Securafy

Human Led. AI Driven. Prevention-First.™

★ SOTERIA AWARD 2024

ADVANCED DOMAIN
SECURITY REPORT

securafy.com

10
/10

Grade A — Excellent — fully protected

Email authentication posture · 100% secured

Your domain is well configured. Continue monitoring for new senders.

90%	$2.9B	72%	48h
Of attacks start with email	BEC losses annually (FBI IC3)	Of domains missing DMARC	Fix time with Securafy

PREPARED FOR
Randy Hall
Securafy Inc.
rhall@securafy.com

PREPARED BY
Securafy Security Team
securafy.com · sales@securafy.com
(330) 906-8888

THIS REPORT COVERS

Report Date: May 8, 2026

CONFIDENTIAL — For authorized recipients only

rhall@securafy.com · (330) 906-8888

securafy.com

What this report shows you

This Advanced Domain Security Report evaluates securafy.com's email authentication posture against six critical protocols. Attackers exploit misconfigured email domains to spoof executives, impersonate your brand, and commit wire fraud. This report shows your exact configuration, where gaps exist, and how to close them — typically in under 48 hours.

10
/10

Grade A — Excellent — fully protected

Email authentication posture · 100% secured

& Your domain is well configured. Continue monitoring for new senders that may need authentication.

SPF PASS 3/3 pts	DMARC PASS 4/4 pts	DKIM PASS 2/2 pts	BIMI PASS 1/1 pts
MTA-STS WARN 0/1 pts	MIME/MX WARN 0/1 pts	Blacklist INFO —	Score PASS 10/10

90% Of attacks start with email

$2.9B BEC losses annually (FBI IC3)

72% Of domains missing DMARC

48h Fix time with Securafy

What this report contains →

SPF | DMARC | DKIM | BIMI | MTA-STS | MIME/MX | Blacklist

SPF — Sender Policy Framework

PASS 3/3 pts

v=spf1 include:_spf.securafy_com._d.easydmarc.pro -all

SPF with hard fail (-all). Optimal configuration.

DMARC — Domain-Based Message Authentication

PASS 4/4 pts

v=DMARC1;p=reject;sp=reject;pct=100;rua=mailto:b517bf990d@rua.easydmarc.us

DMARC p=reject — maximum protection. Includes reporting.

DKIM — DomainKeys Identified Mail

PASS 2/2 pts

selector1, selector2, dkim, mandrill (Microsoft 365)

DKIM configured — 4 selectors across Microsoft 365 and senders.

BIMI — Brand Indicators for Message Identification

PASS 1/1 pts

v=BIMI1;l=https://www.securafy.com/hubfs/Logos/FlatSecurafyLogo.svg;a=

BIMI with VMC — logo appears in Gmail/Apple Mail.

MTA-STS — Mail Transfer Agent Strict Transport

WARN 0/1 pts

No MTA-STS record

MTA-STS not configured. This control enforces TLS on inbound SMTP — preventing email interception. Add _mta-sts TXT record and host policy at https://mta-sts.securafy.com/.well-known/mta-sts.txt

MIME / MX Configuration

WARN 0/1 pts

Provider: Microsoft 365 | MX: 1

Mail via Microsoft 365 (S/MIME capable). S/MIME is not DNS-verifiable — contact Securafy to audit deployment.

Blacklist Status — 7 DNSBL Lists Checked

INFO —

2 IP(s) — hosted infrastructure

Domain resolves to shared cloud infrastructure (15.197.225.128, 3.33.251.168). Blacklist checks on shared provider IPs produce false positives and are skipped. Check your sending IPs directly at mxtoolbox.com if needed.

SPF Lookup Chain — 5/10 lookups

INCLUDE: _spf.securafy_com._d.easydmarc.pro

IP4: 63.251.72.0/24	IP4: 107.150.159.0/24	IP4: 64.95.96.240/28
IP4: 40.92.0.0/15	IP4: 40.107.0.0/16	IP4: 52.100.0.0/15
IP4: 52.102.0.0/16	IP4: 52.103.0.17	IP4: 104.47.0.0/17
IP6: 2a01:111:f400::/48	IP6: 2a01:111:f403:/49	IP6: 2a01:111:f403:8000::/51
IP4: 3.93.157.0/24	IP4: 3.210.190.0/24	IP4: 18.208.124.128/25

May 8, 2026

rhall@securafy.com · (330) 906-8888

securafy.com

Email authentication isn't optional anymore.

Google, Microsoft, and Yahoo require DMARC alignment for bulk senders — and cyber insurance carriers verify these controls at underwriting. Missing even one creates a gap attackers will exploit.

THE FOUR PROTOCOLS THAT PROTECT YOUR DOMAIN

DMARC — CRITICAL

Domain-based Message Authentication, Reporting & Conformance

The policy layer. Tells receiving servers what to do with email that fails authentication — monitor (p=none), quarantine to spam, or reject outright (p=reject). Without p=reject anyone can spoof your domain. Also generates reports showing every service sending as your domain.

SPF — CRITICAL

Sender Policy Framework

A DNS record listing every server authorized to send email on behalf of your domain. Missing or permissive SPF (using ~all instead of -all) is one of the most common gaps. Requires updating whenever you add new email-sending services.

DKIM — HIGH

DomainKeys Identified Mail

A cryptographic signature verifying email wasn't modified in transit. Must be configured for every service sending on your behalf — M365, Google Workspace, your CRM, marketing platform, and billing system each need separate selectors.

BIMI — MEDIUM

Brand Indicators for Message Identification

Displays your logo in supported inboxes (Gmail, Apple Mail, Yahoo) when DMARC, SPF, and DKIM all pass. Requires a verified mark certificate and DMARC p=quarantine or p=reject. Turns authentication into visible brand trust.

FIVE REAL BUSINESS RISKS

Business Email Compromise — #1 Financial Cyber Crime — $2.9B annual BEC losses — FBI IC3

Without DMARC enforcement, attackers spoof your CEO's exact email to trick employees into wire transfers. $2.9B in annual BEC losses — most victims had no email authentication.

Cyber Insurance — Missing Auth Voids BEC Coverage — Carriers verify DMARC at renewal

Major carriers verify DMARC, SPF, and DKIM at underwriting and renewal. Missing authentication can result in denied BEC coverage at the exact moment you need it.

Google & Microsoft Sender Requirements — DMARC required since Feb 2024

Google and Yahoo require DMARC alignment for bulk senders. Organizations without it see legitimate emails going to spam or being rejected — affecting invoicing, sales, and client communications.

Compliance — HIPAA, GLBA, CMMC, CJIS — Cited in audit findings

HIPAA, GLBA, CJIS, and CMMC all include requirements protecting communications. Email authentication is increasingly cited in audit findings as a required control organizations fail to implement.

Customer & Partner Trust — Brand Risk — Your domain weaponized against clients

When attackers spoof your domain to phish your customers, the reputational damage is yours. Your brand becomes associated with fraud even though you weren't breached.

What this means for securafy.com

securafy.com currently scores 10/10 with DMARC at p=reject — the highest enforcement level. Your SPF, DKIM, and BIMI are all passing. MTA-STS is the one remaining gap: without it, a sophisticated attacker could downgrade inbound SMTP connections and intercept email in transit. This is the only action item. Securafy can deploy MTA-STS for you in under 15 minutes.

May 8, 2026
rhall@securafy.com · (330) 906-8888
securafy.com

Step-by-Step Remediation Plan

Step 1 — Deploy DMARC
Week 1 · 15 min

Add TXT at _dmarc.securafy.com: v=DMARC1; p=none; rua=mailto:dmarc@securafy.com

Starts collecting data without affecting mail flow.

Step 2 — Enable DKIM
Week 1 · 30 min

In M365: Admin Center > Security > Email Auth > DKIM > Enable.

Add the 2 CNAME records to DNS. Repeat for every sending service (CRM, marketing, billing).

Step 3 — Harden SPF: ~all to -all
Week 1 · 5 min

Change SPF from soft-fail (~all) to hard-fail (-all).

Verify all senders are in your SPF record first by reviewing DMARC reports.

Step 4 — Deploy MTA-STS
Week 1 · 15 min

Add _mta-sts TXT record and host policy file at https://mta-sts.securafy.com/.well-known/mta-sts.txt

Enforces TLS on inbound SMTP. Eliminates your only remaining gap.

Step 5 — Escalate DMARC to p=reject
Weeks 2–4

Move p=none > p=quarantine > p=reject over 2–4 weeks.

Monitor DMARC reports at each step. At p=reject, spoofing your domain becomes impossible.

REMEDIATION TIMELINE

Week 1	Week 2	Week 3	Week 4
Deploy DMARC + DKIM + Fix SPF + MTA-STS	Review reports · Verify all senders	Escalate to p=quarantine	Escalate to p=reject

Your only action item: MTA-STS

securafy.com scores 10/10 on everything else. Here is the exact fix:

1. Add DNS TXT record: _mta-sts.securafy.com → v=STSv1; id=20260508
2. Host policy file at: https://mta-sts.securafy.com/.well-known/mta-sts.txt
3. Policy file content: version: STSv1 | mode: enforce | mx: *.securafy-com.mail.protection.outlook.com | max_age: 86400
4. (Optional) Add TLS-RPT: _smtp._tls.securafy.com → v=TLSRPTv1; rua=mailto:tlsrpt@securafy.com
5. Verify with: https://mxtoolbox.com/mta-sts/

YOUR NEXT STEP

These vulnerabilities are fixable in under 48 hours.

Securafy's engineers have deployed DMARC, DKIM, MTA-STS, and SPF hardening for hundreds of Ohio businesses. We handle every DNS change, verify propagation, and monitor your DMARC reports — stopping anything that shouldn't be sending as your domain.

Soteria Award 2024
Most Trusted MSP North America — peer-validated, not self-declared.

Zero Client Ransomware Incidents
ThreatLocker Zero Trust + layered security. Zero incidents post-onboarding.

10-Minute Response Guarantee
Certified engineer responds within 10 minutes any time, any day. In writing.

35+ Years of Excellence
Formed from three firms est. 1989–2011. Not a startup. Not a pivot.

WHAT SECURAFY DELIVERS

Essential-CARE
$95–$115/mo
24/7 NOC, help desk, patching, M365, EDR, backup, dark web monitoring.

Secure-CARE
$155–$185/mo
Everything in Essential + ThreatLocker Zero Trust, Cyber Hero 24/7 SOC, SIEM, email security.

Comply-CARE
$210–$260/mo
Everything in Secure + GRC platform, vCISO, quarterly pen testing, HIPAA/CMMC/CJIS.

- ✓ Free 47-Point Network & Security Assessment — $2,500–5,000 value — no obligation
- ✓ 30-Day Risk-Free Trial — full service, zero payment, walk away before day 30
- ✓ 90-Day No-Penalty Exit Window — we earn your business every quarter
- ✓ 10-Minute Response Guarantee — any time, any day, in writing in your contract

Book My Free Strategy Call

(330) 906-8888
Call directly:

★ SOTERIA AWARD 2024

★ SOTERIA AWARD 2024 — Most Trusted MSP North America

Zero ransomware incidents · securafy.com · sales@securafy.com · (330) 906-8888