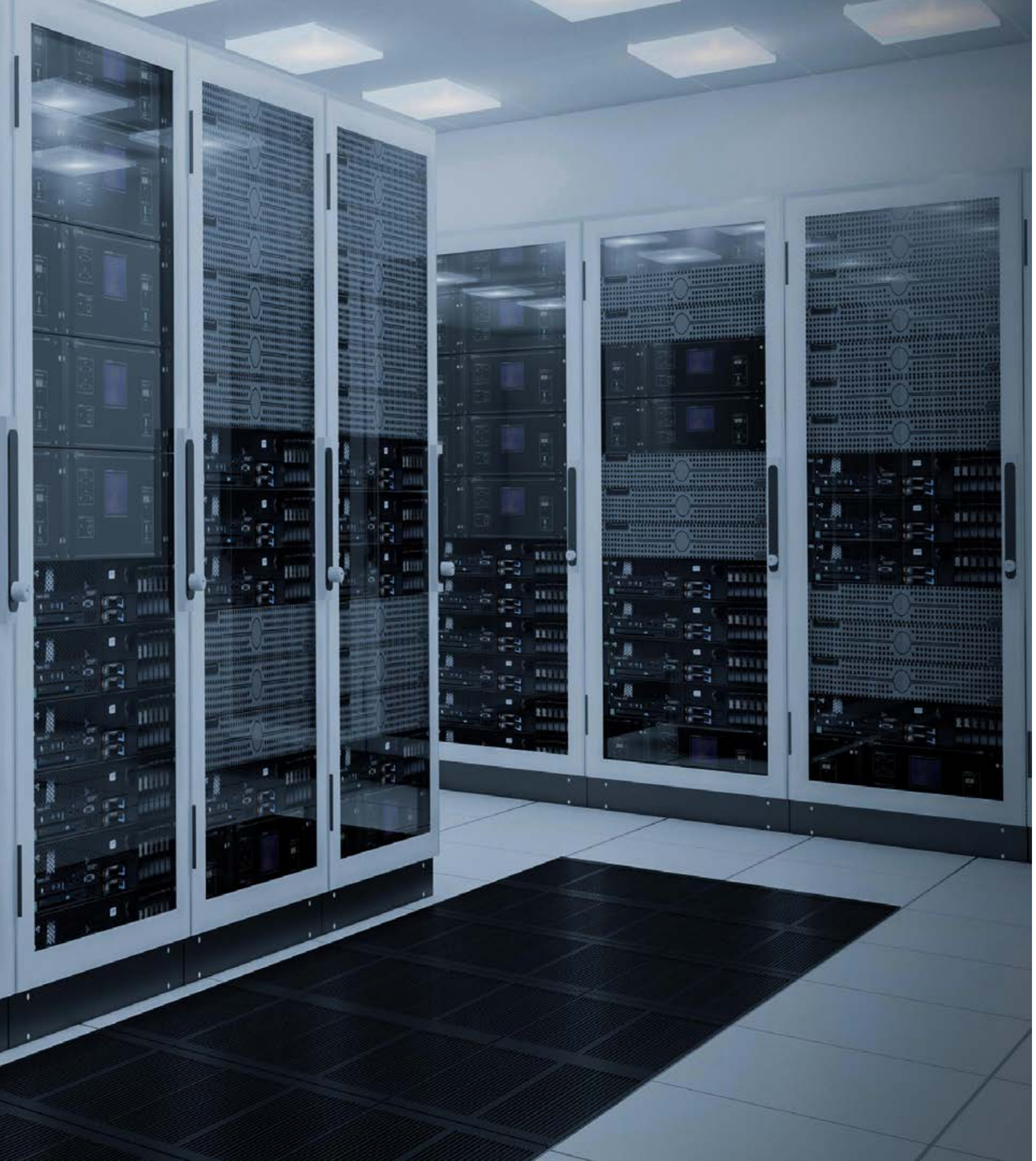
THE SECURITY SCAN PLAYBOOK FOR IT SERVICE AND SOFTWARE PROVIDERS

The Flaw in the Fortress: How IT Service and Software Providers Can Close the Email Gap

A Step-by-Step Playbook for a Post-Pandemic Email Defense

zix



The Danger Is Avoidable

As we covered in the companion piece to this playbook, The Security Scan Guide for IT Service and Software Providers, there's a critical flaw in many IT service and software providers' security architecture. While they've been quick to adopt advanced security solutions like CASBs, cloud-native endpoint protection solutions, and high-end VPNs, many are overlooking a critical vulnerability: their email.

> *A rise in cyberattacks has paralleled the rise of remote work.*

Since the onset of the pandemic, a rise in cyberattacks has paralleled the rise of remote work. A vast majority of those attacks happen through business email. And most of those, via phishing attempts. Now is the time for teams to secure their most sensitive communication channels.

In this playbook, we provide step-by-step instructions on how to conceptualize your new, expanded defense, and actions you can take to harden your network continuously.

Part 1. How to Fix the Flaws in your Defense

The rise of remote work has led to more potentially sensitive information traveling over the open internet via email and file transfers (often, non-InfoSec validated ones like Dropbox and WeTransfer, because of 25MB email file send limits). If these channels aren't adequately secured, they provide weak links where information is either exposed or gaps are left open for malicious actors to enter.

BTo reduce your vulnerability, it's critical to lock down your communication channels. The email threat landscape is constantly evolving, and too many companies place the burden of security—remembering to encrypt emails, staying wise to scams—on stressed employees who are prone to making mistakes. To patch this hole, IT service and software providers need to secure emails and file transfers using tools that remove the cognitive load of security from individual employees.

In the next chapter, we detail the **challenges** that come out of insufficiently secure communication chains, the **fixes** we suggest, and the **opportunities** these solutions create for better financial performance.

Part 2. Challenges and Solutions

For each challenge, we detail steps to remediate and provide ongoing protection. For more details on the challenges, revisit this playbook's companion piece, The Security Scan Guide for IT Service and Software Providers.

1 Challenge: Remote work brings increased security concerns

Solution: Adaptive Email Threat Protection, Encryption, Secure File Sharing, and Continuity

Use out of the box policies. Your email security should be set on autopilot. Choose a solution that doesn't require any end user training and ensures employees never have to leave their inbox. A robust solution will cover:

- **Impersonation defense.** Maintain a real-time understanding of the business' email communication to accurately identify a threat actor.
- **Deep-level attachment and URL analysis.** Stop well-known threats and zero-hour malware through static and dynamic analysis.
- **Compliance-grade email encryption and secure file sharing.** Prevent prying eyes from snooping on your network.
- **Integrated email continuity.** Preserve business productivity even when under a severe DOS-attack.

Benefit: ✓ Lower risk of breach ✓ Increase agility ✓ Innovate faster

2 Challenge: Teams are stretched thin with more endpoints and responsibilities, but less budget

Solution: Secure your email communications and file transfers

- **Provide an intuitive email security software.** Seek out email security software that is easy to use. The more intuitive the software, and the fewer decisions it forces upon users (such as requiring them to press a button to encrypt an email), the safer everyone is by default.
- **Choose an aggressively priced solution.** Email Security is a mature market. Vendors in the top tier like Zix, Mimecast, and Proofpoint can maintain their effectiveness without much user intervention. The difference is price. For tight budgets, Zix offers the best value price.
- **Simplify your email security infrastructure.** Where possible, consolidate cybersecurity vendors and give preference to those that offer multi-function platforms, such as ones that offer both encryption and threat protection. This prevents coverage gaps.
  - Scan all mailboxes for suspicious permissions.
  - Lock inactive mailboxes.
- **A proactive partner.** Ideally, the software provider acts as more than a partner and employs a 24/7 threat analyst team to identify emerging issues for you.
  - Check whether existing vendor offers security insights and real-time updates.

Benefit: ✓ More budget ✓ Lower risk of breach ✓ Reduce cognitive load on employees

Email Encryption: Some encryption vendors, like Zix, offer an entirely secure network, so messages between two Zix customers never touch the open internet.

4 in 10 threats involve employees. -Deloitte

75% of companies lack skilled resources. -Deloitte

3 Challenge: The impending great separation

Solution: Practice what you preach

- **Commit to security best practices.** The security strategies you implement in-house sets the standard for your customers. Make sure you're modeling the kind of behavior you want them to follow. These best practices should include:
  - **Email Incident and remediation.** Use a solution that provides ways to remediate an incident if found within the inbox post-delivery.
  - **Partner-accepted email encryption and secure file sharing.** Vendors that share security best-practice are better positioned to innovate and adapt
  - **SIEM Integration.** Maintain a real-time understanding of the threats targeting the organization so that you can quickly adjust protection and ensure your customer information remains safe
- **Standardize on communication channels.** Get all business units using the same email client, secure file sharing solution and the same collaboration platform. The fewer systems, the fewer weak links.
  - Where possible, securely incorporate suppliers and vendors into collaboration software like Microsoft Teams, to prevent sensitive communications from happening over SMS text.

Benefit: ✓ Be exemplary ✓ Reduce coverage gaps ✓ Increase agility

From Open Windows to a Secure Base

The increased risk of malicious attack threatens IT software and service providers who have had to become more adaptable as a result of the pandemic. It affects nearly all—and by that token, presents a massive opportunity.

IT service and software providers that are able to affordably scale their email and file transfer security across their business will come out ahead. They're better able to reallocate much-needed capital, seize on growth opportunities, and communicate freely and securely with vendors and customers.

IT service and software providers have been at the heart of the COVID-19 digital transformation—and in the future, the secure will continue to dominate.

Learn more at Zix.com/it