CHECK POINT

HARMONY ENDPOINT
THREAT ANALYSIS REPORT

Date

Dec 08, 2025

Customer

GFS Chemicals

Prepared by:

Harmony Endpoint - Check Point Technologies

Table of Contents

This report presents the security assessment of your organization by Harmony Endpoint and the vulnerabilities detected.
This report provides a summary of exposure to ransomware, phishing, zero-day malware, CC communication, data leakage, and other threats.

Malware and Attacks

170
Attacks were prevented

451
Attacks were detected

12 Hosts encountered malicious files

0 Hosts were encountered exploit attack

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

0
Hosts Encountered Ransomware Attack

Check Point's Anti-Ransomware includes active threat prevention that detects and quarantines detect and quarantine ransomware attacks, and of course, the ability to restore your files from routine backups.

Compromised Credentials

0
Credentials leak events were encountered

Re-using corporate passwords on unauthorized or non-corporate sites puts organizations at risk. Access to corporate services are secure when employees are blocked from re-using their corporate credentials on non-corporate websites.

High Risk Web Access

2
Phishing attacks were encountered

Check Point's Zero-Phishing technology identifies and blocks both known and unknown phishing sites. Sites are inspected within the user's browser by analyzing multiple page elements.

369
High risk website access incidents

High risk websites include categories, such as Phishing, Botnets, Spyware and so on. Access to these websites is blocked by the pre-defined policy to prevent risk to the organization.

161.0K
Incidents of access to websites marked as non-compliance by the policy

URL filtering controls access to millions of websites by category, users, groups and machines to ensure your corporate policy is enforced.

Key Findings

Top Protections

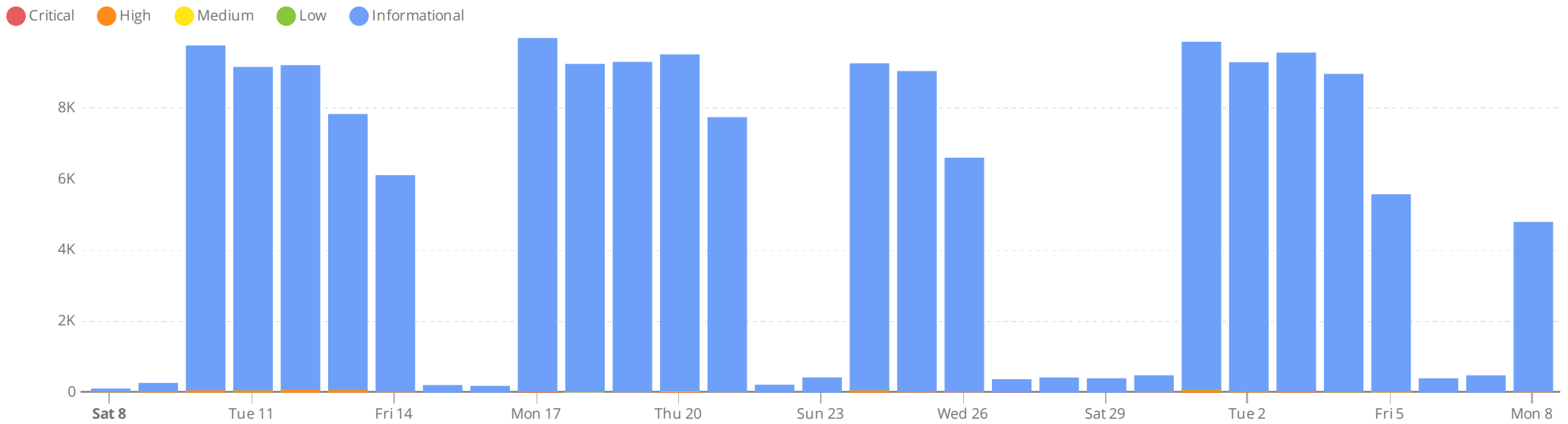
Protection Type	Blade	Severity	Logs
Behavioral	Forensics	Medium	1
EXE	Forensics	High	17
File Monitor	Forensics	Critical	9
File Reputation	Forensics	High	21
	Threat Emulatio.	Critical	3
File System Emulation	Forensics	High	15
	Threat Emulatio.	Critical	2
HTTP Emulation	Threat Emulation	Critical	1

Top Malware Activities

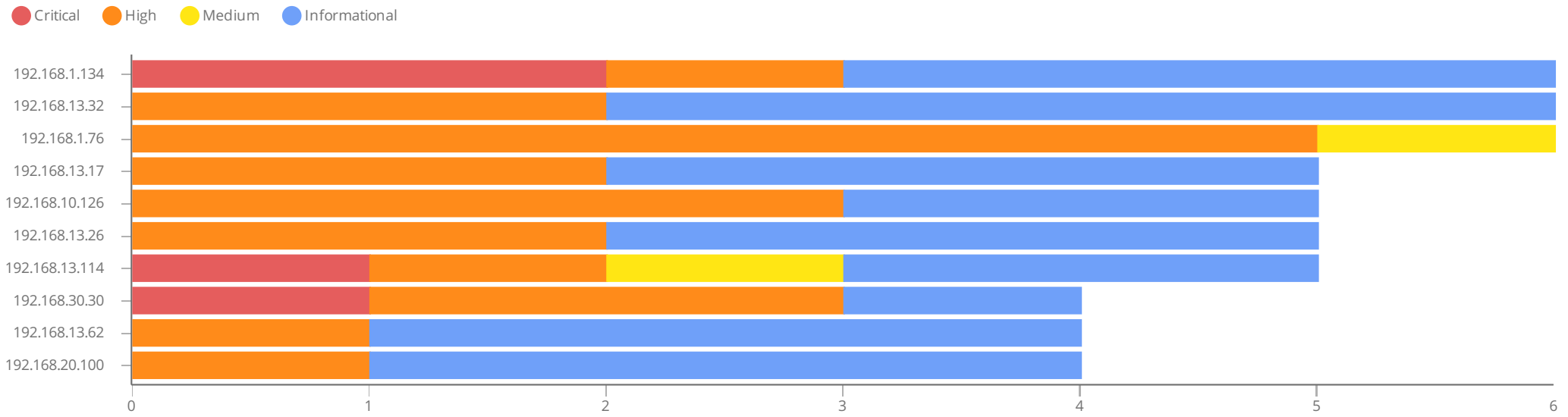
Malware Action	Blade	Logs
Not Supported	Threat Extraction	2.1K
Excluded	Threat Extraction	162
Access to site known to contain malware	Anti-Bot Forensics	123
behavioral	Forensics	4
behavioral, research	Forensics	1
trojan	Forensics	1

Showing only events with severity: Critical, High and Medium

Malware Activity



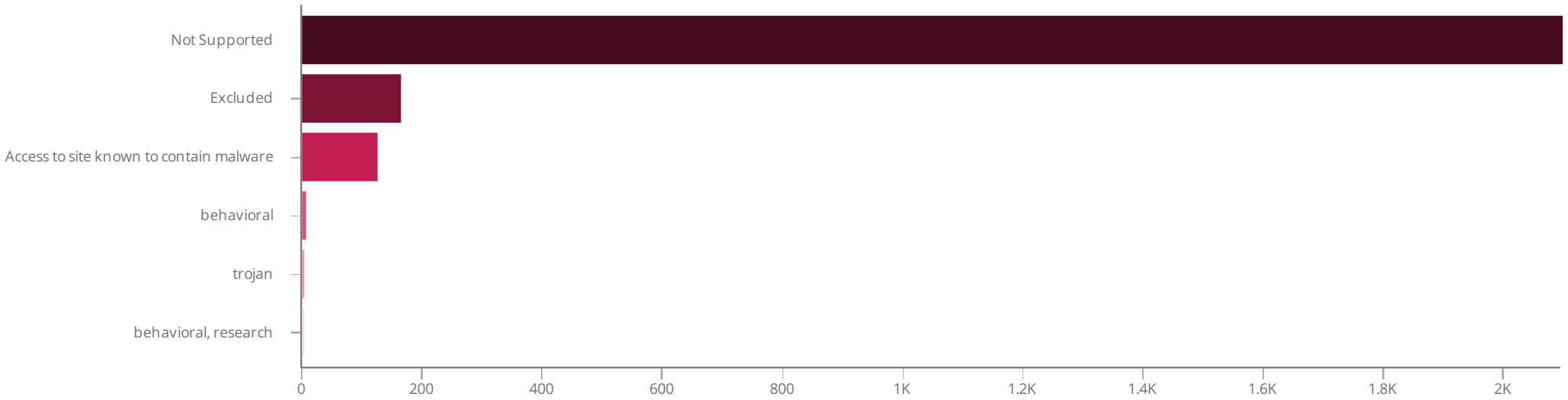
Top Hosts by No. of Incidents



Top Hosts by Severity

Source	Severity	Blade	Protection Name	Protection Type	Action
192.168.1.134	Critical	URL Filtering Threat Extraction Forensics Threat Emulation	gen.urlf Extract potentially malicious content Gen.Rep.exe gen.ba.sb.exe	URL Filtering Content Removal File Reputation HTTP Emulation File System Emulation	Detect Extract Prevent
192.168.30.30	Critical	URL Filtering Anti-Bot Forensics Anti-Malware	gen.urlf CrowdStrike.TC.dfa3TKfS Mal/FakeAle-SK	URL Filtering URL Reputation Protection	Detect Prevent
192.168.10.90	Critical	URL Filtering Forensics Anti-Bot	gen.urlf Conficker.TC.d3cdQjLh	URL Filtering URL Reputation	Detect Prevent

Top Actions by Malware



Top Actions by Malware

Malware Action	Protection Type	Source	Logs
Not Supported	Content Removal	85 Sources	2.1K
Excluded		32 Sources	162
Access to site known to contain malware	URL Reputation	33 Sources	123
behavioral	Behavioral	2 Sources	4
behavioral, research	Behavioral	1 Source	1
trojan	Trojan	1 Source	1

Top Malware Activity and Sources by Severity

Malware Action	Source	Severity	Action	Logs
Access to site known to contain malware	192.168.10.90	Critical	Prevent	3
	192.168.60.6	Critical	Prevent	2
	192.168.13.114	Critical	Prevent	2
	192.168.13.26	High	Prevent	9
	192.168.1.76	High	Prevent Detect	8
	Total: 1 Source	**Critical**	**1 Action**	**107**
trojan	192.168.13.114	High	Detect	1
	Total: 1 Source	**High**	**1 Action**	**1**
behavioral, research	192.168.20.115	Medium	Prevent	1
	Total: 1 Source	**Medium**	**1 Action**	**1**

ACCESS TO HIGH RISK WEB SITES

Web use is ubiquitous in business today. But the constantly evolving nature of the web makes it extremely difficult to protect and enforce standards for web usage in a corporate environment. To make matters more complicated, web traffic has evolved to include not only URL traffic, but embedded URLs and applications as well. Identification of risky sites is more critical than ever. Access to the following risky sites was detected in your network, organized by category, number of users, and number of hits.

Top high risk web sites (Top phishing attempts)

Resource	Time	Username
https://www.fedexnflsweeps.com/	Dec 5, 2025 5:49:07 PM	johnreed
https://documentsharedtobereviewedonline039uyio0u93894yhrusharepoint983.net-isi.com/p347wxbsxw11w1kaykmocx6bvsimojeiiqadbgic69o0sc7mzmkc0uwyzkhtfh3xnnsalf1k2wty47x1yurszqmux4yplfs82zloizgwuefcajwkckwvsrj2fsdd54jzluxwoxh/ybhllgjwagc1	Dec 3, 2025 2:14:48 PM	bgates

Access to non-business websites or to sites containing questionable content can expose an organization to possible productivity loss, compliance and business continuity risks.

Access to Questionable Sites

Category	Hits
Gambling	8
Illegal Drugs, Marijuana	4
Sex, Pornography	1

Users With Credential Leak Events

No data found.

Harmony Endpoint

Harmony Endpoint All The Endpoint Protection You Need

Harmony Endpoint is a complete endpoint security solution built to protect the remote workforce from today's complex threat landspace. It prevents the most imminent threats to the endpoint, such as ransomware, phishing, or driven-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.

Why Harmony Endpoint?

Today more than ever, endpoint security plays acritical role in enabling your remote workforce. With 70% of cyber attacks are through an endpoint, complete endpoint protection at the highest security level is crucial to avoid security breaches and data compromise.

Harmony Endpoint is part of the Check Point Harmony product suite, the industry's first unified security solution for users, devices, and access.

Harmony consolidates six products to provide uncompromised security and simplicity for everyone.
It protects devices and internet connections from the most sophisticated attacks while ensuring Zero-Trust Access to corporate applications - all in a single solution that is easy to use, manage and buy.

How does It work?

- **Block malware** coming from web browsing or email attachments before it reaches the endpoint, without impacting user productivity. Every file received via email or downloaded by a user through a web browser is sent to the Threat Emulation sandbox to inspect for malware. Files can also be sanitized using a Threat Extraction process (Content Disarm Reconstruction technology) to deliver safe and cleaned content in milliseconds.

- **Gain runtime protection against ransomware, malware, and file-less attacks, with instant and full remediation**, even in offline mode. Once an anomaly or malicious behavior is detected, Endpoint Behavioral Guard blocks and remediates the full attack chain without leaving malicious traces. Anti-Ransomware identifies ransomware behaviors such as encrypting files or attempts to compromise OS backups and safely restores ransomware-encrypted files automatically. Harmony Endpoint uses a unique vaulted space locally on the machine that is only accessible to Check Point signed processes - in case the malware attempts to perform a shadow copy deletion, the machine will not lose data.

- **Phishing Protection** - Prevent credential theft with Zero-Phishing® technology that identifies and blocks the use of phishing sites. Sites are inspected and if found malicious, the user is blocked from entering credentials. Zero-phishing® even protects against previously, unknown phishing sites and corporate credentials re-use.

Harmony Endpoint is a Worldwide Major Player

Check Point Harmony Endpoint has been recognized as a major player by IDC Marketplace for its unique strengths, including:

- Distinctive sandboxing and Content Disarm Reconstruction (CDR) capabilities which allow advanced malware protection without reducing user productivity
- Runtime protection and complete remediation from attacks, with the instant and automated restoration of ransomware-encrypted files, even in offline mode.
- Robust sales channel strategy and continuous investment in both innovative and core security technologies which make its endpoint security solution compelling for the enterprise, SMB market, and even consumers.
- Unified security solution with cloud-based management which reduces vendor relationships, and overhead in security operations, and improves security readiness. We were also recognized as a major player in another IDC market scale report for endpoint security for small midsize businesses.

FASTEST RECOVERY

- **Automated attack containment and remediation**:
  the only Endpoint Protection solution that automatically and completely remediates the entire cyber kill chain. Once an attack has been detected, the infected device can be automatically quarantined to prevent lateral infection movement and restored to a safe state.
- **Auto-generated forensic reports:**
  providing detailed visibility into infected assets, attack flow, and correlation with the MITRE ATT&CK™ Framework. The Forensics capability automatically monitors and records endpoint events, including affected files, processes launched, system registry changes, and network activity, and creates a detailed forensic report. Robust attack diagnostics and visibility support remediation efforts, allowing system administrators and incident response teams to effectively triage and resolve attacks.
- **Threat Hunting** powered by enterprise-wide visibility and augmented by globally shared threat intelligence from hundreds of millions of sensors, collected by ThreatCloud™. With the Threat Hunting capability, you can set queries or use predefined ones to identify and drill down into suspicious incidents, and take manual remediation actions.

CONSOLIDATED SECURITY MANAGEMENT

Managing the entire security network is often complicated and demands a high level of human expertise. Check Point Infinity, powered by R80.x security management version, brings all security protections and functions under one umbrella, with a single console that enables easier operation and more efficient management of the entire security network. The single console introduces unparalleled granular control and consistent security and provides rich policy management which enables delegation of policies within the enterprise. The unified management, based on modular policy management and rich integrations with 3rd party solutions through flexible APIs, enables automation of routine tasks to increase operational efficiencies, freeing up security teams to focus on strategic security rather than repetitive tasks.

CHECKPOINT INFINITY

Build on Check Point Infinity, the first consolidated security architecture designed to resolve the complexities of growing connectivity and inadequate security, delivering full protection and threat intelligence across networks, clouds, endpoints, mobile devices, and IoT.

Future-proof your business and ensure business continuity with the architecture that keeps you protected against any threat, anytime and anywhere.

KEY PRODUCT BENEFITS

- **Complete endpoint protection:** prevent the most imminent threats to the endpoint.
- **Fastest recovery:** Automating 90% of attack detection, investigation, and remediation tasks.
- **Best TCO:** All the endpoint protection you need in a single, efficient, and cost-effective.

UNIQUE PRODUCT CAPABILITIES

- Advanced behavioral analysis and machine learning algorithms shut down malware before it inflicts damage.
- High catch rates and low false positives ensure security efficacy and effective prevention.
- Automated forensics data analysis offers detailed insights
  into threats.
- Full attack containment and remediation to quickly restore any infected systems.

About Check Point

Check Point Software Technologies' mission is to secure the Internet. Check Point was founded in 1993, and has since developed technologies to secure communications and transactions over the Internet by enterprises and consumers.

Check Point was an industry pioneer with our FireWall-1 and our patented Stateful Inspection technology. Check Point has extended its IT security innovation with the development of our Software Blade architecture. The dynamic Software Blade architecture delivers secure, flexible and simple solutions that can be customized to meet the security needs of any organization or environment.

Check Point develops markets and supports a wide range of software, as well as combined hardware and software products and services for IT security. We offer our customers an extensive portfolio of network and gateway security solutions, data and endpoint security solutions and management solutions. Our solutions operate under a unified security architecture that enables end-to-end security with a single line of unified security gateways, and allow a single agent for all endpoint security that can be managed from a single unified management console. This unified management allows for ease of deployment and centralized control and is supported by, and reinforced with, real-time security updates.

Our products and services are sold to enterprises, service providers, small and medium sized businesses and consumers. Our Open Platform for Security (OPSEC) framework allows customers to extend the capabilities of our products and services with third-party hardware and security software applications. Our products are sold, integrated and serviced by a network of partners worldwide. Check Point customers include tens of thousands of businesses and organizations of all sizes including all Fortune 100 companies. Check Point's award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.

www.checkpoint.com

CORPORATE HEADQUATERS

United States
Check Point Software Technologies Inc. 959 Skyway Road Suite 300
San Carlos, CA 94070
1-800-429-4391
International
Check Point Software Technologies Ltd.
5 Ha'Solelim Street
Tel Aviv 67897, Israel
+972-3-753-4555
Please contact us for more information and to schedule your onsite assessment:
Within the US: 866-488-6691
Outside the US: +44 2036087492


CHECK POINT
HARMONY ENDPOINT
THREAT ANALYSIS REPORT