

SECURITY CHECKUP

THREAT ANALYSIS REPORT

Date

Customer Name

Prepared By



SECURITY CHECKUP

THREAT ANALYSIS REPORT

Customer

Analysis Duration

Traffic Inspected By The Following Check Point Software Blades:

Industry

Analysis Network

Application Control

URL Filtering

Company Size

Security Gateway Version

IPS

Anti-Bot

Country

Security Device

Anti-Virus

Threat Emulation

Threat Extraction

Content Awareness

Zero Phishing

IoT Protect

TABLE OF CONTENTS

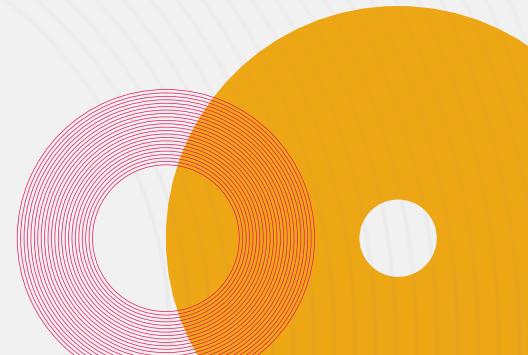
EXECUTIVE SUMMARY

KEY FINDINGS

RECOMMENDATIONS

CHECK POINT INFINITY PLATFORM

ABOUT CHECK POINT



EXECUTIVE SUMMARY

The following Security Checkup report presents the findings of a security assessment conducted in your network. The report uncovers where your organization is exposed to security threats, and offers recommendations to address these risks.

To assess risk, network traffic was inspected by Check Point to detect a variety of security threats, including: malware infections, usage of high risk web applications, intrusion attempts, loss of sensitive data, and more.

Malware and Attacks

1

Computers Infected with Bots

4

Communications with C&C* Sites

3

Known Malware Downloaded by

1


Users

0

Zero-Days Downloaded

20

Unique Software Vulnerabilities were Attempted to be Exploited




* C&C - Command and Control. If proxy is deployed, there might be additional infected computers.

Zero-days downloaded present a unique count of old or new malware variant with un-known anti-virus signature.

Indicates potential attacks on computers on your network.

IoT Devices




0

Discovered IoT Devices


Potential risks: unauthorized access and malicious intent from reaching IoT devices.

High Risk Web Access




0

High Risk Web Applications




0

High Risk Web Sites



0B




0

Hits

Potential risks: opens a backdoor to your network, hides user activity, causes data leakage or malware infections.


Potential risks: Exposure to web-based threats and network infection. Examples: Spam, malicious, phishing web sites.

SaaS Applications



0

SAAS Applications Seen



0

Users Using SAAS Application

Applications that have integration with our Harmony Email & Collaboration solution and can be fully protected by our Threat Prevention engines.

KEY FINDINGS

An abstract graphic consisting of two overlapping circles. The left circle is a solid dark red color. The right circle is composed of many thin, concentric, light red lines, creating a ripple effect. The circles overlap in the center, and the background is a solid dark red color.

Cyber Kill Chain

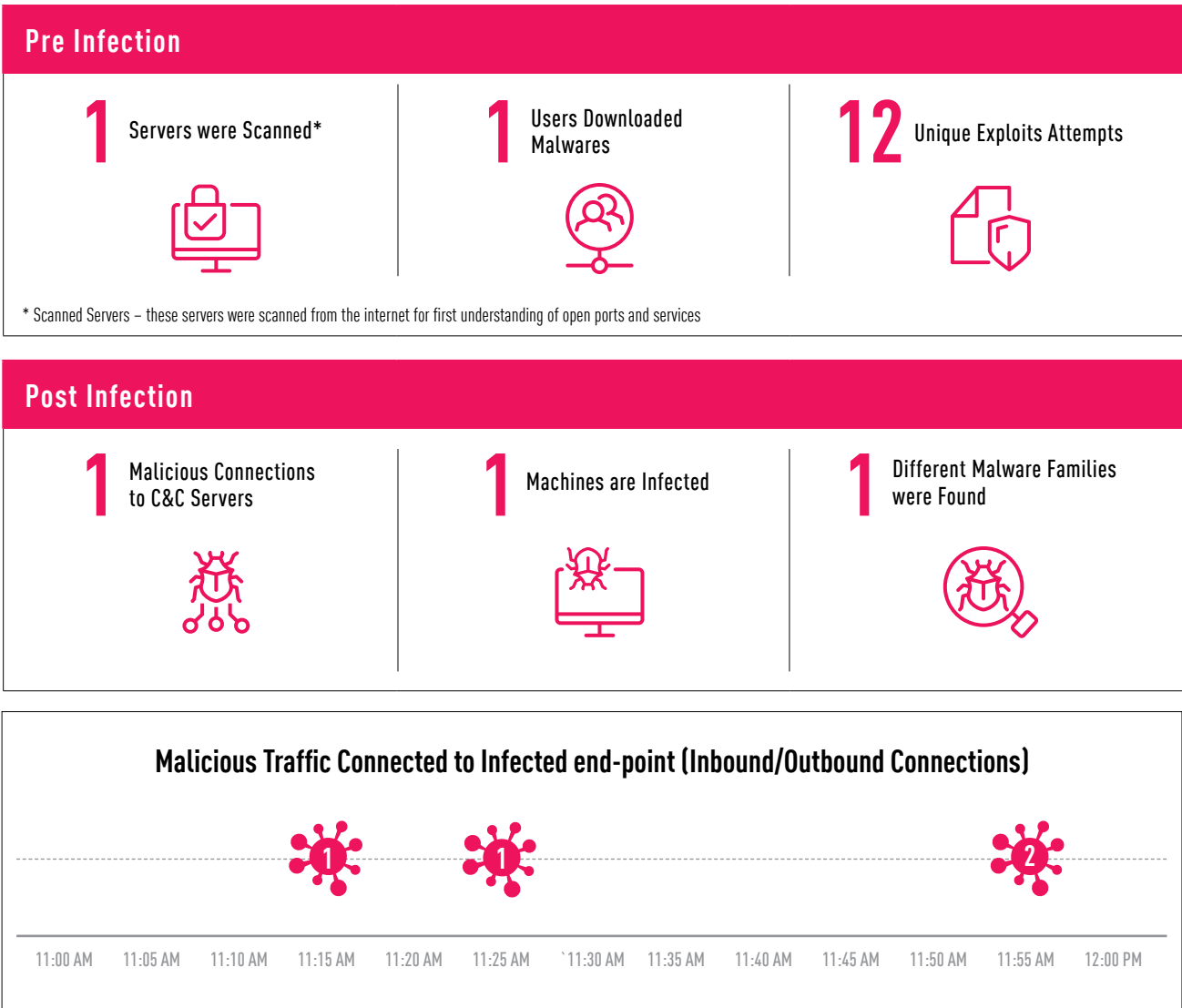
A cyber kill chain reveals the stages of a cyberattack: from reconnaissance to the goal of data exfiltration. The kill chain can also be used as a management tool to help continuously improve network defense.

Pre Infection

- 1. Reconnaissance
- 2. Delivery
- 3. Exploitation
- 4. Installation

Post Infection



- 1. Command and Control
- 2. Propagation



Machines Infected with Malwares and Bots

Bot is a malicious software that invades your computer. Bots allow criminals to remotely control your computer to execute illegal activities such as stealing data, spreading spam, distributing malware and participating in Denial of Service (DOS) attacks without your knowledge. Bots play a key role in targeted attacks known as Advanced Persistent Threats (APTs). The following table summarizes the bot families and number of infected computers detected in your network.

Top Malwares in the Network

Machine	Malware Family	Malware Name*	Protection Type	Destination Country	Connections
1.1.1.10	BoA	Trojan.Win32.BoA.A	 Signature	 United States	1
Total: 1 Machine	1 Family	1 Malware	1 Protection Type	1 Country	1

* Check Point's malware naming convention: <malware type>.<operating system>.<malware family>.<variant> For more details on specific malware, search the malware name on <https://research.checkpoint.com>

** Amount of malicious traffic from end-point.

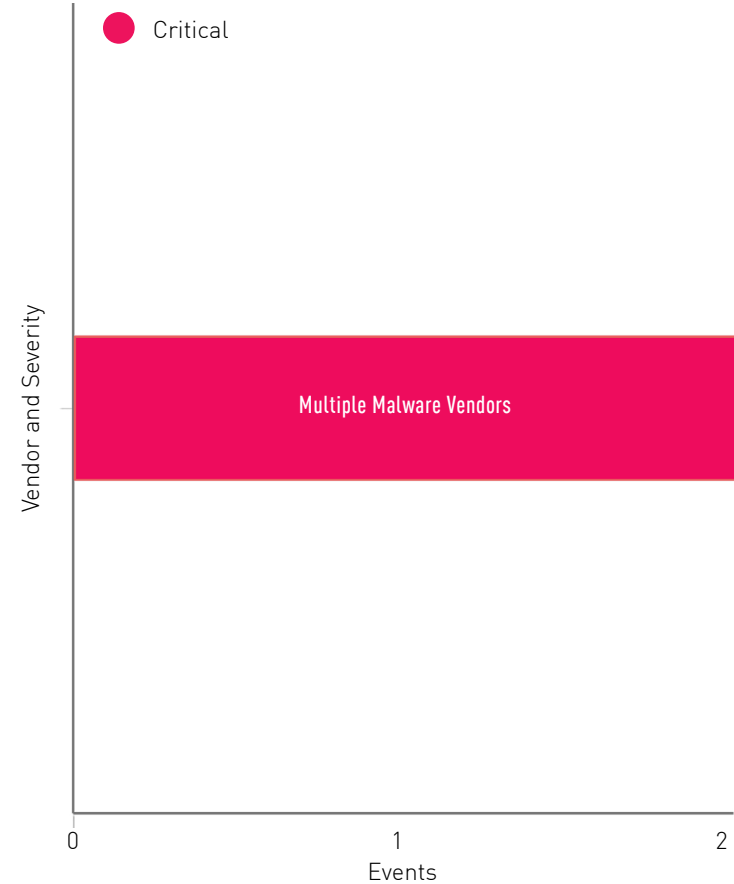
Extended Malware Incidents (Check Point ThreatCloud IntelliStore)

Malware threats were detected by extended security intelligence feeds (via Check Point ThreatCloud IntelliStore*).

Top Threats by Feed

Feed	Threat	Severity	Source	Feed Detection Engine
Multiple malware vendors	Trojan.Win32.Generic.TC.9bbeGVpG	<div></div> Critical	1 Source	Anti-Virus
	Trojan.Win32.Generic.TC.bca5aBMq	<div></div> Critical	1 Source	Anti-Virus
	Total: 2 Threats	<div></div> Critical	1 Source	1 Engine
Total: 1 Feed	2 Threats	<div></div> Critical	1 Source	1 Engine

Feeds by Severity






* For more information on Check Point ThreatCloud IntelliStore please refer to <http://www.checkpoint.com/products/threatcloud-intellicore/>

Malware Downloads (Known Malware)

With the increase in sophistication of cyber threats, many targeted attacks begin with exploiting software vulnerabilities in downloaded files and email attachments. During the security analysis, a number of malware-related events which indicate malicious file downloads were detected. The following table summarizes downloads of known malware files detected in your network and the number of the downloading computers. Known malware refers to malware for which signatures exists and therefore should be blocked by an anti-virus system.

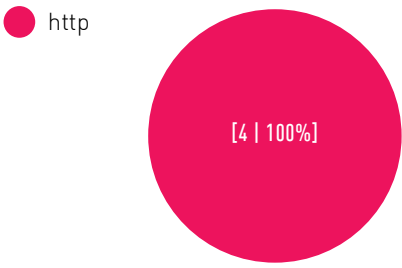
Malware Downloads Over HTTP

Infected File Name	User	Machine Name	Malware Action	Downloaded by	MD5*
e.txt			Malicious file/exploit download	 Host_1.1.1.10 (1.1.1.10)	44d88612fea8a8f36de82e1278abb02f
win7_64bit_big.pdf			Malicious file/exploit download	 Host_1.1.1.10 (1.1.1.10)	c8bdc1044384d9900da05f070185d5fe
win7_64bit_big.zip			Malicious file/exploit download	 Host_1.1.1.10 (1.1.1.10)	a95f35be11785020233644bd6e91160a
Total: 3 Files	0 Users	0 Names	1 Action	1 Source	3 Files

Top 5 Sources Downloaded Malware



Downloads by Protocol



* You can analyze suspicious files by copying and pasting files' MD5 to VirusTotal online service at www.virustotal.com

Downloads of New Malware Variants (Unknown Malware)

With cyber-threats becoming increasingly sophisticated, advanced threats often include new malware variants with no existing protections, referred to as ‘unknown malware’. These threats include new (zero day) exploits, or even variants of known exploits, with no existing signatures and therefore are not detectable by standard solutions. Detecting these types of malware requires running them in a virtual sandbox to discover malicious behavior. During the security analysis, a number of malware-related events were detected in your network. The table below summarizes downloads of new malware variants detected in your network.

Downloads of New Malware Variants

No data found.

Malicious Downloads by Protocol

No data found.

Top Malicious File Types

No data found.

* You can analyze suspicious files by copying and pasting files’ MD5 to VirusTotal online service at www.virustotal.com

Mitre Att&ck

Check Point SandBlast Network uses the MITRE ATT&CK framework in multiple ways in the detection and prevention of malware. SandBlast Network shows the techniques used when a malicious file is discovered.

MITRE ATT&CK Tactics— Attack Count	
3	Initial Access
0	Execution
0	Persistence
0	Privilege Escalation
1	Defense Evasion
0	Credential Access
0	Discovery
0	Lateral Movement
0	Collection
1	Command and Control
0	Exfiltration
1	Impact

The Analyst Holy Grail

Analyzing system logs and efficiently identifying top threats to investigate and remediate is a security analyst’s biggest challenges. Most organizations receive malicious files every day. Without advanced protection technology and analytics, the malware will likely breach the organization’s systems and spread through the corporate networks.

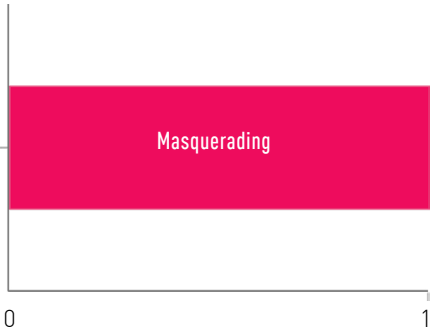
The Solution

Check Point SandBlast Network uses the MITRE ATT&CK framework in multiple ways in the detection and prevention of malware. SandBlast Network shows the techniques used when a malicious file is discovered.

Top 10 Execution Technics Used by Attackers

No data found.

Top 10 Defense Evasion Technics Used by Attackers



Top 10 Persistence Technics Used by Attackers

No data found.

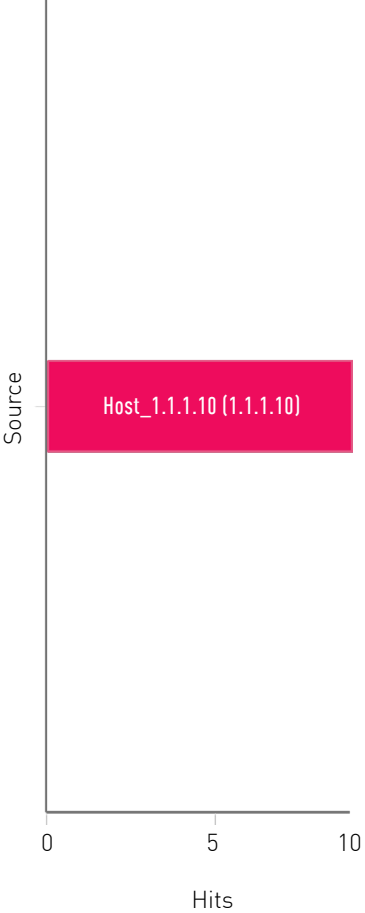
Access to Sites Known to Contain Malware

Organizations can get infected with malware by accessing malicious web sites while browsing the internet, or by clicking on malicious links embedded in received email. The following summarizes events related to sites known to contain malware.

Top Connections to Malicious Sites

Malware Family	Domain	Protection Type	Hits
Generic	http://files.cpcheckme.com/win... http://files.cpcheckme.com/e.tx... http://files.cpcheckme.com/win...	Signature	3
		URL Reputation	1
Eicar	http://files.cpcheckme.com/e.txt? static=CPCheckMe&rand=1712045962395	Signature	1
Total: 2 Families	3 Domains	2 Protection Types	5

Top 5 Sources Accessed Malicious Sites



* You can analyze suspicious URLs by copying and pasting them into VirusTotal online service at www.virustotal.com

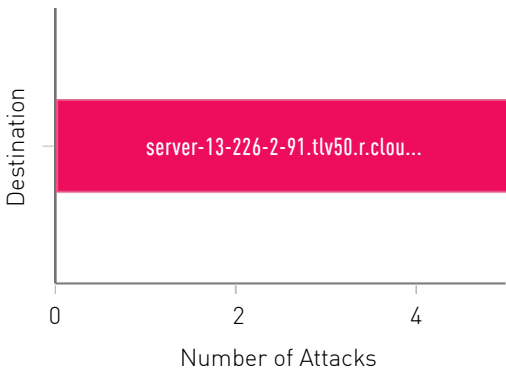
Attacks and Exploited Software Vulnerabilities

During the security analysis, attacks and exploited software vulnerabilities on servers/clients were detected. Such incidents might indicate intrusion attempts, malware attacks, DoS attacks or attempts to bridge security by exploiting software vulnerabilities. The following summarizes all events with known industrial reference.

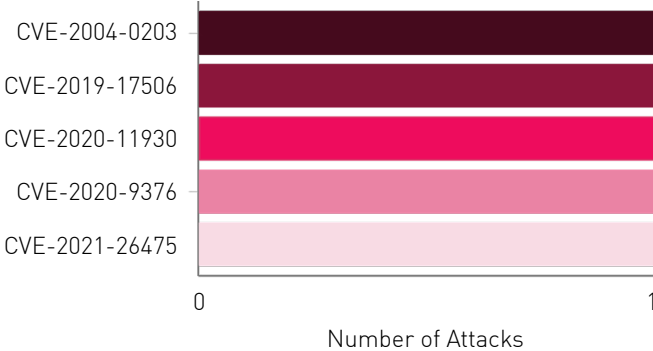
Top attacks and Exploited Software Vulnerabilities

Attacked Destination	Attack / Exploit	Industry Reference	Attack Source	Events
🇺🇸 server-13-226-2-91.tlv50.r.cloudfront.net (13.226.2.91)	Cross-Site Scripting Obfuscation Techniques	CVE-2020-11930 CVE-2021-26475 CVE-2021-26702 CVE-2021-26723 CVE-2021-39496 3 more References	🇺🇸 Host_1.1.1.10 (1.1.1.10)	1
	Cross-Site Scripting Scanning Attempt	CVE-2022-26564 CVE-2022-27166 CVE-2022-27926 CVE-2022-28102 CVE-2022-28363 3 more References	🇺🇸 Host_1.1.1.10 (1.1.1.10)	1
	D-Link Routers Information Disclosure	CVE-2019-17506 CVE-2020-9376 CVE-2023-48842	🇺🇸 Host_1.1.1.10 (1.1.1.10)	1
	EICAR AV test file		🇺🇸 Host_1.1.1.10 (1.1.1.10)	1
	Microsoft Exchange OWA Cross-Site Scripting and Spoofing (MS04-026)	CVE-2004-0203	🇺🇸 Host_1.1.1.10 (1.1.1.10)	1
Total: 5 Exploits		20 References	1 Source	5
Total: 1 Destination	5 Exploits	20 References	1 Source	5

Top Targeted End-Points



Top CVEs





* You can learn more about the vulnerability that IPS detected by copying and pasting the CVE into Check Point Research service at <https://research.checkpoint.com>

Scanned Servers

During the security analysis, attacks and exploited software vulnerabilities on servers/clients were detected. Such incidents might indicate intrusion attempts, malware attacks, DoS attacks or attempts to bridge security by exploiting software vulnerabilities. The following summarizes these events.

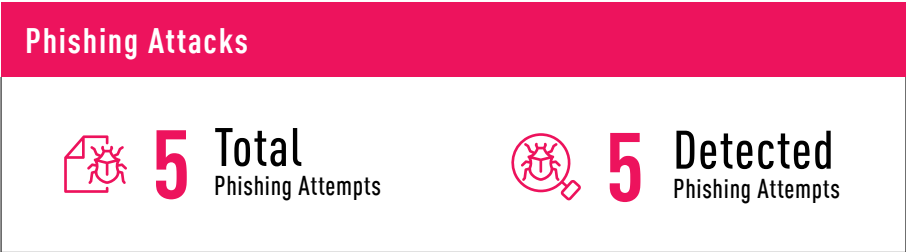
Top Scanned Servers

Target End-Point	Attack / Exploit	Events	Source
 server-13-226-2-91.tlv50.r.cloudfront.net (13.226.2.91)	Cross-Site Scripting Scanning Attempt	1	 Host_1.1.1.10 (1.1.1.10)
	Total: 1 Attack / Exploit	1	1 Source
Total: 1 Destination	1 Attack / Exploit	1	1 Source



Zero-Day Phishing

During the security analysis, we’ve detected attempts of clients to connect to Zero-Day Phishing websites. The following summarizes the Zero-Day Phishing incidents.

Check Point Zero-Day Phishing Prevention, powered by patented technologies and AI engines, prevents access to the most sophisticated phishing websites, both known and completely unknown, without the need to install and maintain clients on end-user devices.



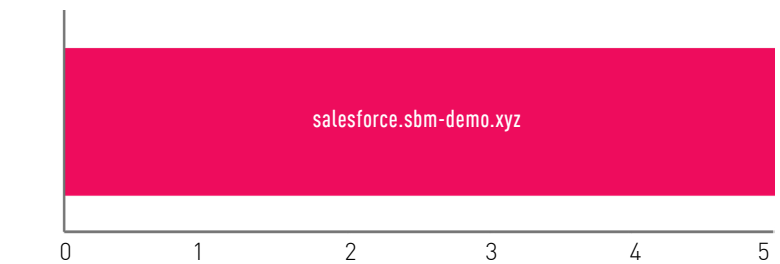
Top 10 Sources

Source	Domain Name	Confidence Level	Destination Country
 Host_1.1.1.10 (1.1.1.10)	salesforce.sbm-demo.xyz	<div><div></div></div> High	 United Kingdom

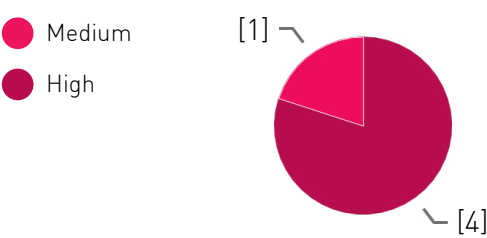
Web Phishing Attack Timeline



Top 10 Phishing Domains



Phishing Attacks Severity



DNS Security

During the security analysis, DNS related malicious activity was detected, such as Command & Control (C2) communication, DNS Tunneling for data exfiltration, and approaches to malicious or suspicious web sites.


Total Malicious



4

Malicious Detect

Malicious - by Techniques



4

Hits
Newly Created Domain

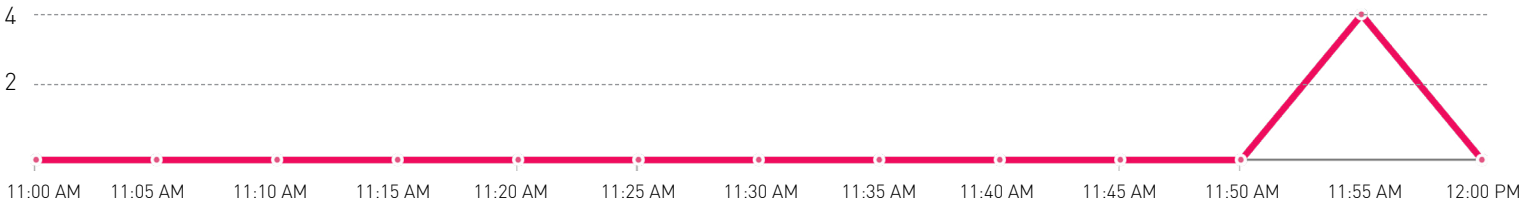
Top Malicious - by Attacks

Protection Name	Hits
Newly created domain	4
Total: 1 Protection	4

Top Malicious - by Domain

DNS Domain Name	Hits
htxhospitality.com	2
icloud-server-app.info	2
beamhub.app	0
Total: 3 DNS Domains Names	4

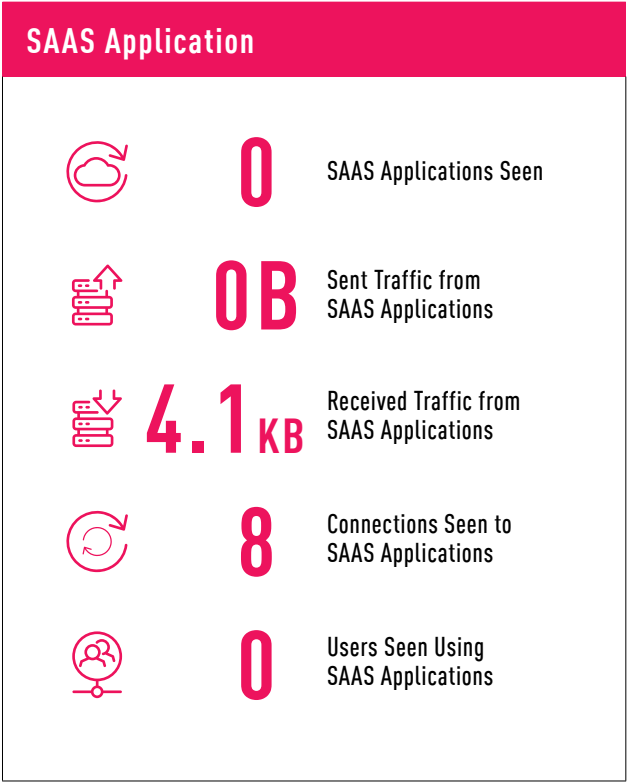
Malicious - Timeline



About Harmony Email & Collaboration Solution

Email is the first link in a chain of attacks, and with the rise of remote work, the use of cloud mailboxes and collaboration apps increased exponentially. Harmony Email & Collaboration provides organizations with complete, full-suite protection that is constantly adapting and evolving to the ever-changing threat landscape, while providing security admins with an easy-to-deploy and manage platform, making your security offerings easy and efficient.

This section covers applications that have tight integration with our Harmony Email and Collaboration solution and can be fully protected by our Threat Prevention engines focusing on File Storage, Cloud Email Services, Collaboration and CRM.



Top Harmony Email & Collaboration Supported Applications

No data found.

Timeline

No data found.

Endpoints Involved in High Risk Web Access and Data Loss Incidents



0

Running High Risk Applications



0

Accessed High Risk Web Sites



0

Users Accessed Questionable, Nonbusiness Related Web Sites



0

Users Involved in Potential Data Loss Incidents

Endpoints Involved in Malware and Attack Incidents



1

Infected with Malware



3

Malwares Downloaded



0

Received Email Containing Link to Malicious Site



1

Accessed a Site Known to Contain Malware



1

Attacked Sources
(Source IP addresses of IPS events)



1

Attacked Destinations
(Destination IP addresses of IPS events)





RECOMMENDATIONS

A decorative graphic consisting of two overlapping circles. The left circle is a solid dark red color. The right circle is composed of many thin, concentric, light red lines, creating a ripple effect. The circles overlap in the center, with the solid red circle partially obscuring the concentric ring circle.

Recommendations for the Security Checkup Key Findings

The Security Checkup assessment report reveals several types of threats that your organization is exposed to. In order to secure your critical assets we recommend you to review the following cyber security solutions and learn more about Check Point most updated technologies.

<p>Malware & Attacks</p> <p>Check Point Solution: Threat Prevention</p>	<p>A key Check Point differentiator when compared to other firewalls is the integration of best-in-class threat prevention across the architecture.</p> <p>While others concede attackers will get in and are pivoting to detection and response, our focus remains on stopping attacks before they succeed.</p> <p>This includes tackling the latest large-scale, multi-vector GenV attacks, in addition to more conventional attacks that are still widely used. Learn more.</p>
<p>High Risk Web Access, Bandwidth Analysis</p> <p>Check Point Solution: Application Inspection and Control</p>	<p>Check Point's Application Control capability supports security policies to identify, allow, block or limit usage of thousands of applications, including web and social networking, regardless of port, protocol or evasive technique used to traverse the network. It currently understands over 8,100 Web 2.0 applications with more being added continuously. Advanced user interaction features allow security administrators to alert employees in real-time about application access limitations, and query them as to whether application use is for business or personal use.</p> <p>This enables IT administrators to gain a better understanding of Web usage patterns, adapt policies and regulate personal usage without interrupting the flow of business. Learn more.</p>
<p>Data Loss</p> <p>Check Point Solution: Data Loss Prevention (DLP)</p>	<p>Check Point Data Loss Prevention (DLP) pre-emptively protects your business from unintentional loss of valuable and sensitive information.</p> <p>Integrated in Check Point Next Generation Firewalls (NGFW), network DLP enables businesses to monitor data movement and empowers your employees to work with confidence, while staying compliant with regulations and Industry standards. Learn more.</p>

<p>Mobile Threats</p> <p>Check Point Solution: Harmony Mobile</p> 	<p>Mobile security is a top concern for every company these days - and for a good reason. In the new normal, your remote workers increasingly access corporate data from their mobile devices, and that means you're exposed to data breaches more than ever. Harmony Mobile is the market-leading Mobile Threat Defense solution. It keeps your corporate data safe by securing employees' mobile devices across all attack vectors: apps, network and OS. Designed to reduce admins' overhead and increase user adoption, it perfectly fits into your existing mobile environment, deploys and scales quickly, and protects devices without impacting user experience nor privacy. Learn more.</p>
<p>Endpoints</p> <p>Check Point Solution: Harmony Endpoint</p> 	<p>Harmony Endpoint is a complete endpoint security solution built to protect the remote workforce from today's complex threat landscape. It prevents the most imminent threats to the endpoint such as ransomware, phishing or drive-by malware, while quickly minimizing breach impact with autonomous detection and response. This way, your organization gets all the endpoint protection it needs, at the quality it deserves, in a single, efficient, and cost-effective solution. Learn more.</p>
<p>IoT Devices</p> <p>Check Point Solution: Quantum IoT Protect</p> 	<p>Quantum IoT Protect provides the industry's only autonomous IoT threat prevention solution that secures both the network and IoT devices end-to-end. The solution automatically identifies, maps, and assesses the risk of any connected IoT device while also preventing unauthorized access to and from IoT devices with zero-trust profiles—all within minutes. Learn more.</p>
<p>Malware & Attacks, High Risk Web Access, Bandwidth Analysis</p> <p>Check Point Solution: Quantum SD-WAN</p> 	<p>Quantum SD-WAN is a software blade in Quantum Gateways that unifies the best security with optimized internet and network connectivity. By deploying Quantum SD-WAN right from your Quantum Security Gateways, network and security teams realize immediate benefits:</p> <ul style="list-style-type: none"> • Protects your branches against zero-days, phishing and ransomware. • No more Zoom interruptions thanks to sub-second failover. • Complete SASE solution managed from the cloud. • Single appliance for security & connectivity. • Installs with your current Quantum Gateways. <p>Learn more.</p>

CHECK POINT INFINITY PLATFORM

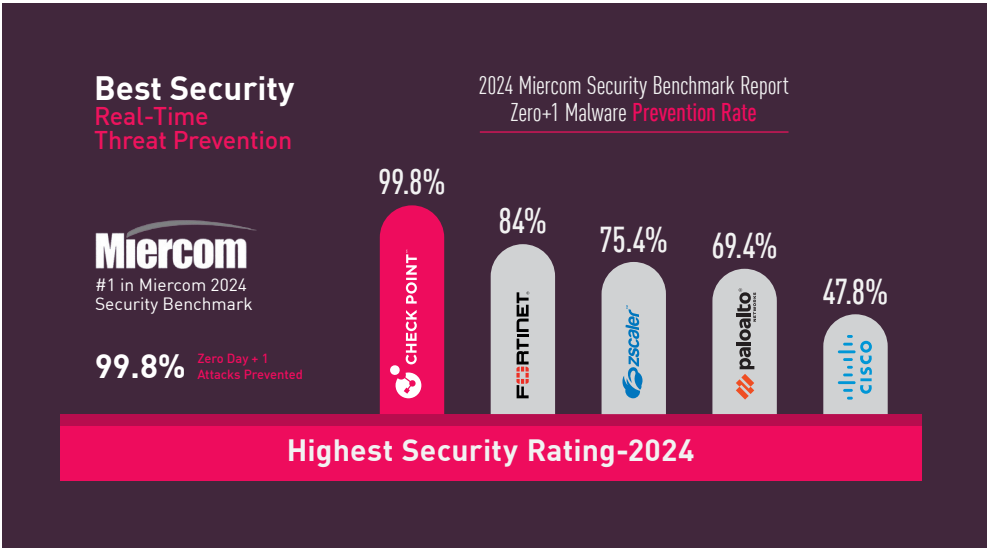
An abstract graphic consisting of two overlapping circles. The left circle is a solid dark red color. The right circle is composed of many thin, concentric, light red lines, creating a ripple effect. The circles overlap in the center, with the solid red circle partially obscuring the concentric ring circle.

The Check Point Infinity Platform addresses the challenges of an evolving threat landscape. It provides AI-Powered and Cloud-Delivered threat prevention across the data center, network, cloud, endpoint, mobile and IoT, with unified management and security operations that leverages real-time shared threat intelligence to prevent cyber attacks.

The Collaborative Security Platform

The Infinity Platform stands alone from other offerings:

- **Industry Leading Threat Prevention:** For the 2nd consecutive year, Check Point’s Infinity Platform was ranked #1 in Threat Prevention by Miercom¹, preventing 99.8% of unknown attacks and 100% of phishing attacks. These accuracy ratings far exceed our competitors.
- **Centralized and Unified Management:** Infinity Portal provides a single pane of glass to manage the Check Point portfolio of security solutions: Quantum, CloudGuard, Harmony and Infinity Platform Services. When recognizing Check Point as a leader in the Forrester Wave for Zero Trust Platform Providers², Forrester stated that “Check Point Sets the Bar for Centralized Management.”
- **Open and Automated:** Check Point defined cyber security interoperability and leads the industry in embracing open standards. We offer multiple API libraries and GitHub code repositories, we maintain compatibility with 3rd-party tools, and we use open threat indicator and signature formats.



Miercom Zero Trust Platform Assessment (2024)

[Download Report](#)

Miercom NGFW Security Benchmark 2024 study

[Download Report](#)

¹ Miercom NGFW Security Benchmark 2024 study

² Forrester Wave™ for Zero Trust Platform Providers Q3'23.

AI in Action

Artificial Intelligence and Generative AI capabilities operate intuitively within the Infinity Platform:

- **AI-Powered Threat Prevention:** Infinity ThreatCloud AI, with 50+ AI engines, powers industry-leading, real-time threat prevention in all Check Point solutions, to block billions of attacks per year, maintain compatibility with 3rd-party tools, and we use open threat indicator and signature formats.
- **Built-In Generative AI:** Infinity AI Copilot transforms cyber security with intelligent GenAI automation and interaction, which accelerates security management by up to 90%.
- **Automated Investigation and Remediation:** Infinity Playblocks and Infinity XDR quickly identify and contain sophisticated attacks to automate remediation and response.

Consolidated and Agile

Comprehensive protections across the enterprise: The Check Point Infinity Platform protects network, data center, cloud and workspace use cases, as well as providing advanced analytics and operations tools for security practitioners. The Infinity Platform includes:

- **Quantum—Secure the Network:** AI-powered threat prevention for securing mesh networks including the data center, perimeter, branch and remote users
- **CloudGuard—Secure the Cloud:** Prevention-first cloud security from code to cloud
- **Harmony—Secure the Workspace:** Comprehensive workspace security, including endpoint, mobile, email, and SaaS applications
- **Infinity Platform Services—Collaborative Security Operations and Services:** Security operations, Extended Prevention and Response (XDR), ThreatCloud AI and Infinity AI copilot, supported by Check Point 24/7 managed security services, consulting and training



Flexible payments to enable consolidation: Infinity Platform Agreements provide access to the full set of Check Point solutions, services, and support programs within a simple procurement framework. From off-the-shelf, all-inclusive programs, to tailor-made contracts, organizations can choose the structure that aligns best with the unique needs of the business and enjoy investment agility and reduced security spend.

About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading AI-powered, cloud-delivered cyber security platform provider protecting over 100,000 organizations worldwide. Check Point leverages the power of AI everywhere to enhance cyber security efficiency and accuracy through its Infinity Platform, with industry-leading catch rates enabling proactive threat anticipation and smarter, faster response times. The comprehensive platform includes cloud-delivered technologies consisting of Check Point Harmony to secure the workspace, Check Point CloudGuard to secure the cloud, Check Point Quantum to secure the network, and Check Point Infinity Core Services for collaborative security operations and services.

Worldwide Headquarters

5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters

100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com

