October 2025

Resilience in the Age of AI

CyberIsle 2025

Lesley Kipling
Lead Investigator *(former)*
Chief Security Advisor

Microsoft

Today I’m going to talk about 3 broad topics

Inflection Points

Threat Landscape

Mission Critical resilience

Threat/Defence Landscape

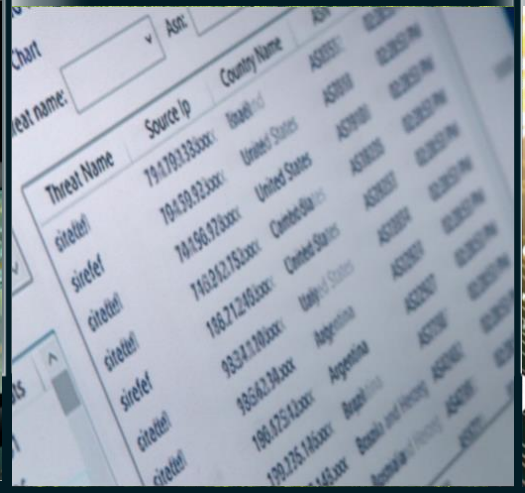
Same tactics. New sophistication (mostly).

Trends in the threat landscape

Thriving: Nation state

National, international, financial motivations

Growing: Ransomware



More elusive, higher stakes

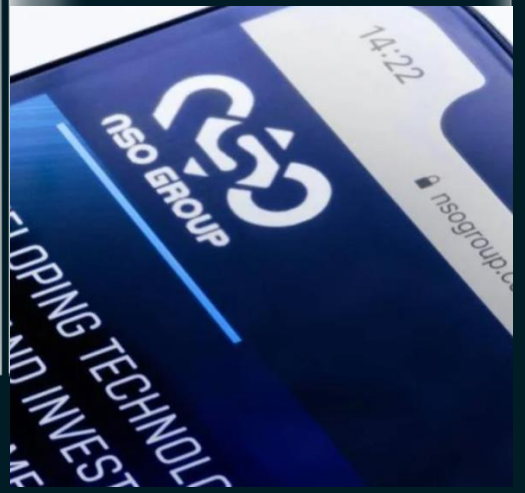
Growing: Supply chain

Trusted channels, broad attacks

Emerging: Local-to-cloud attacks

Target on-premises to enable cloud access

Emerging: Cyber mercenaries



Custom-made services, highly-customized

Our Motivation: Numbers from 2024 MDDR

600.000.000
attacks per day against Microsoft customers

7.000
DDoS attacks per day (2023: 1.500)

1.500
hacker groups tracked (2023: 300+)

7.000
password attacks blocked per second (2023: 4.000)

Base: 84.000.000.000.000 security signals per day

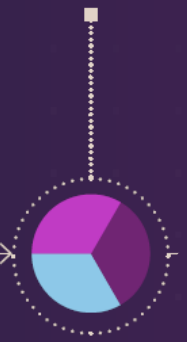
Source: https://aka.ms/mddr

Identity attacks in perspective

Password-based attacks continue to dominate, but can be thwarted by using strong authentication methods.

<1%

of attacks



MFA attacks

SIM swapping
MFA fatigue
AitM

Post-authentication attacks

Token theft
Consent phishing

Infrastructure compromise

Source: Microsoft Threat Intelligence

7,000

Password attacks per second

39,000

Token theft incidents per day

146%

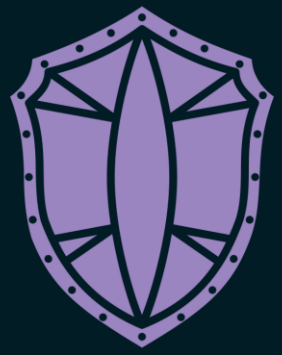
Rise in AiTM phishing attacks

Source: Microsoft Threat Intelligence

- 2014 CYBERSECURITY = TECHNICAL PROBLEM
- 2020 CYBERSECURITY = BUSINESS PRIORITY
- 2024 CYBERSECURITY = ORGANIZATIONAL EXISTENCE

SECURITY

Focus on preventing bad things from happening.



PREVENT
GUARD
PROTECT
SAFEGUARD
SHIELD
DEFEND

RESILIENCE

Getting back up ASAP after bad things happen.

STURDY
RESITANT
ELASTIC
QUICK TO RECOVER
RESTORE
TOUGH
ROBUST
FIXABLE
HARDY
BUOYANT

Reconstructing and repositioning Microsoft for the world that we live in.

Mission Critical

Governments | **Hospitals** | **Banks** | **Factories** | **Supply chains** | **Retailers**

Mission Critical

SFI

Secure Future Initiative

QEI

Quality Excellence Initiative

SFI Principles and Pillars

Secure by design | Secure by default | Secure operations

Security culture and governance

Protect identities and secrets

Protect tenants and isolate production systems

Protect network

Protect engineering systems

Monitor and detect threats

Accelerate response and remediation

Continuous improvement

Paved path → Standards

Quality Excellence Initiative (QEI)

Change management

Safe deployment practices and better tooling

Platform resiliency

Enhance resiliency across Microsoft's services verifiably and by design across zones and regions

Service health measurement and incident management

Measure deeply, improve, and accelerate incident detection and incident management

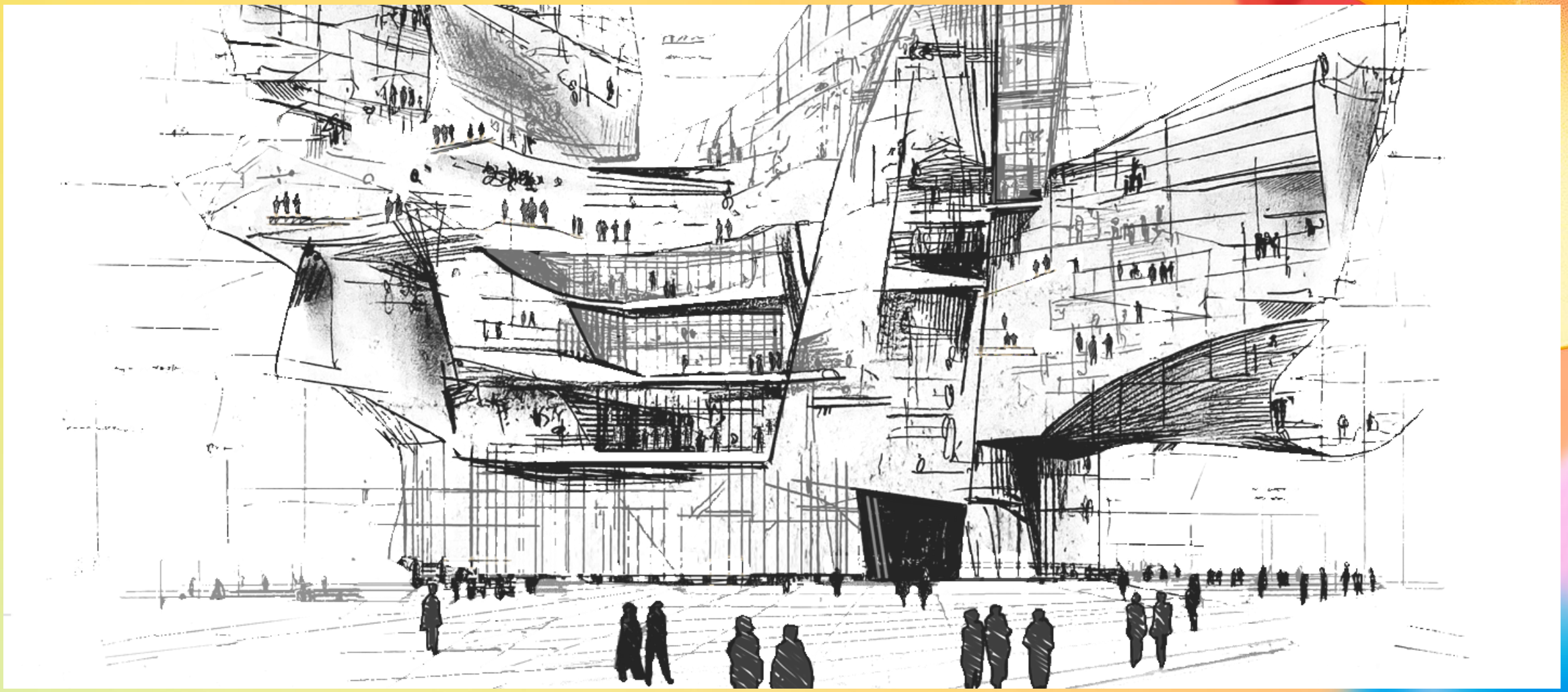
Capacity

Expedite and prioritize capacity and availability against customer demand

Customer resiliency

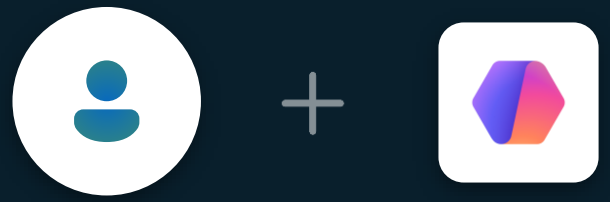
Understand and direct customer implementations with Microsoft to resilient services and design patterns

The Frontier Firm



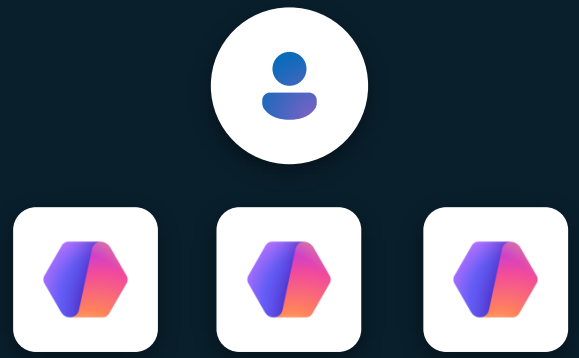
Pattern 1

Human with assistant



Pattern 2

Human-agent teams



Pattern 3

Human-led, agent operated

AI: not so different

Not novel

- Incomplete data
- Over-permissioning/porous access controls
- Traditional software vulnerabilities
- Lack of failure scenario plans
- Features that don't consider the holistic system

Impact potential = faster and broader

To err is AI

5 novel AI error types

- Garbage in, garbage out
- Misinterpreted data
- Ungrounded addition (hallucination)
- Omission
- Unexpected preferences

AI safety

Principles

Fairness • Privacy & security • Transparency
Reliability & safety • Inclusiveness • Accountability

Corporate standard

Goals • Requirements • Practices

Implementation

Training • Tools • Testing

Oversight

Monitoring • Reporting • Auditing • Compliance

AI plays a major part in cyber security

Challenges

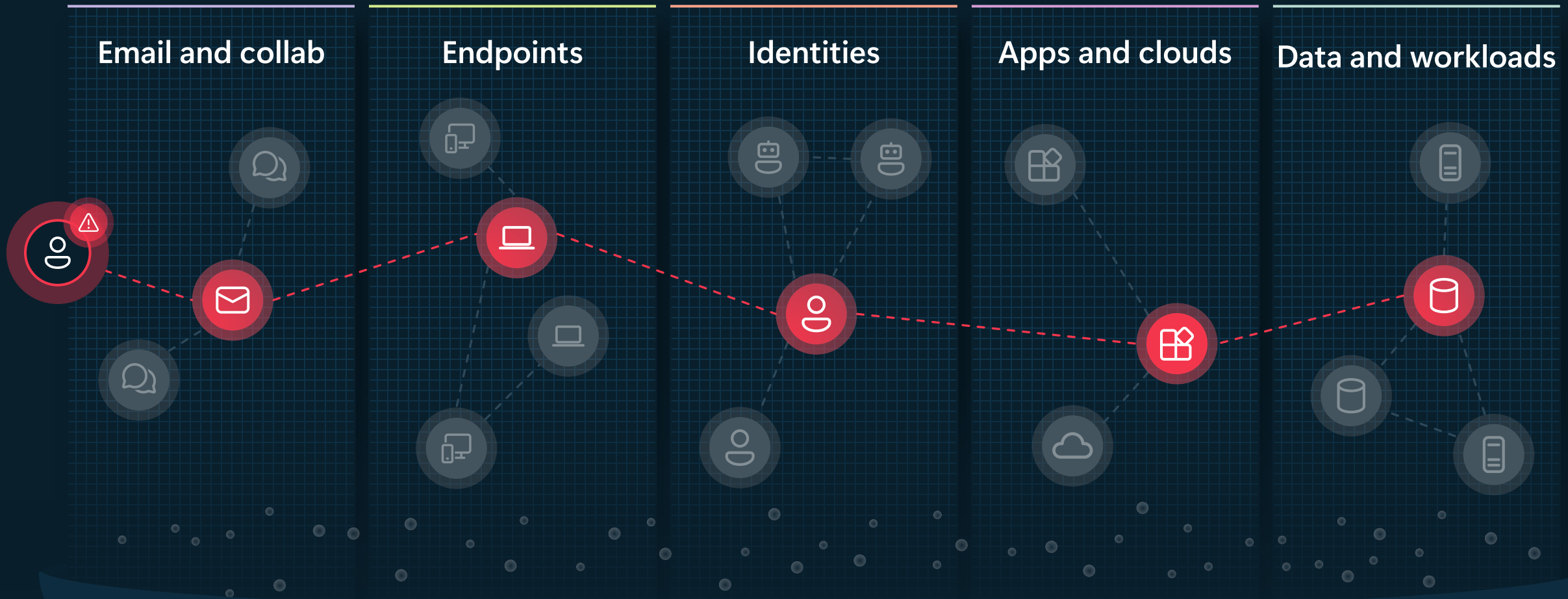
- Advanced threats - APTs, zero-day exploits, ransomware
- Data overload - logs, telemetry
- AI-powered attacks
- Shortage of skilled security researchers

AI augments human expertise & scalability …

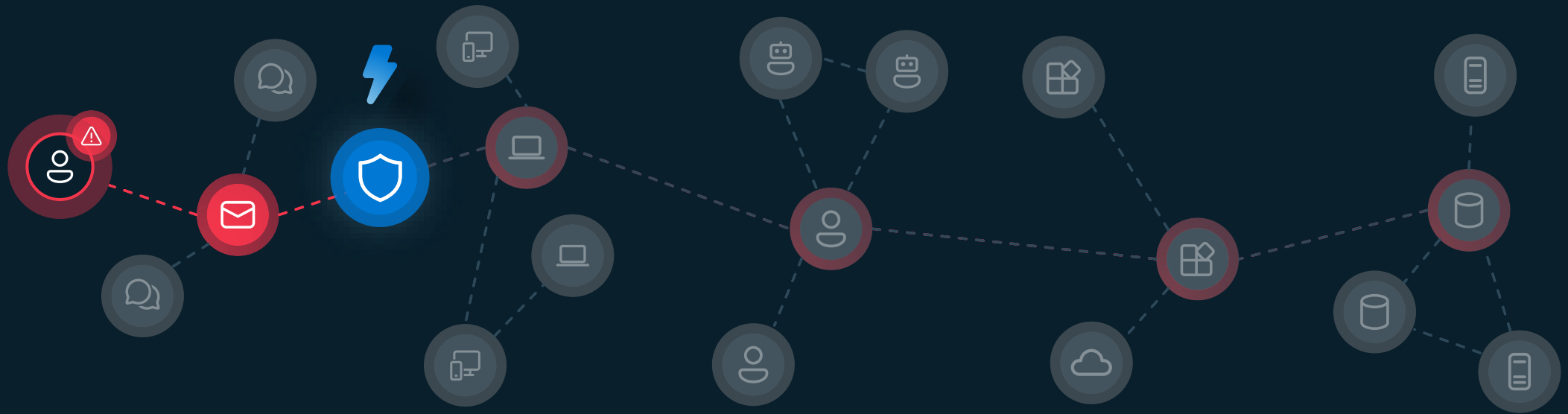
How teams are defending with AI

- Threat detection & analysis
- Incident investigation & response
- Phishing & scam detection
- Reverse engineering
- Security operations automation
- Data risk & compliance
- Validation & pen testing
- [what's next]

Attackers think in graphs

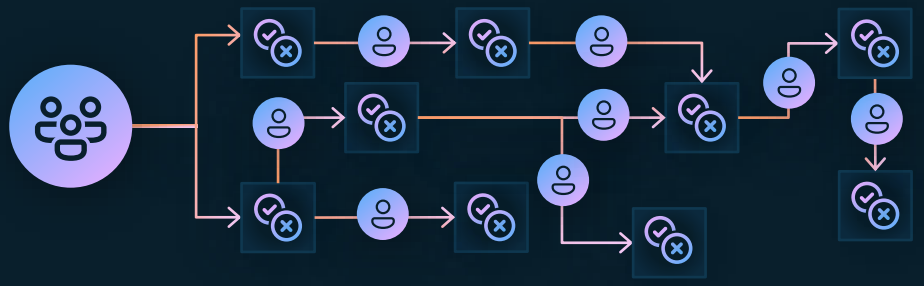


Graph-powered security enables enterprise-wide visibility

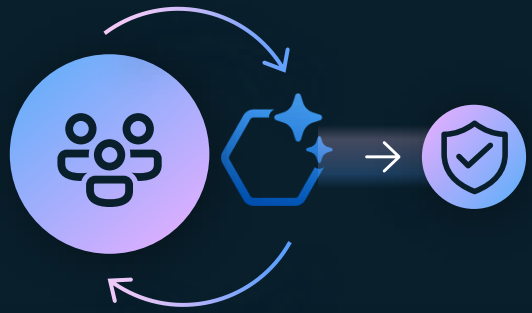


Traditional automation creates gaps in protection

Traditional automation



Agentic AI



Rigid	Adaptive
Static	Dynamic
Manual updates	Continuous learning
Pre-defined	Context-aware
Easily broken	Highly resilient

Call to action

Address the fundamentals

Plan for novel AI threats & failures

Use AI to defend & protect

Start early. Ask for help.

Strength in numbers

Thank you!