

DMARC Visualization

Business Email Compromise (BEC) is one of the most costly and successful forms of cybercrime today, often bypassing traditional security tools by impersonating trusted executives, vendors, or partners. Without DMARC protection, attackers can forge your domain to send fake invoices, phish employees, or trick customers into transferring funds, all while appearing completely legitimate. Implementing DMARC provides your security team with visibility and control over who is authorized to send emails on your behalf.

Spoofed email attacks are on the rise. According to the [FBI](#), BEC has resulted in over \$50 billion in reported losses worldwide over the past nine years, with a 65% increase in global exposed losses in recent years.

Benefits:

Improved Deliverability & Trust
Minimize legitimate email rejection with more accurate SPF & DKIM policies

Comprehensive Visibility
Easily manage email sources across the company in one dashboard

Enhanced Fraud Prevention
Gain confidence in tightening up your DMARC rules with domain traffic mapping

Streamlined DMARC Management
Automation prevents human error of tracking & configuration

Key Features:

- Comprehensive Email Source Mapping**
Identify every server and IP sending emails on your behalf.
- Real-Time Email Authentication Insights**
See whether messages are passing or failing SPF and DKIM checks and quickly identify misconfigurations or spoofing attempts.
- IP Reputation & Sender Classification**
Tag senders as internal, trusted third-party, or malicious. Maintain a clean sender ecosystem and streamline responses to suspicious activity.
- Email Volume Analytics**
Track the volume of emails sent per IP address to detect unusual activity, spot spikes in traffic, and uncover potential abuse or misrouted traffic.
- Low-Risk Monitoring & Domain Status Visibility**
Use "monitor mode" to observe your ecosystem before enforcing policies. View all your domains, including DMARC, SPF, and DKIM configuration status, no guesswork required.

Aggregate Report Summary						
From Domain	First Report	Last Report	IP Addresses	Message Count	SPF Pass %	DKIM Pass %
netcraft.com			3,855	626,730	95.2%	97.1%
ikonbank.com			1,020	145,304	4.8%	97.1%
epycbrands.com			21	61,672	99.6%	0.0%
zephyralr.com			452	19,538	34.6%	78.8%
northkind.com			12	16,205	98.3%	88.8%
acmeusa.com			1,354	12,335	6.2%	91.1%

How it works:

- Email Activity is Reported**
 - When you add a DMARC record to your domain, email providers that receive messages from your domain start sending summary reports. These reports show who sent the emails and whether they passed authentication checks.
- Reports Are Sent to Netcraft**
 - Your DMARC record is set up to send these reports directly to Netcraft.
- Netcraft Turns Reports into Insights**
 - Netcraft processes the information into easy-to-understand dashboards. You'll see which IP addresses are sending email from your domain, whether they passed SPF and DKIM checks, and how many emails they sent.
- You Identify Good and Bad Senders**
 - With clear visuals, you can quickly recognize unauthorized senders and confirm legitimate ones. This helps you adjust your email security settings with confidence.

Netcraft provides brand protection services for many of the world's largest brands: