the newest attacks. The larger the install base of the sensor data, the more visibility is gained into the latest attacks in the wild.

Threat intelligence may also be obtained from multiple sources, including feeds from non-profits such as CERTs and industry alliances, as well as proprietary vendor research and feeds.

By using the latest threat intelligence, organizations can block the newest malware and phishing attacks based on previously discovered indicators of compromise (IoCs), even if their antivirus software has yet to include them.

THREATCLOUD

AI-GENERATED THREAT EMULATION VERDICTS

Where IoCs do not exist for a suspicious email or file, organizations can vet risky documents and messages using the power of data science. In addition to static code analysis, OSINT, file reputation and other sources of data, files that may contain malware, and emails that may harbor phishing, are emulated to examine their runtime behavior.

The file or email is analyzed by rich, exhaustive artificial intelligence (AI) engines using millions of parameters that examine runtime behavior. Examples of AI engines used include:

- Malware DNA analysis that attempts to identify the origins of a malware's code and associate it with known malware families, if any
- Image Recognition, which examines an executable by treating it as a static image
- Code Flow Analysis, which recognizes malicious code flow patterns

An uber-AI engine that interprets and weighs dozens of engines' risk scores can be used to reach a single and final 'malicious' or 'benign' verdict. And finally false positives can be minimized using a dedicated self-learning engine. Heuristics should be continually optimized to detect the latest threats in the wild, as these evolve and change over time.

MOVING TO A PREVENTION-FIRST STRATEGY

By investing in zero-day threat prevention, organizations can save money and breach-related costs downstream by blocking more attacks upstream. When emulation is fast, verdicts are accurate, and network protection follows users seamlessly, prevention becomes not only possible, but practical.

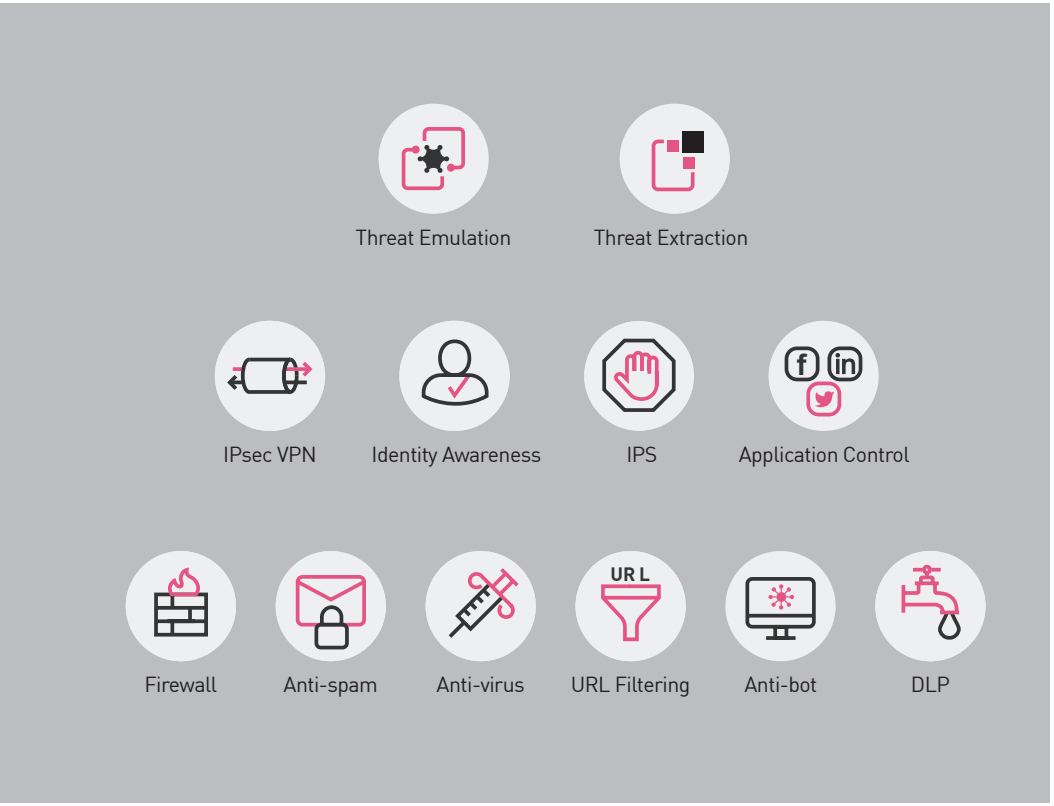
When emulation is fast, verdicts are accurate, and network protection follows users seamlessly, prevention becomes not only possible, but practical.

CHAPTER 3

STREAMLINED SECURITY MANAGEMENT

Configuring the many layers of network protection is anything but easy. Especially as IT administrators with limited security knowledge are often entrusted with this task.

To help organize this daunting duty, here are four best practices that can be automated to configure your network security.



1 DEFINE AND CONQUER—CLASSIFY SEGMENTS FOR CONSISTENT POLICY APPLICATION

Rather than a single network, the fabric of today's networks is comprised of multiple integrated segments, each which require different protections. For example, the guest network may only require protections for browsing the open internet. Meanwhile, the internal network requires setting up policies for your IPS and email gateway.

By first defining what type of network you are protecting, you can define policies once for each segment type and automatically apply the same policies consistently where relevant. Common types of network segments include the perimeter network, data center network, internal network and guest network.

2 USE ONLY WHAT YOU NEED—ENABLE ONLY RELEVANT FUNCTIONALITY FOR BETTER PERFORMANCE

Hundreds of policies can be applied to a network segment, depending on the Oss and protocols it uses and the applications it needs to protect.

By automatically enabling only pertinent functionalities for each network segment, organizations can accelerate the performance of their security gateways. They also save on gateway resources such as bandwidth and CPU consumption. They may even realize they can operate with a more cost-effective network cyber security appliance.

Moreover, by automatically only enabling relevant functionality, the need to have expertise in many different security functions is eliminated.

As an example, MTAs or mail-transport agents are relevant for email management, but not relevant for the guest network. Therefore MTA functionalities on the guest network can be automatically disabled. Similarly, VPN access from your guest network to your enterprise network should be disabled, as well

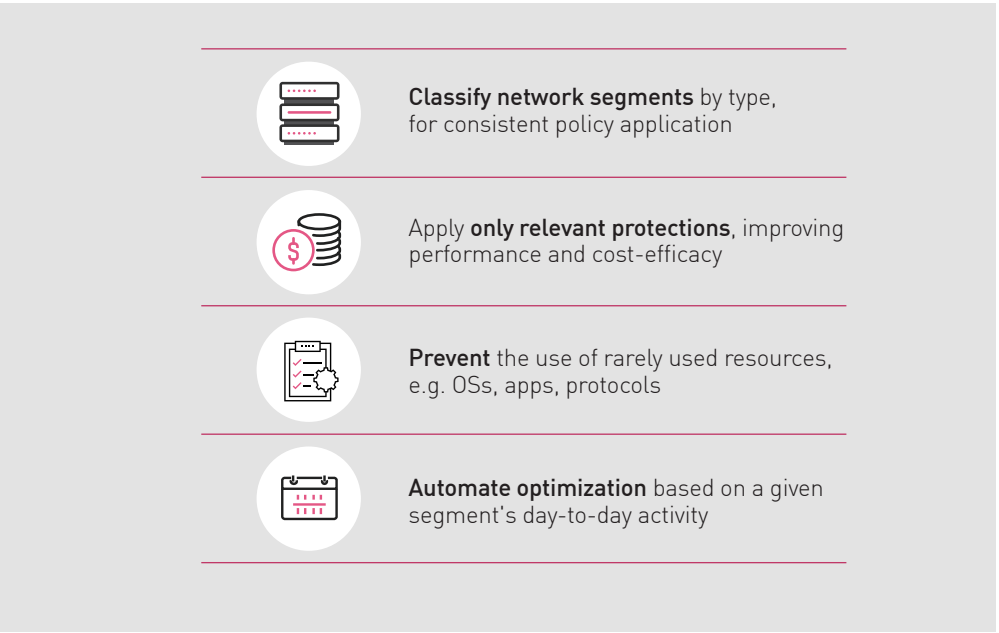


Figure 1: Best Practices for Configuring Network Cyber Security

3 BLOCK WHAT YOU DON'T NEED—APPLY PREVENT-MODE TO RARELY USED RESOURCES

In the same vein, security can be enhanced by tailoring IPS protections to your network according to the OSs, apps and protocols used in a given segment. These may include signatures, software updates and virtual patching against known vulnerabilities.

To demonstrate how such optimization would work, consider an internal enterprise network made up of laptops. That network requires protections for browsing and email. But, since it does not contain industrial control systems or Unix servers, a long tail of unused resources can be activated in prevent mode. For example, industrial control protocols such as Modbus, can be blocked to prevent their abuse .

4 ADAPT AND OPTIMIZE—FINE TUNE PER ONGOING ACTIVITY AND LATEST THREATS

Machine learning can be used to adapt protections, such as those applied by an Intrusion Prevention System (IPS). By only using protections relevant to the actual OSs, protocols and applications used in a given segment, organizations benefit from better performance and cost efficiency.

And when it comes to the latest defenses against the newest threats, it is imperative to keep apprised of the latest published CVEs, and ideally apply virtual patching as a pre-emptive security measure.

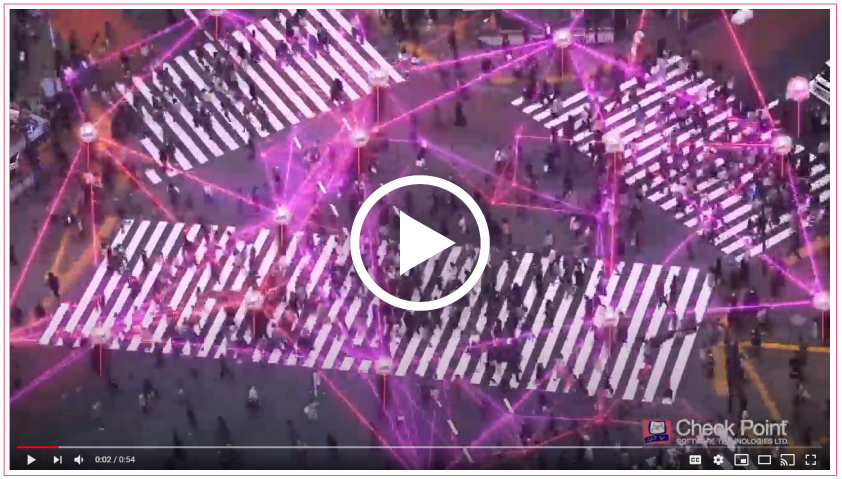
SIMPLE, AUTOMATED NETWORK CYBER SECURITY

Check Point's R80 management portal now offers single-click setup of best practice policies. Thanks to the new Infinity Threat Prevention Management console supported by R80.40 and later, you can select the appropriate network profile, apply it once, and enjoy set-and-forget management. To learn more, including Early Availability details, go to Check Point Checkmates.

WRAP-UP: PRODUCTIVITY AND ZERO-DAY PREVENTION—A ZERO-SUM GAME?

Adding layers of security often results in poor usability, administration overheads and downtime. That is why, when it comes to unknown threats, organizations often resort to running their sand-boxes in detect-mode rather than prevent-mode.

So are productivity and zero-day prevention a zero-sum game? They don't have to be. Here is why.



PRE-EMPTIVE CONTROLS OFFER A SEAMLESS USER EXPERIENCE

You want to keep users productive, and you don't want to keep them waiting for a threat analysis verdict as they browse the web and open their email.

By pre-emptively removing risky content elements from web downloads and email attachments (for example, macros) you can ensure users remain productive while the original, unknown file is prevented from entering the network until a malicious or benign verdict is reached. It takes less than 1.5 seconds to deliver this type of risk-free content using threat extraction, so user workflows are not compromised; meanwhile your attack surface shrinks and your security posture is greatly enhanced.

As unknown threats account for 57% of malicious files reaching organizations, according to Check Point Research, an ounce of pre-emptive controls is worth a pound of cure.

To protect users from email-based fraud and phishing (sent with no attachment), all email aspects including links, sender, recipient and email language can be transparently vetted and blocked within seconds—thanks to the power of artificial intelligence (AI).

THREAT ANALYSIS VERDICTS CAN BE ACCURATE AND FAST

To maintain productivity, analyzing unknown threats should not cause downtime or delays. Otherwise, IT and security teams will be asked to revert to 'detect-mode.' To this end, speed is paramount. And how do you reach speed? With data science, of course.

By utilizing a sequence of signature lookups, static code analysis and evasion-resistant threat emulation, AI engines can reach a malicious/benign verdict within just a few minutes. That verdict, specific to the analyzed file, can in turn be added as a new signature (e.g. MD5 or SHA hash) so that future encounters with that malicious file will result in its immediate blocking.

Leveraging AI engines that study the broader campaign associated with that malware file may yield a collection of broader malware campaign IoCs, such as C2 domains, IP addresses, and others.

By sharing the newly-identified malware signature and broader IoCs through a global threat intelligence network, organizations across the globe can block that very same threat—and other related threats—within seconds.

MANAGEMENT CAN BE MINIMAL

When it comes to setting up and optimizing network protection policies, complex and fragmented configuration, combined with tedious manual updates, may also contribute to downtime and loss of productivity.

This can be addressed with three-fold optimization:

- **Profile-based policies**—By applying consistent best-practice policies to the same type of network segment, e.g. internal network, guest network, perimeter etc. the time required to set up policies can be slashed by up to 70%.
- **Automated policy updates**—To ensure that policies are always up to date based on the latest vulnerabilities and technology, these can be pushed automatically in the background, removing the need to push policies manually.
- **Automated optimization of protections**—Different network segments operate with different protocols, OSs and applications. To ensure optimized performance, including bandwidth and CPU consumption, controls such as IPSs can be continually and automatically optimized to only include and update protections relevant for a given segment

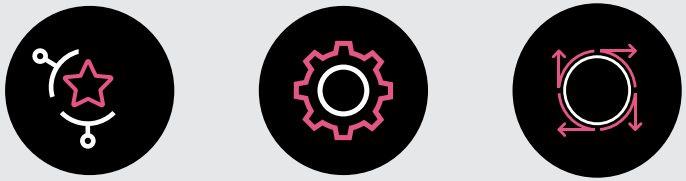
SANDBLAST NETWORK— STOP ZERO DAYS AT THE SPEED OF DIGITAL

Check Point SandBlast Network provides the world's best[1] zero-day protection through a combination of pre-emptive user protections, real time threat intelligence and blazing-speed AI-generated threat analysis verdicts.

Empowering organizations to take a prevention-first strategy to cyberattacks, SandBlast Network deploys with your current infrastructure, and offers fully automated policy configuration that protects your business without compromising on productivity and agility.

[1] According to NSS Lab's Breach Prevention Systems (BPS) Group Test results: https://pages.checkpoint.com/nss-breach-prevention-report-2019.html

YOUR FIRST LINE OF DEFENSE



Best Zero Day Catch Rate | **Simple Management** | **Seamless Productivity**

Check Point SandBlast™ NETWORK

Contact us today for a free security check up, or a live demo.

Demo URL: https://pages.checkpoint.com/cyber-security-management-demo.html

Free Security checkup: https://pages.checkpoint.com/security-checkup.html

CHECK POINT'S SUITE OF SANDBLAST ZERO-DAY PROTECTION SOLUTIONS

Empowering organizations to take a prevention-first strategy against cyber attacks, Check Point's suite of SandBlast Zero-Day Protection solutions leverage the power of data science to detect the newest threats and stop them in their tracks.

SandBlast minimizes risk through pre-emptive controls such as threat extraction and advanced email protections. It identifies threats before they enter the network through evasion-resistant threat emulation. And it reaches blazing speed verdicts through the power of artificial intelligence (AI), protecting your users and digital assets from the latest, most targeted and most sophisticated cyber attacks.

The SandBlast suite of mobile, endpoint and network Zero-Day Protection solutions utilizes ThreatCloud, the world's most extensive threat intelligence network sustained by hundreds of millions of sensors worldwide, enriched industry feeds and leading-edge research by a top notch unit of reverse engineers and ethical hackers.

Serving over 100,000 customers worldwide, across governments, leading financial institutions and Fortune 500 companies of all industries, SandBlast Zero Day Protection seamlessly follows users wherever they go, making threat prevention not only possible, but practical.

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

Check Point®
SOFTWARE TECHNOLOGIES LTD