DARKTRACE

Darktrace / EMAIL - DMARC

Brings enterprise-grade email authentication to organizations of all sizes, without the complexity or cost of traditional solutions.

It streamlines SPF/DKIM/DMARC deployment with guided setup, smart alerts, and continuous monitoring to stop spoofing, improve deliverability, and ensure compliance with evolving standards. Unlike outsourced services, it keeps you in control with full visibility into your email infrastructure and third-party senders. It also supports BIMI logo verification to strengthen authenticity and trust in every communication.

A new layer of trust beyond the inbox

Most DMARC solutions are expensive, service-heavy tools that externalize risk and limit visibility. They often require outsourcing configuration and monitoring, making organizations dependent on third parties and disconnected from important insights.

Many are also overbuilt, putting them out of reach for smaller enterprises. A more flexible, cost-effective way to protect domains, ensure deliverability, and keep up with evolving email authentication standards is needed.

That's where Darktrace comes in.

Why DMARC?

Email remains the most targeted vector for cyber-attacks, with phishing and domain spoofing continuing to rise in both volume and sophistication.

Attackers often impersonate trusted brands to deceive recipients, evade filters, and deliver malicious content. DMARC (Domain-based Message Authentication, Reporting & Conformance) helps prevent these attacks by verifying sender identity and directing email providers on handling unauthenticated messages. Major providers now require DMARC for bulk senders, starting with a p=none policy. Strong DMARC policies reduce domain spoofing, credential phishing, and CEO-style impersonation targeting employees.

Benefits

- **Comprehensive anti-impersonation and brand defense** to block attackers from sending emails that appear to come from you.
- **Attack surface reduction and infrastructure visibility** by ensuring only trusted senders can deliver message on your behalf.
- **Enhanced deliverability and trust** to ensure authenticated emails reach inboxes.
- **Full ownership, transparency, and flexible deployment** so you retain complete control over your records.
- **Intuitive, step-by-step setup and management** so DMARC deployment is rapid and error-free, with tailored instructions.
- **Lowers the barrier to entry for email authentication** by simplifying the process of implementing best-in-class security.
- **Data-rich analytics and proactive monitoring** so you can easily visualize authentication performance and spoofing activity.
- **Secure mail delivery enforcement with MTA-STS and TLS,** ensuring safe server communication.
- **Granular third-party control** with Domain Breakdown, so you can maintain a clean, trusted SPF configuration.
- **Flexible data export capabilities** for deep analysis, with DMARC reports in multiple formats for custom workflows.

Requirements

Darktrace / EMAIL – DMARC is only available for **Microsoft 365 / Office 365 users**.

Customers do not require any other product to purchase or use Darktrace / EMAIL – DMARC.

16%

of successful breaches in 2024 were caused by phishing, making it the most common initial vector for gaining entry.[1]

[1] IBM Cost of a Data Breach 2025

Feature	Darktrace / EMAIL - DMARC	Most competing vendors at similar price points
Sending Service Identification (TPS)	Large network of sending services	Limited network of sending services
Add New Sending Services	Custom TPS	Custom TPS not supported
SPF/DKIM/DMARC Record Management	■ Recommendations for setting up valid records to protect your brand identity ■ Visibility over all records in your domain	Limited to number of domains
Brand indicators for Message Identification	Complete BIMI support	None/Minimal support
Active Domain Monitoring	Up to 10,000 domains	<15
Users	Unlimited	1
DMARC-Capable Messages per Month	Unlimited	<100,000
Data History	12 months minimum	<3 months
Domain Groups	100	Additional cost
Enriched DMARC Data with Sources	Yes	Yes
Automatic Subdomain Detection	Yes	Yes
SPF/DKIM/DMARC Checker	Yes	Yes
Unlimited Inactive Domains	Yes	Yes
DMARC Report Processing (RUA)	Yes	Yes
Two-Factor Authentication	Yes	Yes
MTA-STS	Yes	Yes
TLS Reporting	Yes	Yes
Data Exports	Yes	Yes
Alert Central	Roadmap	No
RUF Processing	Yes	No
Forensic Report Analysis	Roadmap	No
User Access Controls	Yes	No
Single Sign On	Yes	No