YOUR EMAIL HAS A TRUST PROBLEM. ANYONE WITH YOUR EMAIL ADDRESS CAN ACCESS YOUR INBOX WITHOUT PERMISSION.

AN MSP's GUIDE

Zero Trust Email Security

Why SPF, DKIM, and DMARC Still Fall Short

mailprotector

Source: 2024 Verizon Data Breach Investigations Report

Introduction

Email security is broken. Despite decades of advancement in cybersecurity, email is still the primary attack vector.

This comprehensive guide for MSPs reveals why traditional solutions fail and introduces a revolutionary approach: Zero Trust Email Security.

What you'll learn:

- Why email's original design creates inherent vulnerabilities
- How past security solutions failed to address the core problem
- Why SPF, DKIM, and DMARC provide incomplete protection
- The essential components of Zero Trust Email Security
- How to implement a comprehensive trust-based solution

By the end of this guide, MSPs will be equipped with the knowledge to build a future-proof email security strategy that protects clients, simplifies security stacks, and adds competitive differentiation.

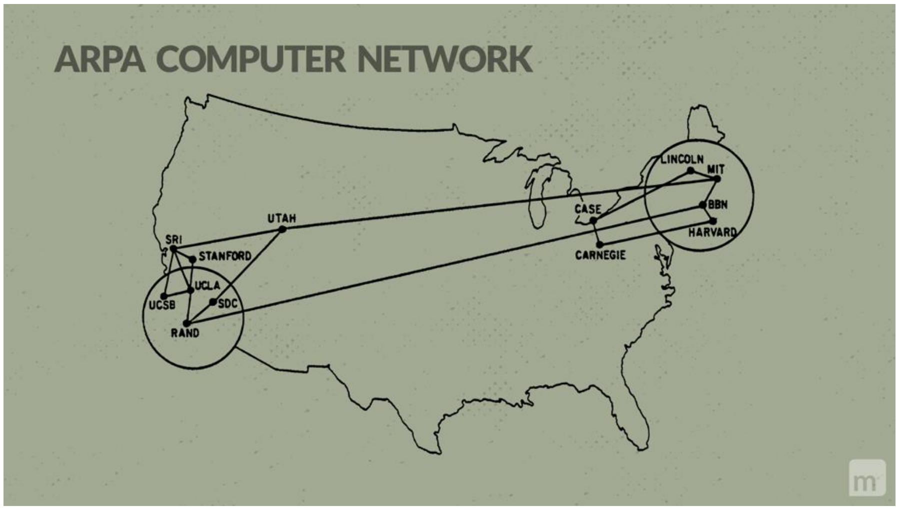
Table of Contents

Chapter 1

Email’s Trust Problem

Your email has a trust problem. Anyone with your email address can access your inbox without permission.

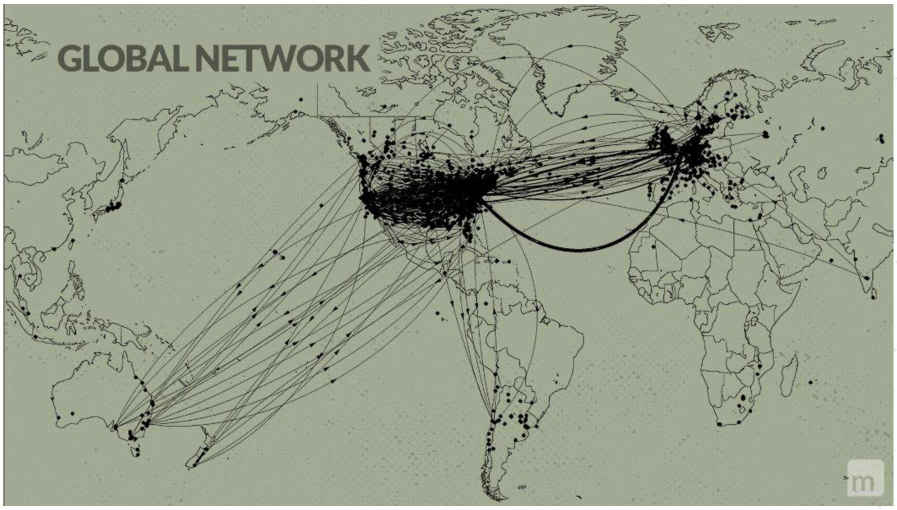
This powerful communication tool has become vulnerable to exploitation, making it the primary entry point for cyberattacks.



How Did We Get Here?

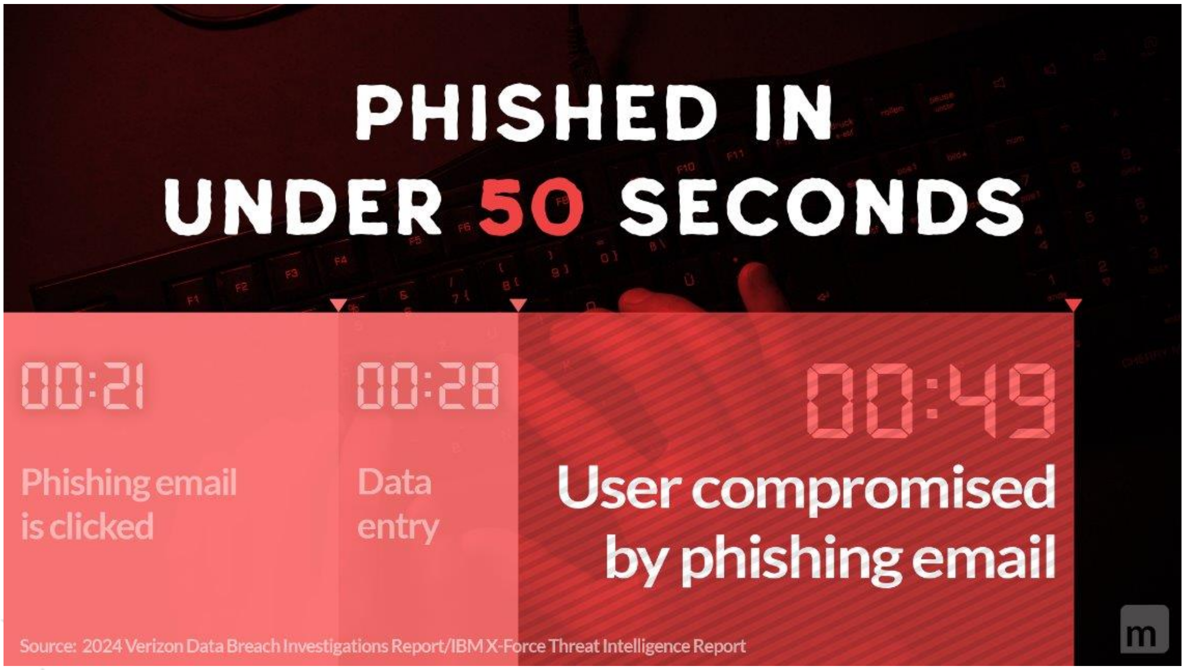
To understand how we got here, we have to go back to the beginning. Email predates the internet itself. Created for ARPANET, email was designed for a small, closed network where security came from two fundamental factors: limited access to the network and knowledge of other users on the network. This worked perfectly in a controlled environment. But when email moved to the internet, everything changed.

Suddenly, a system designed for a trusted network of known users was exposed to the entire world. The original security model was shattered, yet the underlying technology remained unchanged.



The Impact of Broken Trust

The consequences of this architectural flaw are severe. Phishing has become particularly devastating. The speed at which users fall victim is alarming: the median time for a user to click a phishing email is just 21 seconds, with data entry occurring within 28 seconds after that. This means the total time from receiving a phishing email to a compromise is less than 50 seconds.



Source: 2024 Verizon Data Breach Investigations Report/IBM X-Force Threat Intelligence Report

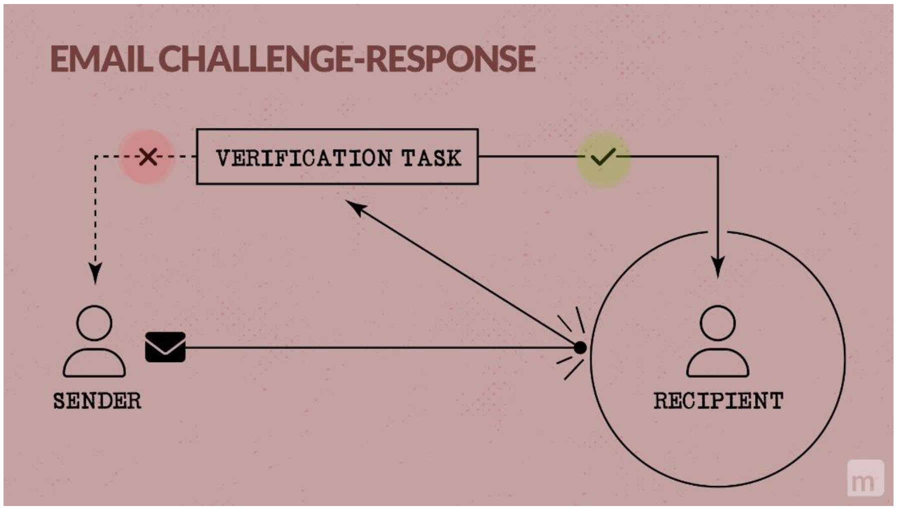
This makes email security the foundation of your entire cybersecurity stack—if you don't get this right, everything else is just playing catch-up.

Chapter 2

Past Failed Attempts

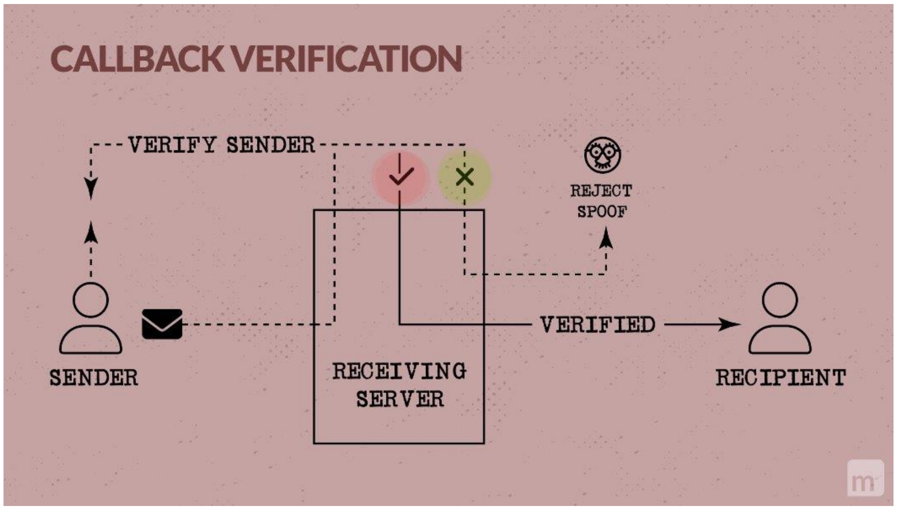
There have been attempts to solve the email trust problem over the years, but they've failed. Even though these methods are no longer used in practice, it's important to understand why they fell short.

Challenge-Response Systems



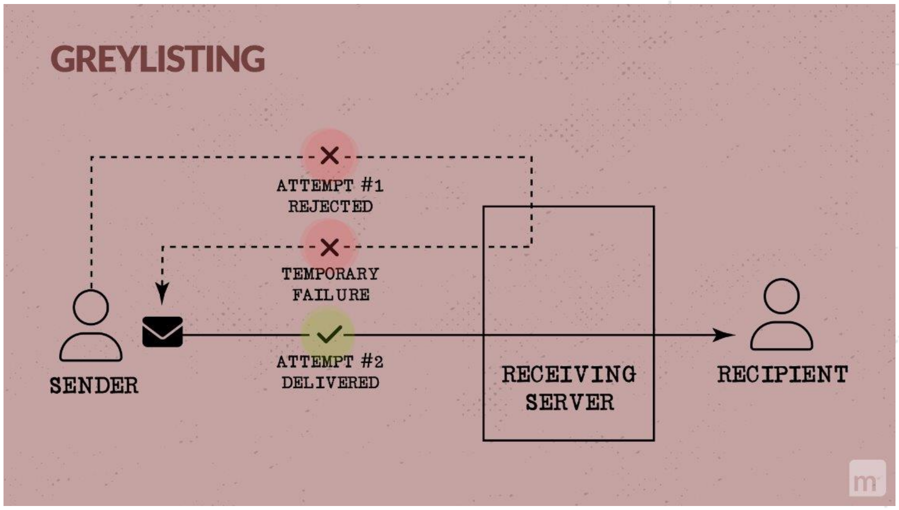
Early attempts to solve email's trust problem focused on challenge-response systems. These required senders to verify their identity before message delivery. While logical in theory, this approach created significant user friction, delayed legitimate email delivery, and generated problematic auto-reply loops. It fails to fix the trust problem because control still lies with the sender and can easily be bypassed by bad actors.

Callback Verification



Callback verification, also called sender address verification, emerged as another solution to validate senders through SMTP callbacks. This method proved ineffective because most attacks use legitimate spoofed addresses. The system only verified address existence, not authenticity, while creating compatibility issues and often leading to blacklisting.

Greylisting



Greylisting represented another failed attempt, temporarily rejecting emails from new senders under the assumption that legitimate servers would retry. This introduced unacceptable delivery delays, created server performance issues, and generated user frustration. Like its predecessors, threats easily circumvented this approach.

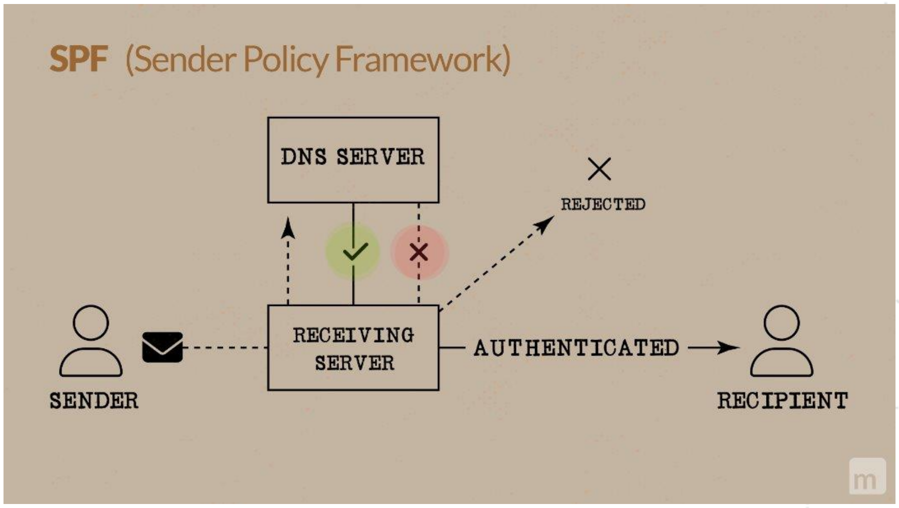
All three of these tactics failed. Why? Because they didn't address the root of the issue: email's trust problem on an open network.

Chapter 3

Current Tools: Necessary but Insufficient

More recent methods are effective to varying degrees but still fall short on their own.

Sender Policy Framework (SPF)



SPF prevents basic email spoofing by validating the IP addresses authorized to send on behalf of a domain. It strengthens email authentication, reduces spoofing attempts, and builds trust in email delivery.

However, SPF has a limited scope with inherent limitations:

1. **Breaks with email forwarding**: SPF validation often fails when emails are forwarded unless the forwarding server implements Sender Rewriting Scheme (SRS).

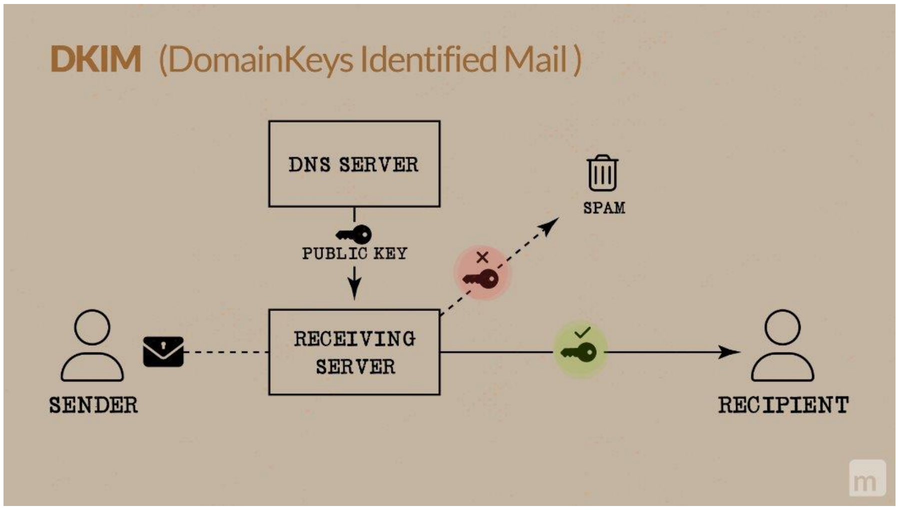
2. **IP-based verification only**: SPF focuses solely on IP addresses and does not authenticate email content or the sender's identity.

3. **DNS dependency**: SPF depends on accurate and reliable DNS records, making it vulnerable to misconfigurations or DNS outages.

4. **Limited protection against sophisticated attacks**: Threat actors can bypass SPF through compromised accounts or spoofing methods that exploit gaps in email systems.

Domain Keys Identified Mail (DKIM)

DKIM helps protect against impersonation attacks by using cryptographic signatures in email headers to verify the authenticity of the sending domain. It also ensures that email content isn't altered in transit, like a digital wax seal.



However, DKIM also has limitations:

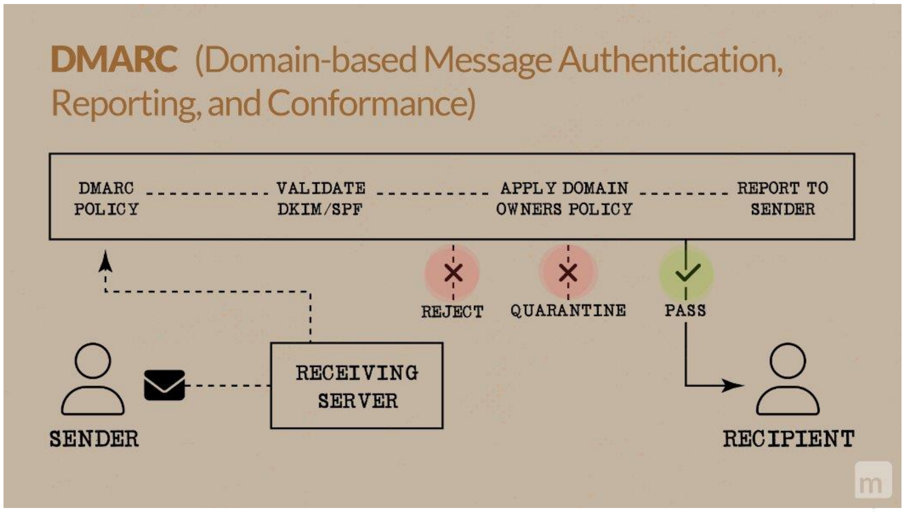
1. **Limited scope**: DKIM only verifies that the email originated from an authorized server and hasn't been tampered with. It doesn't address whether the sender should be trusted.

2.Exploitable by sophisticated threats: Bad actors exploit DKIM's scope by crafting phishing emails that meet DKIM's checks, especially in targeted spear phishing attacks.

3.Dependency on configuration: Misconfigurations or missing keys can render DKIM ineffective.

Domain-based Message Authentication (DMARC)

DMARC builds on SPF and DKIM by adding alignment mechanisms and reporting capabilities. It allows domain owners to specify how legitimate messages should be sent and enables policies to reject or quarantine unauthorized emails.


DMARC (Domain-based Message Authentication, Reporting, and Conformance)
DMARC POLICY
VALIDATE DKIM/SPF
APPLY DOMAIN OWNERS POLICY
REPORT TO SENDER
REJECT
QUARANTINE
PASS
SENDER
RECEIVING SERVER
RECIPIENT

While DMARC effectively prevents most impersonation and spoofing attacks, it too has limitations:

1.Limited scope: DMARC focuses on identifying and stopping spoofing based on the source of the email, without addressing broader trust or content-based threats.

2.Dependency on SPF and DKIM: DMARC's effectiveness depends on proper implementation of SPF and DKIM, which can still fail in scenarios like email forwarding or misconfigurations.

3.Not a complete solution: Sophisticated attacks, such as those leveraging compromised accounts or advanced social engineering, can bypass DMARC's protections.

While SPF, DKIM and DMARC are critical components of email security, they do not fully address the trust problem alone. To truly solve this challenge, a stronger and more comprehensive security foundation is required.

Chapter 4

Flipping the Paradigm

A comprehensive security model that assumes **no entity** (inside or outside the network) can be **trusted by default.**

We don’t have to look far to find a proven security model that can serve as the foundation for solving email’s trust problem. Zero trust is now a cornerstone of modern cybersecurity. Yet, despite its widespread use across other domains, it’s been noticeably absent from email security. Why? Because applying zero trust to email is uniquely challenging.

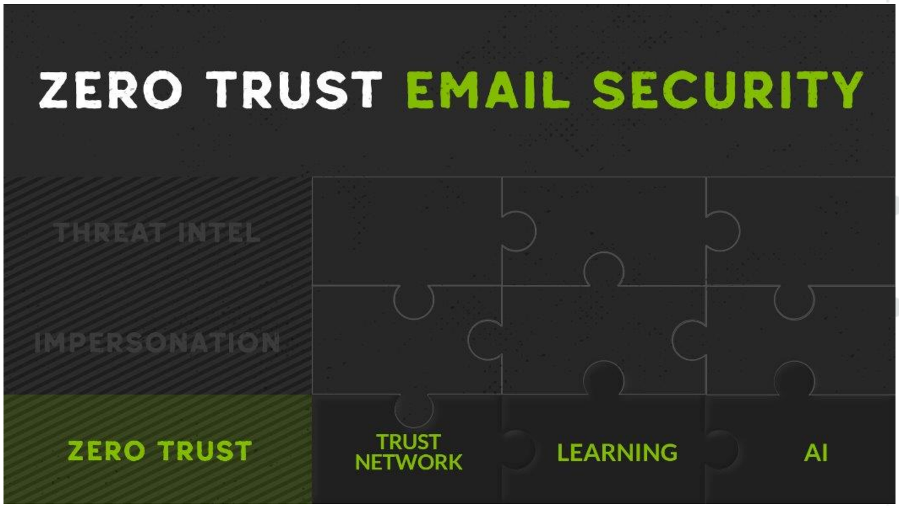
Solving email’s trust problem requires more than just adapting traditional zero trust principles—it demands a complete rethinking of email security itself. Instead of trying to identify the bad within a flood of assumed-good traffic, zero trust email security flips the paradigm: *all messages are untrustworthy until proven safe.*

Achieving this, however, isn't as simple as flipping a switch. It requires a multi-tiered approach that combines advanced technologies, layered defenses, and user empowerment. This complexity is the price of solving the trust problem for good, but it's a price worth paying to build a future-proof email security strategy.

Chapter 5

How to Build Layers of Trust

Step One: A Zero Trust Foundation



First, we must decide what our trust model will be based on. You could apply trust based on the message's source, but as we've seen with SPF and DKIM, this isn't enough. You could apply trust based on content, but that's dangerous because it can easily be faked, especially given the recent explosion of AI.

Email's origins on ARPANET relied on a closed network for security. However, that trust model collapsed as email moved to the open Internet, leaving it vulnerable.

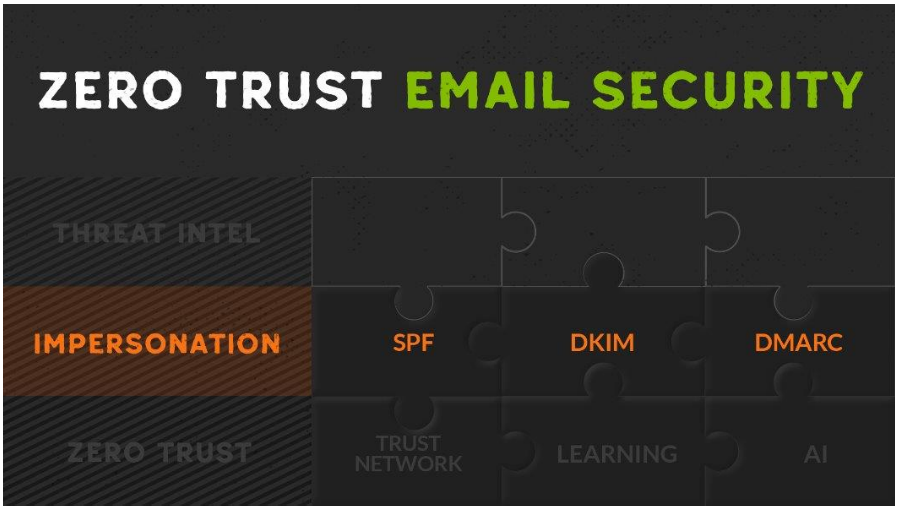
How do we adapt to this new reality and restore trust in a system built for a different era? We shift focus. *Trust must be built around the people and organizations you communicate with.*

Building A Trust Network

The foundation of zero trust email security starts with a dynamic trust network that recognizes legitimate communication patterns. This network continuously learns from user behavior, including who they communicate with and how they interact with messages.

As communication patterns evolve, the system adapts automatically, refining its trust model. AI and machine learning play a critical role by transforming behavioral data into actionable intelligence, ensuring the network remains personalized and responsive to changes in communication over time.

Step Two: Impersonation Defense

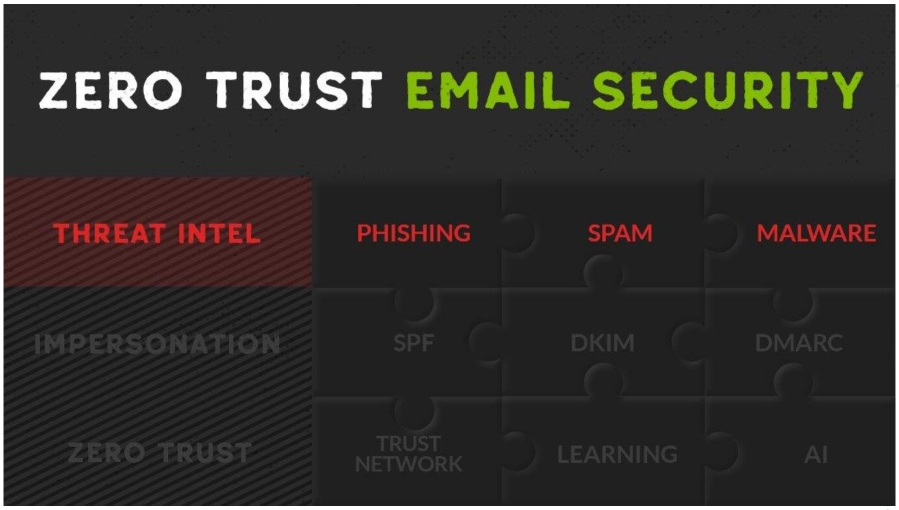


Now that we have an intelligent trust network that understands who you communicate with, the next step is to protect against impersonation attacks. Before we can grant trust to any sender, we need to ensure they are who they claim to be.

Spoofing attacks, where bad actors impersonate legitimate senders, are a major risk. To defend against these attacks, we need mechanisms that can validate the sender's authenticity.

This is where SPF, DKIM, and DMARC come into play. These established protocols work together to authenticate the sender's identity, providing a layer of defense that ensures only trusted senders can interact with your network. By combining these mechanisms with the trust network, we can prevent spoofing and ensure the integrity of your communications.

Step Three: Threat Intelligence



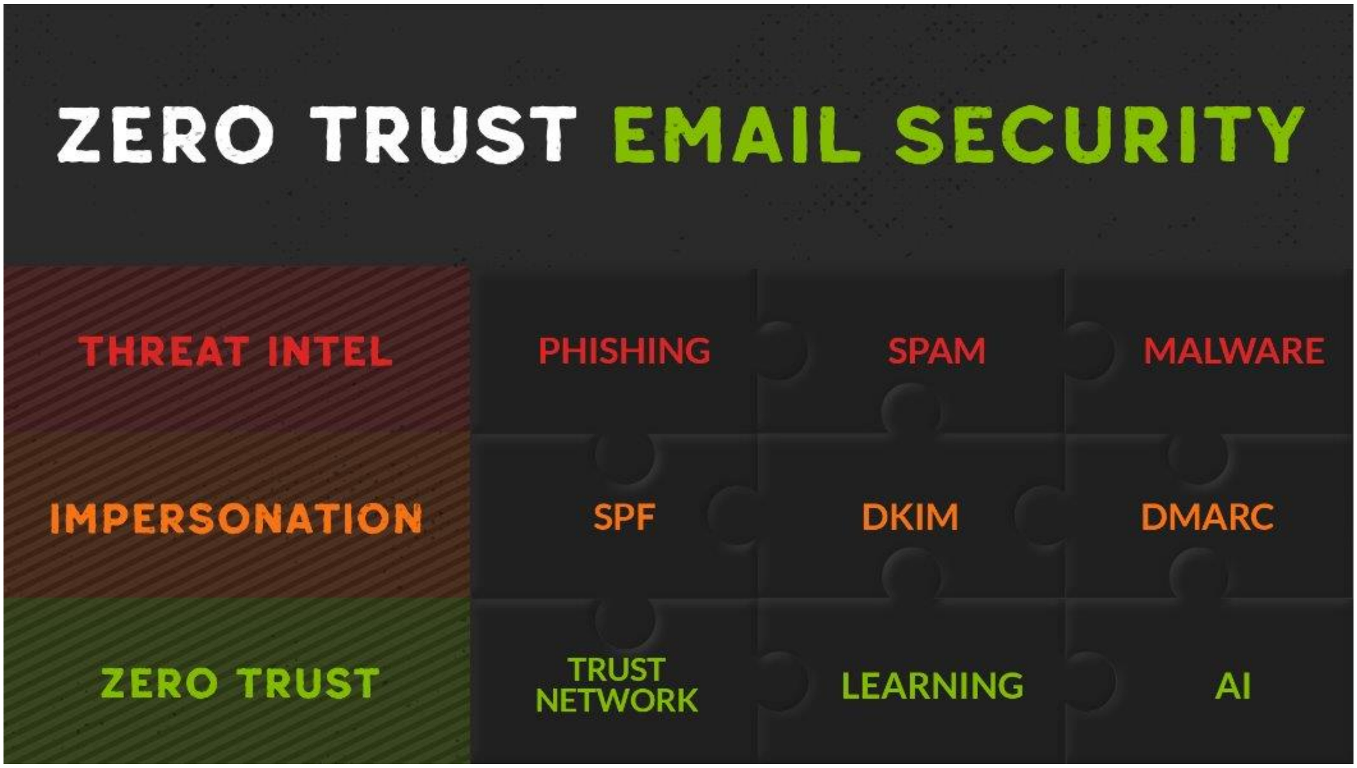
There’s still one more layer needed for comprehensive protection.

While we’ve ensured the sender's authenticity, there’s always a possibility that a trusted account could be compromised. In these cases, harmful messages might still come from within your trust network, making it harder to spot the threat.

That’s where threat intelligence comes in. Regardless of the source, it recognizes suspicious patterns to stop sophisticated phishing attempts, spam, malware, and other malicious content. Even if a valid account sends “authentic” messages with harmful intent, threat intelligence ensures that these threats are caught and stopped, adding an extra layer of protection to your email security.

Chapter 6

Putting It All Together



ZERO TRUST EMAIL SECURITY

THREAT INTEL	PHISHING	SPAM	MALWARE
IMPERSONATION	SPF	DKIM	DMARC
ZERO TRUST	TRUST NETWORK	LEARNING	AI

This is what a complete solution to email's trust problem looks like.

It begins with a new foundation: zero trust. This model brings the security of a closed network combined with an intelligent trust network that learns from user behavior.

Next comes impersonation defense to ensure trust is only granted to valid and authentic senders, using mechanisms like SPF, DKIM, and DMARC.

Finally, threat intelligence catches and blocks harmful content—even when it appears to come from trusted sources, such as compromised accounts.

With zero trust email security, the defaults are flipped, putting control back in the right hands. When the trust problem is solved, email can be restored to the powerful, reliable communication tool it was always meant to be.

Chapter 7

Introducing a New Era in Email Security

Email security demands a complete reinvention. After decades of breaches, compromises, and failed solutions, it became clear to us that fixing email required more than just adding new layers to a broken foundation.

That's why Mailprotector created Shield, the first-of-its-kind zero trust email security solution.

While others layer multiple products attempting to patch email security gaps, Shield integrates edge-to-inbox protection into one seamless platform. Think of it as noise-cancelling headphones for your inbox—eliminating threats, spam, AND all the unwanted noise you've learned to live with.

Enhances M365
Heads-Up Display
Spy Tracker Blocking
Intelligent Desirability
Shield™
Zero Trust Email
Spotlight
Bundler
Zero Trust Email
Burner Addresses
X-ray
Email Security Briefing
VIP Address
Threat Intelligence
Noise-Cancellation
Lockbox
>_Ctrl

At Shield's core lies our patented zero trust security model, delivering the comprehensive protection we've discussed throughout this guide. But that'sjust the beginning. Shield combines this revolutionary foundation with powerful features that put you back in control of your inbox.

The result? A calm, clean inbox that only delivers the email you want. No more juggling multiple solutions or accepting "good enough" security. Shield is the consolidated, trusted solution that finally solves email's trust problem.

Visit ***mailprotector.com/shield*** to see zero trust email security in action.

Conclusion

Building a Secure Email Future

The path to secure email requires a shift in mindset as much as technology. It’s more than adding layers to a broken foundation—it demands a complete reimagining of how we approach trust.

While SPF, DKIM, and DMARC play important roles, the next chapter of email security combines:

1. A zero trust foundation that validates every message
2. An intelligent trust network that learns and adapts
3. Robust impersonation defense
4. Comprehensive threat intelligence

The future of email security lies in intelligent, adaptive systems that combine zero trust principles with advanced analytics and authentication. These systems will continue to evolve, incorporating new technologies and responding to emerging threats. The key is maintaining the core zero trust principle: trust must be earned and verified, never assumed.

By implementing zero trust email security, organizations can protect against current attacks while building a foundation for addressing future challenges. This comprehensive approach represents the best path forward for building a secure email future for everyone.