



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 to build a layered remote security stack and position it to your clients to keep them productive and secure while working remotely.

Introduction

Shifting the Security Focus: From the Perimeter to Endpoints 2

Building the Foundation for Remote Security

1. Put Endpoint Security in Place 3

2. Layer on Additional Email Security..... 4

3. Begin Ongoing End User Security Training 5

Standardizing Your Remote Security Stack: Trending Solutions 6

Fortifying Remote Defenses

Other Tools to Secure Remote Work Environments 7

Advancing the Conversation

Remote Security Checklist 8

Email Template for Layered Security 9

Education, Enablement & Professional Services

Your Expert for Secure Remote Work..... 10

INTRODUCTION

Shifting the Security Focus: From the Perimeter to Endpoints

A Shift in Security Focus: While the global spike in remote work in 2020 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 related to the corporate network and firewalls, IT security focus shifted to endpoints, email, and end users as the first line of defense.

36%

of remote workers say their biggest challenge is collaboration and communication¹

A Wave of COVID-19 Related Cyber Risks: The surge in remote work due to COVID-19 (and the resulting security vulnerabilities) fueled an alarming rise in cybercrime – the FBI reported in August 2020 that cyberattack complaints were up by 400%!² Microsoft reported that pandemic-themed phishing and social engineering attacks jumped by 10,000 a day, while cybersecurity experts reported that ransomware attacks were up by 800%.²

The Challenges of Defending a Distributed Workforce: The convergence of the rise of unsecured remote workers with the surge in cybercrime created a highly vulnerable state for SMBs. However, many SMBs don't have endpoint-related security layers beyond anti-virus. 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

64% of SMBs experienced one or more endpoint attacks that successfully compromised data in 2018.³



EMAIL

65% of organizations in the United States experienced a successful phishing attack in 2019.⁴



END USERS

55% of organizations don't provide any sort of email security training on a frequent basis.⁵

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 organization. In addition to servers and desktops, each employee laptop, tablet, and smartphone adds another possible vulnerability that can be exploited to give incoming malware access to the corporate network.

70%
of breaches originate at the endpoint, but 42% of all endpoints are unprotected at any given time! ⁶

Going Beyond Anti-Virus

Simply installing antivirus software is no longer enough due to the proliferation of cyber threat 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 behavioral 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

20% of SMBs don't have or don't know if they have endpoint security. ⁷

BUILDING THE FOUNDATION FOR REMOTE SECURITY

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 organization 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.

96%

Email is the top delivery mechanism for 96% of phishing attacks and 49% of malware attacks.⁸

Two Layers of Email Security



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.

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 ever-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.

65%

of SMBs currently don't undergo end user training, even though end users are the number one cause of data breaches.⁹

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.

78%

of end users don't click on a single phishing email after training.¹⁰

Ongoing Security Microtraining

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 organization.

70%

Security risks are reduced by 70% when businesses invest in security awareness training.¹¹

BUILDING THE FOUNDATION FOR REMOTE SECURITY

Standardizing 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 three leading solutions that Pax8 partners have begun offering as a bundle that complement each other to cover the gaps around endpoint and email security.



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.



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.



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.

Phishing Simulation Training

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

Pax8 understands the unique challenges MSPs are facing right now and offers a top-notch selection of tech vendors. Iconic IT has standardized our security stack around SentinelOne, Proofpoint, and IRONSCALES to make sure we're protecting our clients against even the most advanced security threats out there.

- Matt Lee, Director of Technology and Security at Iconic IT

FORTIFYING REMOTE DEFENSES

Other Tools to Secure Remote Work Environments

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

- 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, use DNS filtering to 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 defense 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 Center (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 out-of-date 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!

A graphic showing the number 99 followed by a percentage sign, rendered in a light blue, outlined font against a dark blue background.

Microsoft reports that 99% of account hacks are blocked using multi-factor authentication (MFA).⁹

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 while transitioning to remote work.

- 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 remotely wipe company data 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 recognize 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 who have moved to remote work 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.

New Email – □ ×

To: Client

Subject: 3 layers of security for your remote workers 🔗

Dear [Client Contact First Name],

If [Client Company Name] has enabled remote work to stay productive during the pandemic, I wanted to check in to see how you're securing employees and protecting your company data. Microsoft reports that pandemic-themed phishing and social engineering attacks have jumped by 10,000 a day, while cybersecurity experts report that ransomware attacks are up by 800%!

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 anti-virus by using automation, machine learning, and behavioral monitoring to detect and eliminate a diverse range of cyber threats 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]

⌵ | 🗑️ | 📍 ☆ 📎 | 📧 Send

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 while adapting to remote work, know that you're not alone in this either! Rest assured, as a born-in-the-cloud company, the Pax8 team is fully remote-enabled and standing by to assist you with product guidance and technical support.

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

If you feel stretched thin by the influx of clients transitioning to remote work and you need a boost to secure your clients' remote environments, our Professional Services team is available to serve as an extension of your team. 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 OpenVPN, Remote Work Is the Future — But Is Your Organization Ready for It?, 2019
- 2 <https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html>
- 3 2018 State of Endpoint Security Risk. Ponemon Institute for Barkley, 2018, <https://cdn2.hubspot.net/hubfs/468115/whitepapers/state-of-endpoint-security-2018.pdf>
- 4 <https://www.tessian.com/blog/phishing-statistics-2020/>
- 5 <https://www.zdnet.com/article/phishing-why-remote-working-is-making-it-harder-for-you-to-spot-phoney-emails/>
- 6 2019 Endpoint Security Trends Report. Absolute, 2019, <https://www.path.absolute.com/resources/2019-endpoint-security-trends>
- 7 SMB Pulse Survey. Webroot, 2018, <https://www-cdn.webroot.com/5715/3728/5184/Webroot-SMB-Pulse-Survey-9-18-18.pdf>
- 8 A Visual Landscape of Cybersecurity. Optiv Security Inc., 2019.
- 9 SMB Pulse Survey. Webroot, 2018, <https://www-cdn.webroot.com/5715/3728/5184/Webroot-SMB-Pulse-Survey-9-18-18.pdf>
- 10 2018 Data Breach Investigations Report. Verizon, 2018, https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf
- 11 Infographic: 10 statistics that show why training is the key to good data protection and cybersecurity. Pensar, 2018, <https://www.pensar.co.uk/blog/cybersecurity-infographic>