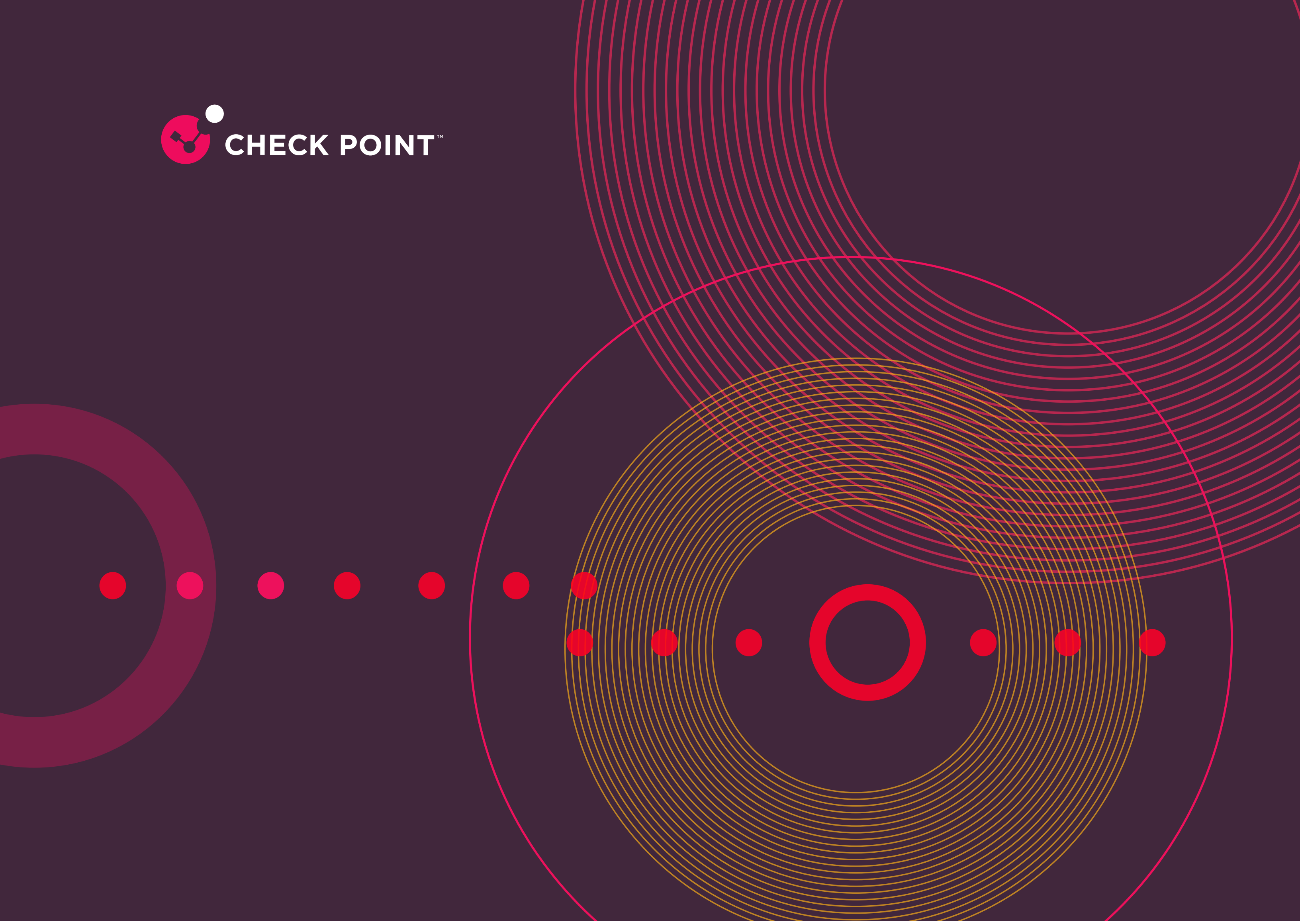
CHECK POINT™



ESSENTIAL GUIDE
TO RANSOMWARE PREVENTION

About This Guide

This guide provides vital tips and guidelines to understand, improve and protect business networks against ransomware using cloud-based, converged network security. It focuses on practical data to ensure business continuity with the right security technology. In this guide you will:

- Understand ransomware attacks and their implications
- Discover the cybersecurity challenges businesses face
- Become familiar with modern network security technology such as ZTNA
- Learn the best approach to prevent ransomware from infecting your network

Billions of Potential Victims in the Hybrid Workforce

Cyberattacks and their residual damages are rising exponentially. With three billion phishing emails sent out each day, the chances of becoming a victim of a cyberattack is simply a numbers game. It only takes one employee to innocently open a malicious email to let the hackers begin their work. In a recent survey by the CyberRisk Alliance, respondents named ransomware as one of their top cybersecurity concerns.

Even worse, some boardrooms still aren't getting the message. "If we were hit with any of the majority of types of ransomware out there right now, we would be utterly helpless, and getting budgeting for this has been surprisingly difficult," an IT Director in Manufacturing told CRA's survey team.

Compared to the alternative, confronting ransomware with an effective security solution is a no-brainer. The average cost of a ransomware attack in 2022 was $4.54 million, according to IBM.

Ransomware is one of the fastest-growing cyber threats. The high financial or economic costs make ransomware prevention a top concern. Hackers are becoming more strategic and thinking big. They are attacking federal governments, municipalities, hospitals, infrastructure, the software supply chain, and MSP management platforms. Targeting organizations upstream, a successful phishing and ransomware attack can shut down many companies at once. Businesses everywhere must put in place proper ransomware defenses.

The Surge in Ransomware

Cyberattacks in recent years demonstrate the potential scale of ransomware's devastation on businesses. After cybercriminals hacked the accounting systems of the Colonial Pipeline in May 2021, for example, the company shut down operations. This caused panic-induced hoarding and fuel shortages, forcing President Biden to declare a state of emergency. After paying 75 bitcoin in ransom (about US $5 million), Colonial Pipeline could restart operations after a 4-day hiatus.

In July 2021, thousands of businesses were affected by the malware hack of the Kaseya platform used by MSPs to manage the networks of other businesses. The cybercriminals demanded $50,000 to $5 million in ransom directly from affected companies rather than the MSPs or Kaseya.

After several days, Kaseya mysteriously announced it had obtained a REvil ransomware decryptor "from a third party," and much of the damage appeared to have been mitigated. Additional high-profile attacks included Nvidia, Optus, Bernalillo County, New Mexico, Toyota, Kia Motors, Acer, the Washington DC Police Department, Accenture, and many more.

To Pay or Not to Pay?

Ransomware attacks often threaten a company so directly that they quickly pay the required ransom to regain control of their records and systems. However, law enforcement agencies and cybersecurity companies do not recommend payment. Not only does it set a bad stand, but it's no guarantee for success. According to a recent survey, 17% of victims who paid ransoms never recovered their stolen data.

So why do so many ransomware victims pay? Payment is often the quickest and cheapest solution for the victims, especially since so many businesses now have cybersecurity insurance. The costly May 2019 ransomware attack on the City of Baltimore, Maryland, is a case in point. At the advice of the FBI, the city did not pay the 13 Bitcoin ransom (about $100,000). But non-payment cost the city nearly $18 million in lost revenues and clean-up costs—almost 180 times the ransom. But as the scope and scale of ransomware attacks grow, the cost savings of paying the ransom are disappearing.

Insurance Companies Are Pushing Back

Insurers are rethinking coverage — and even the viability of offering coverage — in the face of the pandemic and home-working-driven surge in ransomware attacks. Burdened with heavy payouts and the growing sophistication of attackers, insurers are increasingly wary. AXA, one of Europe's biggest insurers, announced in 2021 that it would no longer cover ransom payments in its cyber insurance policies. Lloyds of London, holding nearly a fifth of the cyber insurance market, advised against providing coverage against state-sponsored cyberattacks beginning in March 2023. And while insurers are struggling to recover losses and deploy new approaches, companies are left underinsured. Even if they get the same limits, they pay 50 or 100% more for their coverage. And it may still not be enough.

Governments are Finally Waking Up

The May 2021 White House Executive Order on cybersecurity signals a coordinated effort to fight cybercrime and make the Internet a safer place. Federal government agencies are now creating cybersecurity standards and practices for federal networks and their suppliers. In addition, the Cybersecurity and Infrastructure Agency (CISA), the FBI, and the intelligence community are finally sharing information and working with tech giants other governments on deterring, investigating, and handling cyberattacks. A new Cybersecurity Safety Review Board will be called into action when a significant cyber incident occurs. The team will analyze what happened, and make concrete recommendations to avoid similar situations in the future.

In November 2021, the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System, and the Office of the Comptroller of the Currency (OCC) ruled that US banks regulated by the FDIC must report a computer security incident within 36 hours. The joint ruling defines a computer security incident as "something that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits." These actions show that the idea of a national network, a corporate network, or even a home network is becoming passé. Today there is just one network, and it's called the Internet.

The Risks of Hardware VPNs

Successful phishing campaigns and stolen usernames and passwords have made VPNs a weak link in network security.
A critical risk with VPNs is that they typically give users access to the entire internal network, and many networks don't bother to segment properly since configuration is so time consuming. VPNs are also not suited for dynamic networks because they require expensive computer hardware, constant management updates, and do not adjust easily to network or server changes. Lastly, VPNs can impact performance since they require remote workers to backhaul their internet traffic to a data center that could be an ocean away.

Protecting the WFH Workforce: Zero Trust Network Access and Secure Web Gateway

In today's hybrid world, where work from home (WFH) or hybrid work scenarios are common, hardware-based VPNs are no longer sufficient. Instead, companies need unified solutions that can protect the blurred lines between the corporate network and the Internet.

To truly secure a hybrid workforce, businesses must implement Zero Trust Network Access (ZTNA). Employees are granted access to networking resources based on what they need, while everything else is off-limits. This prevents attackers from moving laterally through the network should they acquire legitimate user credentials.

In addition, a secure web gateway (SWG) bars access to harmful sites, protects against malware, and keeps browsing habits consistent with company policies and local business regulations.

Converged network security: A Modern and Holistic Approach

ZTNA is a key component of cloud-based, converged network security. With today's modern workforce comprising unprecedented numbers of remote and hybrid employees, converged network security gives organizations a more efficient and effective way to identify users and devices and apply policy-based security wherever they're located.

This approach enables organizations to better adapt to the cloud, embrace mobility, protect against security threats, and deliver a superior user experience. The key components of converged network security include:

- Zero Trust Network Access (ZTNA)
- Firewall as a Service (FWaaS)
- Hybrid Secure Web Gateway (SWG)

Stopping Ransomware with Harmony SASE

Harmony SASE offers a powerful solution against ransomware built into its platform that streamlines network security with its groundbreaking ease-of-use and radically simple design. Its ZTNA micro-segmentation lets any business close a variety of attack vectors within a simple, unified interface that's easy to manage.

Security managers can block suspicious links, enforce network security policies and deny access to insecure or unknown devices at login to prevent malicious attacks from happening.

Plus, Agentless ZTNA lets you safely grant access to unmanaged devices from contractors, partners, and employees.

In addition, Hybrid SWG malware protection is constantly on the lookout for malicious content headed to user devices, including ransomware.

Make Your Business Safer Today

Defending a company's attack surface is challenging. The never-ending wave of data breaches and ransomware illustrates the critical need for converged network security to prevent and mitigate ransomware attacks.

Old VPN-based models no longer work as new modes of operation in the cloud become the norm.

The lines between the corporate network and the public Internet are blurring. Defend your company resources by providing access based on ZTNA where employees access only what they need to do their jobs, and nothing more.

Harmony
SASE

Meet Harmony SASE

2x Faster Internet Access | Full Mesh Private Access | Secure SD-WAN

Offering a game-changing alternative, Harmony SASE delivers 2x faster internet security combined with full mesh Zero Trust Access and optimized SD-WAN performance—all with an emphasis on ease-of-use and streamlined management.

Combining innovative on-device and cloud-delivered network protections, Harmony SASE offers a local browsing experience with tighter security and privacy, and an identity-centric zero trust access policy that accommodates everyone: employees, BYOD and third parties. Its SD-WAN solution unifies industry-leading threat prevention with optimized connectivity, automated steering for over 10,000 applications and seamless link failover for uninterrupted web conferencing.

Harmony SASE enables any business to build a secure corporate network over a private global backbone in less than an hour. The service is managed from a unified console and is backed by an award-winning global support team that has you covered 24/7.

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