Zaperon

WHITEPAPER

Your Essential Cybersecurity Checklist for Remote Work



Staying secure while working remotely has become a critical component of cybersecurity for organizations worldwide. This shift demands a comprehensive approach to hybrid work security that addresses risks from all angles. A Cisco survey found that **84% of businesses prioritize cybersecurity** in their remote work technology investments.

Remote work introduces multiple vulnerabilities with far-reaching consequences. Millions of new endpoints and connections require constant monitoring and protection. Employees need secure, seamless access to corporate resources, often necessitating an upgrade of legacy systems and infrastructure.

FAILING TO ADDRESS THESE CHALLENGES CAN LEAVE ORGANIZATIONS EXPOSED TO SIGNIFICANT CYBER THREATS:

PHISHING

Remote workers are more vulnerable to phishing scams than office-based employees. A StationX survey revealed that 80% of infosec professionals saw increased phishing attacks due to remote work.

RANSOMWARE

Malicious software locks systems until a ransom is paid. In 2023, ransomware attacks occurred every 14 seconds, and this is expected to rise to every 2 seconds by 2031.

SPYWARE

Covert software secretly collects sensitive data, exposing it to fraudsters or competitors. This poses significant risks to privacy and security and can lead to serious financial and reputational damage.

ZERO-DAY ATTACKS

Exploits target unpatched systems, making remote monitoring harder. In 2023, 97 zero-day vulnerabilities were exploited, a sharp increase from 62 in 2022, indicating growing cyber threats.

DATA THEFT

Stolen credentials give unauthorized access to sensitive databases, affecting both customers and employees. The average cost of a data breach reached $4.88 million in 2024, with severe consequences.

SABOTAGE

Unmonitored employees can unintentionally or intentionally harm corporate assets. In 2023, 76% of organizations reported insider attacks, with sabotage causing significant operational disruptions and long-term damage.

Mitigating these risks requires a holistic strategy. A dual approach that combines top-down policies with bottom-up security practices delivers more effective results than relying solely on individual vigilance.

Cybersecurity Best Practices For Secure Remote Working

1

GO PASSWORDLESS

Over **86% of data breaches** are caused by stolen employee credentials, as per Verizon's 2023 DBIR. Implement passwordless authentication methods, such as biometrics or authentication apps, to eliminate the vulnerabilities of traditional passwords.

2

ENABLE MULTI-FACTOR AUTHENTICATION (MFA)

MFA adds an extra layer of security by requiring additional verification (e.g., OTP, biometrics) before granting access.

3

UPDATE SOFTWARE REGULARLY

Keep your operating system, antivirus software, and applications up to date to patch vulnerabilities. According to Ponemon Institute, 60% of breaches in 2023 were linked to unpatched software.

4

AVOID LEGACY VPNs

Replace outdated VPNs with modern, secure alternatives that offer better encryption and protection against evolving threats. A Gartner report highlights that 60% of organizations will phase out legacy VPNs by 2025 in favor of Zero Trust Network Access (ZTNA).

5

BEWARE OF PHISHING EMAILS

Do not click on suspicious links or attachments in unsolicited emails. Always verify the sender's identity and domain before taking any action or responding to requests.

6

SECURE YOUR DEVICES

Ensure your laptop, mobile devices, and other electronics are secured with biometric authentication or strong passwords. Lock devices when not in use to prevent unauthorized access and potential threats.

7

AVOID UNAUTHORIZED DEVICES FOR WORK

Use only authorized devices that are pre-equipped with enterprise-grade security tools and configurations to conduct any work-related activities, minimizing risks associated with unapproved devices.

8

REGULARLY BACK UP DATA

Schedule secure, automated backups for your work files and sensitive data to prevent loss from cyberattacks, device malfunctions, or unexpected incidents, ensuring data integrity and accessibility.

9

LIMIT ACCESS TO SENSITIVE DATA

Implement the principle of least privilege by restricting access to sensitive or critical data. Only authorized users should have permissions to access, modify, or share confidential information.

10

MONITOR USER ACTIVITY

Deploy advanced monitoring solutions to track and analyze user activity on all systems. This helps identify unusual behavior and potential security breaches, allowing for timely intervention and mitigation.

How Zaperon Secures Remote Workspaces?

Zaperon provides a unified zero trust security platform to address the diverse challenges organizations face in securing their remote workforce. Through the combination of **Identity & Access Management (IAM)**, **Multi-factor Authentication (MFA)** & **Zero Trust Network Access (ZTNA)**, it ensures that only verified users and devices can access specific applications and data, effectively reducing the risk of exposure to potential threats. The **Secure Web Gateway (SWG)** offers an added layer of protection by filtering harmful websites and preventing web-based attacks, which is crucial for protecting remote employees who often interact with unfamiliar or unsafe online resources. Additionally, Zaperon's **Passwordless Authentication** eliminates the risks associated with traditional passwords, opting for a more secure PKI-based authentication, further bolstering security measures.

The Zaperon platform leverages an intelligent, built-in **Cloud Access Security Broker (CASB)** engine to provide visibility and control over cloud-based application data, ensuring compliance and preventing unauthorized access to critical business resources. The **Identity Threat Detection & Response (ITDR)** component of the platform further detects suspicious activities and blocks access in real time, proactively responding to identity-based threats before they can escalate. Together, these integrated capabilities of the Zaperon platform create a robust, seamless security framework that enables organizations to secure their remote work environments, protect critical data, and ensure smooth operations without compromising on security.

Zaperon is a unified zero-trust platform that provides comprehensive, scalable security for organizations by protecting applications, data, and cloud infrastructure from users and devices connecting from any location. The platform leverages PKI-based passwordless authentication, phishing-resistant MFA, and least privilege access control to prevent unauthorized access to enterprise applications (saas, on-premise, desktop-based), servers and network devices. The platform continuously enforces zero-trust policies, monitors user behavior and device posture, and prevents data leakage. With real-time URL filtering, traffic monitoring, and proactive identity threat detection, Zaperon protects from web-based threats. Furthermore, Zaperon also helps organizations in compliance with regulations such as GDPR, PCI-DSS, HIPAA, SOX, RBI, SEBI, etc. while helping reduce their cyber insurance costs.

+1 202 600 5234
+91 8800 170387
sales@zaperon.com
www.zaperon.com
© 2024 Zaperon, Inc.
All Rights Reserved.