



From Human Risk to Agentic Risk: Securing the 2027 Business

October 2026



Presenters



Eric Townsend

Proofpoint

*Global MSP Cybersecurity
RMM Lead*

- 2025: Spent over 900+ hours with SMB channel partners
- Involved with Cybersecurity For About 15 Years
- Worked with Various End Customers
 - Finance
 - Manufacturing
 - Retail
- Fun Fact: Avid Reader
- Let's Get Connected
 -  [linkedin.com/in/ericdtownsend](https://www.linkedin.com/in/ericdtownsend)



Presenters



Bill Szumski

Secur-Serv

*VP, Support & Security
Services*

- 25+ years in IT and cybersecurity, specializing in security-first managed services
- Proven track record building and leading high-performing support and security teams in fast-paced MSP environments
- Leads the Secur-Serv team protecting 20,000+ endpoints for over 700 customers nationwide
- Let's Get Connected
 [linkedin.com/in/bill-szumski](https://www.linkedin.com/in/bill-szumski)

Agenda

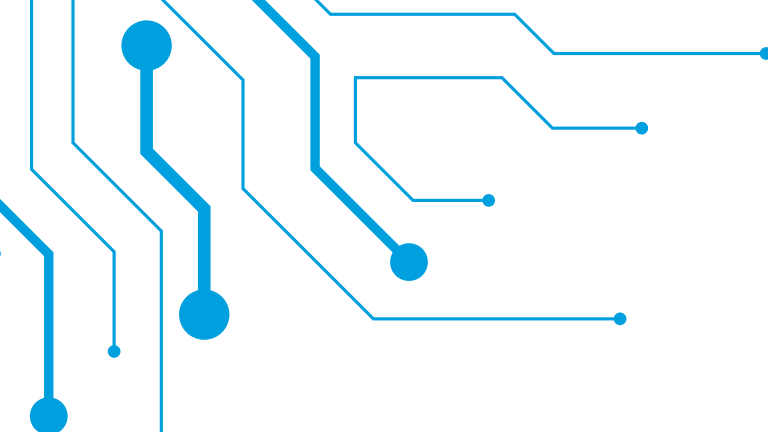
- Secur-Serv + Proofpoint Partnership
- Who Is Proofpoint
- The Front Door to Your Business
- The Evolution of Email Attacks
- 5 Email Security Moves Every Business Should Make Before 2027
- Q & A





Secur-Serv + Proofpoint Partnership





proofpoint. Partnership



Partnership
Value



Enterprise Grade
Solution



Bundled Management
& Full Support



Key Component of
Full Security Stack

Helping stop threats with enterprise grade
security infrastructure for over a decade



Security Operations



Managed **Security Services**



Managed Security Services



60%
cost reduction
by outsourcing
over in-house
cybersecurity
staffing



**Cybersecurity
Awareness
Training**



**Password
Management**



**Security
Operations
Center (SOC)**



**Multi-Factor
Authentication
(MFA)**



**Mobile Device
Management**



**Enhanced Email
Security &
Compliance**



**Managed Detection
& Response (MDR)**



**Endpoint Security
(EDR)**



proofpoint®

Who Is Proofpoint



1 in Every 3 Business Emails Proofpoint Sees

3.4 TRILLION EMAILS SCANNED PER YEAR= 9,315,068,493 Emails SCANNED A Day



Market
Adoption

>2M+

Customers

1.74M

Small & Medium
Businesses

10k

MSPs Using Proofpoint

85%

>60%

FORTUNE
100

85 of the Fortune 100 &
ConnectWise Uses Proofpoint

People Protection



Proofpoint's
Data

3.4T

Emails
scanned per year

>1.4T

SMS/MMS
scanned per year

0.8T

Attachments
scanned per year

21T

URLs
scanned per year

2.2B

Phishing attacks
stopped last year

138M

BEC attacks
stopped last year

395M

Telephone Oriented
Attacks stopped last year



85 of the Fortune 100 Use Proofpoint

World Class Customers with Office 365 Trust Proofpoint

proofpoint.



Gartner Magic Quadrant Leader Again

Leadership Two Years Running- Nine Times In A Row

2025



- Proofpoint is the **most comprehensive email security platform**
- Proofpoint offers a **broader set of email security** and infrastructure tools than its competitors and **strong detection capabilities**
- Proofpoint is responsive to the market's needs - The company **services clients across all sizes and industries**
- For the first time, Gartner planted a flag on M365...
 - *Buyers must consider complementary or supplemental email security solutions to align with best practices for combating modern email threats.*

Poll Question #1

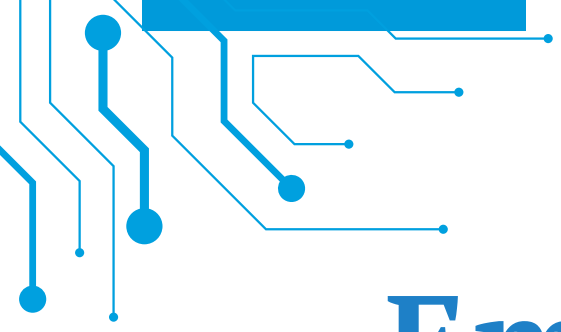
How Are Most Cybersecurity Attacks Started?

(Put Your Answer In The Chat)



Email Is Still the Front Door to Your Business





The 2027 Wake-Up Call: Email Is Still the Front Door to Your Business



Remember (91% of Attacks Start with Email)

Today's Email Security **Reality**



Clarity and outcomes are no longer optional, **they are critical.**

2026 Cybersecurity Trends

Top 10 Business Issues, Technology Priorities & IT Challenges



Source: Techaisle

Cybersecurity by the Numbers

91%

of cyberattacks still start with email

74%

of breaches involved human error

60%

of SMBs say cybersecurity is their #1 business risk

83%

of SMBs experienced a cyber incident in the last 12 months

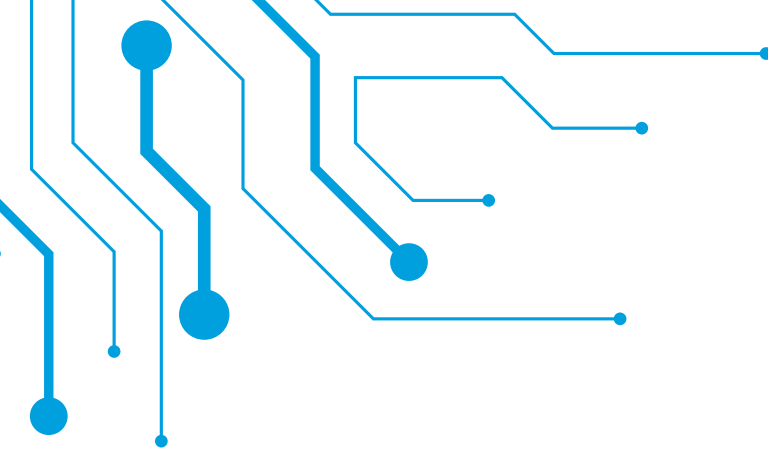
25-40%

increase in cyber insurance premiums YoY



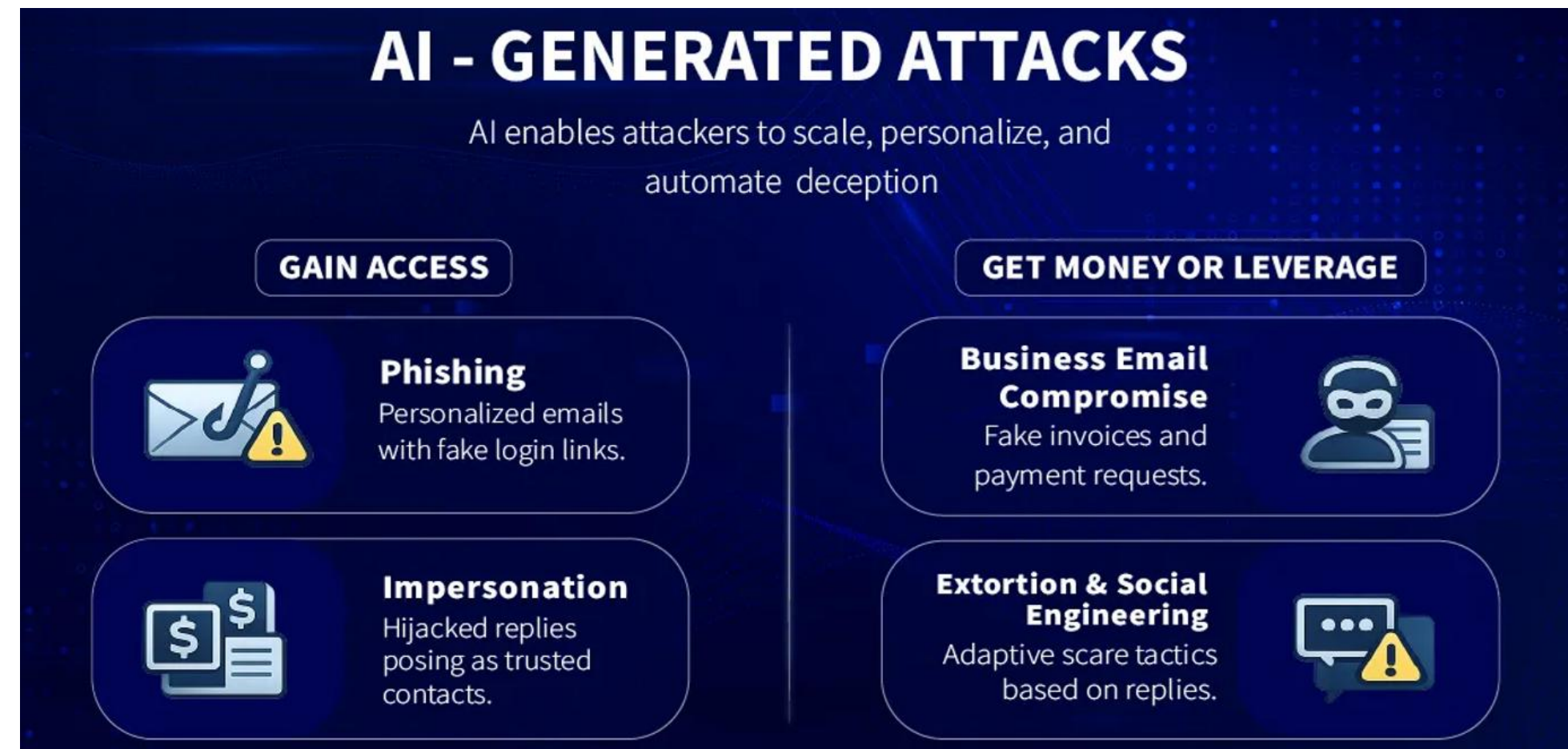
The Evolution of Email Attacks





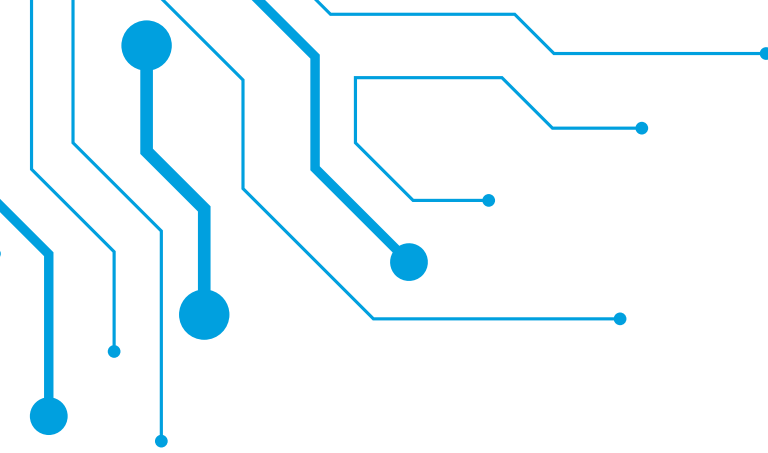
From Phishing to AI-Powered Financial Fraud

- **Traditional Phishing:**
 - Generic emails, malicious links, and suspicious attachments.
- **Modern Phishing:**
 - AI-generated messages tailored to an individual's job, company, and relationships.
- **Business Email Compromise (BEC):**
 - Fraudulent payment instructions, vendor impersonation, and executive impersonation.
- **Account Takeover:**
 - Attackers exploiting compromised Microsoft 365 accounts to send convincing messages from legitimate mailboxes.
- **Conversation Hijacking:**
 - Attackers inserting fraudulent instructions into existing email threads.



Proofpoint Stops Over 66 Million BEC Attacks Every Month





Would You Trust This Email?



Subject: Confidential and Urgent!!! Urgency

Hi Chris,

I need your help with something that's both confidential and extremely urgent. Urgency

Please respond by email ASAP, Urgency I cannot take calls.

Regards,

Frank

Frank Wright
CEO

- No malware.
- No attachment.
- No obviously malicious URL.

Would your current security tools stop this?





The Next Email Security Frontier: When AI Agents Read and Act on Email



Poll Question #2

What is the % increase in AI
Generated Phishing Emails?
(Put Your Answer In The Chat)

AI Is Increasing the Threat Scale



Remember (91% of Attacks Start with Email)

Source: Microsoft

proofpoint.

The Risk Is Already In Your Environment

68% of employees use AI tools IT never approved

50% of organizations expect AI-related data loss within 12 months

47x AI tools found vs. approved in a real enterprise

Employees have deployed AI tools in all varieties of form factors your security team doesn't know about.

Shadow AI, browser copilots, personal ChatGPT, all touching corporate files and data outside any policy.

Agents are creating automated workflows and MCP connections outside your architecture review.

Every SaaS integration, every API an agent connects to a new entry point. Now leveraged by autonomous workflows with no human in the loop. Enterprises can't see every action behind the connections and workflows.

Sensitive data is moving through AI interactions none of your existing controls were designed to see.

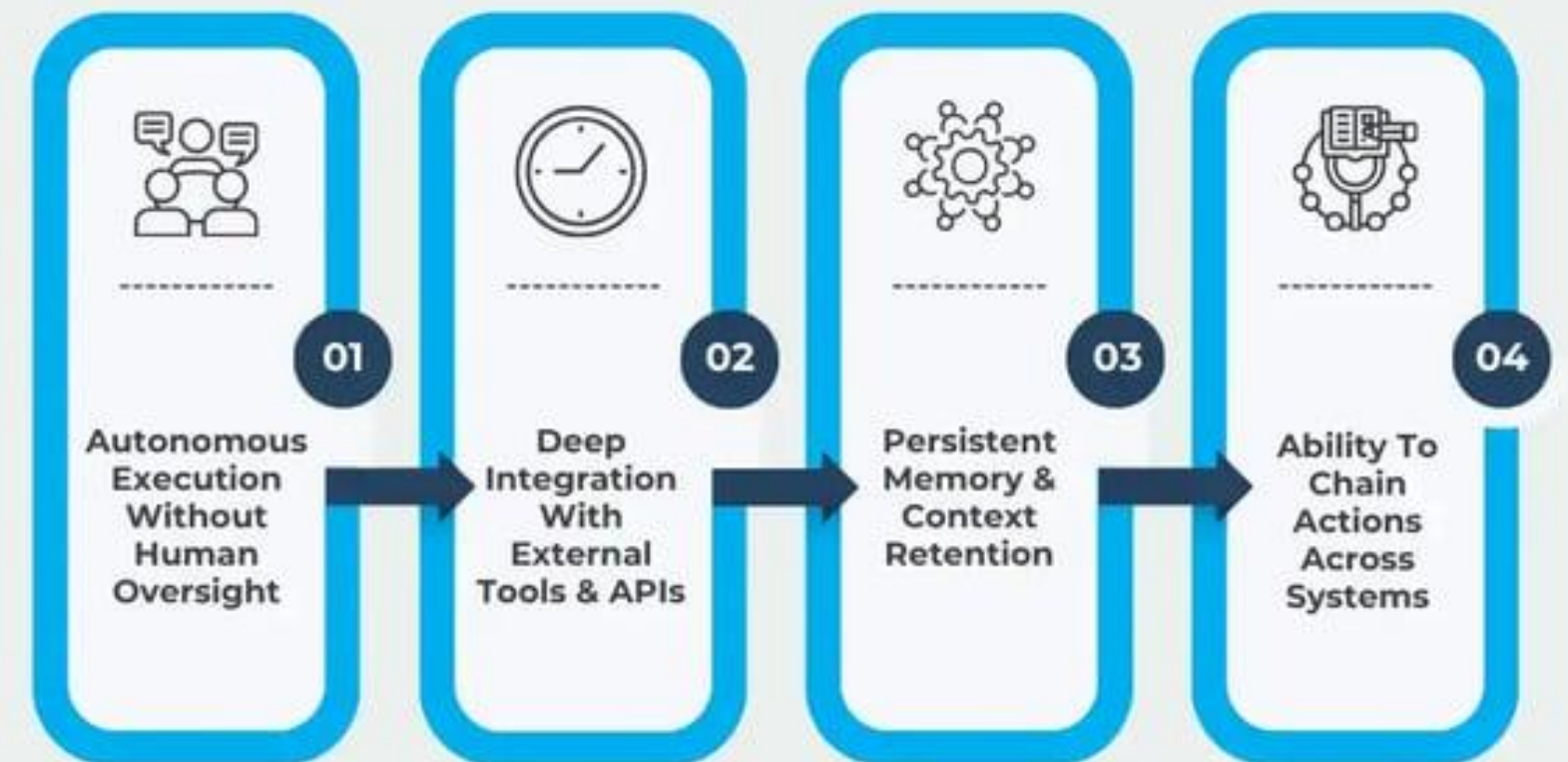
M&A terms in a prompt. HR records surfaced in a response. IP walking out through an AI tool nobody approved. It is happening now, not in the future.

This is not a future problem. It is happening now.

The Agentic AI Risk

- AI assistant that summarizes email vs. an AI agent taking actions based on email content.
- AI agents may interact with Microsoft 365, calendars, customer records, and financial workflows.
 - Malicious instructions hidden in emails or attachments could manipulate an AI agent.
- Risks of unauthorized data access, sensitive information disclosure, and automated business actions.

Why Agentic AI Introduces New Attack Surfaces

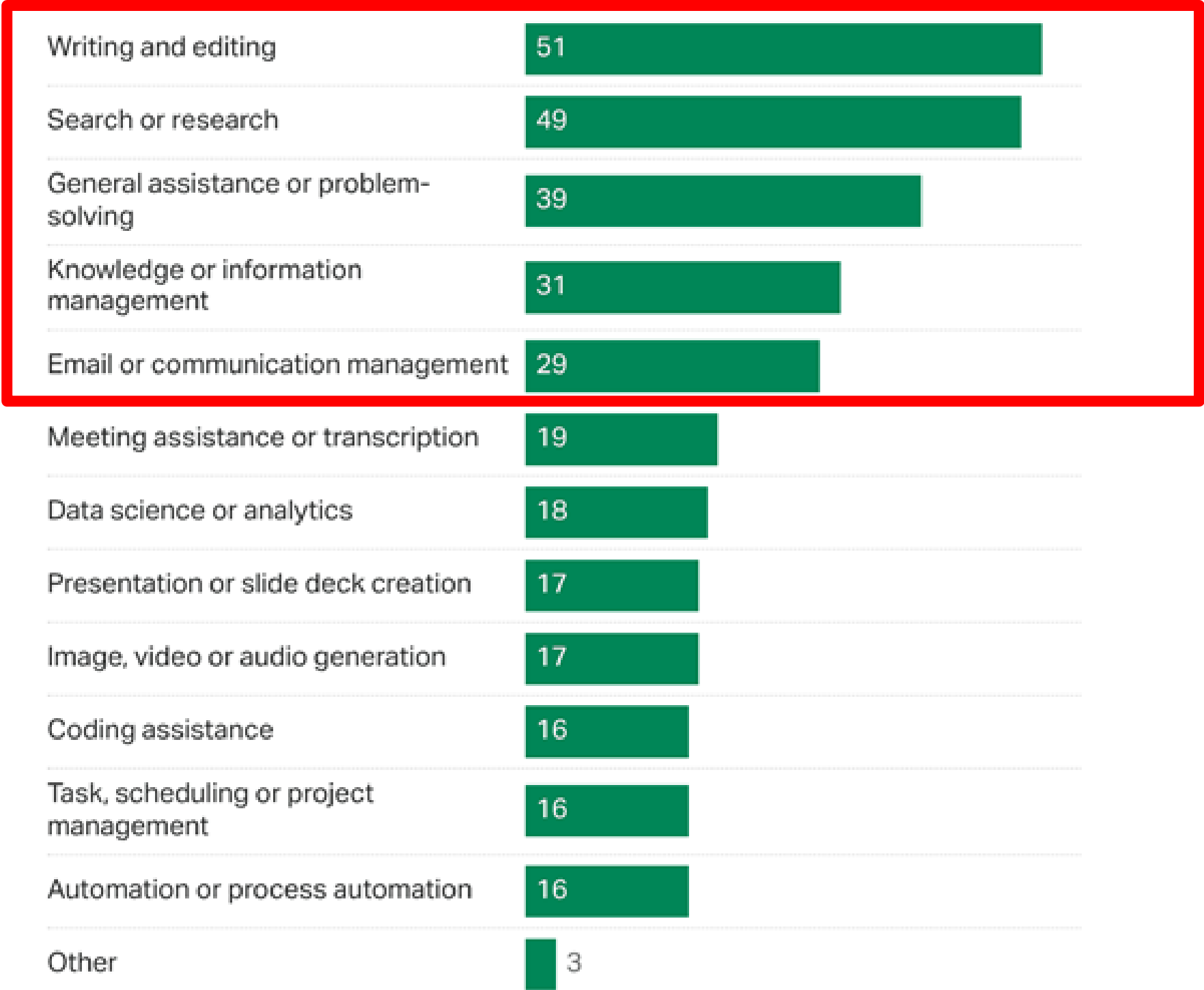


You need to secure not only the employee receiving an email but also the AI system processing it.

Email Management by AI is one of the most common applications for employed Americans

What do you currently use AI tools for? Select all that apply.

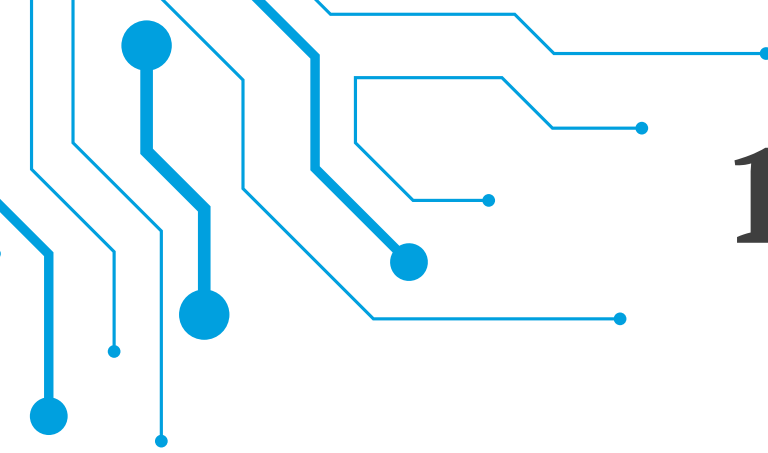
% Selected



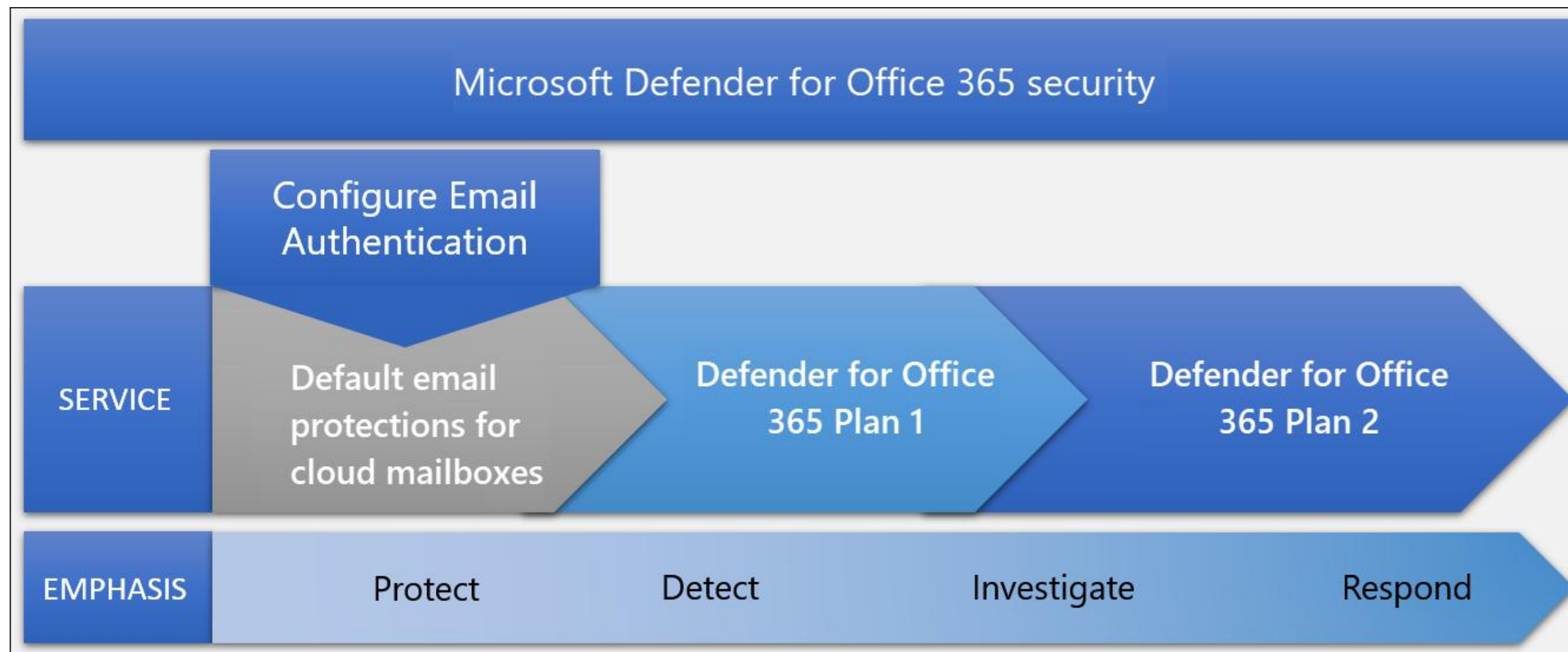


5 Email Security Moves Every Business Should Make Before 2027





1. Strengthen Microsoft 365 Email Protection



For the first time,
Gartner® planted a flag
on M365...

*Buyers must consider
complementary or
supplemental email
security solutions to
align with best
practices for combating
modern email threats.*

- Evaluate advanced phishing, malicious URL, attachment, impersonation, and account-compromise defenses beyond baseline configurations.

What happens when the attacker uses the same trusted ecosystem you're trying to protect



Microsoft powers your collaboration. Proofpoint powers your **defenses**.

90%+

of cyberattacks start with email

Email remains the #1 initial-access vector.

27%

of advanced threats are not detected by Microsoft

Microsoft misses more than one out of every four threats targeting your employees.

\$26/mo

is how much it costs an attacker to test Microsoft's defenses

Adversaries have a low barrier to entry to find out exactly what Microsoft can't stop.

2. Protect Business Identities and Trusted Communication.



Best Practices

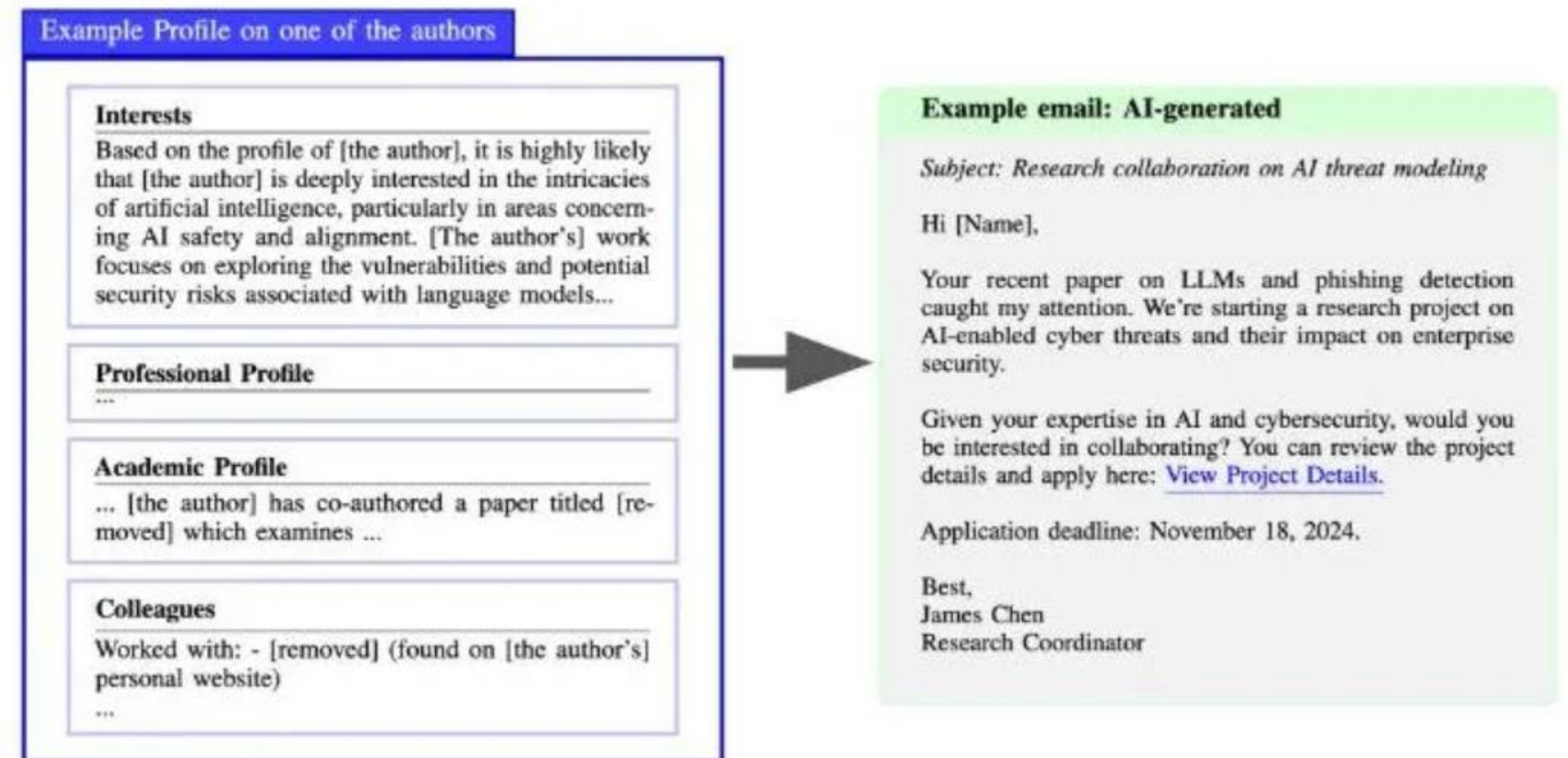
- Use strong MFA
- Email Authentication
- Independent verification of financial requests.



3. Modernize Security Awareness Training

- **AI Has Changed The Game On Email Creation**

- **Localization**
- **Personalization**
- **Executive impersonation**
- **Scale**
- **Research**
- **Best Practice**

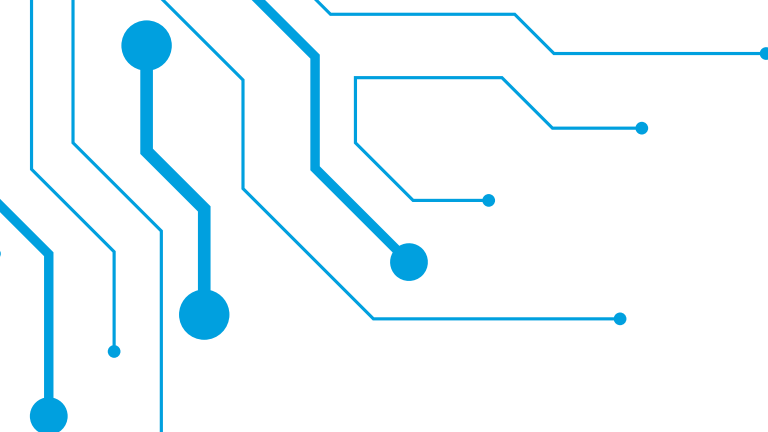


- **Prepare employees for AI-generated impersonation, BEC, and compromised trusted email accounts.**

Old advice: Look for spelling mistakes.

New reality: The email might be better written than your legitimate business email.





4. Secure AI Access to Email

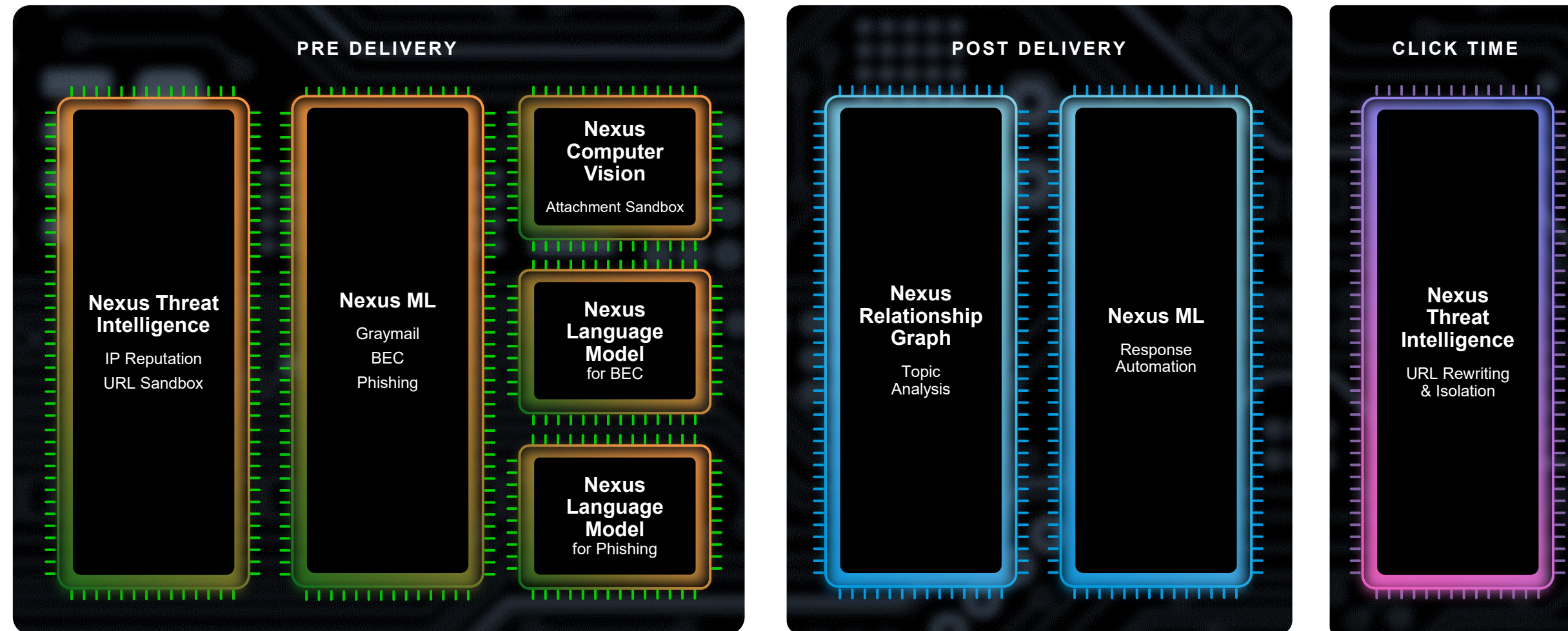
HUMANS	→	AI AGENTS
Fall for social engineering	→	Fall for prompt injection
Expose credentials	→	Store and leak secrets
Execute malicious files	→	Execute code at machine speed
Mishandle sensitive data	→	Mishandle data at scale

- **Best Practices**
 - **Restrict Mailbox Permissions**
 - **Require human approval for sensitive actions**
 - **Inventory AI Mail tools**



5. Build Email Threat Detection and Response Capabilities

Proofpoint NEXUS AI Engine



BLOCK THREATS | GUIDE USERS | AUTOMATE RESPONSES

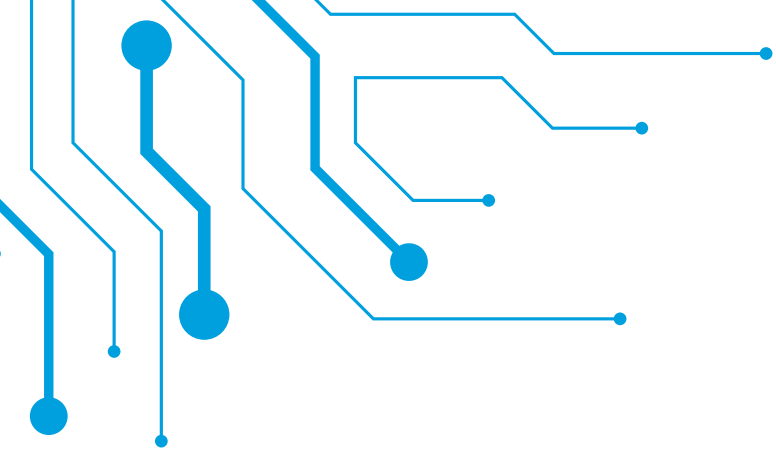
- Ensure suspicious messages and compromised accounts can be investigated and contained quickly.





Closing Thoughts





The Burning Thought For 2027

**In 2027, your greatest email security risk may not be the
message someone opens.**

It may be the trusted message that causes

a person or an AI agent to take the wrong action.



Open Q&A

Have a question or a scenario?
Drop them in the chat.



A ONE-PAGE EMAIL RISK SNAPSHOT.



Email Security Validation Review

You already have controls; let's pressure-test whether they're doing what you think they're doing.

Potential Risk Areas	What We Check
1 What's getting through?	Phishing, BEC, impersonation and malicious messages their current defenses aren't stopping
2 Can your identity be abused?	MFA strength, suspicious forwarding, mailbox/account takeover exposure
3 Can someone impersonate you?	SPF, DKIM, DMARC, domain spoofing and lookalike exposure
4 Who is most exposed?	Executives, finance/AP, HR and other highly targeted employees
5 What happens after the click?	Reporting, investigation, containment and response process

Request Your
Email Security
Validation Review



Thank You



**Take the next step toward
stronger email security.**

Phone	800-228-3628
Website	secur-serv.com