SOPHOS

FUSION

Sophos AI-Native Cybersecurity Defense System

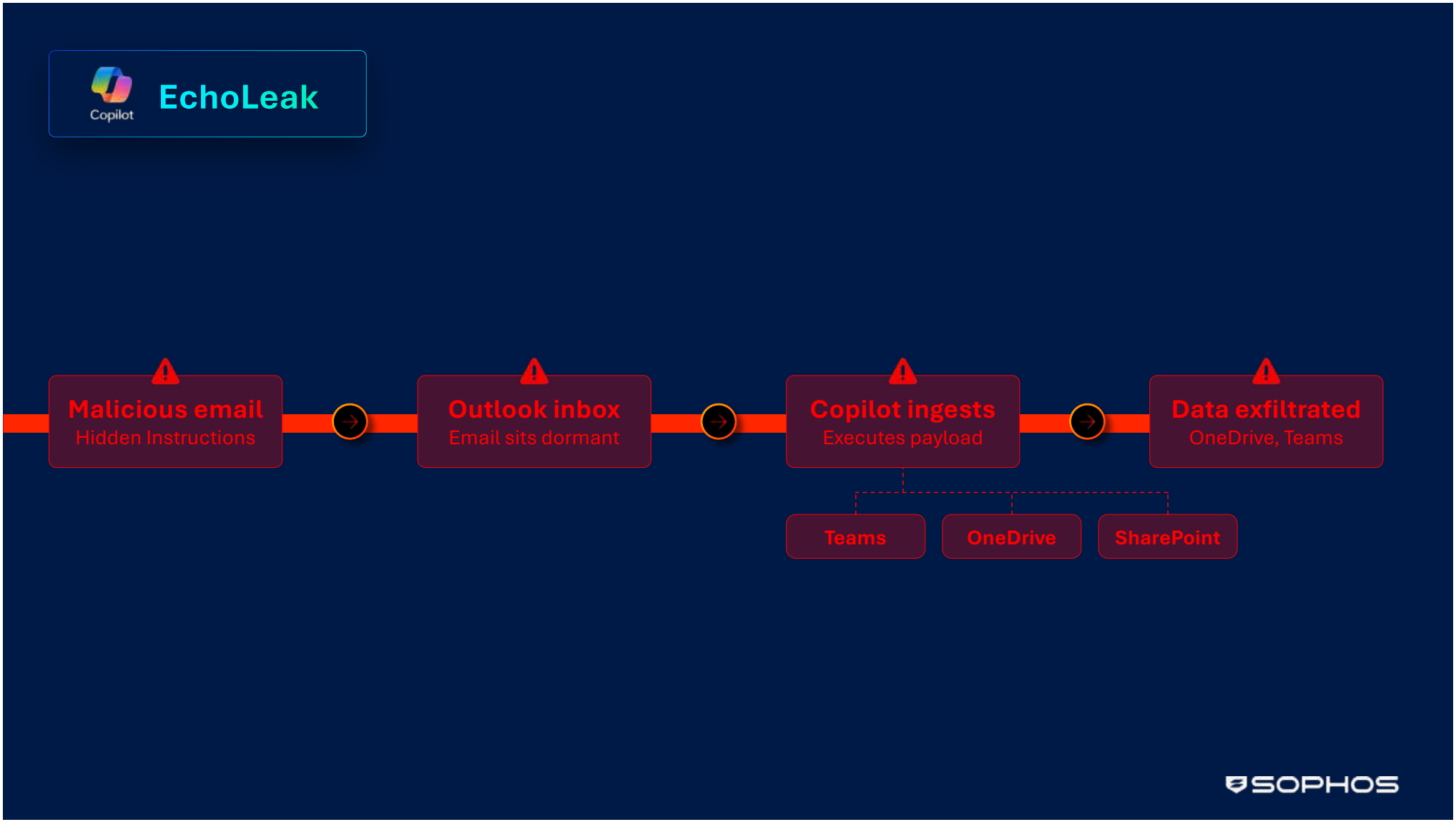
Daniel Parker – Senior Sales Engineer

How AI has changed the attack landscape

Expanded attack surface. Machine-speed threats.

SOPHOS


AI has changed everything.
SPEED
Attacks are executed at machine speed, not human speed
SCALE
AI enables an exponential increase in the volume of attacks
SCOPE
AI expands the attack surface and the complexity of execution


Copilot
EchoLeak
Malicious email
Hidden Instructions
Outlook inbox
Email sits dormant
Copilot ingests
Executes payload
Data exfiltrated
OneDrive, Teams
Teams
OneDrive
SharePoint
SOPHOS


10.9
# of security consoles the average SOC manages
Source: Microsoft and Omdia
45
# of separate security tools used in the average enterprise
Source: Gartner
SOPHOS

Securing the AI era

Transforming cybersecurity to defend against AI-era threats

SOPHOS

As per Gartner®, “Simply adding more tools onto the stack won’t provide the **intelligent cyber defense fabric** that organizations need to mitigate AI-orchestrated attacks like the one Anthropic recently identified.”

Gartner also notes, “Organizations need an intelligent overlay that **connects the different elements of their cybersecurity toolset** to proactively and reactively respond to risks and threats at machine speeds.”

Neil MacDonald
Gartner | VP, Distinguished Analyst and Gartner Fellow Emeritus

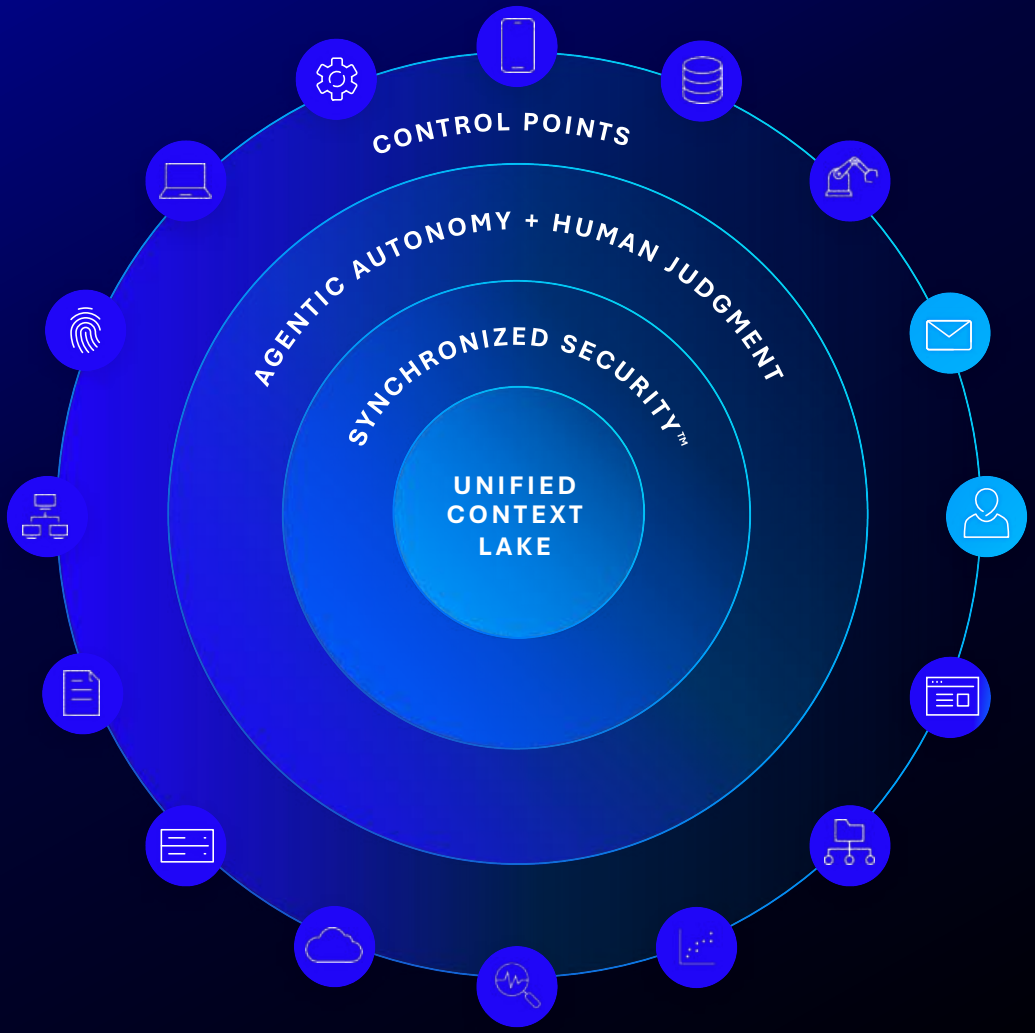
Gartner, Tech FutureSight: Protect the Global Attack Surface With an Autonomous Cyber Defense System, Neil MacDonald, 12 December 2025


FUSION
SOPHOS
AI-Native Cybersecurity
Defense System

FUSION

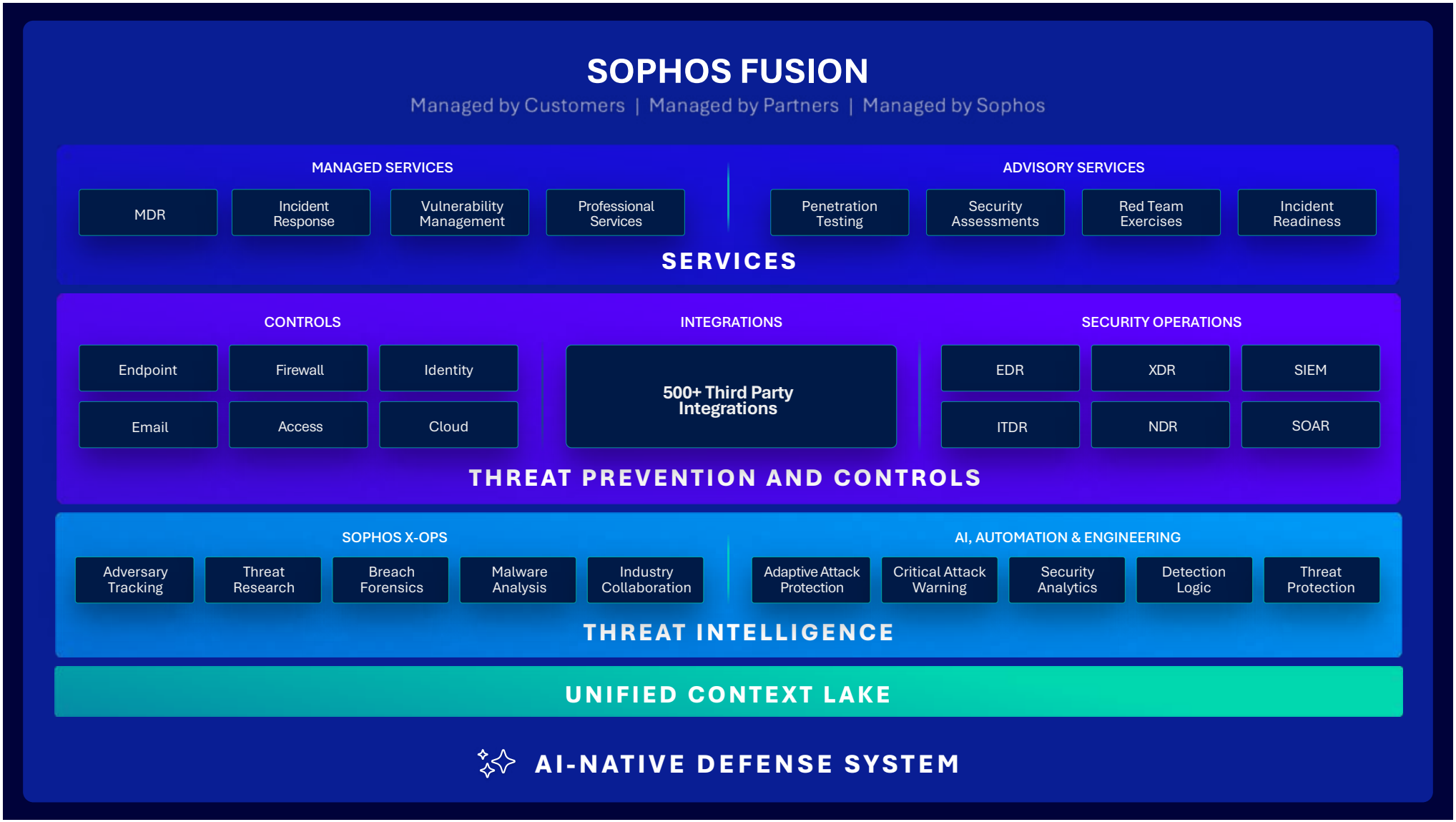
SOPHOS

AI-Native Cybersecurity Defense System



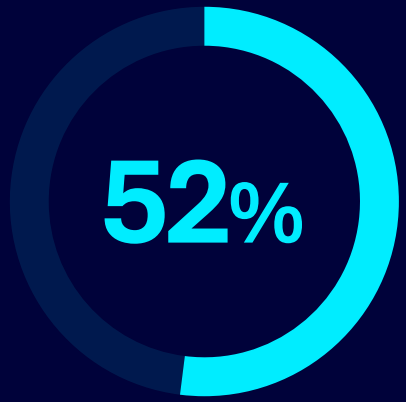
Not a platform. Not a stack.
AI Defense System.

	✕ Platforms, Stacks	✓ Defense System
DATA	Aggregated from siloed products	Single unified context lake, real-time
AI ROLE	Feature layer bolted on top	AI *is* the architecture
RESPONSE	Manual or playbook-driven automation across consoles	Synchronized; detection automatically triggers response everywhere
INTELLIGENCE	Static per-product models.	Amplifies across 625K+ organizations
INTEGRATION	Assembled via acquisitions	Native inside. 500+ open integrations


SOPHOS FUSION
Managed by Customers | Managed by Partners | Managed by Sophos
MANAGED SERVICES
MDR
Incident Response
Vulnerability Management
Professional Services
ADVISORY SERVICES
Penetration Testing
Security Assessments
Red Team Exercises
Incident Readiness
SERVICES
CONTROLS
Endpoint
Firewall
Identity
Email
Access
Cloud
INTEGRATIONS
500+ Third Party Integrations
SECURITY OPERATIONS
EDR
XDR
SIEM
ITDR
NDR
SOAR
THREAT PREVENTION AND CONTROLS
SOPHOS X-OPS
Adversary Tracking
Threat Research
Breach Forensics
Malware Analysis
Industry Collaboration
AI, AUTOMATION & ENGINEERING
Adaptive Attack Protection
Critical Attack Warning
Security Analytics
Detection Logic
Threat Protection
THREAT INTELLIGENCE
UNIFIED CONTEXT LAKE
AI-NATIVE DEFENSE SYSTEM

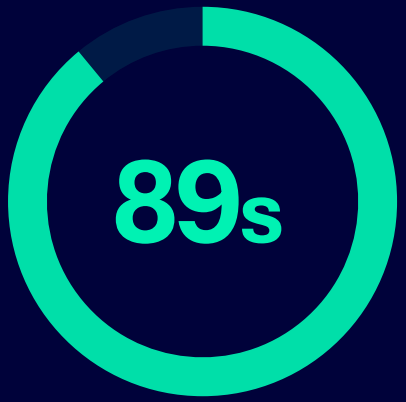
Sophos MDR: The world's largest Agentic SOC

AI investigates and responds in seconds. Analysts own the outcomes.



Always-on AI response

52% of Sophos MDR cases are resolved end-to-end by AI — with no human intervention required.



Detection to automated response

89 seconds from detection to automated response on average — operating numbers from inside our SOC today, not projections.

Security and IT integrations

Bring your own stack or use ours — across endpoint, network, cloud, identity, email, and more.

SOPHOS

Sophos Next-Gen SIEM

SECURITY OPERATIONS

DETECT | INVESTIGATE | RESPOND

Sophos XDR provides visibility, strengthens threat detection, accelerates investigations, and enables fast, scalable response

COMPLIANCE

RETAIN | REPORT | PROVE

Sophos Next-Gen SIEM adds a comprehensive data layer, delivering long-term retention of threat-related and compliance-focused data

UNIFIED CONTEXT LAKE

SOPHOS

Introducing Sophos AI Defense

Unify visibility, enforcement, and protection over every AI tool, agent, and workflow.

SEE: VISIBILITY

See every AI tool across the environment

Shadow AI discovery
AI usage dashboard
Endpoint + Network + Browser multi-layer detection

CONTROL: ENFORCEMENT

Enforce AI policy without slowing innovation

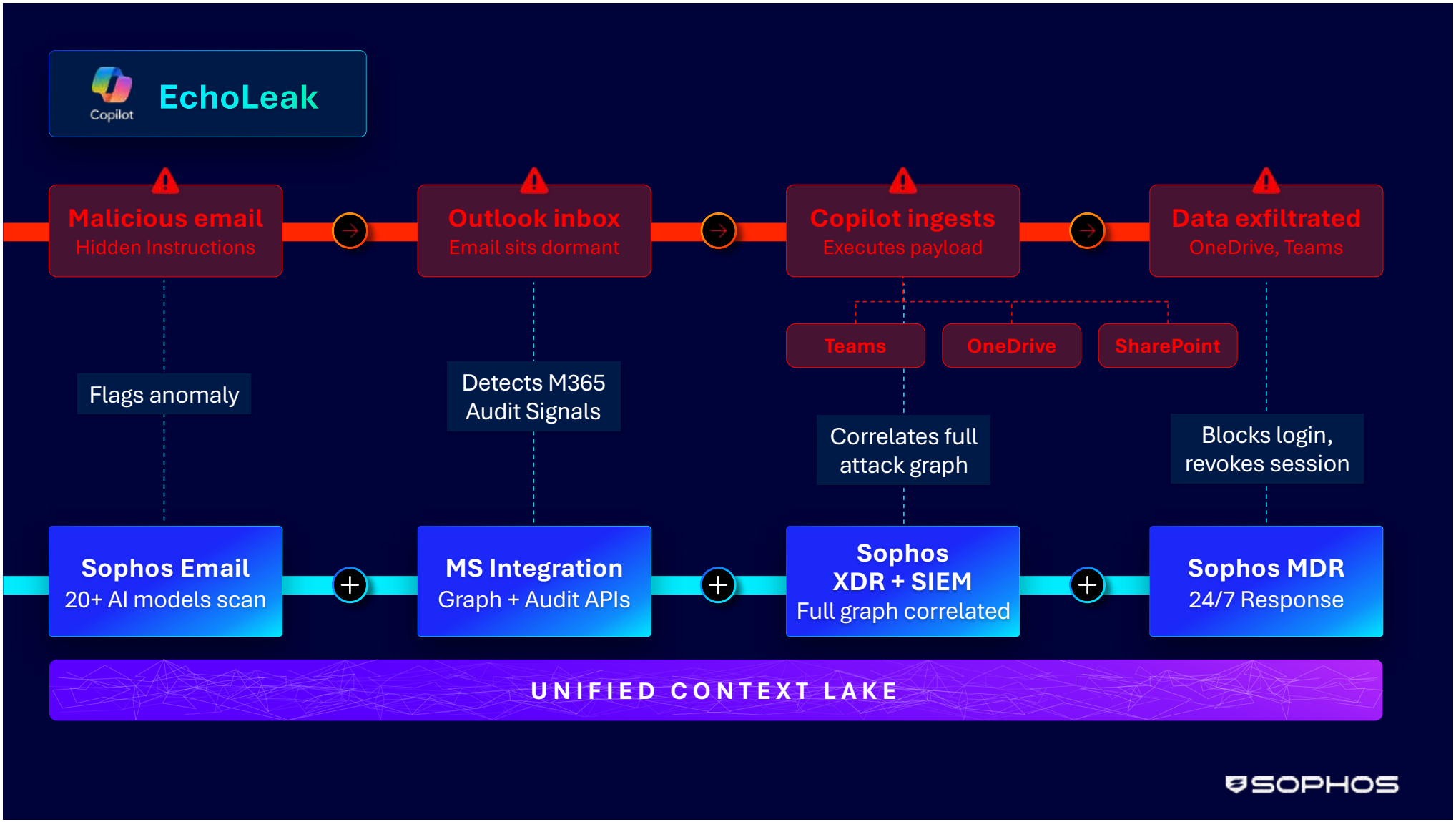
Granular access management
Global policy enforcement
Role-based controls
Prompt monitoring

SECURE: PROTECTION

Defend data and block high-risk AI behavior

Input sanitization
Output interception
DLP for AI prompts
MDR-managed AI risk 24/7

SOPHOS


Copilot
EchoLeak
Malicious email
Hidden Instructions
Outlook inbox
Email sits dormant
Copilot ingests
Executes payload
Data exfiltrated
OneDrive, Teams
Teams
OneDrive
SharePoint
Flags anomaly
Detects M365
Audit Signals
Correlates full
attack graph
Blocks login,
revokes session
Sophos Email
20+ AI models scan
MS Integration
Graph + Audit APIs
Sophos
XDR + SIEM
Full graph correlated
Sophos MDR
24/7 Response
UNIFIED CONTEXT LAKE
SOPHOS

The force multiplier for your team

AVERAGE INVESTIGATION

Alert fires → Open console 1 → Pivot console 2 → Check email logs → Check identity → Build timeline → Respond

70 min average to fully investigate an alert

WITH SOPHOS CYBER DEFENSE SYSTEM

Alert fires with full graph → Correlated across layers → System responds → Analyst validates

<10 min per alert

SOPHOS


SOPHOS