

Symantec Email Fraud Protection

Automate DMARC enforcement

Without email sender authentication, anyone can send email using your company's identity to spoof your executives, employees, and brand. Criminals can easily send emails using your exact email domain to devastating effect. For example, impersonating your organization by sending emails to your clients or other partners in order to commit fraud, which damages your reputation. Sender authentication provides another layer of defense to stop these attacks, at a time when email impersonation attacks are on the rise.

Spear-phishing emails are the most widely used attack vector, employed by 71% of target attack groups. 1 in 33 users received a phishing attack in Dec 2017. (ISTR 23, Symantec)

Getting it right is critical

It is essential to implement sender authentication correctly to realize the full benefits. Get it wrong and you may inadvertently block good email from being delivered. Unfortunately, implementing DMARC at enforcement is hard, and most organizations fail because they take a manual, one-time project approach to enforcement. They underestimate both the complexity and need for never-ending maintenance. In fact, the majority of companies attempting email authentication fail to ever achieve success (defined as blocking the spoofed email but still letting the good email through). More importantly, even fewer manage to stay at enforcement because they don't have an automated platform that addresses the technical issues to get to and stay at enforcement.

Automating DMARC Enforcement with Symantec

Symantec Email Fraud Protection

- Achieve DMARC enforcement faster (average 180 days)
- Catalogs thousands of third-party email services, single click to approve who can send email on your behalf
- Automatically provides the correct SPF, DKIM, and DMARC configuration, and solves the SPF 10 domain lookup limit (patented)



Symantec Email Security.Cloud or Messaging Gateway

- Integrates with Email Fraud Protection to support SPF, DKIM and DMARC standards to block email impersonation attacks
- Blocks spam, malware and phishing attacks with advanced multi-layered defense
- Minimize malware and phishing risk by opening links safely with Email Threat Isolation



Comprehensive Email Security

- Defends your organization from spam, malware, phishing and advanced attacks
- Protects internal and external recipients from spoofing attacks
- Increase recipient confidence in your email domain and therefore, in your brand

Our recommendation? Use a fully automated sender authentication solution that makes DMARC enforcement easy and accessible, and couple this with a robust Secure Email Gateway solution from Symantec.

Challenges with the manual approach to enforcement

Obtaining 100% sender visibility

It takes considerable effort to identify all traffic on the domain name, find all third-party senders, and verify who to approve with your organization's business owners. Manually inspecting a large volume of DMARC reports (thousands of lines of XML with IP and header information) and identifying all third-party services accurately is next to impossible. Also, many cloud apps that send email use infrastructure from popular ESPs (Email Service Providers), making it hard to distinguish between multiple apps on a shared cloud. No wonder most organizations end up with an incomplete picture.

Working with unforgiving open source standards

DNS was not designed to provide email authentication and pre-dates today's world of cloud services that send email on your behalf. It is a static secure database with no concept of cloud services or dynamic responses, has no error handling, and is often closely guarded by IT and subject to strict change control. It can take weeks to move through the IT bureaucracy and effect a single SPF, DKIM, or DMARC change; typically, organizations need to make hundreds of changes. And making authentication record changes in DNS must be done in TXT which is quite error-prone. When it comes to SPF, most organizations cannot manually overcome the SPF ten domain lookup limit, resulting in their SPF authentication breaking.

Dealing with a resource intensive process

Organizations typically commit significant staff resources to the manual process of establishing and maintaining DMARC enforcement. Not only does this tie up scarce security and messaging personnel, it puts pressure on other high-priority security projects at a time when CIOs and CISOs are challenged to do more with less. Protecting the enterprise from email impersonation with the least impact on staff resources is critical.

Symantec Email Fraud Protection

The Symantec automated cloud service for sender authentication makes every step to DMARC enforcement simpler and more seamless compared with all other methods. Enforcement allows recipients to quarantine or reject all emails that originate from unauthenticated sources. Having achieved enforcement, email receivers/Mail Transfer Agents know they can trust your domain.

Symantec Email Fraud Protection supports SPF, DKIM, DMARC, ARC and BIMI; providing extensive reporting that gives domain owners 100% visibility into all email traffic using their domains. Authorizing senders is simple with a one-click process. Symantec Email Fraud Protection does this by cataloging thousands of SaaS and third-party emailing services, and dynamically updating configuration changes for you. We build and maintain a global whitelist of approved third-party senders on your behalf, so you don't have to. Symantec Email Fraud Protection simplifies the process of ongoing maintenance by dynamically mapping services and providing customers with the ability to add or remove approved services with one-click. Extensive reporting is also provided, giving you full visibility into all senders and traffic sent using the domain. Critical privacy standards are complied with as Symantec Email Fraud Protection does not use personally identifiable information (PII).

Get started, quickly

Symantec Email Fraud Protection guides customers along a journey to email authentication enforcement. Customers need only point a DMARC record to the Symantec cloud and we'll automatically analyze aggregated and anonymized DMARC reports. An easy to understand report of all senders utilizing that domain is provided; your only role is to have business owners confirm that the observed senders are both legitimate and authorized to send on your behalf. Assuming the services are both legitimate and authorized, we will enable these services to continue sending once enforcement is enabled. All other services and senders that spoof email (i.e. those not on the whitelist) will get blocked by the email recipient. Once at enforcement only mail from legitimate senders is allowed with unauthorized mail being either quarantined or rejected, giving customers a critical new layer of security.

Rock-solid impersonation protection starts with email authentication enforcement

Symantec Email Fraud Protection helps organizations overcome the complexity of achieving sender authentication. Combining fully automated DMARC enforcement with Symantec's industry-leading secure email gateway provides a rock-solid defense against both advanced and more traditional phishing attacks. Symantec Email Fraud Protection works alongside both Symantec Email Security.Cloud and Symantec Messaging Gateway, as part of a comprehensive email security system to defeat spam, malware, data loss and mitigate phishing and impersonation attacks.

Find out more www.symantec.com/products/messaging-security.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com, subscribe to our [blogs](#), or connect with us on [Facebook](#), [Twitter](#), and [LinkedIn](#).



350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com