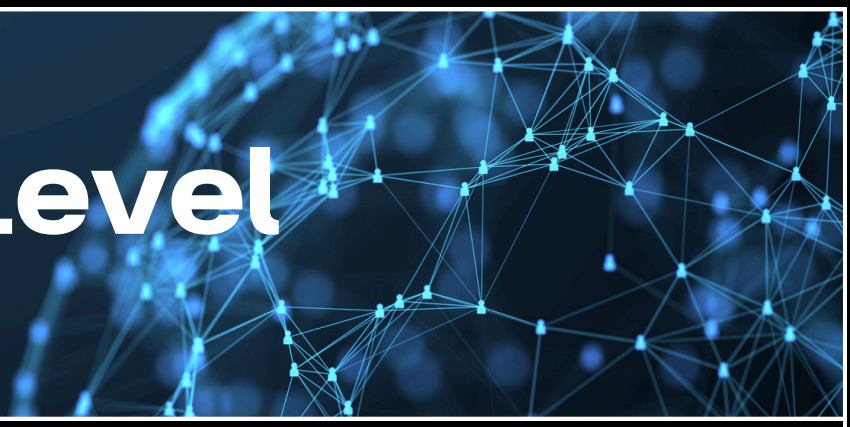
PREPARED BY
Technology By Design

Domain-Level Security



Your domain name is more than just your email address or website; it's a core part of your digital identity. Threat actors routinely target business domains to impersonate, spoof, or hijack them for fraudulent purposes. Without strong domain-level security, attackers can erode customer trust, bypass email filters, or impersonate executives to execute wire fraud and phishing campaigns.

How Can We Help?

Our domain-level security services establish, monitor, and enforce protections around your business's digital footprint. Key functions include:

Implementing domain-level security gives your organization foundational protection that enhances email trust, safeguards your brand, and helps ensure that your communications are always authenticated and secure.

- **SPF (Sender Policy Framework) Configuration**
- **DKIM (DomainKeys Identified Mail) Setup**
- **DMARC (Domain-based Message Authentication, Reporting & Conformance) Enforcement**
- **DNS Security Practices**
- **Ongoing Review and Reporting**

Why It Matters?

Securing your domain ensures that only authorized systems and people can send messages on your behalf. It prevents impersonation, protects your brand, and reduces your organization's exposure to Business Email Compromise (BEC), phishing, and other forms of digital fraud. As email authentication standards become increasingly required for compliance and delivery, domain-level security is no longer optional, it's essential.