StrongestLayer

DMARC for CISOs

What It Actually Protects (And What It Doesn't)

Muhammad Rizwan
Chief Technology Officer, StrongestLayer
April 2026

For CISOs, security architects, and IT leaders evaluating whether email authentication equals email security.

$3.0B BEC losses in 2025 (FBI IC3)	**10.7%** Domains at strict enforcement	**56.4%** Attacks using domain lookalikes	**~1%** Effective DMARC coverage

The Misconception Problem

If you're a CISO reading this, you probably think DMARC is working harder than it actually is. Most organizations that have deployed DMARC believe it's a comprehensive email security control. It shows up on audit checklists. It's part of compliance frameworks. You've probably spent resources implementing it. But here's the reality: DMARC protects your organization's ability to send trusted email. It does almost nothing to protect your people from inbound attacks.

This distinction matters. And it's one that most security teams blur in their own thinking.

The confusion isn't your fault. DMARC implementation is presented as part of a holistic email security strategy. It sits in infrastructure. It involves domain authentication. It feels like it should be stopping attacks aimed at your organization. But that's not what it does. Not even close.

> *Organizations deploy DMARC, check the box, and then assume their domain reputation is protected. This false sense of security is one of the costliest mistakes in email security today.*

Before we talk about what DMARC actually does, we need to clear away this misunderstanding. Because unless you understand what it genuinely protects, you'll allocate security resources in the wrong places and leave real gaps unaddressed.

What DMARC Was Built to Solve

DMARC stands for Domain-based Message Authentication, Reporting and Conformance. The name describes its scope accurately. It does one thing: it tells receiving mail servers how to handle email that claims to come from your domain but fails authentication checks.

Email authentication has three layers. SPF (Sender Policy Framework) publishes a list of servers authorized to send on your behalf. DKIM (DomainKeys Identified Mail) adds a cryptographic signature your sending server applies and the receiver verifies via your DNS. DMARC sits on top: it says, "I have SPF and DKIM set up. If an email claims to be from my domain but fails these checks, here's what I want you to do."

This is a useful system designed to address one specific problem: exact domain spoofing, where attackers forge your exact domain to send deceptive email. If an attacker sends an email claiming to be from john.smith@yourdomain.com and it fails SPF and DKIM checks, DMARC tells the receiving server to reject or quarantine it.

But here's what matters: DMARC only works if the receiving mail server enforces it. That's not guaranteed.

The Herd Immunity Problem

DMARC deployment statistics tell a revealing story. Cloudflare's 2026 Email Security Report, based on analysis of 450 million emails processed daily, found that 46 percent of all emails still fail DMARC validation. Across nearly one million domains analyzed, only 10.7 percent enforce a strict reject policy at full coverage (p=reject with pct=100). That's the only configuration that reliably blocks spoofed email. The other 70.9 percent of domains have no effective DMARC protection at all.

> *Your DMARC policy is a request that 70.9 percent of the email ecosystem ignores. Not a command. A request.*

This is the herd immunity problem. DMARC only works at scale if the majority of the email ecosystem enforces it. With only 10.7 percent of domains at strict enforcement, we have not reached that threshold. We are nowhere close.

The maturity gap between enterprise and everyone else makes this worse. Among the Fortune 500, 475 of 500 companies have published DMARC records, and over 80 percent enforce at quarantine or reject. That sounds encouraging until you realize your employees do not only exchange email with the Fortune 500. They exchange email with vendors, partners, contractors, and clients across the full spectrum of organizational maturity. The weakest links in the chain are the ones attackers exploit.

So who is most likely to be hit by an attacker using a spoofed domain? Organizations with less sophisticated email security. Which organizations are most likely to enforce your DMARC policy? Organizations with sophisticated email security. The organizations you actually need protection from are the least likely to enforce your DMARC policy.

Despite Google, Yahoo, and Microsoft tightening sender requirements throughout 2025 and 2026, movement has been slow. The 10.7 percent figure reflects the current state after those mandates took effect.

Outbound Reputation vs. Inbound Threat

Here's the clearest way to think about what DMARC actually does: it protects your domain's reputation outbound. It makes it harder for attackers to use your exact domain as a spoofing vector. It's a lock on your front door.

> *A lock on your front door doesn't stop someone from putting on your face and knocking on your neighbor's door.*

DMARC does nothing to protect you from inbound attacks. It doesn't stop attackers from targeting your employees. It doesn't prevent business email compromise. It doesn't protect against display name spoofing. It doesn't guard against lookalike domains. It doesn't prevent account compromise. These are the threats that actually damage organizations.

A CFO receives an email that looks like it came from the CEO. The sender address shows the CEO's name. The request is urgent, time-sensitive, and carries authority. The CFO transfers half a million dollars. How did DMARC protect against this? It didn't. The attacker used a lookalike domain, a common name variation, or compromised an external vendor's account. DMARC is irrelevant in all of these scenarios.

The FBI's IC3 reported $3.0 billion in losses from business email compromise attacks in 2025 alone. The vast majority came from attacks that DMARC would never catch: lookalike domains, compromised vendor accounts, display name spoofing, account takeovers. These aren't exact domain spoofing.

What DMARC Cannot Protect You From

Lookalike domains are the most straightforward gap. An attacker registers a domain one letter different from yours. Your DMARC policy covers acmecorp.com, not acmecorpp.com. The lookalike passes through entirely.

Display name spoofing is even simpler. An email comes from noreply@thirdparty.com but the display name says "CEO." DMARC checks the sending domain, not the display name. They don't intersect.

Compromised vendor accounts are common and devastating. An attacker compromises your vendor's email system and sends emails that pass all DMARC checks because they're actually coming from the vendor's infrastructure.

Account compromise within your own organization is perhaps the most dangerous. An attacker compromises an employee's email account and sends emails from it. The email passes DMARC because it's actually coming from your infrastructure. DMARC can't stop it by design.

These aren't edge cases. These are the primary vectors in actual email-based attacks.

The Attacker's DMARC

Here's something most CISOs haven't considered: attackers deploy DMARC too.

When an attacker registers a lookalike domain, one of the first things a sophisticated operator does is configure SPF, DKIM, and DMARC on that domain. They set it to p=reject. The phishing email your employee receives from acmecorpp.com doesn't just pass DMARC. It passes with flying colors. If anything, the attacker's DMARC configuration makes the email look more trustworthy, not less.

> *A well-configured lookalike domain with proper authentication may actually receive better inbox placement than a poorly configured legitimate domain. The attacker invested five minutes in DNS configuration. Your security stack rewarded them for it.*

Security tools that give weight to DMARC pass/fail as a trust signal are actively being gamed by this approach. The presence of valid DMARC on a sending domain tells you exactly one thing:

somebody configured DNS records. It tells you nothing about whether the sender is who your employee thinks they are.

This is not a theoretical concern. StrongestLayer's threat research team analyzed 5,000 email-based attacks that evaded secure email gateways between December 2025 and February 2026. An important caveat on that dataset: it measures attacks that survived existing defenses, not the total threat landscape. It reveals what is actually getting through, not what is being attempted. With that framing, the findings are striking: 56.4 percent of those surviving attacks used domain lookalike techniques. That figure is directionally consistent with Cloudflare's broader observation that domain spoofing and impersonation remain the dominant vectors in emails that fail or bypass authentication checks. Every one of those lookalike domains can carry a fully valid DMARC configuration. The attacker's DMARC is not an edge case. It is the majority pattern in attacks that reach the inbox.

The Coverage Gap in Numbers

Exact domain spoofing, the one attack vector DMARC was designed to prevent, accounts for a declining share of email-based attacks. Across enterprise environments, exact domain spoofing represents roughly 5 to 10 percent of successful email-based compromises. The other 90 to 95 percent use techniques DMARC was never designed to address.

Even within that 5 to 10 percent, DMARC's protection is partial. It requires two things to work: the spoofed domain must have published a p=reject policy, and the receiving mail server must enforce it. Major receivers like Gmail and Microsoft 365 do enforce DMARC, so that side of the equation works for most enterprises. The bottleneck is on the sending side: only 10.7 percent of domains worldwide publish p=reject. When an attacker spoofs one of the other 89.3 percent, there is simply no policy for the receiver to enforce. The effective coverage is roughly 10.7 percent of 5 to 10 percent. That is around 1 percent of your total email threat surface.

StrongestLayer's evasion research adds texture to this gap. Recall that their dataset measures attacks that survived existing defenses, so these figures describe what is getting through, not what the total landscape looks like. With that framing: 14 percent of those 5,000 attacks succeeded through pure social engineering with zero technical evasion signatures at all. No malicious links, no weaponized attachments, no domain tricks. Just language crafted to manipulate the recipient. DMARC has no mechanism to address this. Neither does any authentication protocol.

Another 27.8 percent used telephone-oriented attack delivery, where the email contains nothing but a phone number and a pretext. These attacks are architecturally invisible to header-level analysis. The average attack in the dataset layered 4.11 evasion techniques simultaneously, meaning the threat surface is not a set of discrete vectors but a combinatorial problem that authentication alone cannot decompose.

> *A compromised legitimate account passes SPF, DKIM, and DMARC with flying colors. The email is real. The infrastructure is real. The authentication is valid. DMARC was not designed to catch this, and it never will be.*

This directional pattern is not unique to StrongestLayer's dataset. Proofpoint's and Abnormal Security's published threat research shows similar trends: the volume of attacks using lookalike domains, social engineering, and supply chain compromise has grown relative to exact domain spoofing year over year.

This is not an argument against deploying DMARC. It is an argument against treating DMARC as though it covers more than it does. One percent protection is worth having. But it should not consume a disproportionate share of your email security attention, budget, or risk narrative.

The Compliance Trap

One reason DMARC deployment is so widespread despite its limited real-world impact is that it appears on compliance checklists. This creates a powerful incentive to deploy it: organizations want to check the box.

This is the compliance trap. It's a form of audit theater where organizations implement controls because they're required for compliance assessment, not because they're the most effective security measures available. DMARC deployment looks good in an audit. But it doesn't demonstrate that your organization has reduced email-based threat risk. The compliance value and the security value are almost completely disconnected.

This matters because security budgets are finite. Resources allocated to DMARC deployment and monitoring are resources not allocated to controls that would actually reduce email-based compromise risk: user training, business process controls that verify unusual requests, technical controls that identify malicious intent regardless of sender domain, and verification systems for high-risk transactions.

Why DMARC Breaks in the Real World

Email forwarding breaks DMARC. When an email is forwarded, the message is re-sent from a different server and may no longer pass authentication checks. Third-party services that send email on your behalf create similar problems: newsletters, customer service systems, marketing automation, HR platforms. Each needs to be added to your SPF record or DKIM-signed by your infrastructure.

ARC (Authenticated Received Chain) was introduced specifically to address the forwarding problem by preserving authentication results across intermediary hops. Major providers like Gmail use ARC signals to override a DMARC reject policy for forwarded mail. While ARC helps with the forwarding gap, it does nothing to expand DMARC's scope to cover lookalike domains, display name spoofing, or compromised accounts. It solves a plumbing problem, not the fundamental coverage limitation.

Shadow IT compounds this constantly. Business units use email-sending services that security teams don't know about. Managing DMARC in a real organization is a perpetual game of whack-a-mole. This operational complexity is invisible in the compliance frameworks. But it's very real in operational practice.

The False Security Problem

An organization deploys DMARC. They set it to p=reject. They document it. They tell their security team that email spoofing has been addressed. This reduces the perceived risk in the CISO's mind. That perception influences resource allocation. Other security initiatives get deprioritized because the team believes the spoofing problem is solved.

But the spoofing problem, narrowly defined, is solved only against receiving mail servers that enforce DMARC. Against 70.9 percent of the email ecosystem, it is a suggestion that gets ignored.

> *When a CISO believes DMARC is protecting the organization from email-based attacks, they're vulnerable to a specific kind of failure: the thing they think they've protected against isn't the thing actually attacking them.*

A broken technical control is obvious. You see the failure. You investigate. You fix it. A control that works partially but creates a false sense of comprehensive protection is insidious. You don't see failures because you're not looking for them where the risk actually lives.

How to Talk About This With Your Board

If you're a CISO who reports to a CFO or a board, you need language that explains the DMARC gap without sounding like you're asking for more budget. Here's a framework.

Start with what you've done. "We've deployed DMARC at enforcement level. This prevents attackers from sending email using our exact domain to organizations that enforce the standard. This addresses a compliance requirement and protects our brand reputation in the portions of the email ecosystem that participate."

Then explain the coverage gap. "DMARC addresses exact domain spoofing, which represents roughly 5 to 10 percent of email-based attacks. Cloudflare's 2026 data shows only 10.7 percent of domains enforce DMARC at the strictest level, and 46 percent of all emails still fail validation entirely. That limits our real-world protection to roughly 1 percent of the total email threat surface."

Then frame the actual risk. "The threats that cause the largest financial losses—business email compromise, compromised accounts, and supply chain attacks—all pass DMARC validation entirely. Our deployment is necessary for compliance and baseline hygiene. But it does not reduce our exposure to the attack types that drove over $3.0 billion in BEC losses in 2025."

> *DMARC satisfies the audit requirement for email authentication. But email authentication and email security are not the same thing. Authentication verifies that an email comes from who it claims. Security determines whether an email is a threat. Those are different problems requiring different controls.*

The Right Question

Should you deploy DMARC? Yes. It's infrastructure hygiene. It belongs in your stack the same way locks belong on your doors.

But the right question is not whether to deploy DMARC. The right question is the one most organizations have not asked yet: “What email-based threats pose the biggest risk to our organization, and what controls would actually protect us?”

When you answer that question with honesty and data, you will find that exact domain spoofing is a small fraction of your exposure. You will find that DMARC covers roughly 1 percent of your real email threat surface. And you will find that the threats driving the largest losses require controls that understand intent, context, and organizational relationships, not just sender authentication.

DMARC will find its appropriate place in your strategy. It will not be the centerpiece. It will be one small part of a much larger program. And recognizing that distinction is the first step toward building email security that actually works.

The next generation of email security does not ask whether the sender passed authentication. It asks what the email is trying to accomplish, whether the sender should be asking for it, and whether the request is reasonable given the organizational context. DMARC headers remain a useful input signal within that broader reasoning, but they are one data point among many. Intent analysis, behavioral context, communication pattern history, and relationship verification are the controls that address the 99 percent of the threat surface that authentication alone cannot reach.

Sources

Cloudflare 2026 Email Security Report. Analysis of 450 million daily emails covering DMARC validation rates, SPF failures, and DKIM adoption. https://blog.cloudflare.com/2026-threat-report

DMARC Adoption Report via RedSift (2026). Survey of 990,232 domains measuring DMARC policy distribution and enforcement levels. https://dmarcdkim.com/dmarc-adoption

EasyDMARC DMARC Adoption Report 2026. Global adoption trends and enforcement gap analysis across industries. https://easydmarc.com/blog/ebook/dmarc-adoption-report-2026

SC Media, “Email authentication in 2026: What every organization still gets wrong.” Analysis of endemic misconfiguration patterns. https://www.scworld.com/resource/email-authentication-in-2026

FBI Internet Crime Complaint Center (IC3). Business Email Compromise losses data ($3.0 billion in 2025; 2025 Internet Crime Report). https://www.ic3.gov

StrongestLayer Evasion Technique Combinations Research (2026). Analysis of 5,000 email-based attacks that evaded secure email gateways, December 2025 through February 2026. StrongestLayer Threat Research

---

Muhammad Rizwan is Chief Technology Officer and Co-Founder of StrongestLayer, where he leads the engineering and research teams building AI-native email security. Prior to co-founding StrongestLayer, Muhammad held senior engineering leadership roles across enterprise security infrastructure.

Version: 1.0 | Date: April 2026 | Muhammad Rizwan, Chief Technology Officer
Contact: riz@strongestlayer.ai | strongestlayer.com/resources