



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

- 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 + ProofPoint Partnership





proofpoint. Partnership



Partnership
Value

Part of Security
Partner Suite

Bundled Management
& Full Support

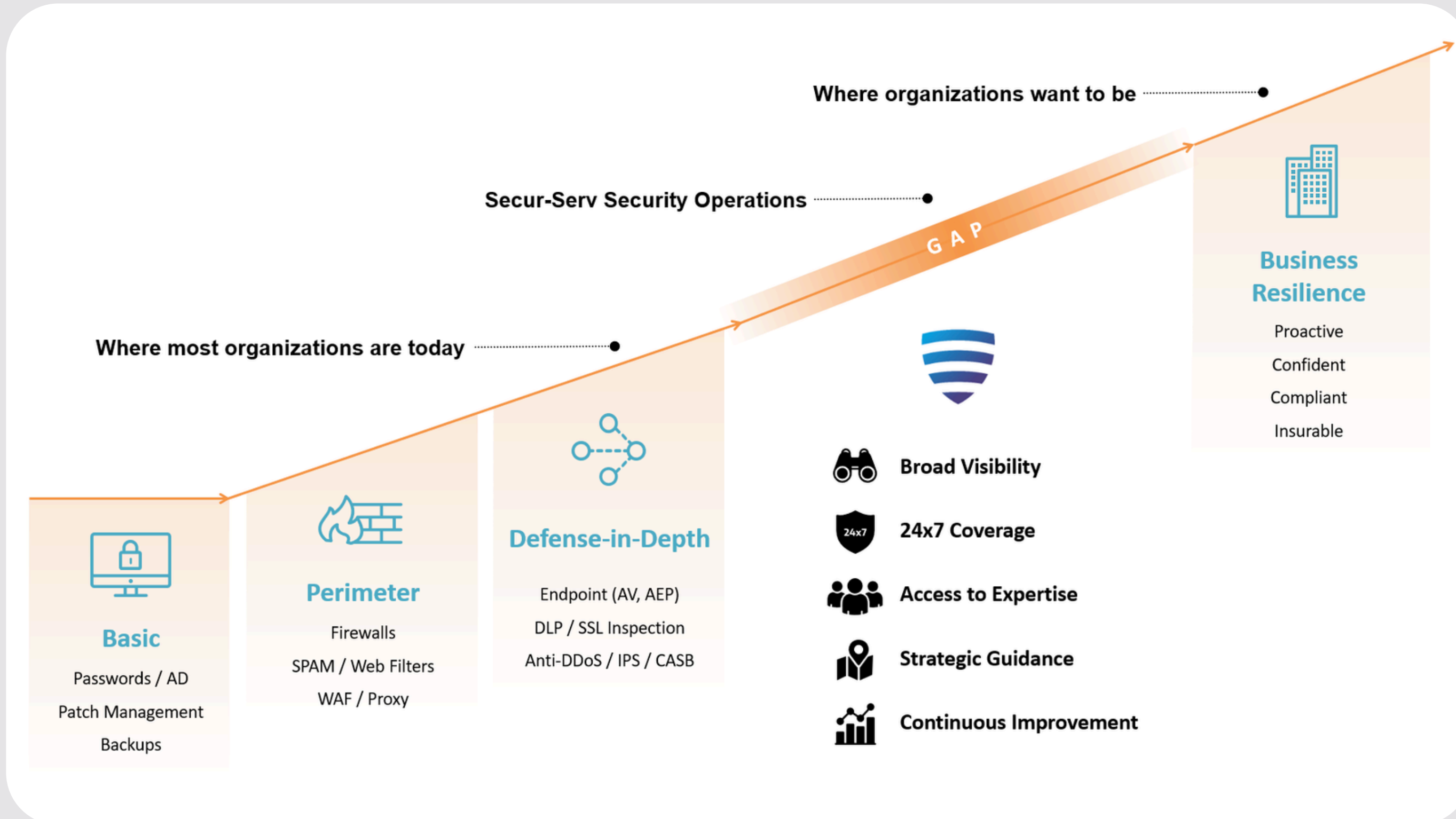
Key Component of
Full Security Stack

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





Security Operations



Managed Security Services



Managed Security Services



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



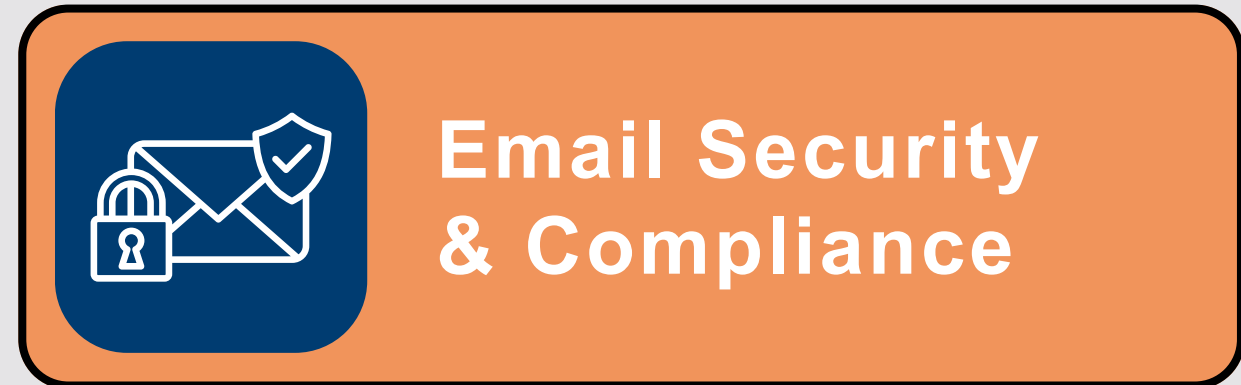
Cybersecurity Awareness Training



Mobile Device Management



Password Management



Email Security & Compliance



Security Operations Center (SOC)



Managed Detection & Response (MDR)



Multi-Factor Authentication (MFA)



Endpoint Security (EDR)





Modern Threat Landscape



2026 Cybersecurity Trends



Top 10 Business Issues, Technology Priorities & IT Challenges

BUSINESS ISSUES	TECHNOLOGY PRIORITIES	IT CHALLENGES
1 Driving Profitable Growth	1 GenAI & Agentic Automation	1 Budget Constraints & Cost Predictability
2 Managing Inflation & Costs	2 Zero Trust Security Architecture	2 Data Trust & Sanitization For AI
3 Attracting & Retaining Talent	3 Cloud-Native Modernization (SaaS)	3 Bridging Tech Skills Gap
4 Maximizing Tech Value (ROI)	4 Total Experience (TX) Platforms	4 Governance Of "Shadow AI"
5 Delivering Personalization	5 Unified Data & Analytics	5 Integrating SaaS Silos
6 Strengthening Cyber Resilience	6 Strategic Managed Services	6 Securing Remote/Hybrid Work
7 Improving Cash Flow/Liquidity	7 AI-Native Infrastructure (Hybrid)	7 Vendor/Subscription Fatigue
8 Ensuring Regulatory Compliance	8 Intelligent Edge (Edge AI)	8 Modernizing Legacy ERP/Finance
9 Accelerating Speed To Market	9 AI TRiSM (Trust, Risk, Security Management) & Governance	9 Ensuring Business Continuity
10 Building Brand Reputation	10 Collaboration & Future Of Work	10 User Resistance To Change

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

Source: Techaisle

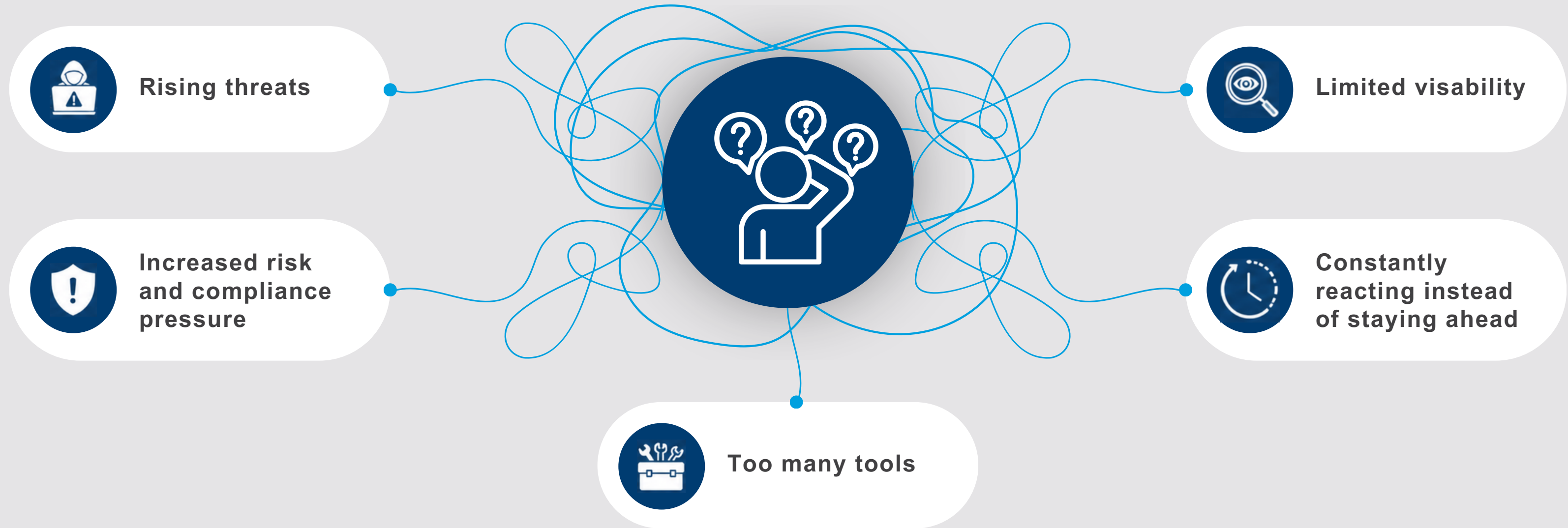




Today's Email Security Reality



Financial institutions are facing growing challenges:



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



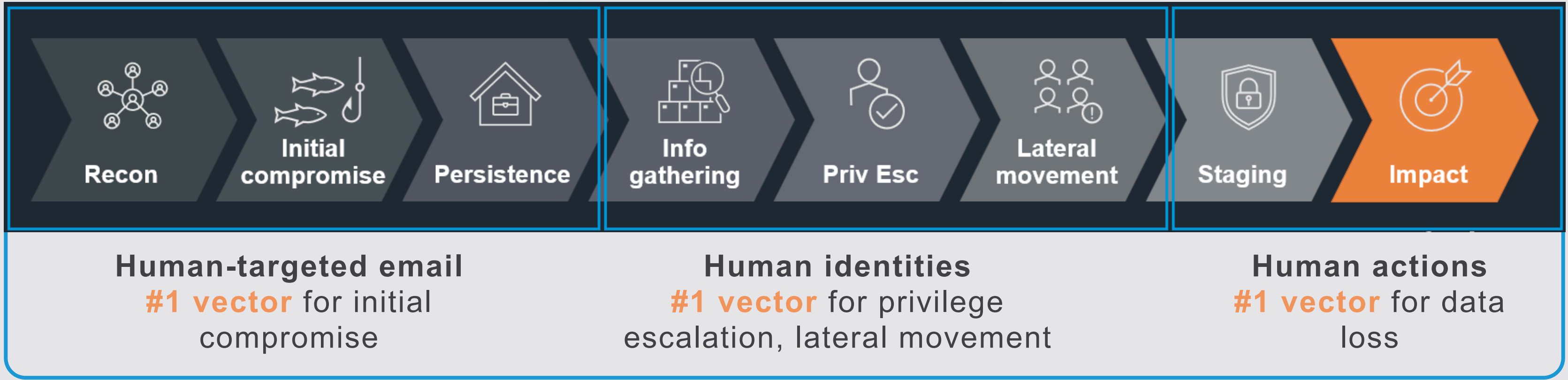
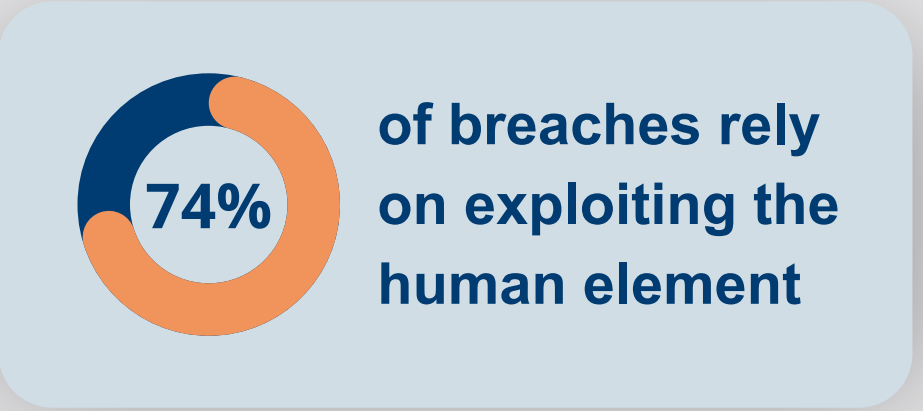


3 Key Technology Shifts





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





Shift #2: AI is Accelerating BOTH Sides

 **AI-driven phishing attacks have increased 1265%**

Your current security was built for yesterday's threats, not AI-powered ones.

Email is the control surface for attackers and **its only getting worse**

4.5x More Effective Breaches with AI

50x More Profitable

1,265% Surge in Phishing Emails Since Generative AI

 Microsoft

- **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

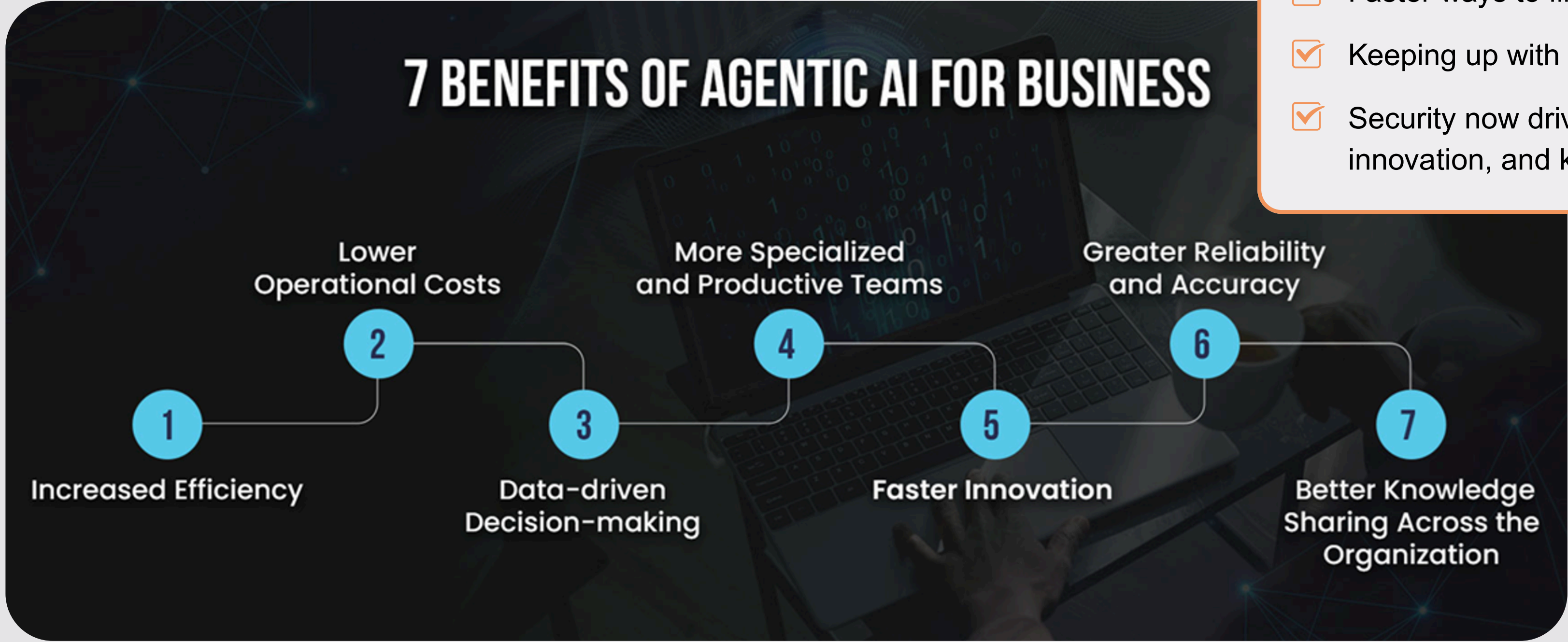




Shift #3: The ROI of Agentic AI Is Real

7 BENEFITS OF AGENTIC AI FOR BUSINESS

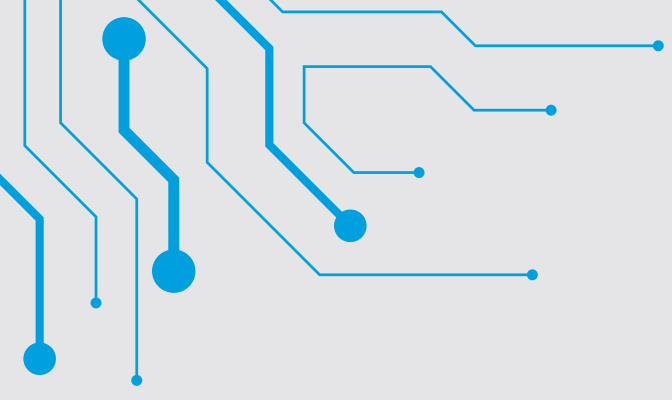
- ✓ Faster ways to find solutions
- ✓ Keeping up with the new threats
- ✓ Security now drives efficiency, innovation, and knowledge





Impact of Agentic AI





The New Security Threat: Agentic AI

• LEAKED // CLASSIFIED

CAPYBARA TIER // BEYOND OPUS

CLAUDE MYTHOS

Step-change AI model with **unprecedented cybersecurity** capabilities. What it means for defenders.

Anthropic just announced an AI model so powerful the company has decided not to release it to the public

It's so powerful that it found bugs in every major operating system and browser in the world

Anthropic @AnthropicAI

Introducing Project Glasswing: an urgent initiative to help secure the world's most critical software.

It's powered by our newest frontier model, Claude Mythos Preview, which can find software vulnerabilities better than all but the most skilled humans.

Project Glasswing
Securing critical software for the AI era

Project Glasswing: Securing critical software for the AI era

✗ 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



```
<code><pre><code></pre></code>
```

A.I. POWER UNDER SCRUTINY AFTER DATA WIPE
A.I. TOOL REPORTEDLY WIPED COMPANY DATA WITHOUT CONSENT

abc7
abc7.com





The New Security Threat: Agentic AI



- 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



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.



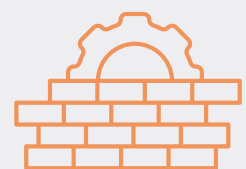
Simplify Cyber Operations

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



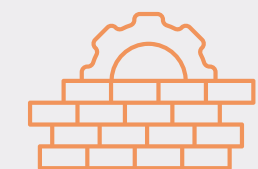
Reinforce Effective AI Practices

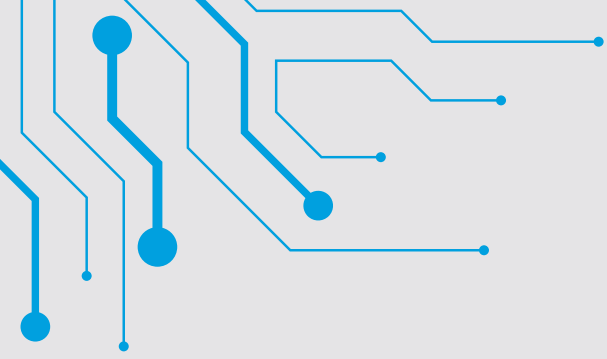
Tools and guidance enable better visibility and management of GenAI usage, supported by awareness training and in-context coaching to strengthen responsible AI practices.



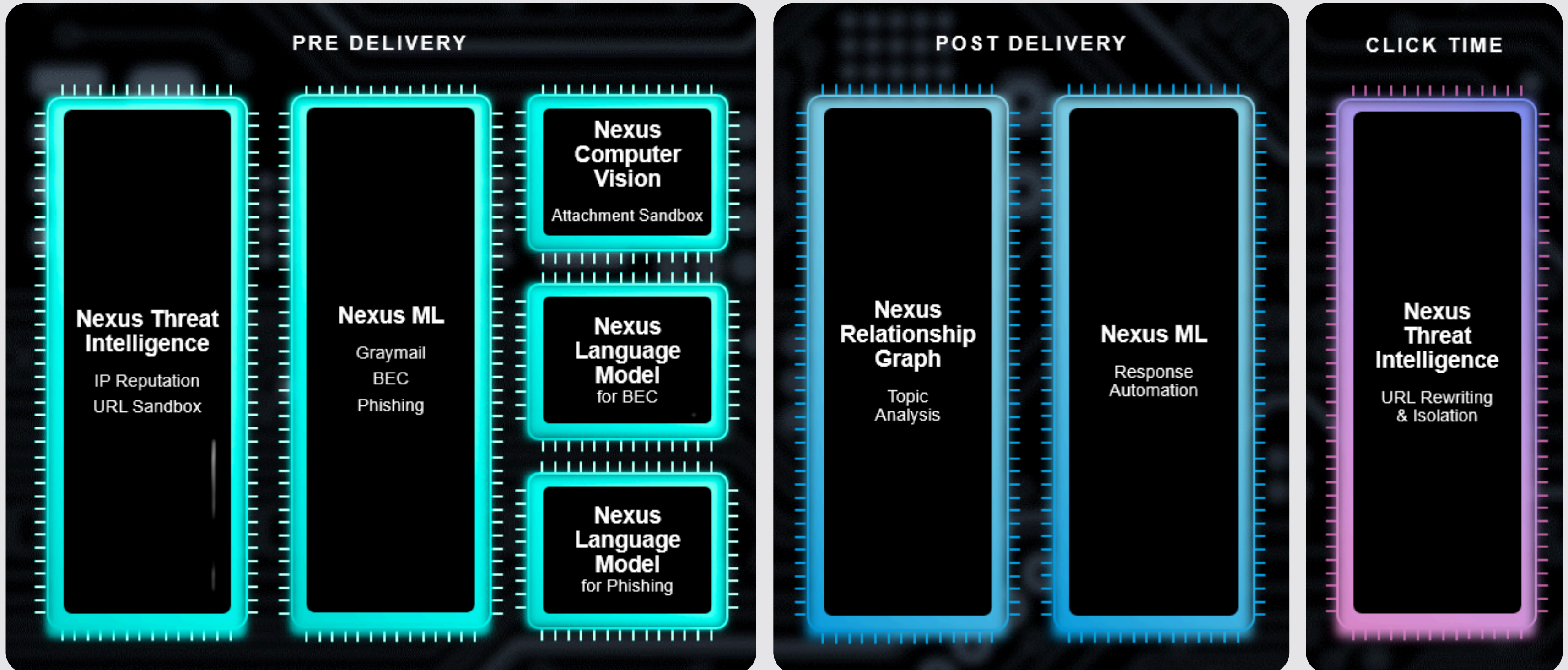
Foundation

Data Security | Data Privacy | Data Confidentiality | Data Sovereignty





Protecting Email at Every Stage





Defense & Best Practice





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.



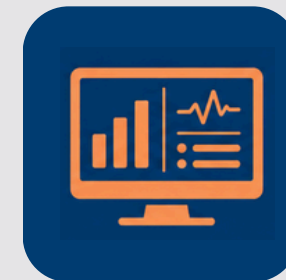
Identity & Access Security

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**



- 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



See If Your Domain Is Vulnerable



Scan Here to Request Your
Free DMARC Scan



Q & A



Take the next step toward stronger email security.

Email Pat.Heller@secur-serv.com

Phone 800-228-3628

Website secur-serv.com