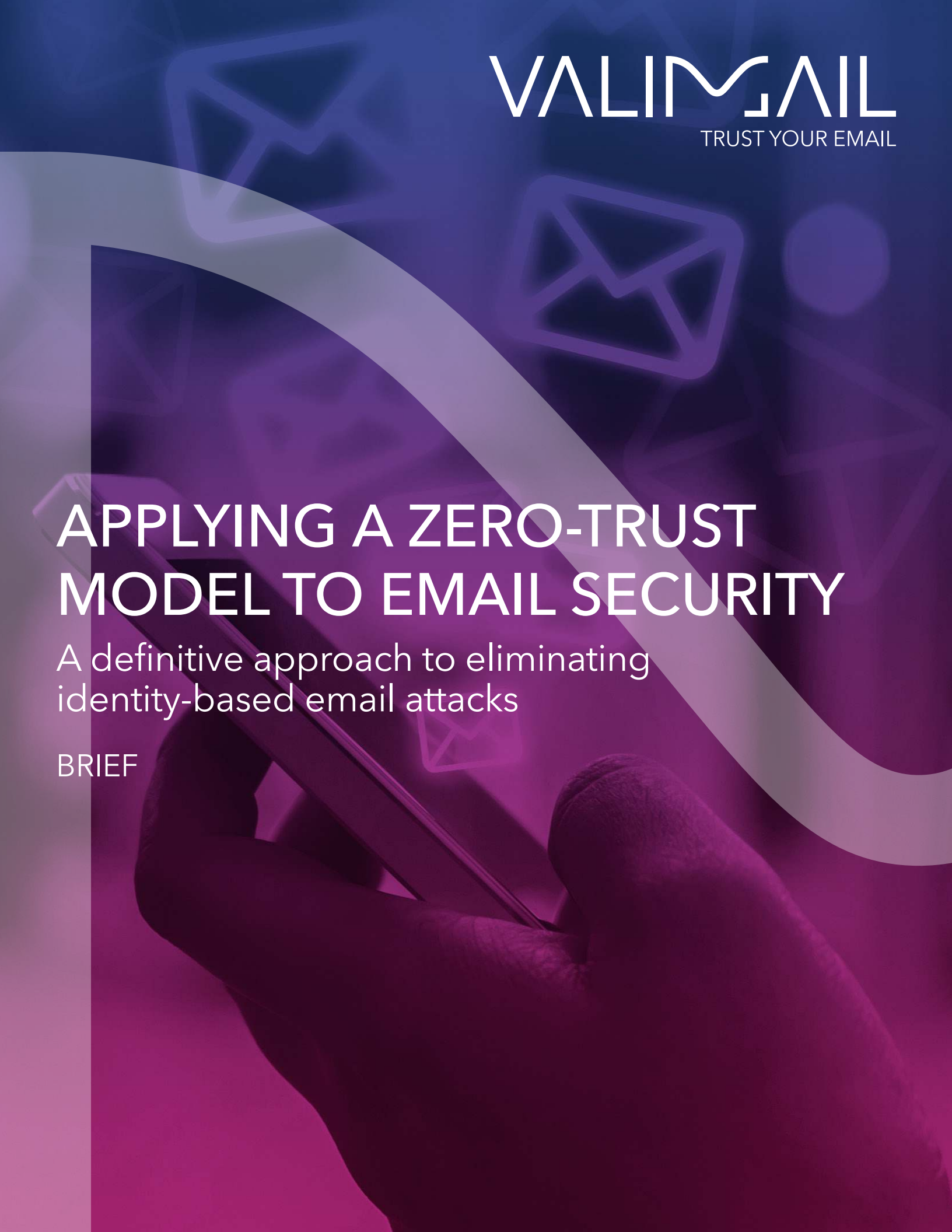
VALIMAIL

TRUST YOUR EMAIL

APPLYING A ZERO-TRUST MODEL TO EMAIL SECURITY

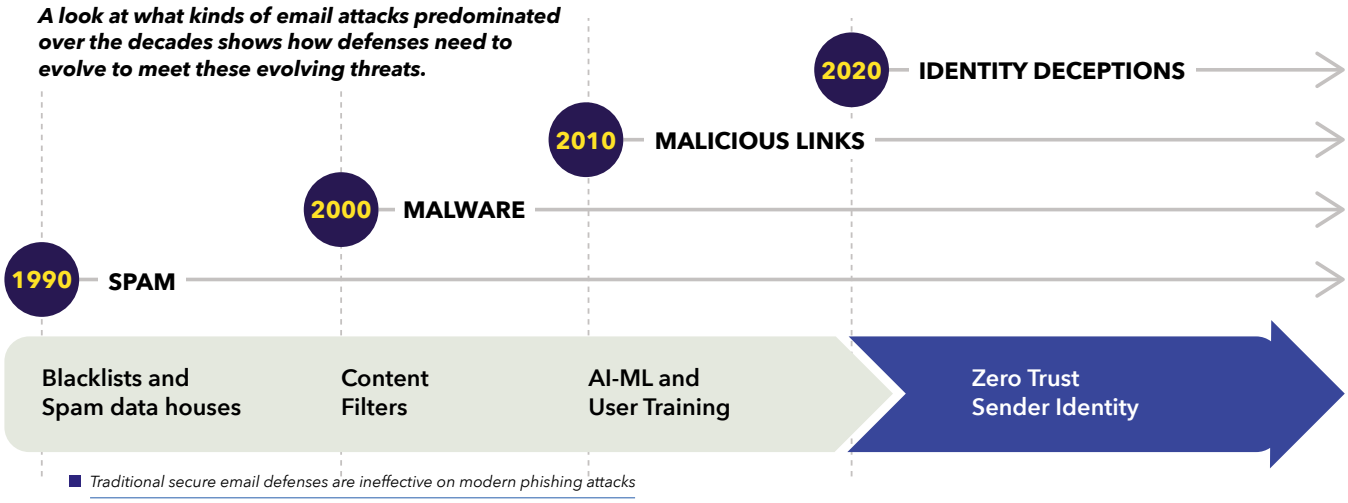
A definitive approach to eliminating identity-based email attacks

BRIEF



AT A GLANCE

Current email threats have moved past a content-centric approach (aimed at delivering malicious links and attachments) to more sophisticated gambits. Almost 90% of email attacks manipulate sender identity to fool recipients and initiate social engineering attacks – and their lack of identifiably malicious content means they can easily bypass most current defenses.



Traditional secure email defenses are ineffective on modern phishing attacks

Valimail's zero-trust approach to email security is purpose-built to focus on the root cause of these attacks – sender identity – eliminating the uncertainty and complexity of other email security solutions.

By identifying and authenticating senders before they get to the inbox, Valimail delivers fully automated protection against both inbound and outbound phishing and BEC attacks.

TYPES OF IDENTITY-BASED ATTACKS:

- **Exact-domain attacks** (aka domain spoofing): Emails that directly impersonate a trusted sender by putting their domain in the "From" field of a message
- **Untrusted-domain attacks** (aka domain impersonation): Emails that are sent from slightly altered "lookalike" or "cousin" domains
- **Open-signup attacks** (aka user impersonation or friendly-from): Emails that show a legitimate sender name in the "friendly from" field but are sent from an account created on a free consumer webmail service like Gmail or Yahoo

Risks organizations face without a zero-trust approach

ZERO-DAY PHISHING ATTACKS

According to Google, 68% of phishing attempts have never been seen before – and the average campaign lasts only 12 minutes. That's because criminals have automated phishing to avoid detection. Existing email security systems are content- and context-centric, using AI/ML modeling to estimate risk factors based on what's in a message. This type of system needs to see and classify a phishing attack type at least once before it can block the same type of attempt in the future. Yet, as statistics show, many of these attempts are brand new, leaving such systems vulnerable to zero-day phishing attacks.

The end result means the speed and frequency used by modern attackers will result in phish getting through existing defenses.

BRAND REPUTATION RISKS

According to the FTC, over 96% of companies operating today suffer from domain spoofing attacks in one form or another. Without a zero-trust approach that authorizes or blocks services based on validated sender identity, brands are left vulnerable to domain spoofing attacks that erode trust between supply chain partners and consumers.

WHY USE ZERO-TRUST SENDER IDENTITY FOR EMAIL SECURITY?

For email, the zero-trust model means not allowing delivery of messages unless they originate from a sender who can be authenticated and who has been granted explicit permission to deliver messages to that inbox.

AI/ML solutions can be effective when it comes to identifying trends in social engineering and malicious content, but they don't provide much usable information when it comes to sender identity, due to the rapidity with which email attackers mutate their identities.

Instead, with a zero-trust approach, you focus on definitively identifying trusted senders. Once you do that, you can flag or block everything else: You don't have to worry about finding, analyzing, or scoring the infinite variety of possible malicious senders.

THINK OF IT THIS WAY:

A traditional login system positively identifies known, trusted users (and doesn't make you worry about analyzing the infinite variety of possible bad logins).

Valimail's zero-trust approach means that every email sender is untrusted unless we can prove that it's trustworthy.

How Valimail delivers results

Applying zero-trust to email security hinges on knowing the trustworthy senders' identities with certainty. So how do we make these real-time decisions without risk of blocking the good email?

Since the platform is zero-trust by design, all unknown entities, such as domains, sending services, and contacts, are considered untrusted unless explicitly granted access through policies. Entities can be re-classified and authenticated, authorized and then continuously verified based on organization policy.

For outbound mail

Valimail ensures that only authorized third-party sending services are allowed to send email on your organization's behalf, eliminating brand and executive spoofing.

a. We identify all third party senders at the service level (not IP addresses), regardless of sending volume

b. Valimail can accurately identify over 5,500 different sending services by name right out of the box – more than 20x more than competing services, and about 95% of all email sending services in the world

c. We provide a simple, automated, point-and-click dashboard to authorize or deauthorize services and manage configurations of all domain authentication standards (DMARC, DKIM, SPF, BIMI)

For inbound (inbox) protection

Valimail validates sender identity by checking against thousands of recognized, reliable, real-world data repositories to determine the authenticity of every inbound sender.

a. We've built the most comprehensive – and constantly expanding – database of known good sending domains, with over 30M known good domains – and growing

b. Our system validates domains based on dozens of individual signals, and includes cross-checking against thousands of public databases

c. We check all incoming email messages into your organization from open-signup addresses (Gmail, Yahoo, etc.) against your organization's list of trusted contacts

d. For most customers we achieve a 90% recognition rate for inbound senders immediately, and achieve 99%+ recognition within two weeks

BENEFITS OF THE VALIMAIL APPROACH

Built on open standards like DMARC, DKIM, SPF, and BIMI, as well as proprietary, patented technology, Valimail validates every message in real time, with powerful automation, to make sure every corporate message is secure.

In addition, Valimail provides granular, policy-based controls based on roles and risk appetite for your organization, so you decide how you want to handle untrusted services, senders, and contacts – quarantine, delete, or simply monitor. For inbound email, policy controls can be applied company-wide or on an individual or group basis, depending on your organization's and each group's particular needs.

Exact-domain protection and global visibility

- Automated DMARC, DKIM, and SPF configurations
- Industry leading discovery of 5,500+ sending services
- No manual DNS updates
- Zero risk of blocking good email at enforcement

Untrusted-domain protection

- Blocks inbound email from all untrusted and fraudulent sending domains
- Seamless integration with Microsoft Office 365 and Google G Suite via one-click authorization
- Continuous and automated updates for unknown, untrusted, and trusted domain repositories

Open-signup protection

- Synchronizes your organization's list of trusted contacts from open-signup systems (Gmail, Yahoo, etc.)
- Checks all incoming email messages against those trusted contacts
- Blocks unknown (and therefore untrusted) senders from open-signup systems

Brand amplification

- Provides global control over logo display in email inboxes
- Drives new brand impressions and increases email open rates
- Automated support for BIMI (Brand Indicators for Message Identification) and Microsoft Business Profiles

Valimail's zero-trust, identity-based platform works

Valimail's product suite provides global, identity-based phishing protection and brand amplification that benefits all internal stakeholders, from IT and security to compliance and marketing.

As part of a layered email security approach, Valimail closes the gap left by content-centric security approaches that focus on **what** email messages contain, not on **who** sent them. Valimail:

- Defends your inbox from rapidly mutating phishing attacks that traditional email security defenses miss
- Blocks impersonation attacks that use your domain and are targeted at your employees and everyone else you do business with
- Amplifies your brand by delivering your authenticated logo in every email to Microsoft, Yahoo, and Google inboxes

Get started for free with a phishing assessment to see exactly which advanced threats are manipulating your sender identity and making it to your corporate inbox.

valimail.com/analysis

VALIMAIL ZERO-TRUST EMAIL SECURITY FOR OFFICE 365 AND G SUITE

Valimail is the only solution that reliably stops phishing threats at the source to secure your inboxes and amplify your brand.

- **Domain protection**
  - Stops impersonation attacks spoofing your domain
  - Prevents brand abuse
  - Protects partners and customers
- **Inbox protection**
  - Stops lookalike-domain attacks
  - Stops friendly-from attacks
  - Prevents BEC and CEO fraud attacks
  - Protects employees
- **Brand amplification**
  - Increases brand impressions
  - Boosts email open rates
  - Gives you control of your brand in the inbox

TRUST YOUR EMAIL

Valimail is a pioneering identity-based anti-phishing company that has been ensuring the global trustworthiness of digital communications since 2015. Valimail delivers the only complete, cloud-native platform for validating and authenticating sender identity to stop phishing, protect and amplify brands, and ensure compliance. Valimail has won more than a dozen prestigious cybersecurity technology awards and authenticates billions of messages a month for some of the world's biggest companies, including Uber, Fannie Mae, Mercedes Benz USA, and the U.S. Federal Aviation Administration. For more information visit www.valimail.com.