CHECK POINT™

COMPLETE RANSOMWARE PROTECTION

Multi-layered protection across endpoints, mobile devices, email, web, and networks

YOU DESERVE
THE BEST SECURITY

Contents

Executive summary 3

The current threat landscape 4

The latest techniques being used by cybercriminals............ 5

Ransomware-as-a-service 5

Partial encryption 6

The multithreaded model 7

The triple extortion strategy............ 7

Industries at risk 8

Healthcare 8

Higher education 8

Manufacturing 8

Healthcare 9

Higher education 9

Manufacturing 9

Anatomy of an attack 11

The target 11

The attack 11

The Black Basta toolbox 12

The response............ 12

Lessons learned............ 13

Ransomware protection best practices 14

Check Point complete ransomware protection 16

Harmony Endpoint 16

Harmony Mobile 16

Harmony Email & Collaboration 17

Browser Security 17

Horizon XDR/XPR............ 18

Quantum Firewalls 18

Infinity Global Services 19

Conclusion 20

Executive summary

The frequency and damage of ransomware attacks continue to grow at a record-breaking pace. Nearly three-quarters of all organizations fall victim sooner or later. And the financial ramifications are dire, with losses coming in at an average of $4.35 million per data breach.

The battle is fierce. Ransomware attacks are becoming increasingly more sophisticated with complex strategies such as ransomware-as-a-service and advanced techniques such as partial encryption coming to the fore.

Moreover, cybercriminals have started demanding ransom not only from the infected organization, but also from its customers, partners, and suppliers.

To make things worse, of those who have been hit, 80% are hit again with 40% paying again, of which 70% pay a higher amount.[1] And even after paying the ransom, few organizations wind up being able to reconstruct all the data that has been compromised.

All this makes cyber insurance carriers weary, resulting in a higher cost to insure, a lower chance of receiving full coverage, and heightened risk to CISOs (Chief Information Security Officers) of being held personally accountable.

This is why it is incumbent upon security leaders and their teams to make sure that they fortify the weak links across every vector, including the network, endpoints, mobile devices, browsers, and email and collaboration tools.

In this paper we will discuss the latest techniques being used by cybercriminals so you can be ready, best practices for enhancing protection, a breakdown of a recent attack and the lessons learned, and how the Check Point anti-ransomware solution has you covered with complete, multi-layered protection.

[1] https://www.securityweek.com/it-doesnt-pay-pay-study-finds-eighty-percent-ransomware-victims-attacked-again/

The current threat landscape

Ransomware continues to pose a major threat to organizations all over the world and across every industry.

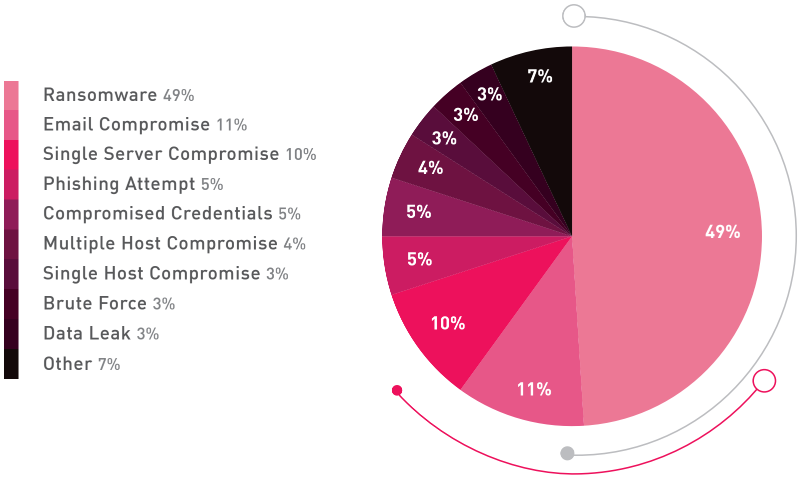
71%
of organizations
have been attacked[2]

$4.35 million
is the average
cost of a data breach[3]

$265 billion
is the expected cost of
ransomware damage by 2032[4]

In fact, ransomware accounts for nearly half of all the initial threat indicators in the cases handled last year by the Check Point Incident Response Team.

Check Point Incident Response Team cases in 2022 by initial threat indicators



The ongoing increase in frequency and damages is due in part to the continued proliferation of remote work as well as to the accelerated adoption of cloud computing.

And the damage can be great, not just because of the cost of the actual breach, but also from multiple additional domains, including:

- **Forensic assistance** from legal and other third parties.
- **Equipment and staff hours** required for rebuilding the environment.
- **Revenue lost** due to stalled production and manual data processing.
- **Litigation** by employees, customers, partners, and other affected parties.
- **Reduced productivity and employee engagement** due to the stress involved with handling incidents and the extensive time required for resolving them.
- **Inefficiencies** resulting from having to bring legacy systems online and the associated reconfiguration complexities that are particularly challenging when the personnel who made the original configurations are no longer with the company.
- **Fines** from regulators for any mishandling or privacy transgressions that resulted from the breach.

[2] https://aag-it.com/the-latest-ransomware-statistics/#:~:text=71%25%20of%20organisations%20worldwide%20were,successful%20ransomware%20attacks%20in%202021.

[3] https://www.ibm.com/reports/data-breach

[4] https://securityintelligence.com/news/ransomware-costs-expected-265-billion-2031/

The latest techniques being used by cybercriminals

Ransomware today is more difficult than ever to prevent and resolve with cybercriminals using new and sophisticated approaches, tools, and techniques, such as:

- Ransomware-as-a-service
- Partial encryption
- The multithreaded model
- The triple extortion strategy

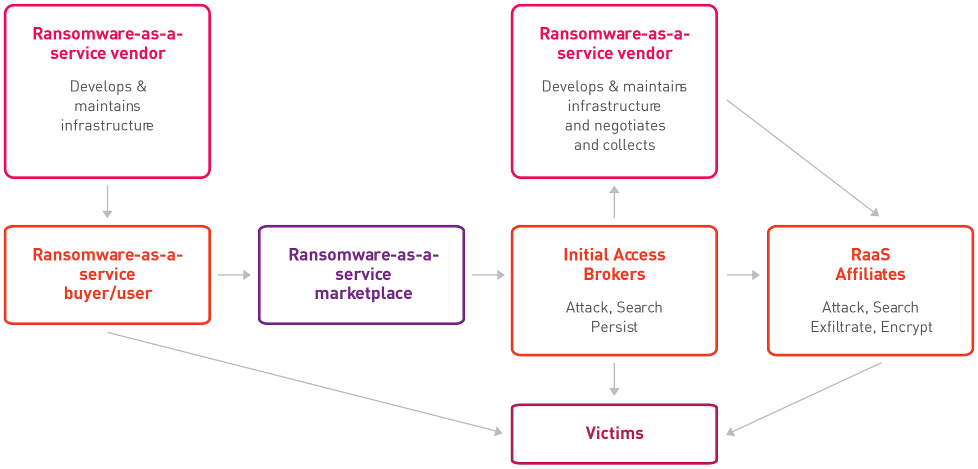
Ransomware-as-a-service

The traditional, direct route from threat actor to victim has been augmented with an approach that makes the battle to protect all the more challenging for security professionals.

With ransomware-as-a-service, threat actors develop the ransomware, encryptors, and related decryptors, to offer them as a service to interested parties. And sometimes they even conduct the negotiations on their behalf.

By offering ransomware tools and services for hire, RaaS has expanded the pool of potential attackers, making it easier for even non-technical individuals to launch sophisticated attacks against major organizations.

The complex web of ransomware-as-a-service


Ransomware-as-a-service vendor
Develops & maintains infrastructure
Ransomware-as-a-service vendor
Develops & maintains infrastructure and negotiates and collects
Ransomware-as-a-service buyer/user
Ransomware-as-a-service marketplace
Initial Access Brokers
Attack, Search Persist
RaaS Affiliates
Attack, Search Exfiltrate, Encrypt
Victims

Partial encryption

One of today's fastest growing ransomware trends is partial encryption, also known as intermittent encryption, which enables cybercriminals to be faster and more efficient.

With this technique, they avoid the need to encrypt all the files that are being held for ransom – a very time intensive task.

Instead, they encrypt just a portion of the target's files. This can be done randomly, or by encrypting a certain percentage of the data, or only the most critical files.

Threat actors can also selectively encrypt files related to a specific project, crippling the initiative until payment is made.

The advantages of partial encryption

Speed

Faster and less resource-intensive than traditional encryption, enabling attackers to finish the task before victims notice the intrusion.

Complexity

With only some of the data being encrypted, it's harder for victims to restore it from backups, making it much more likely that they will pay the ransom.

Less detectable

Automated scanners might not notice the smaller-scale modifications made by partial encryption and compromised systems may not behave as erratically, triggering fewer alerts.

A partial encryption incident

On Wednesday morning, May 3rd, 2023, security personnel at the City of Dallas became the target of a ransomware attack that leveraged partial encryption.

Multiple servers across a range of departments were affected, preventing 911 dispatchers, courthouse personnel, and police officers from using their computers for days.

Moreover, sensitive data had been stolen from 800,000 files containing the full names, home addresses, social security numbers, dates of birth, and the health and insurance data of at least 30,000 city employees and other individuals.

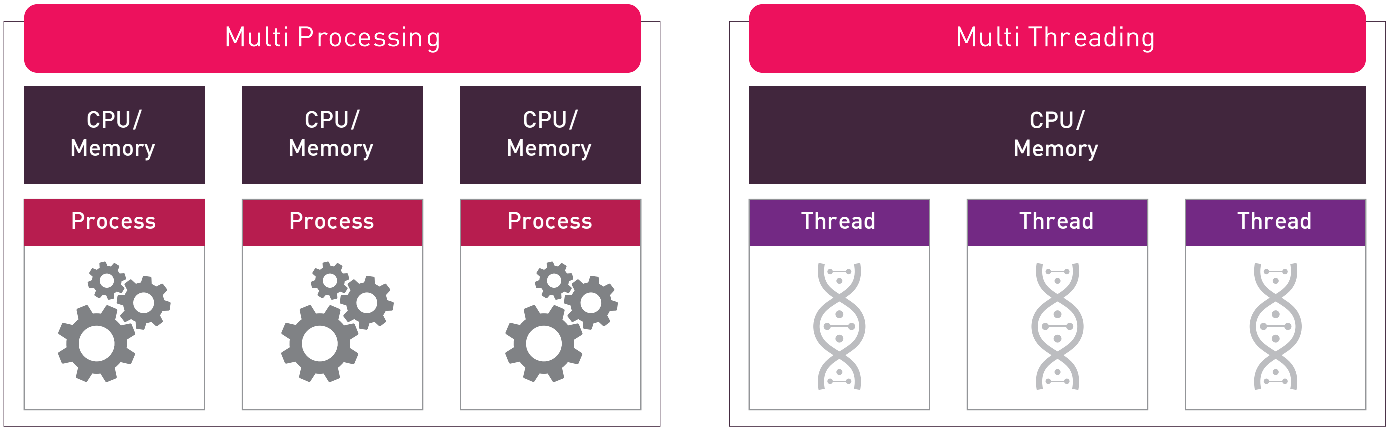
The Royal ransomware group, which took responsibility for the attack, threatened to release the information. This had the potential to bring great harm to the impacted parties. For, if the personal data of police officers, for example, would wind up in the hands of violent offenders seeking retaliation, the outcome could be life threatening.

The multithreaded model

The multithreaded model is another strategy that is becoming increasingly popular among cybercriminals.

In this type of attack, multiple CPU cores are used to encrypt files simultaneously. This can quickly overwhelm the organization's available processing power and make the attack more difficult to stop.

Even if one or two child processes are stopped, the remaining ones will continue to encrypt files. This can be very destructive for the targeted organization.



Multi-threading Vs. Multiprocessing

The triple extortion strategy

In a double extortion strategy, attackers first hold the encrypted drives for ransom, and then threaten to release or sell encrypted data if the organization doesn't pay.

For the victim, this means that even if the files are restored from a backup, they must still pay to avoid data leakage.

By contrast, when a triple extortion attack unfolds, as the name suggests, it does so in three stages:

Infiltrate and encrypt
the attacker profits when the victim makes the ransom payment to decrypt the data

Exfiltrate and threaten to sell
the attacker profits from payment made to avoid the sale of data

Extract a ransom from third parties
the attacker gains additional profits by putting pressure on the victim or through third parties whose data has been stolen

Industries at risk

There is no industry that is immune to the risk of a ransomware attack. Yet, there are those who are targeted more often than others. These include healthcare, higher education, and manufacturing.

Healthcare

In 2022, the healthcare industry saw an average of 1,426 attempted breaches per week per organization, a 78% year-over-year increase.

Healthcare data is valuable and very sensitive, due to privacy regulations and the fact that lives are at stake. In a recent Ponemon study of healthcare IT professionals[5], nearly half (45%) said that ransomware had led to increased complications from medical procedures.

It's no surprise then that healthcare organizations are more likely to pay a ransom as compared with other industries.

Higher education

Attacks against higher education institutions are on the rise, with 64% of higher education institutions having experienced attacks[6] over the past year.

Colleges and universities are seen as attractive targets because they hold valuable data, their IT departments are often understaffed, they are typically allotted only limited security resources, and their time to recover can be longer than in other industries.

Manufacturing

The manufacturing sector is often the industry most heavily hit by ransomware[7]. The primary vector for these organizations is unpatched vulnerabilities, particularly in industrial control systems.

Manufacturers may also be more likely to pay the ransom to avoid production disruptions and financial losses.

[5] https://www.healthcareitnews.com/news/ransomware-stakes-are-life-or-death-says-ponemon-report

[6] https://edscoop.com/ransomware-colleges-universities-data/#:~:text=The%20survey%2C%20published%20last%20week,79%25%20reporting%20attacks%20this%20year.

[7] https://newsroom.ibm.com/2022-02-23-IBM-Report-Manufacturing-Felt-Brunt-of-Cyberattacks-in-2021-as-Supply-Chain-Woes-Grew

Recent attacks on organizations in high-risk industries

Healthcare

The Rhysida ransomware group attacked Prospect Medical in August of 2023[8]. As a result, the company, which operates 16 hospitals and numerous clinics across the US, was forced to use time consuming and often error-prone paper charts until the systems could be restored.

Higher education

Just as schools were opening all over the country, in September of 2021, Howard University, a top academic institution in the US, was forced to cancel all of the scheduled classes due to a ransomware attack[9].

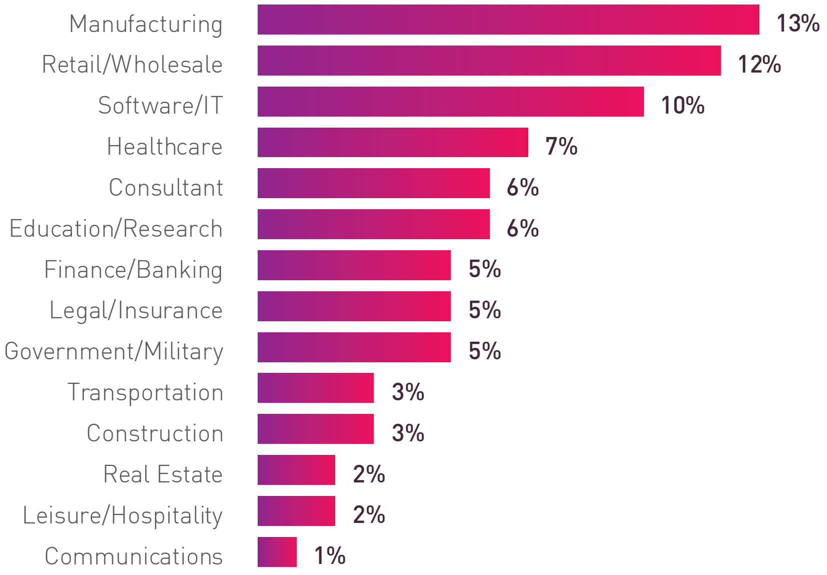
Manufacturing

Taiwan Semiconductor Manufacturing Company (TSMC), the world's largest chip manufacturer, was hit by the LockBit ransomware group in June 2023, which demanded $70 million.

But it's not just healthcare, higher education, and manufacturing industries that are in the line of fire. Any organization storing sensitive data is at risk.

Ransomware per industry, Check Point Research mid-year report 2023

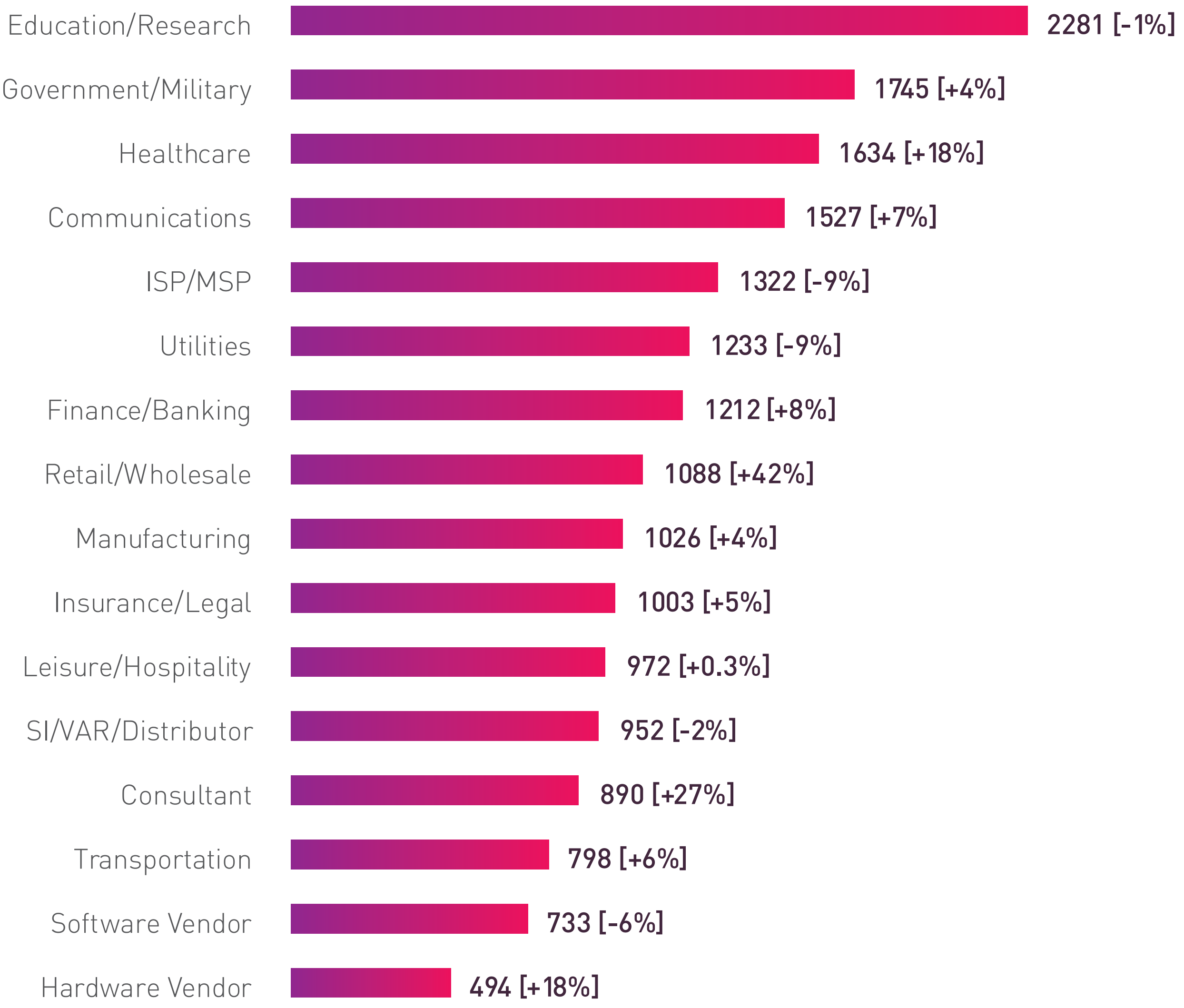
Industry Distribution of Ransomware Victims, as Reported on Shame Sites - H1 2023



[8] https://www.bleepingcomputer.com/news/security/rhysida-claims-ransomware-attack-on-prospect-medical-threatens-to-sell-data/

[9] https://techcrunch.com/2021/09/07/howard-university-cancels-classes-after-ransomware-attack/

Global average of weekly attacks per industry, Check Point Research mid-year report 2023



This is especially true today, with the use of partial encryption and other hyper efficient techniques likely to increase in popularity. This makes it easier for threat actors to be more effective than ever in stealing assets and avoiding interception.

Anatomy of an attack

To gain a fuller understanding of how today's sophisticated ransomware attacks unfold, let's take a look at one recent example.

The target

The target in this case is a leader in manufacturing that has a $400 million turnover, presence in over 19 countries, and more than 80 partners worldwide.

The manufacturer's environment

300	**150**	**AWS**	**Small IT team**
hosts	servers	cloud assets	on the entire environment

While the team is agile and experienced, they were faced with great challenges in protecting systems and data.

Security resources were limited, and the technology stack is ever growing. This hindered visibility, limited awareness, and made it very difficult to manage operational security products. It also placed formidable hurdles on the path to accelerated response and effective prevention.

In fact, for any organization, lacking the required security personnel will profoundly impact readiness and situational awareness. It will also undermine the ability to monitor actively in between incidents and to react and investigate effectively when they happen.

The attack

The group behind the attack was Black Basta, which launched a double extortion attack, as follows:

- Initial access was achieved by sending a phishing email that duped unsuspecting employees into clicking on a malicious link.
- Privilege escalation was enabled by accessing the cpassword string, which stores valid encrypted credentials associated with group policy preferences, and by using Mimikatz to steal credentials.
- Persistence was facilitated by creating additional user accounts and by deploying Cobalt Strike.
- Lateral movement was propagated by sending out additional internal phishing emails and by deploying IPScanner, Splashtop, Anydesk, and more.
- Evading defenses was accomplished by disabling the EDR and clearing event logs.
- Exfiltration was done with Rclone.
- Data upload was done to Mega.

At this point, the ransomware was deployed.

The Black Basta toolbox

Phishing	cpassword	Mimikatz	Cobalt Strike	IPScanner	Mega
Splashtop	Anydesk	EDR disablement	Event logs clearing	Rclone	

As a result, the manufacturer's environment suffered a severe impact. There were 150 servers hit, 3,000 hosts that needed to be reconstructed, and valuable customer data that was exfiltrated.

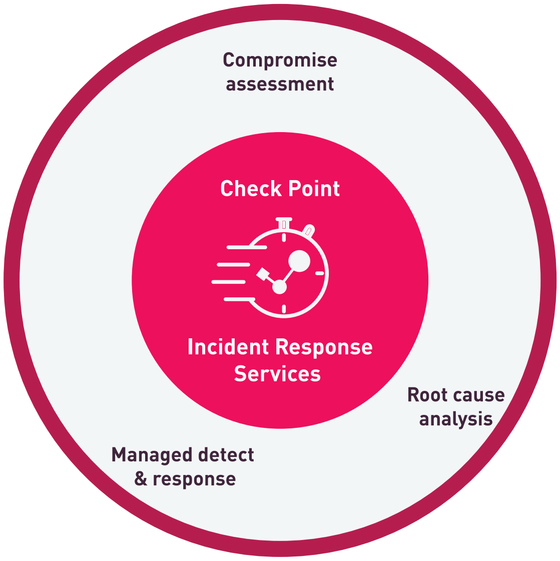
The response

Once alerted to the attack, the manufacturer immediately reached out to the Check Point Incident Response Team.

To contain the incident, the team first performed a compromise assessment and detected where the threat actors had been present and may still be active.

They also performed a root cause analysis to deliver a full understanding of how and why the incident unfolded as it did along with actionable recommendations to minimize the risk of suffering such an attack in the future.

The teams worked 24/7 for several days and achieved full recovery in just under four weeks, considerably reducing potential impact on the business.



Lessons learned

As a result of the insights provided by the Check Point IR team, the organization understood where its security was lacking, and that bolstering posture meant that they needed to:

Enhance **user awareness**	Deploy **multi-factor authentication**	Deploy **additional email security**	Enhance **patch management**	Increase **endpoint protection**
Update the **password policy**	Enhance the **firewall policy**	Improve **logging, monitoring, alerting**	Expand **team security knowhow**	Create **an IR plan and playbook**

This realization helped them to accelerate their time to cyber maturity by two years. They allocated budgets faster than ever before, expedited implementation of the required technologies, and quickly onboarded the required cyber experts.

Ransomware protection best practices

With the high cost of a ransomware infection, proper preparation can dramatically reduce the impact of an attack.

The first step towards preparation is to create a robust incident response plan (IRP). The plan should include clear definitions for roles and responsibilities, the response flow, the battle rhythm, an escalation policy, and specific playbooks for various incident scenarios.

Along with the right plan in hand, implementing the following best practices will further help minimize exposure and damage.

Inventory assets

Every security strategy should begin with a comprehensive assessment of what you need to protect and should include taking stock of the OT assets that may be the weakest security link in the organization.

Patch, patch, patch

Keep up to date with a rigorous patching regimen, since known vulnerabilities are a popular attack vector, and automate patching wherever possible.

Watch for pre-ransomware

Trojan malware infections such as Trickbot, Emotet, Dridex, and Cobalt Strike should be dealt with immediately, as these can all be used to let ransomware in the door.

Minimize the blast zone

Reduce the impact of a potential attack with security measures such as strong user authentication and network segmentation to limit the radius of an attack's spread.

Assess ransomware risk

Prepare for ransomware by evaluating how current defenses align with security best practices, covering all cyber vectors, including cloud, network, endpoint, mobile, and IoT. In addition, make sure to perform thorough penetration testing and a compromise analysis.

Stay on guard 24/7

When it comes to ransomware attacks, hackers usually take advantage of times when people are less vigilant. During the past year, most breaches occurred during weekends and holidays.

Back up your data

Store multiple copies of data in different locations, including on-premises, physical, and cloud. Establish a backup testing regimen, and never attach an uninfected backup to an infected

In addition to the above steps, it is also important to be aware of and correct some of the more prevalent failures in traditional defenses:

- **Backups** that aren't kept offline, which doesn't prevent their encryption and manipulation by bad actors
- **Cloud protections** that do not block phishing emails
- **Desktop antivirus** that doesn't prevent the ransomware from launching
- **No consolidation** of tools, which impacts collaboration, time to resolution, costs, and more
- **Alert overload** on SOC analysts
- **No prioritization** of SIEM logs
- **End user training** that isn't up-to-date and frequent
- **Security tools** that aren't tuned, which increases false positives and impacts efficacy.

Ultimately, the key to avoiding the high cost of a ransomware attack is a mitigation strategy that implements best practices, addresses the most common failures, and is executed with complete protection that is driven by a multi-layered approach.

This is what Check Point Ransomware Protection is all about.

Check Point complete ransomware protection

Check Point offers a multi-layered range of protections against ransomware attacks across endpoint, mobile, email and collaboration applications, internet access, and network environments, including:

- Harmony Endpoint
- Harmony Mobile
- Harmony Email & Collaboration
- Browser security
- Horizon XDR/XPR
- Quantum
- Infinity Global Services

Harmony Endpoint

Endpoint protection (EPP) and endpoint detection and response (EDR) serve as the first and last line of defense against the growing wave of ransomware attacks.

Harmony Endpoint provides runtime protection against ransomware with instant automated remediation, even in offline mode. In case of an anomaly caused by a ransomware, Harmony Endpoint Behavioral Guard identifies, blocks, and remediates the full attack chain.

Harmony Mobile

Once a mobile device is infected with malware, it can be used as an entry point to your organization's most sensitive assets. This vector is even more vulnerable when a company has a "bring your own device" (BYOD) policy in place, which enables employees to access the network and assets with private devices that are often inadequately protected.

Harmony Mobile is the only solution that tackles the challenge with complete file protection for mobile devices. It blocks malicious file downloads, scans for malicious files in storage, and blocks the download of malicious applications in real time.

Harmony Mobile also protects against Active Directory (AD) passwords from being used and against both phishing and vishing attacks, which use the voice medium to trick employees into putting corporate assets at risk.

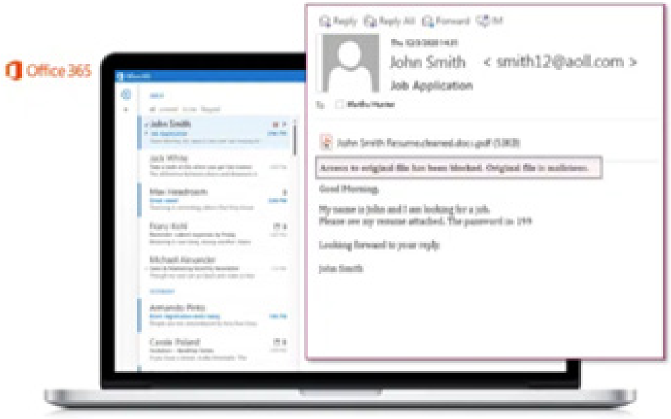
Harmony Mobile management console

Harmony
Email & Collaboration

Harmony Email & Collaboration offers complete protection for Office 365 and G Suite email and collaboration apps. It also blocks the spread of ransomware through productivity apps such as SharePoint, One Drive, and Slack.

With advanced sandboxing it blocks malicious email attachments that contain ransomware files or executables, before they reach user mailboxes.

Blocking ransomware with Harmony Email & Collaboration



John Smith < smith12@aoll.com >
Job Application

John Smith Resume.cleaned.doc.pdf (53KB)

Access to original file has been blocked. Original file is malicious.

Good Morning,

My name is John and I am looking for a job.
Please see my resume attached. The password is 199

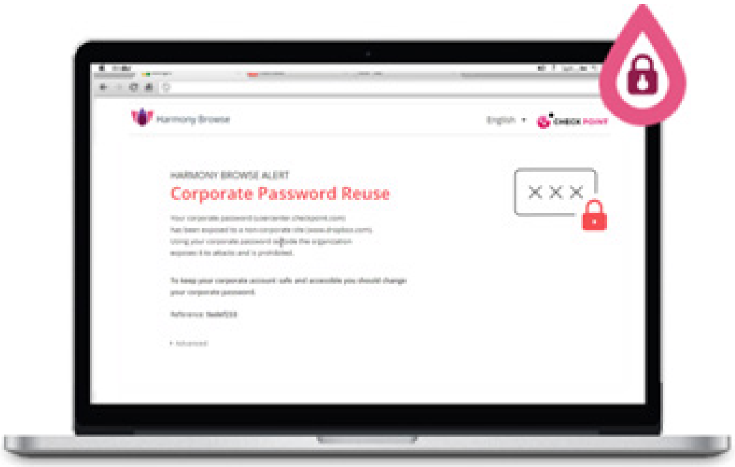
Looking forward to your reply

John Smith

Harmony
Browse

Browser Security, part of the Check Point endpoint protection offering, provides unique in-browser protection against phishing and malware download and uploads.

Comprehensive threat prevention is ensured across every browser through seamless integration with both Harmony Endpoint as well as with products from third-party vendors. And deployment requires no more than a few seconds.



HARMONY BROWSE ALERT
Corporate Password Reuse

Your corporate password (usercenter.checkpoint.com) has been exposed to a non-corporate site (www.dropbox.com). Using your corporate password outside the organization exposes it to attacks and is prohibited.

To keep your corporate account safe and accessible you should change your corporate password.

Reference: [illegible]

Advanced

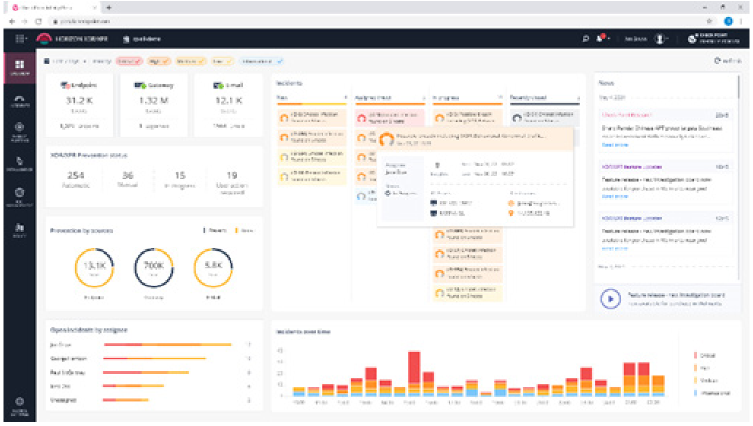
Check Point Browser Security with password reuse prevention

Horizon
XDR/XPR

Horizon XDR/XPR is a comprehensive security operations platform that empowers SOC teams with prevention-first XDR/XPR across the entire security estate.

Endpoint devices that report ransomware activity are quarantined on the gateway automatically. Outgoing traffic is blocked by the gateway from the quarantined devices, thus preventing the ransomware from spreading.

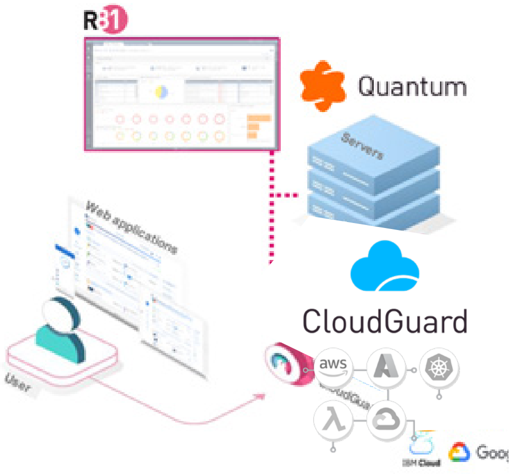
Ransomware incident insights with Horizon XDR/XPR



Quantum
Network Security

Quantum firewalls prevent the penetration and spread of ransomware inside the network, cloud, and data centers.

With advanced AI, Quantum gateways stop zero-day threats, phishing attempts, and malicious downloads. They perform complete file protection with sandboxing, content disarm, and reconstruction.



Quantum: deep learning & AI driven network security

Check Point Infinity
GLOBAL SERVICES

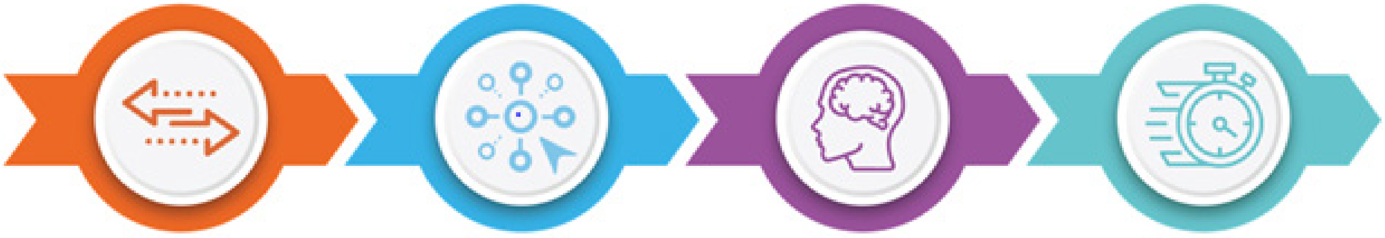
Infinity Global Services include a comprehensive set of services that are led by Check Point elite experts and real time threat intelligence.

Among these services is Ransomware Readiness Assessment for providing a threat intelligence briefing and evaluating your organization's current ransomware incident response plan. With this information, the team tests your defenses, identifies gaps, and determines the actions to take for preventing attacks.

Moreover, Incident Response Services provide proactive incident response to quickly mitigate effects and prevent ransomware and other attacks altogether.

Maximize resilience with Check Point Infinity Global Services

Design threat prevention into your defenses with our portfolio of readiness assessment, security blueprint, risk



ASSESS

Evaluation, policy review, and best practices-based services.

OPTIMIZE

Optimize your security and extend team capabilities with proactive cyber monitoring, blueprint designs, and enhanced defenses that stop threats in real time.

MASTER

Strengthen your team's expertise from security practitioners to CISOs, with heightened security awareness, hacking skills, cloud training, and security certifications.

RESPOND

Increase response readiness with services designed to enhance incident response planning, proactively identify vulnerabilities, hunt threats, analyze digital forensics, and accelerate recovery.

Conclusion

With the sophistication of cybercriminal strategies and techniques on the rise, ransomware will continue to be among the most significant concerns of security leaders worldwide.

The key to meeting the daunting and complex task head on is complete ransomware protection that has the organization covered across all vectors – endpoints, mobile devices, email, web, and networks.

Check Point provides this coverage, protecting you against ransomware attacks, safely recovering encrypted data, reducing the attack surface, and minimizing impact, so you can avoid the damage and ensure business continuity.

Check Point complete ransomware protection

Real-time ransomware protection and recovery on the endpoint

Block mobile ransomware hiding in malicious files and mobile apps

Block email attachments containing malicious files and executables

Block ransomware disguising in malicious web downloads and websites

Prevent penetration and lateral movement of ransomware inside your network, cloud and data centers

To learn more about how Check Point can help you safeguard your business from today's most urgent ransomware threats, we invite you to visit our website or speak with an expert.

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