SECUR-SERV + proofpoint.

EMAIL SECURITY

Current Trends & Threats for Financial Institutions

May 14, 2026

Presenters

Pat Heller

Secur-Serv

Vice President,
FI Sales

Eric Townsend

ProofPoint

Global MSP
Cybersecurity RMM Lead

Agenda

SECUR-SERV

1. Secur-Serv + ProofPoint Partnership
2. Modern Threat Landscape
   - Technology Shift
   - Top Security Risks in 2026
   - AI Impact
3. Defense & Best Practices
4. Q&A

SECUR-SERV

Secur-Serv + ProofPoint Partnership

SECUR-SERV

proofpoint. Partnership

Partnership Value

Part of Security Partner Suite

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

SECUR-SERV

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
- **Email Security & Compliance**
- Managed Detection & Response (MDR)
- Endpoint Security (EDR)

SECUR-SERV

Modern Threat Landscape

2026 Cybersecurity Trends

SECUR-SERV

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

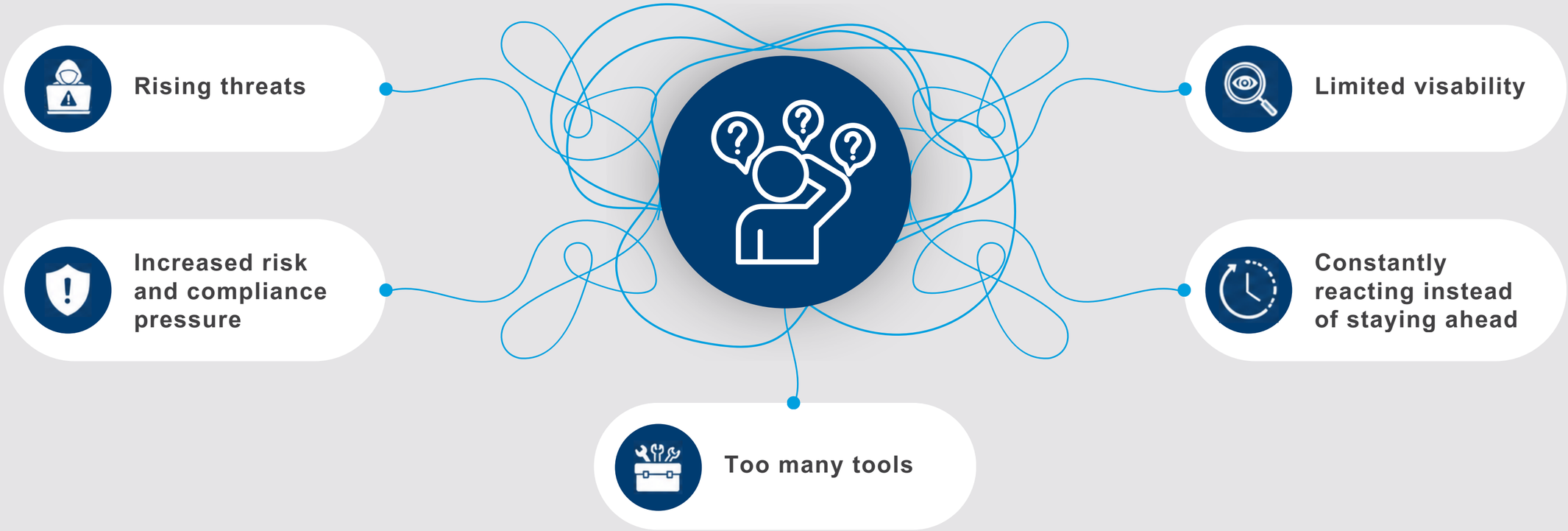
83%
of SMBs experienced a cyber incident in the last 12 months

25-40%
increase in cyber insurance premiums YoY

Today's Email Security Reality

SECUR-SERV

Financial institutions are facing growing challenges:



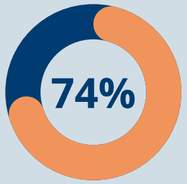
Clarity and outcomes are no longer optional—they are critical.

SECUR-SERV

3 Key Technology Shifts

Shift #1: From Tool-Based Security to Human-Centric Security

SECUR-SERV



of breaches rely on exploiting the human element

Human-targeted email
#1 vector for initial compromise

Human identities
#1 vector for privilege escalation, lateral movement

Human actions
#1 vector for data loss

Shift #2: AI is Accelerating BOTH Sides

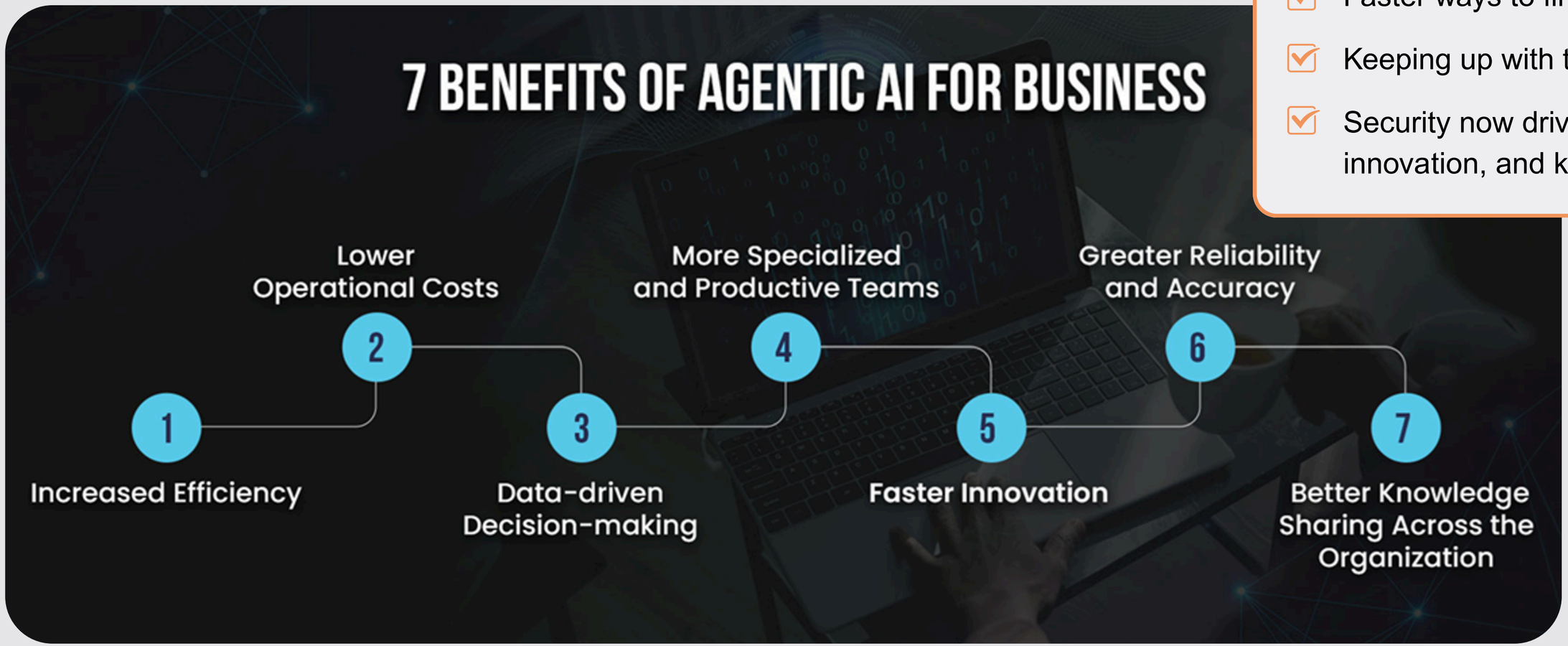
AI-driven phishing attacks have increased 1265%

- **Attackers using Agentic AI**
  - Faster, smarter, scalable attacks
  - Defenders must use AI too
- **2026 Security Stack Must Be AI Driven**
  - Behavioral detection
  - Real-time analysis
  - Continuous learning

Shift #3: The ROI of Agentic AI Is Real

SECUR-SERV

- Faster ways to find solutions
- Keeping up with the new threats
- Security now drives efficiency, innovation, and knowledge



SECUR-SERV

Impact of Agentic AI

The New Security Threat:
Agentic AI

✕ In a Mythos world, the question is no longer just *"Are we patched?"*

✓ It is *"What protects our clients when a patch doesn't exist yet and the attacker already has a working exploit?"*

That answer has to be cyber deception and compensating controls.

The New Security Threat:
Agentic AI

SECUR-SERV

The New Security Threat:
Agentic AI

SECUR-SERV

- Thousands of critical zero-days found autonomously across every major operating system and browser.
  - 27-year-old OpenBSD flaw
  - 16-year-old FFmpeg bug that survived five million automated test runs
- Generated 181 working exploits for Firefox in a single run.
- Phishing 3.0- AI-powered, multi-channel attacks that adapt in real time and are unique to each recipient.

Leveraging AI to Empower Defenders & Protect Humans

SECUR-SERV

Excel at Threat Detection

AI is combined with multiple detection methods to identify and respond to emerging threats quickly—improving detection accuracy while reducing operational overhead.

Simplify Cyber Operations

Advanced AI is integrated into cyber operations to streamline workflows and deliver clear, actionable insights from threat intelligence and operational data.

Reinforce Effective AI Practices

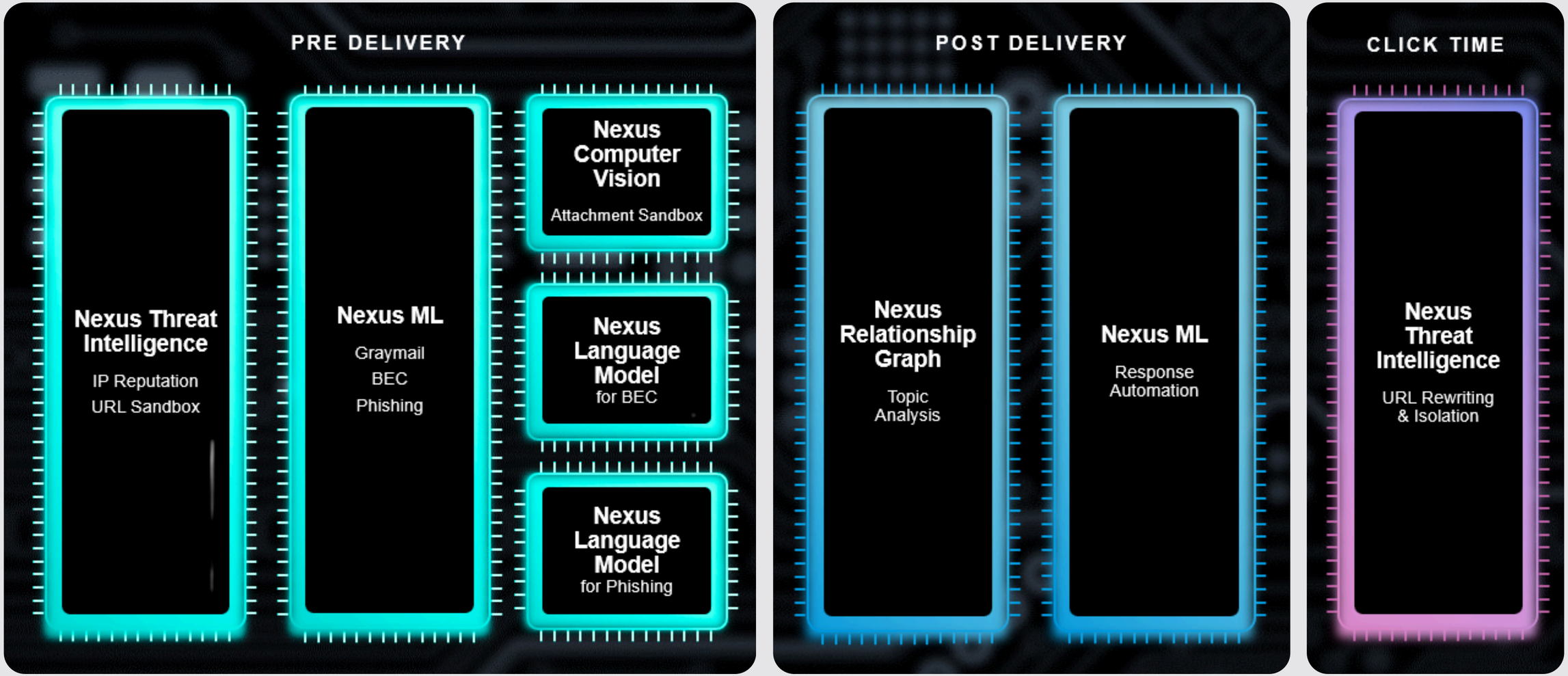
Tools and guidance enable better visibility and management of GenAI usage, supported by awareness training and in-context coaching to strengthen responsible AI practices.

Foundation

Data Security | Data Privacy | Data Confidentiality | Data Sovereignty

Protecting Email at Every Stage

SECUR-SERV



SECUR-SERV

Defense & Best Practice

SECUR-SERV

Defense & Best Practice

Tenant Security

Review controls, harden configurations, and continuously monitor your security posture.

Advanced Email Protection

Filtering and sandboxing to detect and stop threats before they reach users.

Email Authentication

DMARC and DKIM management to prevent spoofing and protect your domain.

Identity & Access Security

MFA and Zero Trust to reduce unauthorized access and limit risk exposure.

Employee Awareness

Ongoing training to reduce human error and strengthen security culture.

Monitoring & Visibility

SIEM and log ingestion to detect, investigate, and respond to threats faster.

Turning Insight into Action

SECUR-SERV

- Security is shifting to a human-centric approach
- AI is driving the need for modernized security stacks
- Ongoing monitoring and hardening are essential

Ready to take the next step?

Connect with your Secur-Serv representative or reach out to our team to explore what this looks like for your environment.

800-228-3628

SECUR-SERV

See If Your Domain Is Vulnerable

Scan Here to Request Your Free DMARC Scan

SECUR-SERV

Q&A

SECUR-SERV

Take the next step toward stronger email security.

Email Pat.Heller@secur-serv.com

Phone 800-228-3628

Website secur-serv.com