Work from Anywhere Security Guide

How to layer and sell security solutions to protect your clients' remote workers, data, and devices.

About this guide

This guide offers recommendations for building a layered remote security stack and positioning it to your clients so they can stay productive and secure while working from anywhere.

Introduction

Building the foundation for remote security

Fortifying remote defences

Advancing the conversation

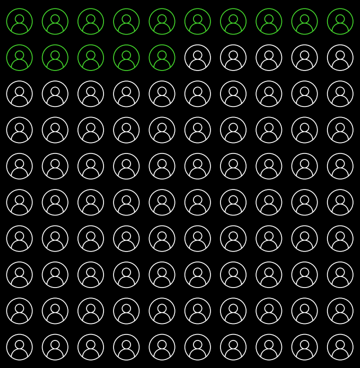
Education, enablement & Professional Services

Introduction

Shifting the security focus: from the perimeter to endpoints

A shift in security focus

While the global spike in remote work in 2020 and its continued rise helped many companies stay productive, it also increased security challenges as employees remotely accessed company networks, files, and data. With more employees working outside of the safety of perimeter security from the corporate network and firewalls, the IT security focus has shifted to endpoints, email, and end users as the first line of defence.



15% of remote workers say their biggest challenge is collaboration and communication.[1]

The challenges of defending a distributed workforce

The convergence of the rise of unsecured remote workers with the surge in cybercrime, and increasingly more advanced methods of attack, has created a highly vulnerable state for SMBs. However, many SMBs don't have endpoint-related security layers beyond antivirus. They need solutions that can provide visibility into distributed endpoints, layers of email protection, and end user training on remote security best practices and phishing awareness.

Endpoints

68% of organisations experienced one or more endpoint attacks that successfully compromised data and IT infrastructure in 2022.[2]

Email

93% of organisations experienced email security incidents with Microsoft 365 in 2022.[3]

End users

Only **55%** of organisations with a security awareness programme train all their employees.[4]

Building the foundation for remote security

1. Put endpoint security in place

The rise of wireless devices has drastically increased the number of endpoints in an organisation. In addition to servers and desktops, each employee's laptop, tablet, and smartphone adds another possible vulnerability that can be exploited to give incoming malware access to the corporate network.

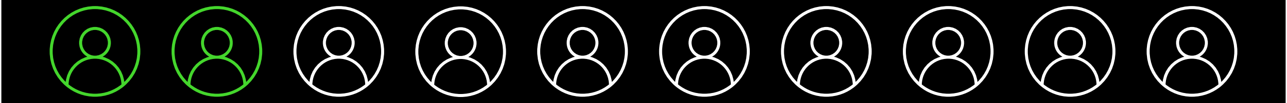
70% of successful breaches begin on endpoint devices.[2]

Going beyond antivirus

Simply installing antivirus software is no longer enough due to the proliferation of cyberthreat surfaces. While traditional antivirus solutions simply try to prevent attacks, modern endpoint detection and response (EDR) solutions actively discover and remediate threats across devices, desktops, and servers.

Advanced endpoint protection solutions use automation, machine learning, and behavioural monitoring to detect, respond to, and eliminate a diverse range of threat vectors, including executable or fileless malware, document and browser exploits, malicious scripts, and credential scraping. Features to look for include:

- Visibility into endpoints, apps, running processes, and encrypted traffic
- Threat forensics
- Ability to isolate and disconnect infected endpoints from the network
- File recovery and device rollback



26% don't have an endpoint solution that can automatically detect and stop ransomware attacks.[2]

2. Layer on additional email security

With email as the #1 vulnerability for phishing, ransomware, and malware, it is critical to protect sensitive data from leaving the organisation and stop threats before they can enter your network through email. The native security features of most email solutions don't offer enough built-in protection to combat today's advanced threats – you should layer on third-party solutions that can provide advanced security features at both the server and mailbox levels.

37% of SMBs feel that phishing emails are the main reason for their security issues, with 53% saying they plan to implement email and spam protection in the next year.[5]

Two layers of email security

Advanced phishing identification and protection

1. Phishing security

Phishing security solutions directly integrate with email applications to protect and remediate emails at the mailbox level by flagging suspicious emails and providing a way for users to report phishing attacks.

Antivirus and zero-hour threat protection

Data loss protection

Compliant email retention and archiving

Policy-enforced encryption

Spam and content filtering

URL scanning and attachment defence

2. Email security

Email security solutions scan and filter incoming messages to prevent spam, phishing, and other malicious emails from reaching the inbox, while protecting outbound emails with encryption and data loss protection policies.

3. Begin ongoing end user security training

A company's security posture is only as strong as their least secure employee. And with phishing attempts growing more and more sophisticated, even savvy users can find themselves accidentally clicking malicious links, opening risky attachments, or mistaking a spoofed URL for a familiar website and offering up sensitive information or credentials. Empower end users by engaging them with ongoing security training to teach them how to spot and respond to various types of threats.

57% of SMBs don't conduct security awareness training, even though 42% blame their security issues on lack of training.[5]

Phishing simulation training

Phishing simulation tools are a great way to teach employees to be alert for and identify phishing emails in their inbox. Most importantly, phishing simulation tools also train users to report suspected phishing attempts – a critical component to effectively combat phishing company-wide.

Only 35% of organisations conduct phishing simulations training.[4]

Ongoing security micro-training

As cybercriminals continue to innovate, continual education is important so that users stay up-to-date on the latest threats. Security awareness training solutions use microcontent and quizzes to build security scores and track progress throughout the organisation.

74% of businesses have formal security training programmes.[4]

Building the foundation for remote security

Standardising your remote security stack: trending solutions

Offering a comprehensive bundle that covers the main threat vectors for remote work can be easier for clients to adopt, rather than adding products individually over time. Below are leading solutions that Pax8 partners have begun offering as a bundle that complement each other to cover the gaps around endpoint and email security.

SentinelOne™

Endpoint security

The SentinelOne endpoint protection platform prevents and detects attacks across all major vectors, rapidly eliminates threats with fully automated, policy-driven response capabilities and artificial intelligence, and provides full-context, real-time forensics.

IRONSCALES SAFER TOGETHER

Email security (phishing)

IRONSCALES anti-phishing solutions use a multi-layered and automated approach starting at the mailbox level to prevent, detect, and respond to email phishing attacks. IRONSCALES expedites the time from phishing attack discovery to company-wide remediation from months to seconds.

proofpoint.

Email security (MX-level)

Proofpoint provides affordable email security for SMBs using the same core technology that protects over 65% of the Fortune 100. The cloud-based, multi-tenant platform offers spam, virus, and threat protection, as well as outbound filtering, email encryption, and data loss protection.

IRONSCALES SAFER TOGETHER

Phishing simulation training

IRONSCALES also provides phishing attack simulation capabilities to train users to identify and report suspected phishing attempts.

> At Pax8, we understand the vital role security plays in the technology industry, and we emphasize our strong commitment to offer our partners the finest cybersecurity solutions available from top vendors.
>
> *- Sophie Merrifield, CVP of Vendor Operations, Pax8*

Fortifying remote defences

Other tools to secure remote work environments

The following tools can provide additional layers of security for remote employees.

Microsoft reports that 99% of compromised accounts didn't have multi-factor authentication (MFA) enabled.[6]

1. **Virtual private network (VPN):** A VPN provides an encrypted, private connection so employees can securely access company resources and applications from home or public networks.

2. **Web security / DNS filtering:** Since users working remotely on company devices don't have the protection of the company firewall, DNS filtering can protect them from malicious websites and prevent them from visiting inappropriate websites on company devices.

3. **Multi-factor authentication (MFA):** By requiring a second form of authentication, MFA is the best defence to strengthen access security. Make sure that MFA is required for all employees when off-network.

4. **Conditional access (CA):** Use conditional access to control who can access which apps and data, and leverage location awareness to enforce additional security and authentication.

5. **Device management:** Restrict corporate network access to approved devices. Use solutions that provide the ability to remotely wipe or encrypt company data if a laptop or mobile device is lost or stolen.

6. **Security Operations Centre (SOC) as a Service:** When employees (and their devices) aren't in the office, admins lose a lot of visibility. SOC-as-a-Service solutions can monitor endpoints to detect vulnerabilities and suspicious activity to reduce the reaction time to security threats. These solutions also provide insight into misconfigurations and outdated apps and provide remediation guidance.

7. **MSP tool for remote diagnostics:** Get visibility into what's wrong with an end user's computer with the press of a button. Remote diagnostic tools take snapshots and send a report to show what processes and apps are running in order to diagnose the issue – in certain solutions, this can even be done if the computer is offline.

Advancing the conversation

Remote security checklist

In the rush to roll out remote work capabilities, many businesses have left security considerations behind. But with remote users “in the wild” and unprotected by the company firewall, security is more critical than ever. This checklist can help you guide the conversation to make your clients aware of their security needs.

☐ Is multi-factor authentication (MFA) enabled? Did employees receive guidance on how to use MFA (and authenticator apps, if applicable)?

☐ Is conditional access enabled and configured?

☐ Do you have the ability to wipe company data remotely from lost or stolen laptops and mobile devices? Are you using whole disk encryption to encrypt the physical hard drive of company laptops?

☐ Do you have an email security product in place? Were employees trained to recognise and report phishing attempts?

☐ Have you installed a web security app to prevent users from visiting malicious sites?

☐ Have you set up data loss prevention policies and/or set applicable restrictions on external file sharing?

☐ Have you created a remote work and data protection policy for employees to sign?

☐ Have you conducted end user training on remote security policies and best practices?

☐ Do you have endpoint protection and endpoint detection and response installed for all remote machines?

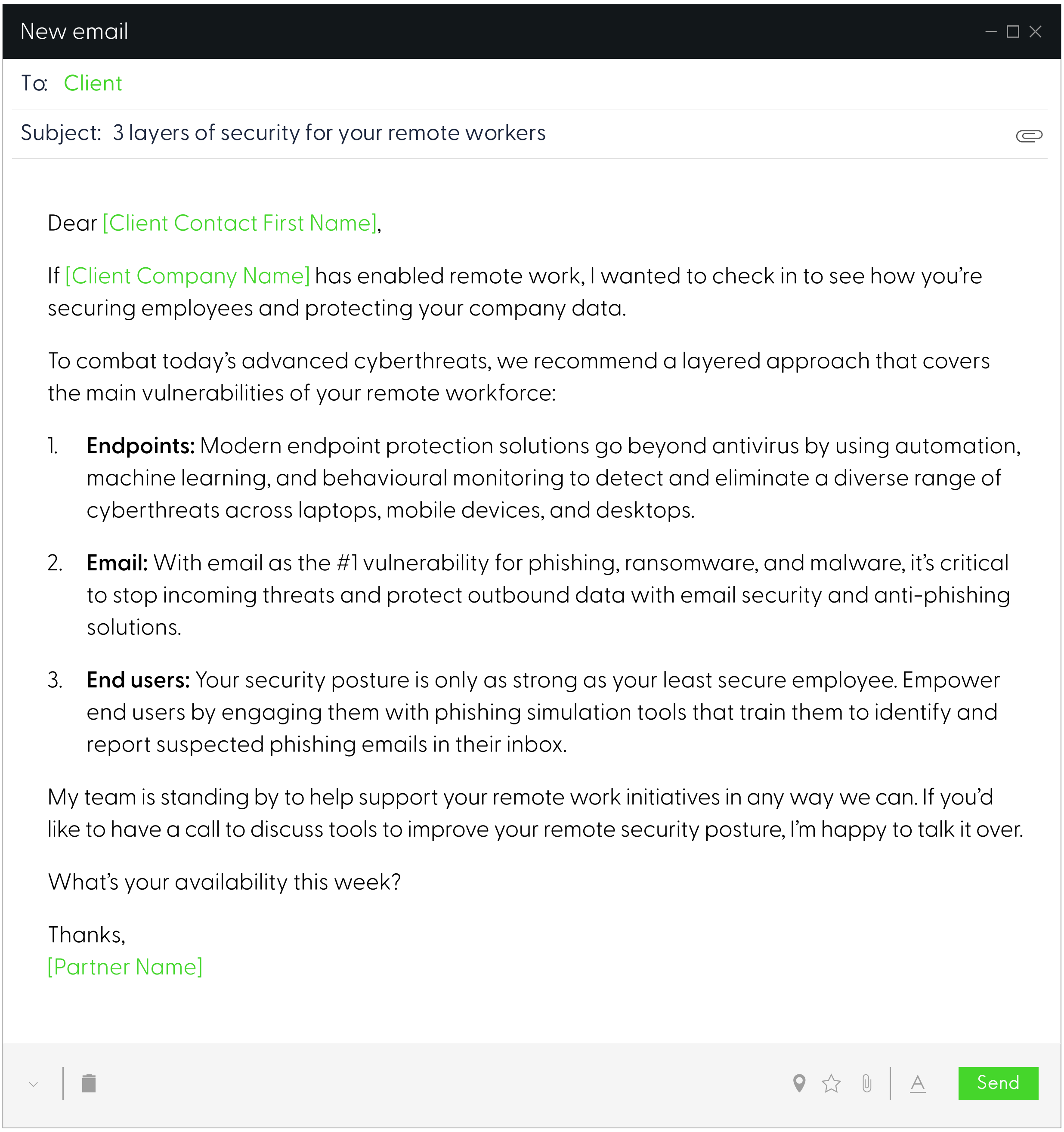
☐ If you are subject to compliance regulations, do you have policies and procedures in place to ensure compliance? Are employees trained to enforce those policies?

☐ What is your incident response plan during times of company-wide remote work?

Advancing the conversation

Email template for layered security

Clients with a remote workforce might not be aware of all the vulnerabilities to their endpoints and end users. This email template can help you advance a discussion around securing their remote work experience with a layered security bundle.



To: Client

Subject: 3 layers of security for your remote workers

Dear [Client Contact First Name],

If [Client Company Name] has enabled remote work, I wanted to check in to see how you're securing employees and protecting your company data.

To combat today's advanced cyberthreats, we recommend a layered approach that covers the main vulnerabilities of your remote workforce:

1. **Endpoints:** Modern endpoint protection solutions go beyond antivirus by using automation, machine learning, and behavioural monitoring to detect and eliminate a diverse range of cyberthreats across laptops, mobile devices, and desktops.
2. **Email:** With email as the #1 vulnerability for phishing, ransomware, and malware, it's critical to stop incoming threats and protect outbound data with email security and anti-phishing solutions.
3. **End users:** Your security posture is only as strong as your least secure employee. Empower end users by engaging them with phishing simulation tools that train them to identify and report suspected phishing emails in their inbox.

My team is standing by to help support your remote work initiatives in any way we can. If you'd like to have a call to discuss tools to improve your remote security posture, I'm happy to talk it over.

What's your availability this week?

Thanks,
[Partner Name]

Education, enablement & professional services

Your experts for secure remote work

Just as your clients need you to be their expert to help them stay secure, Pax8 is here to help you be that expert with product guidance, technical support, and in-depth solution training.

Need a boost when securing remote work solutions for your clients?

If you feel stretched thin with requests from clients, especially regarding securing remote workforces, our Professional Services team is available to serve as an extension of your own. In addition to remote security bundles for hardening M365 and Teams, we also offer Proofpoint deployment services to provision subscriptions, create your MSP profile, build downstream clients, import users, and configure policies.

Want to learn more about how to build a layered remote security stack?

Pax8 is here to help

Schedule a call

Sources

1. Buffer, State of Remote Work 2023, 2023, https://buffer.com/state-of-remote-work/2023
2. PurpleSec, Cyber Security Stats for 2023, 2023, https://purplesec.us/resources/cyber-security-statistics/#Start
3. Egress, 2023 Email Security Risk Report, 2023, https://pages.egress.com/Whitepaper-Risks-in-M365-03-23_2023-Landing-Page.html
4. Proofpoint, 2023 State of the Phish Report, 2023, https://www.proofpoint.com/us/resources/threat-reports/state-of-phish
5. Datto, 2022 SMB Cybersecurity Report for MSPs, 2023, https://www.datto.com/resources/datto-smb-cybersecurity-for-msps-report
6. Microsoft, 2023 identity security trends and solutions from Microsoft, 2023, https://www.microsoft.com/en-us/security/blog/2023/01/26/2023-identity-security-trends-and-solutions-from-microsoft/