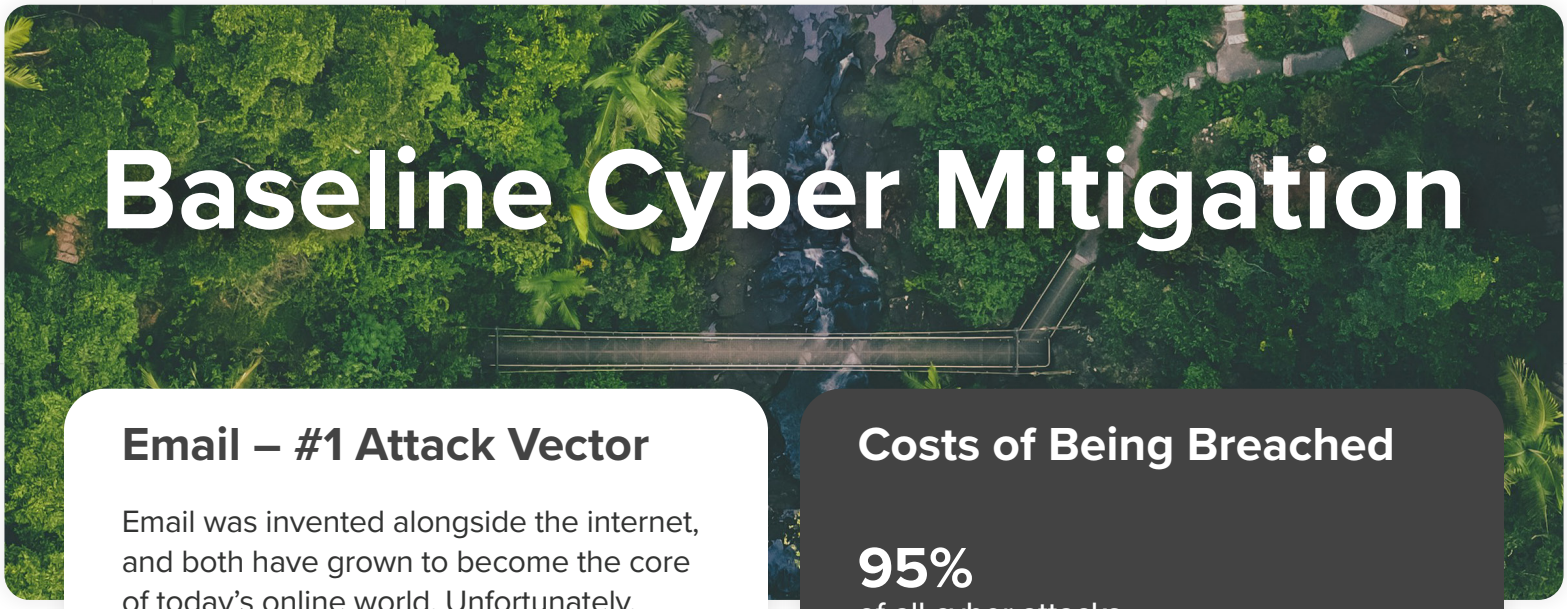
dmarcian



Baseline Cyber Mitigation

Email – #1 Attack Vector

Email was invented alongside the internet, and both have grown to become the core of today's online world. Unfortunately, **by default, anyone can send email pretending to be someone else, which is why email is the #1 attack vector.**

DMARC is built upon SPF & DKIM to create links between email and internet domains.

- **SPF** is a way of publishing a list of servers that are authorized to send email on behalf of a domain. **DKIM** is a method of adding a tamper-proof domain seal to a piece of email.
- **DMARC** brings consistency to how these are configured so that a check is performed to see if the email really does come from the domain it says it does.

Costs of Being Breached

95%
of all cyber attacks begin with phishing
cisa.gov

88%
of organizations reported at least one phishing attack
Verizon Data Breach Insights Report

$2.9 billion
in losses from Business Email Compromise
2023 FBI Internet Crime Report

DMARC – Foundational Cyber Defense

Email lacks the ability to verify the authenticity of the sender; this vulnerability is exploited by cyber criminals. DMARC solves this problem by giving email domain owners visibility on who is sending emails on their behalf, which can help prevent abuse and unauthorized use.

DMARC is an open-source, DNS-based specification that establishes an enforcement policy for authorizing outbound email. Because it is DNS based, **DMARC is a public facing, provable record that an organization is doing their due diligence to protect their email and the people who depend upon it.**

Mitigating Cyber Risk

- Ransomware, Financial Transfer Fraud, Phishing—mitigating cyber risk can be complicated, but it starts with securing the #1 cyber attack surface: email.
- **DMARC allows you to control who can send email using your internet domains,** bringing Zero Trust to the world's #1 communication medium.
- By deploying DMARC with dmarcian, your organization protects the #1 cyber attack surface while creating an operational process to tackle more complicated cyber risks.

Avoid mitigating just the symptoms – remediate cyber risk by systematically controlling who can use your internet domains and the services that run on top of them, starting with email.

DMARC Benefits

- **Email Fraud:** DMARC's original use-case. DMARC provides visibility of how a domain is used and prevents unauthorized senders from sending email on behalf of an organization.
- **Email Reliability:** Organizations need email to be reliable. DMARC is the foundation for reliable email delivery, and is often the first step taken to resolve email delivery issues.
- **Compliance:** Industries, governments, and regulations are increasingly requiring DMARC to be in place. It is also becoming a requirement for many cybersecurity insurance providers.

dmarcian Solutions

Through our DMARC Management Platform, we process data, categorize sources, and alert you of potential threats. Together with our Deployment Services and Dedicated Support teams, we aim to make your journey through DMARC as easy and informative as possible.

dmarcian's Mission

dmarcian is dedicated to upgrading the entire world's email by making DMARC accessible to all. We have offices around the world in key locations of North America, Europe and Asia Pacific. From small governmental organizations to Fortune 500 companies, dmarcian has an international track record for helping organizations across the globe and of all sizes successfully deploy DMARC. dmarcian is fully self-funded, so our focus is on our clients, not an investor group.