VARONIS

REMEDIATION

EMAIL RISK ASSESSMENT

PREPARED FOR AETHERION RESEARCH

CRITICAL FINDINGS

0 10 20 30 40 50 60 70

TOC

TABLE OF CONTENTS

WHY DID AETHERION RESEARCH START A VARONIS EMAIL RISK ASSESSMENT?

Aetherion Research has a board-level mandate to strengthen defense against social engineering. Beyond traditional email-based phishing, a new class of advanced attacks now blends text, images, links, and behavioral cues delivered via multiple channels. These attacks evade both humans and legacy tools.

To understand its exposure to these evolving threats, Aetherion Research launched this assessment to evaluate organizational risk across multiple attack vectors:

Plain-text BEC

Lateral phishing

Abuse of trusted senders

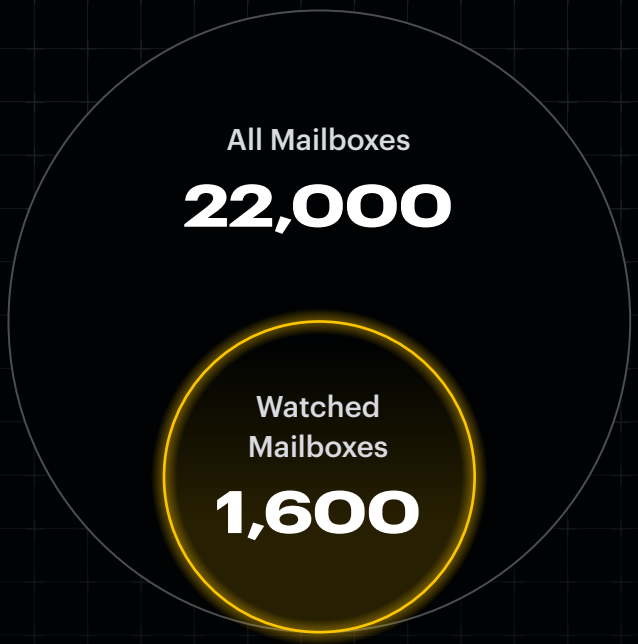
Abuse of trusted websites

Supply chain–based phishing campaigns

SCOPE

AETHERION RESEARCH'S RISK ASSESSMENT OVERVIEW

The assessment examined current risks and included a three month retrospective analysis to uncover past threats that were not detected by the existing email security solution, focusing on key departments and high value individuals.



Departments

+ Marketing
+ Sales
+ Engineering
+ Legal
+ HR

Key Individuals

+ CEO
+ CFO
+ CRO
+ CTO
+ CHRO

CRITICAL FINDINGS

8,000 Threats Missed

by the existing email security solution

615K+
Phishing link and QR attacks

15.3K+
Targeted BEC threats

1.9K+
Malicious attachments

1,290
Social engineering attacks

21,000 Spam & Bulk

emails flagged

10K+
Marketing ads

6.3K+
Sales outreach

235
Announcements

4,290
Hybrid spam

BUSINESS IMPACT

Business Impact Summary

Email-based attacks put organizations at risk of identity compromise, financial loss, and operational disruption. This assessment quantifies Aetherion Research's exposure and highlights the measurable improvements in threat protection and ROI.

2,434
Total phishing threats mitigated

415
High-impact phishing threats mitigated[1]

136
BEC threats mitigated

$137,132
Average cost of successful BEC attack[2]

$695,074
High-impact phishing cost exposure mitigated[3]

1,255
Number of mailboxes targeted

16-30 min
SOC OpEx saved per phishing investigation[4]

Most attacked users

These are the top recipients of phishing emails within your organization.

Display Name	Email	Department	Threat Count
Mia Renshaw	mia.renshaw@aetherion-research.com	Legal	78
Lucas Thornwell	lucas.thornwell@aetherion-research.com	Sales	76
Erin Callister	erin.callister@aetherion-research.com	Legal	52
Dante Hargrove	dante.hargrove@aetherion-research.com	Legal	44
Sophie Durant	sophie.durant@aetherion-research.com	HR	41
Julian Mercer	julian.mercer@aetherion-research.com	Legal	39
Talia Greystone	talia.greystone@aetherion-research.com	Sales	36
Caden Westfall	caden.westfall@aetherion-research.com	Engineering	34
Rhea Lonsdale	rhea.lonsdale@aetherion-research.com	Legal	31
Harper Vecchio	harper.vecchio@aetherion-research.com	HR	28

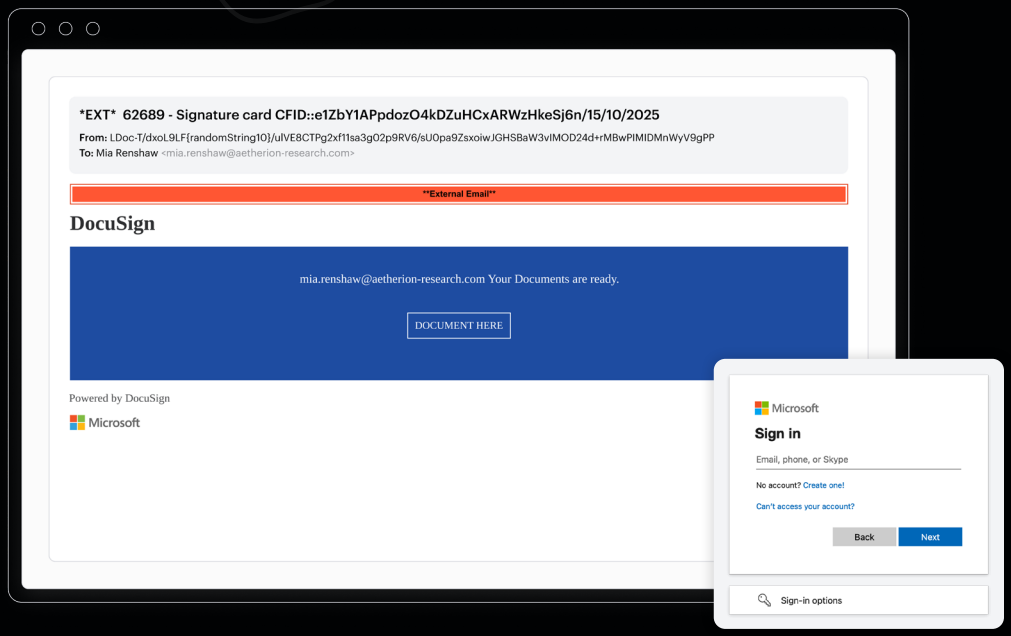
Top malicious email senders

These are the top 10 malicious email senders for your organization.

Display Name	Email	Domain	Threat Count
--	inbox@follow2.com	follow2.com	42
--	mailer@thebullishtrader.com	thebullishtrader.com	36
Stock Market Monster	mailer@stockmarketmonster.com	stockmarketmonster.com	36
Daily Stock Watcher	mailer@dailystockwatcher.com	dailystockwatcher.com	32
Ever Crest Invest	mailer@evercrestinvest.com	evercrestinvest.com	28
DailyDelli Trending News	team@newsdelli.com	news.dailydelli.com	27
--	mailer@conservativeinvestingnews...	conservativeinvestingnews.com	27
--	mail@shrellefurnishings.com	shrellefurnishings.com	27
--	mailer@novaheartinvesting.com	novaheartinvesting.com	24
Investing District	info@investingdistrict.com	investingdistrict.com	20

ATTACK SPOTLIGHT #1

DocuSign Credential Phishing



Attack description:

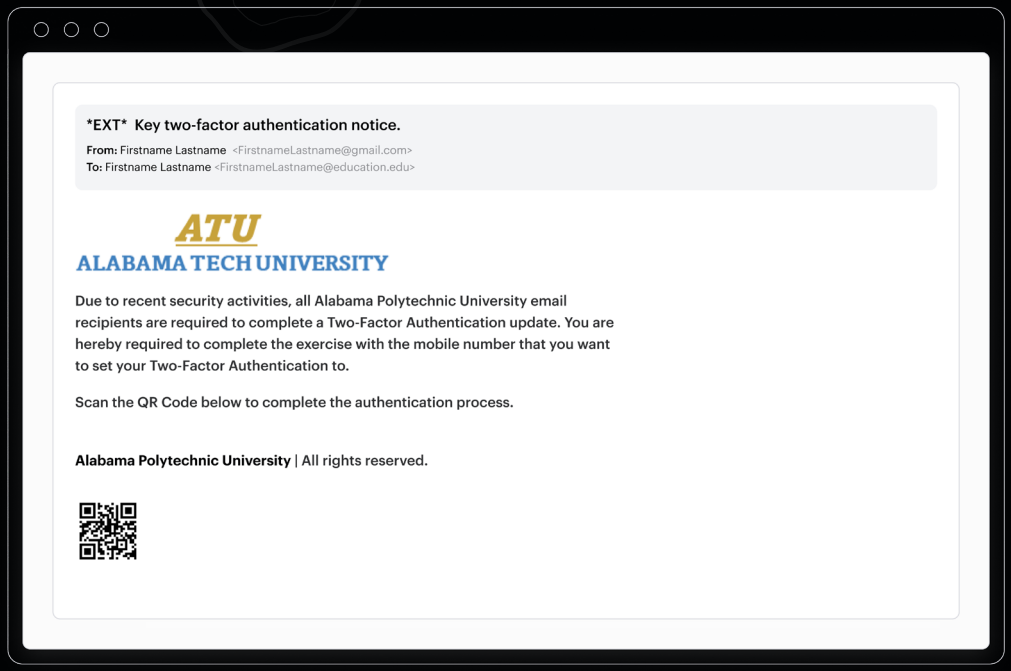
The attacker impersonated the DocuSign brand to trick users into entering credentials. The email linked to a convincing landing page designed to harvest authentication details.

Why other solutions miss this:

The attack relied on a trusted hosted site (dynamics.com) and employed multiple evasion techniques, such as browser fingerprinting, CAPTCHA challenges, and IP filtering, to bypass traditional email security tools.

ATTACK SPOTLIGHT #2

QR Code Phishing



Attack description:

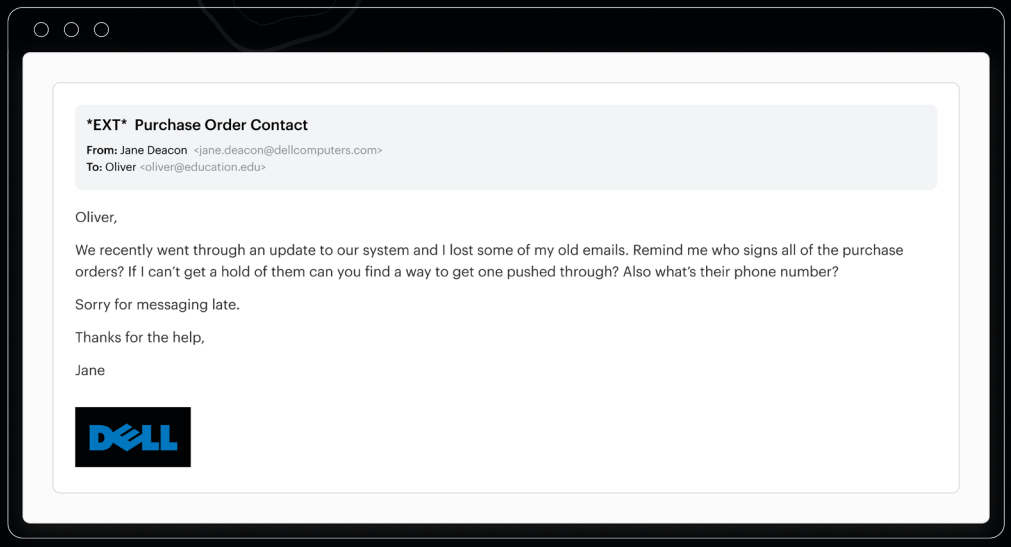
The attacker embedded a QR code to conceal a malicious URL and redirect recipients to a fake login page on their mobile device. These pages steal credentials while appearing legitimate.

Why other solutions miss this:

Few security tools can interpret QR codes or analyze the URLs they contain. This attack originated from a trusted Gmail sender and used a reputable hosted site (wixsite.com), further reducing detection likelihood.

ATTACK SPOTLIGHT #3

BEC: Vendor Email Compromise



Attack description:

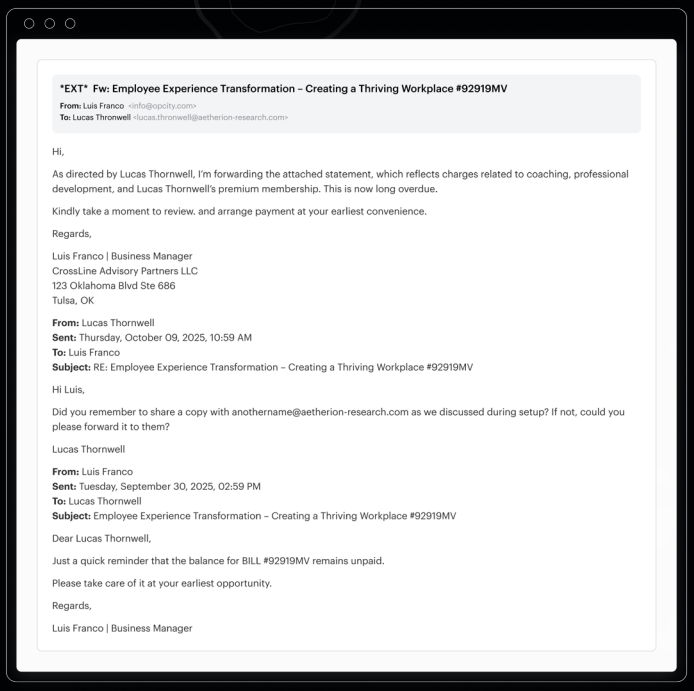
The supplier's email account is taken over or impersonated and used to send fraudulent messages that trick the victim into paying fake invoices or sharing sensitive information.

Why other solutions miss this:

Vendor email compromise attacks succeed because attackers hijack trusted vendor threads and send plain-text, highly contextual messages that easily bypass legacy filters, especially when no links or attachments are present. They bypass existing supply-chain defenses because many email security tools focus on simple relationship graphs. In this case, the attack is coming from a trusted user, and the AI-crafted messages leverage history and legitimate workflows that singular behavior models fail to flag as abnormal.

ATTACK SPOTLIGHT #4

BEC: Invoice Fraud



EXT Fw: Employee Experience Transformation – Creating a Thriving Workplace #92919MV

From: Luis Franco <info@opcity.com>
To: Lucas Thronwell <lucas.thronwell@aetherion-research.com>

Hi,

As directed by Lucas Thornwell, I'm forwarding the attached statement, which reflects charges related to coaching, professional development, and Lucas Thornwell's premium membership. This is now long overdue.

Kindly take a moment to review, and arrange payment at your earliest convenience.

Regards,

Luis Franco | Business Manager
CrossLine Advisory Partners LLC
123 Oklahoma Blvd Ste 686
Tulsa, OK

From: Lucas Thornwell
Sent: Thursday, October 09, 2025, 10:59 AM
To: Luis Franco
Subject: RE: Employee Experience Transformation – Creating a Thriving Workplace #92919MV

Hi Luis,

Did you remember to share a copy with anothername@aetherion-research.com as we discussed during setup? If not, could you please forward it to them?

Lucas Thornwell

From: Luis Franco
Sent: Tuesday, September 30, 2025, 02:59 PM
To: Lucas Thornwell
Subject: Employee Experience Transformation – Creating a Thriving Workplace #92919MV

Dear Lucas Thornwell,

Just a quick reminder that the balance for BILL #92919MV remains unpaid.

Please take care of it at your earliest opportunity.

Regards,

Luis Franco | Business Manager

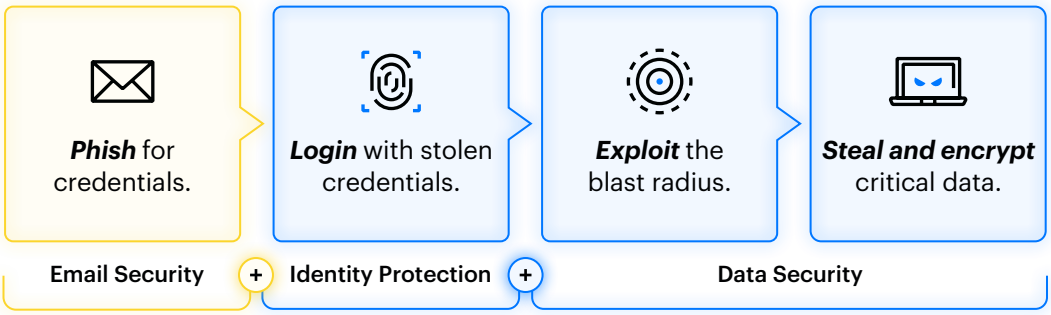
Attack description:

This email impersonates a legitimate invoice request and appears to continue an existing internal conversation. The attacker reinforces credibility by attaching a fake W9 and invoice.

Why other solutions miss this:

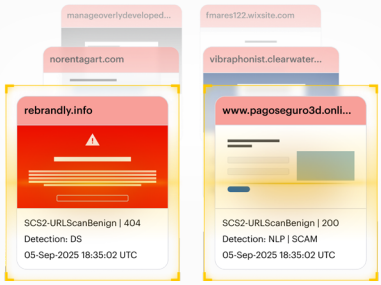
The attacker incorporated accurate business details gathered through reconnaissance, making the request appear authentic. As a clean, language-based attack originating from a known cloudhosting provider, the message contains no indicators that traditional solutions rely on, which makes the intent difficult to detect.

Comprehensive breach prevention at every stage.

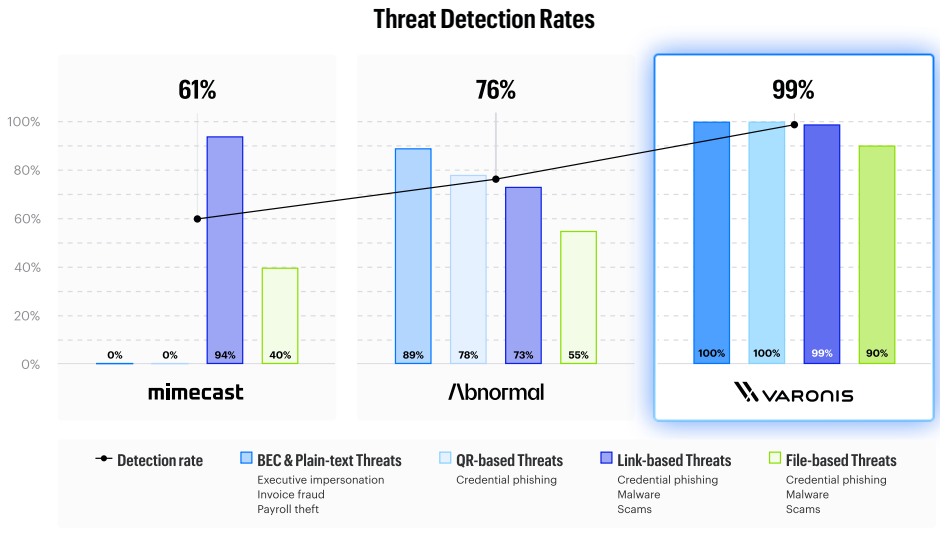


Predictive AI that sees what others can't.

Varonis Interceptor catches advanced business email compromise, social engineering, and phishing attacks that other products simply can't see. Interceptor uses multiple specially trained predictive AI models to see through evasive tactics and remove threats from inboxes in real-time.



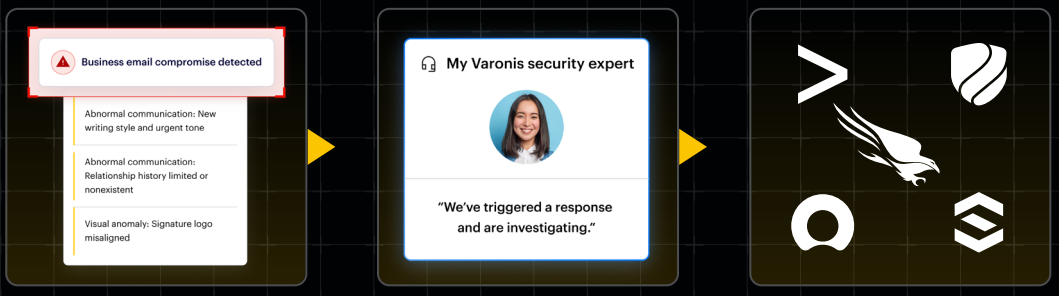
The best detection engine on the planet



24x7x365 MDDR

WE WATCH YOUR ALERTS, SO YOU DON'T HAVE TO.

Always-on detection and response for email, identity, and everywhere data lives.



We monitor everything

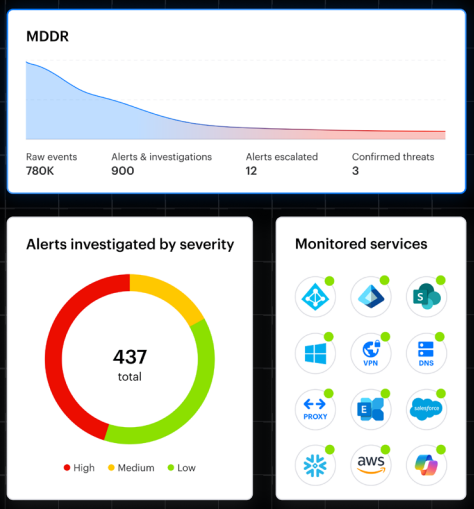
We respond within minutes

Fully integrated with your stack

Immediate time-to-value

Our global team of elite cybersecurity experts solves the challenge of investigating multi-channel threats and their potential impact, with 24x7x365 incident response and alert monitoring.

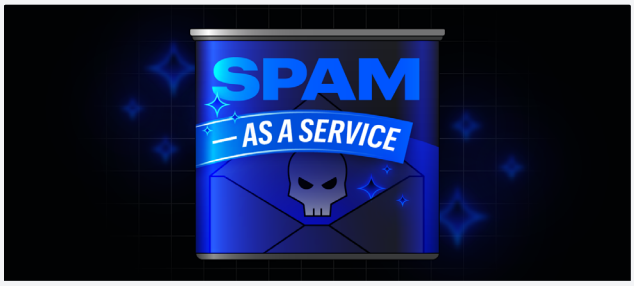
Try Varonis MDDR for free



VARONIS
THREAT LABS

WORLD-CLASS THREAT INTELLIGENCE

Our team hunts for and discloses vulnerabilities and toxic configurations.



SpamGPT: The AI Tool Elevating Email Security Threats for Enterprises

Spiderman Phishing Kit Mimics Top European Banks With A Few Clicks

About Varonis Threat Labs

Our team of security researchers and data scientists are among the most elite cybersecurity minds in the world. With decades of military, intelligence, and enterprise experience, the Varonis Threat Labs team proactively looks for vulnerabilities in the applications our customers use to find and close gaps before attackers can. All these learnings are programmed into our platform to help you stay ahead of cyberattacks.

Check out the latest research: **www.varonis.com/blog/tag/threat-research**

TRUSTED LEADER

Partner with the leader in data security.

Gartner	FORRESTER®	GIGAOM
Named a Customers' Choice by Gartner®	A Forrester Wave™ DSP Customer Favorite	A GigaOm Radar Leader for Data Security Platforms

TRUSTED LEADER

0 10 20 30 40 50 60 70

VARONIS