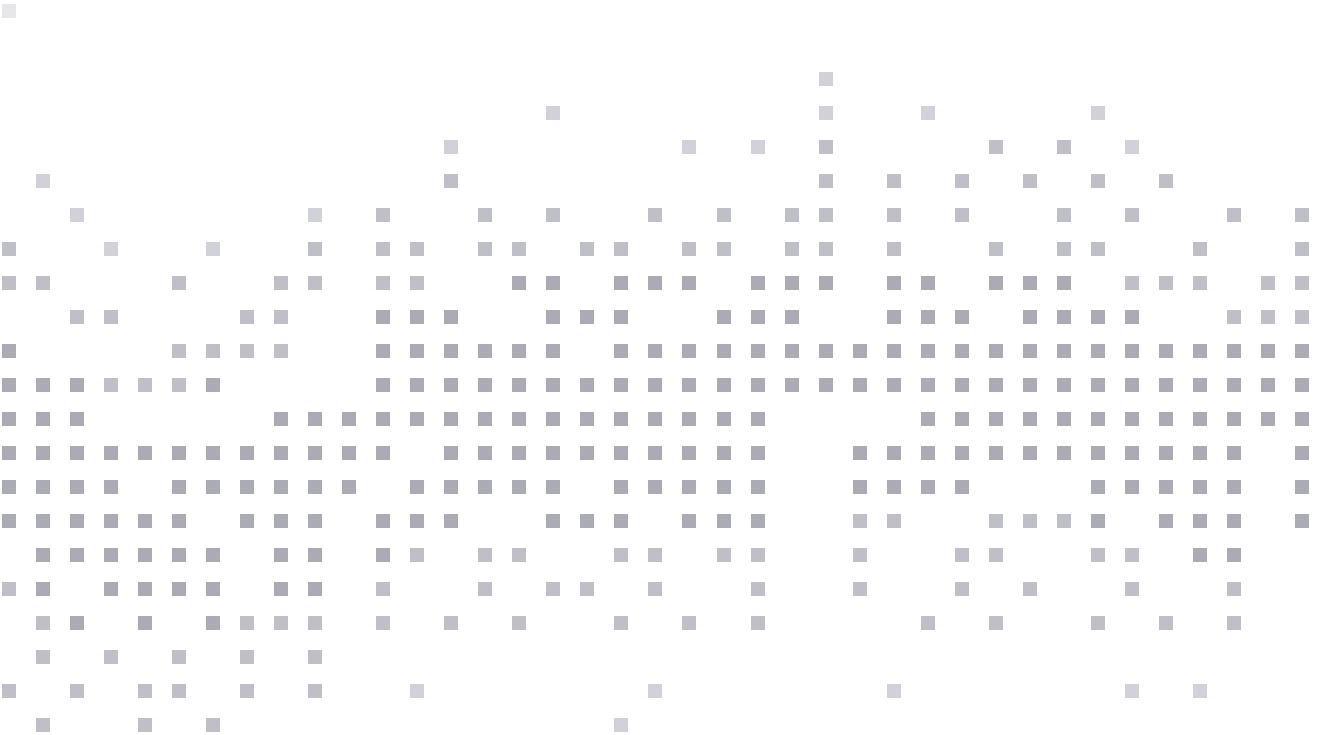




Email security & deliverability report

Prepared by Summit Managed Services · Jul 7, 2026



Prepared for **Acme Corporation**

1 domain analyzed

Domain analyzed

example.com

50/100

Email security score

High risk

1

High risk issue

1

Medium risk issue

Security findings

Identity protection (DMARC)	Warning
Your DMARC is enforcing security, but you are not monitoring authentication results.	
Sender verification (SPF)	Secure
You have a valid list of approved IP addresses authorized to send email for your domain.	
Digital signature (DKIM)	Critical
You are not cryptographically signing your emails. Receivers trust your messages less.	

Domain analyzed

example.com

CHECK	STATUS	RISK	CATEGORY
Identity protection (DMARC)	Warning	Medium risk	Security
Sender verification (SPF)	Secure	Low risk	Deliverability
Digital signature (DKIM)	Critical	High risk	Deliverability

Findings detail

Identity protection (DMARC) Add a rua=mailto: address to your DMARC record to receive daily XML reports. Without it, you have no visibility into which emails pass or fail authentication.	Warning
Sender verification (SPF) Keep this record updated when you add new email services (CRM, marketing tools, etc). Each new sender must be included in the SPF record.	Secure
Digital signature (DKIM) Set up DKIM with your email provider: add the DNS record they provide, then enable signing in your mail settings. Most providers support it.	Critical

Common threats

Phishing & credential theft

Attackers impersonate your domain to trick employees and customers into revealing passwords or sensitive data.

Business email compromise

Criminals spoof executive email addresses to authorize fraudulent wire transfers. These attacks cost billions annually.

Brand, reputation & deliverability damage

When your domain is used for spam or phishing, providers flag your legitimate emails as suspicious, damaging sender reputation.

Frequently asked questions

■ How is this going to help me grow my business?

Strong email authentication builds trust with customers and partners. When your emails consistently reach inboxes instead of spam folders, your marketing campaigns perform better, sales communications get through, and your brand maintains its professional reputation.

■ Isn't DMARC set and forget?

DMARC requires ongoing monitoring and maintenance. New email services, marketing tools, and infrastructure changes can break authentication. Without continuous oversight, you risk deliverability issues or security gaps going unnoticed.

■ How does DMARC increase my revenue?

Proper DMARC implementation improves email deliverability by 10-20% on average. More emails reaching inboxes means higher open rates, better engagement, and increased conversions from your email marketing and sales outreach.