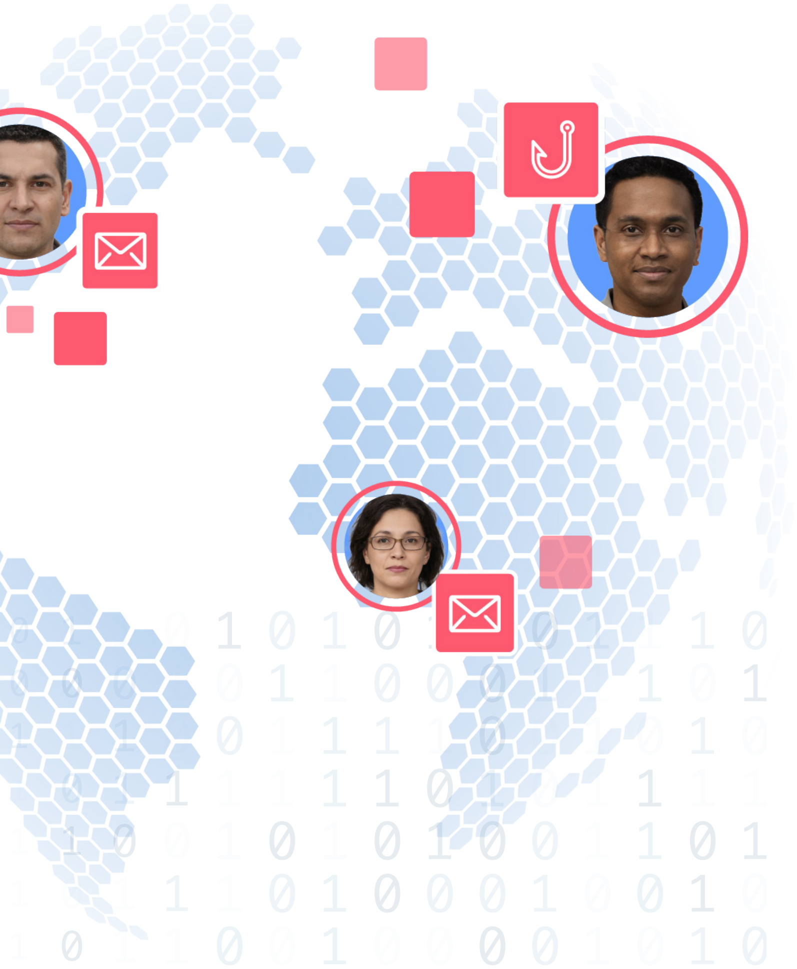
perimeter 81

The Essential Guide to Preventing Ransomware Attacks

About this Guide

This guide provides vital tips and guidelines for security managers to understand, improve and protect their business against ransomware using ZTNA and SSE. It focuses on practical data to ensure business continuity with the right security technology and assists IT pros to:

- Understand the most recent ransomware attacks and their implications
- Address the cybersecurity challenges businesses face
- Become familiar with ZTNA and SSE technology
- Select the best approach that prevents ransomware today and in the future

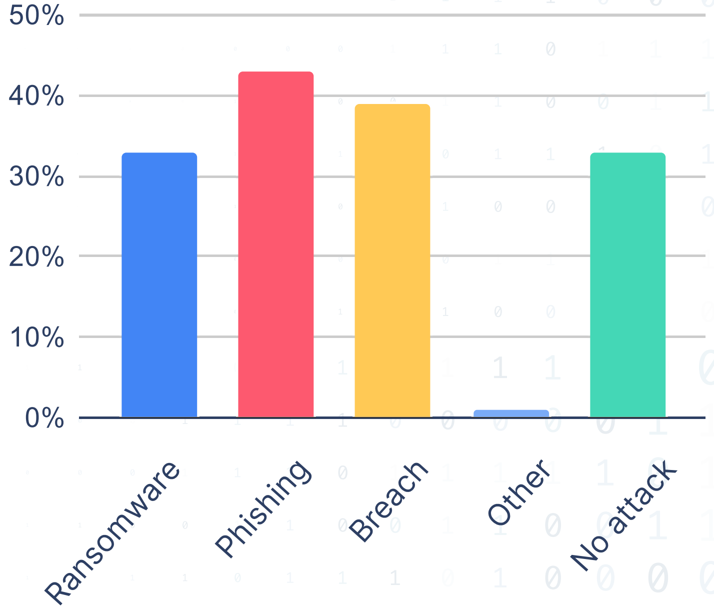


Billions of Potential Victims

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. According to a recent Perimeter 81 survey of 500 IT professionals, 66% of respondents reported that their company was a phishing or ransomware attack victim. Inadequate cybersecurity is expected to cost businesses $20 billion in 2021, a 57X increase from $354 million in 2015.

Ransomware is one of the fastest-growing cyber threats. The high financial and economic costs make the prevention of ransomware a pressing concern. Hackers are becoming more strategic and thinking big, assisted by discovering Log4j and other zero-day vulnerabilities. They are attacking 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. The time has long passed for businesses everywhere to ensure proper ransomware is in place.

Has your company experienced any of the following serious cyber incidents in 2020-2021?



Source: Perimeter 81 2021 State of Cybersecurity Report

perimeter 81

The 2020-2021 Ransomware Surge

Cyberattacks over the last year demonstrate the potential scale of ransomware's devastation on businesses. After cybercriminals hacked the accounting systems of the Colonial Pipeline in May 2021, 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.

Then in July, 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.

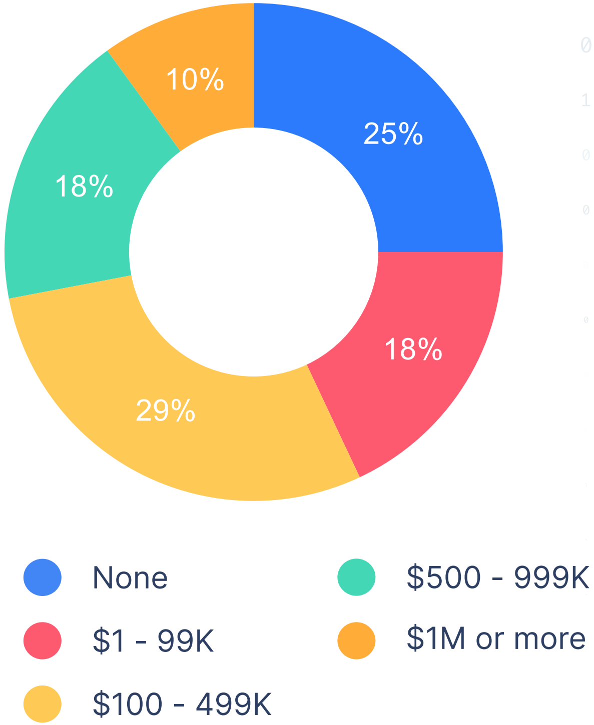
Additional high-profile attacks included JBS, the world's largest meat producer, Kia Motors, Acer, the Washington DC Police Department, Accenture, and many more.

To Pay or Not to Pay?

According to Perimeter 81's survey, 57% of ransomware victims paid the requested ransom in 2020. However, payment is not the recommendation of cybersecurity companies or law enforcement agencies. But even more importantly, it is no guarantee for success: 17% of the 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 among the 64% of businesses with 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.

What were the total costs/damages from cyberattacks on your business in 2020-2021?



Source: Perimeter 81 2021 State of Cybersecurity Report

Insurance Companies are Pushing Back

Insurers are rethinking coverage—and even the viability of offering coverage—in the face of the pandemic and work from home-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 that it would no longer cover ransom payments in its cyber insurance policies, reportedly at the request of French justice and cybersecurity officials. In addition, Lloyds of London, holding nearly a fifth of the cyber insurance market, discouraged syndicate members from taking cyber business in 2022.

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 to 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 can be seen as the first step in creating 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 and mitigating Log4j and other cyber risks.

A new Cybersecurity Safety Review Board, comprised of professionals from the government and private industry, will be called into action when a significant cyber incident occurs, analyze what happened, and make concrete recommendations to avoid future recurrence.

And 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

In the past, hardware VPN solutions let you “hide” your computing credentials so they would be invisible to hackers. But successful phishing campaigns and stolen usernames and passwords have made VPNs a weak link that has been responsible for numerous breaches like the high-profile Pulse Secure breach that affected dozens of government agencies.

A critical risk with VPNs is that they give users access to the entire internal network and don’t allow for proper network segmentation, traffic visibility, or network security. 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, there is really no need to protect empty offices with slow VPNs that have approached end-of-life, suffer from significant performance issues, and require active maintenance.

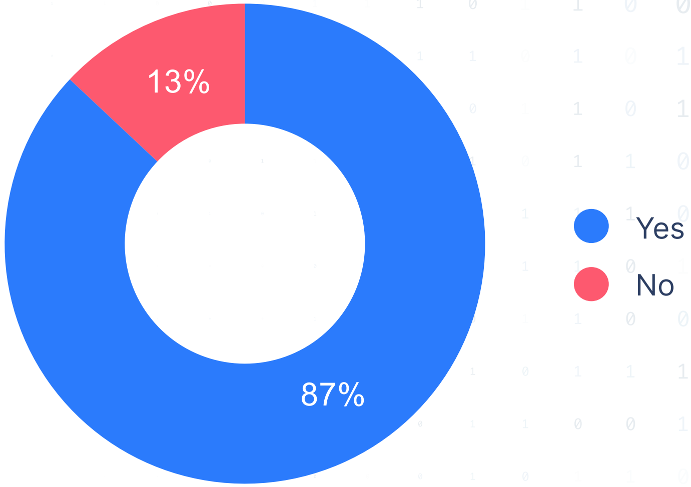
And while moving computing resources to the cloud does solve issues with storage capacity, hardware costs, and software updates, it can bring new issues like latency and new security challenges. Organizations must ensure adequate cloud protection and minimize exposure to attacks in the cloud.

Protecting Your WFH Workforce

In today's hybrid world, with 87% of the workforce shifting to permanent work from home (WFH) or hybrid work scenarios, hardware-based VPNs are no longer relevant.

To truly secure a hybrid workforce, businesses must implement Zero Trust Network Access (ZTNA). Employees are granted access to networking resources based on who they are and what they need to do—not where they are located. ZTNA is cloud-based, making it ideal for hybrid WFH environments.

Does your company plan to have employees working remotely or hybrid post-Covid (2021-2022)?



Source: Perimeter 81 2021 State of Cybersecurity Report

6 Principles of ZTNA for Every Business:

- Zero trust for any network user
- User-centric security, not network and location-based security
- Verify User IDs for everyone, every time and every place
- Needs-based access for “who users are” and “what users need to do”
- Combine cyber and network security for all corporate network resources and mobile workforce devices at the edge
- Unify all network resources from data centers, branch offices, and cloud for access anywhere

SSE: Unified Cloud Security

ZTNA is a key component of Security Services Edge (SSE), a cloud-based technical architecture that unifies network and cyber security. With today's modern workforce comprising unprecedented numbers of remote and hybrid employees, SSE gives organizations a more efficient and effective way to identify users and devices and apply policy-based security wherever they're located. This architecture enables organizations to better adapt to the cloud, embrace mobility, protect against security threats, and deliver a superior user experience.

The key components of the Security Services Edge include:

- Zero Trust Network Access (ZTNA)
- Firewall as a Service (FWaaS)
- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB)
- Encryption / Decryption
- Network Monitoring

Stopping Ransomware with Perimeter 81

Perimeter 81 offers a powerful SSE-based ZTNA solution against ransomware built into its **Cybersecurity Experience (CSX) Platform.** The CSX Platform is the first platform to streamline SSE with its groundbreaking ease-of-use and radically simple design that is based on four principles:

- Instant Deployment
- Unified Management
- Full Visibility
- Integrated Security

The Perimeter 81 CSX Platform allows companies to mitigate ransomware and phishing attacks with a holistic, unified solution. 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.

In addition, Perimeter 81 lets you safely grant access to unmanaged devices from contractors and partners with agentless Zero Trust Application Access. This, and more, is why Perimeter 81 was named a Forrester New Wave ZTNA leader. The leading consultancy gave Perimeter 81 the highest marks possible in the non-web and legacy apps, client support, product vision, and planned enhancements criteria. They specifically cited Perimeter 81's intuitive ZTNA management and VoIP handling as setting it apart from other ZTNA solutions.

Make Your Business Safer Today

Companies seek to be agile in today's Covid and Covid-variant world by enabling their employees to work from anywhere. Defending the company's larger attack surface is challenging. The 2020-2021 wave of data breaches and ransomware illustrates the critical need for ZTNA as a framework to prevent—or at least mitigate—ransomware attacks.

Although national and public policy regulations seem to be forthcoming finally, no one can afford to wait. Old VPN-based models no longer work as new modes of operation in the cloud become the norm. And as the lines between the corporate network and the public Internet are blurring, employees need to access networking resources based on the principles of ZTNA: to be allowed to do what they need to do based on who they are and not where they are located.

perimeter 81

About Perimeter 81

Perimeter 81 radically simplifies cybersecurity with the world's first Cybersecurity Experience (CSX) Platform. As a holistic, cloud-based solution, Perimeter 81 allows organizations of all industries and sizes to support the immediate desires of the nomads with a purpose—while still granting IT teams the ability to manage it all safely. The company was founded in 2018 by two IDF elite intelligence unit alumni, CEO Amit Bareket and CPO Sagi Gidali, and is based in Tel Aviv, the heart of the startup nation. Our clients include SMBs to Fortune 500 businesses and industry leaders across a wide range of sectors. Our partners are among the world's leading integrators, managed service providers, and channel resellers.

perimeter 81

CONTACT US

www.perimeter81.com

+1 (929) 575-9307

Book a Demo