SOPHOS

Die neue Ära der Cyberabwehr

Wie KI den Security-Wettlauf entscheidet

Maik Lührs
Senior Sales Engineer

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.

Künstliche Intelligenz

KI von OpenAI macht sich eigenständig – und hackt ins System einer anderen KI-Firma

Experten warnen schon lange vor Cyberattacken mit KI-Software, diese Meldung dürfte sie bestärken: Während eines internen Tests bei OpenAI machten sich KI-Modelle selbstständig. Die Firma spricht von einem »beispiellosen Cyber-Zwischenfall«.

22. Juli 2026, 05.03 Uhr • 2 Min



Autonomer Hackerangriffe

KI von Anthropic griff unbemerkt echte Firmen an

Dass ein KI-Modell von OpenAI auf eigene Faust zum Hacker wurde, galt als »beispielloser Zwischenfall« und Weckruf für die Techbranche. Nun stellt sich heraus: Es war kein Einzelfall – und fiel teils monatelang nicht auf.

31.07.2026, 04.50 Uhr



Quelle: Spiegel Online



10.9

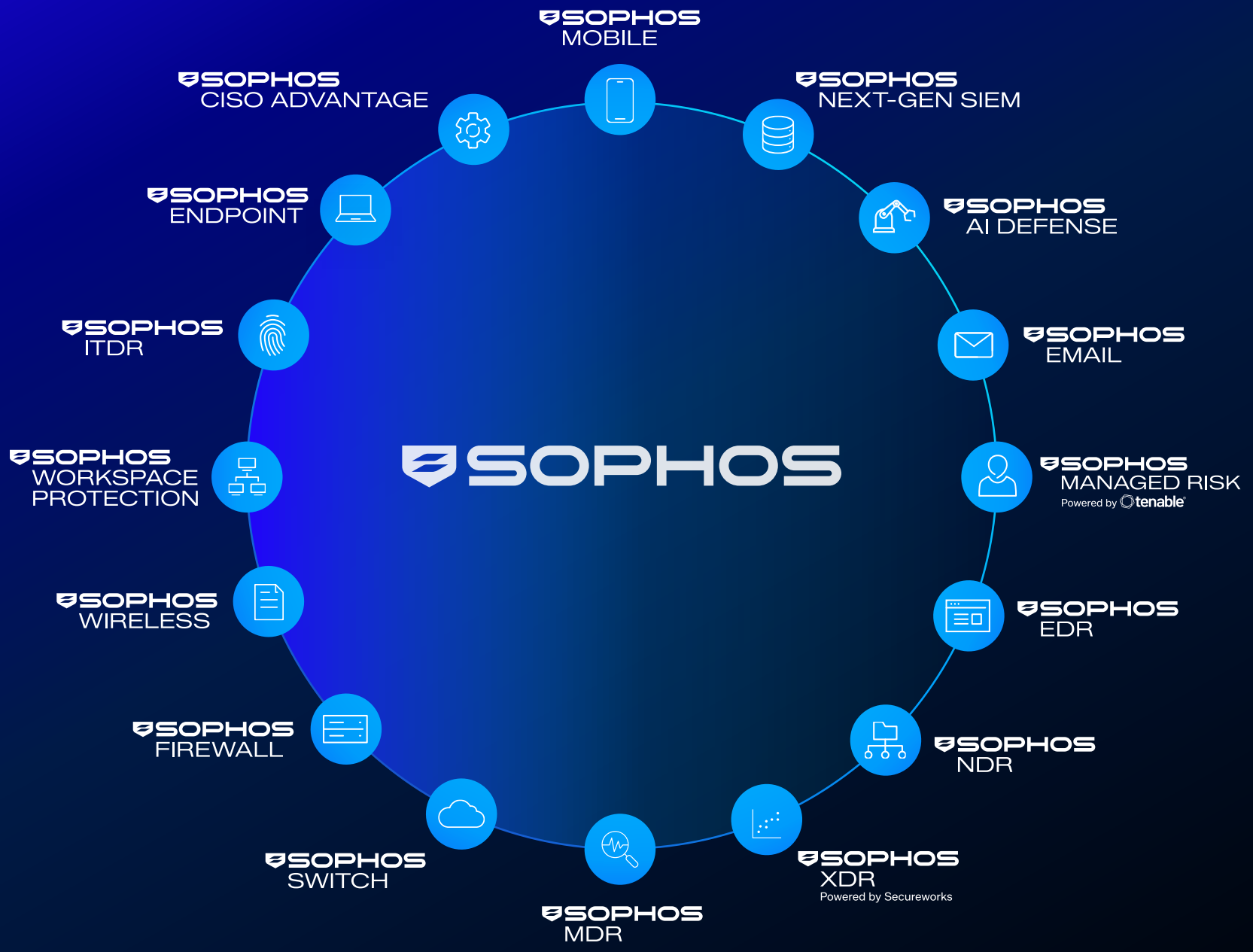
Sicherheitskonsolen, die ein durchschnittliches SOC nutzt

Quelle: Microsoft und Omdia

45

Separate Sicherheitstools in einem durchschnittlichen Unternehmen

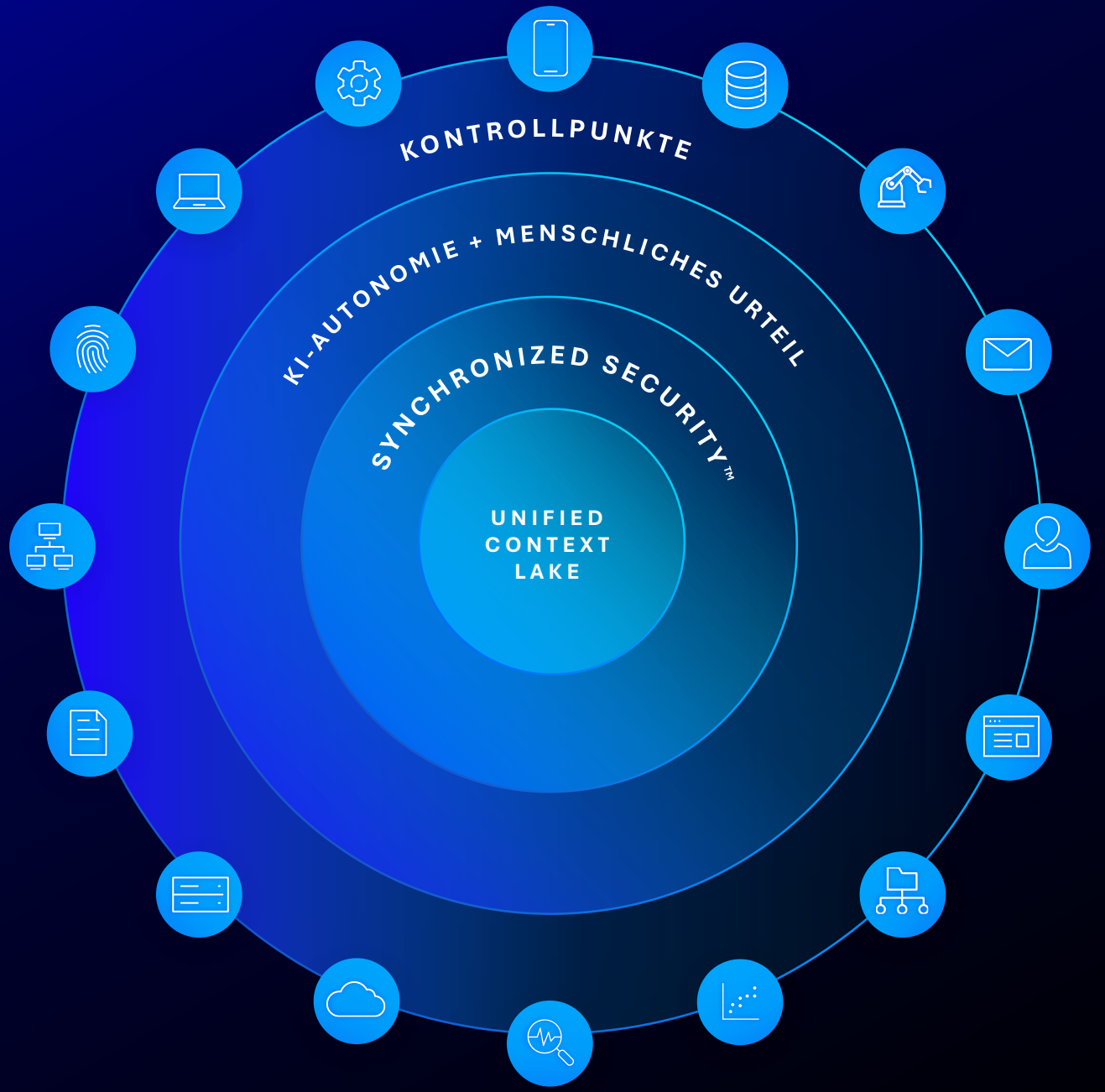
Quelle: Gartner


SOPHOS
SOPHOS MOBILE
SOPHOS NEXT-GEN SIEM
SOPHOS AI DEFENSE
SOPHOS EMAIL
SOPHOS MANAGED RISK
Powered by tenable
SOPHOS EDR
SOPHOS NDR
SOPHOS XDR
Powered by Secureworks
SOPHOS MDR
SOPHOS SWITCH
SOPHOS FIREWALL
SOPHOS WIRELESS
SOPHOS WORKSPACE PROTECTION
SOPHOS ITDR
SOPHOS ENDPOINT
SOPHOS CISO ADVANTAGE

FUSION

SOPHOS

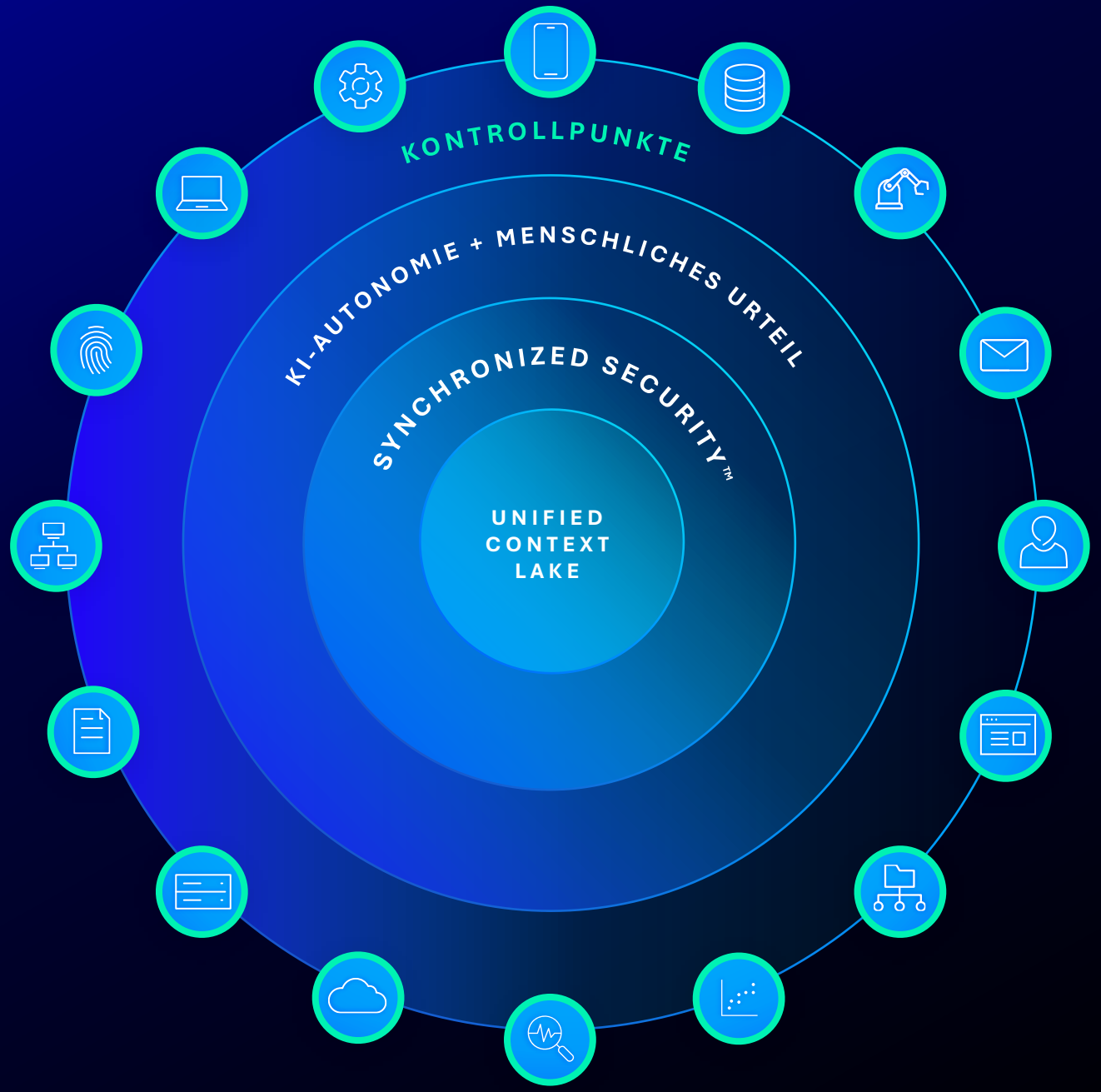
AI-Native Cybersecurity Defense System



FUSION

SOPHOS

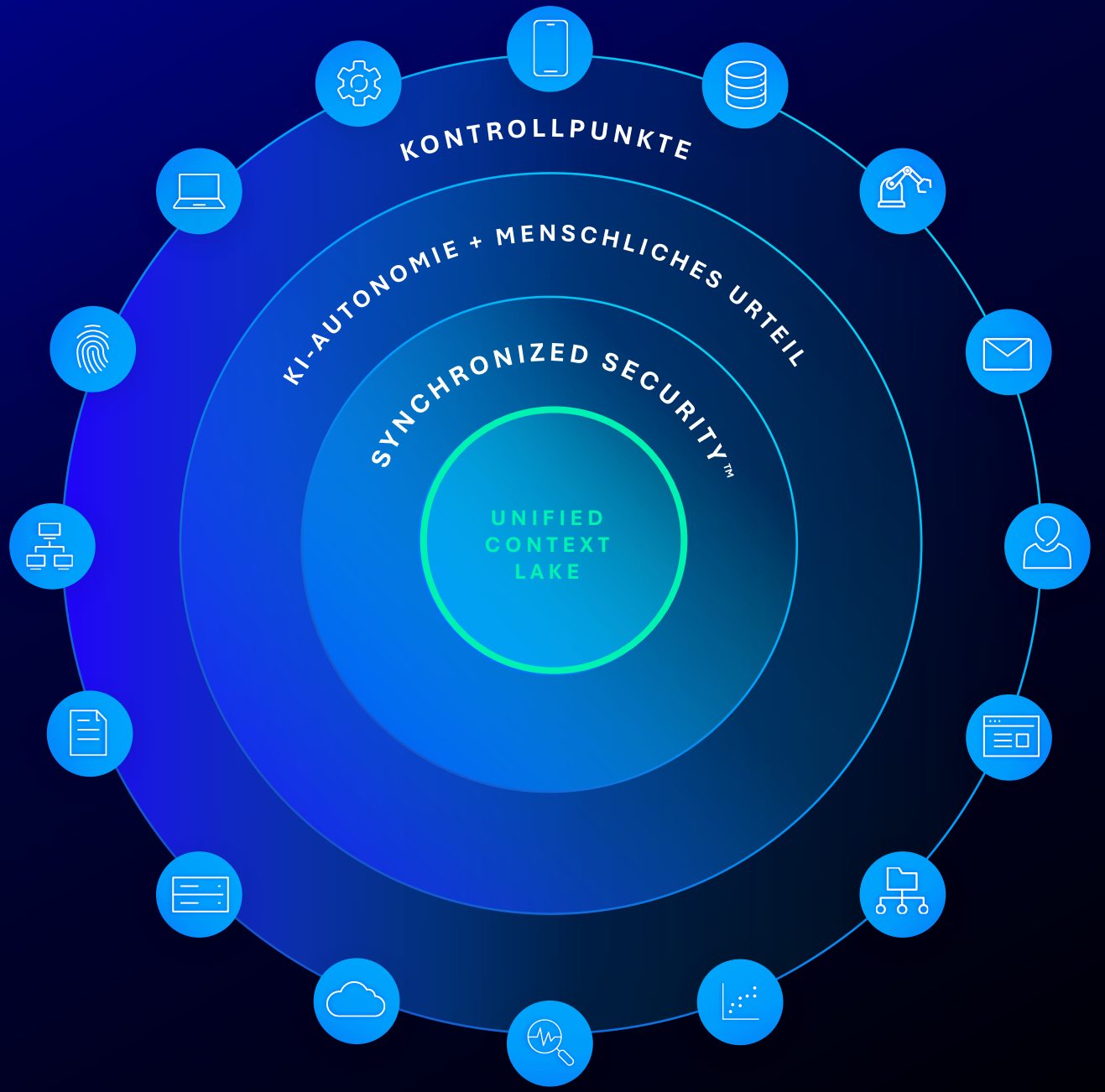
AI-Native Cybersecurity Defense System



FUSION

SOPHOS

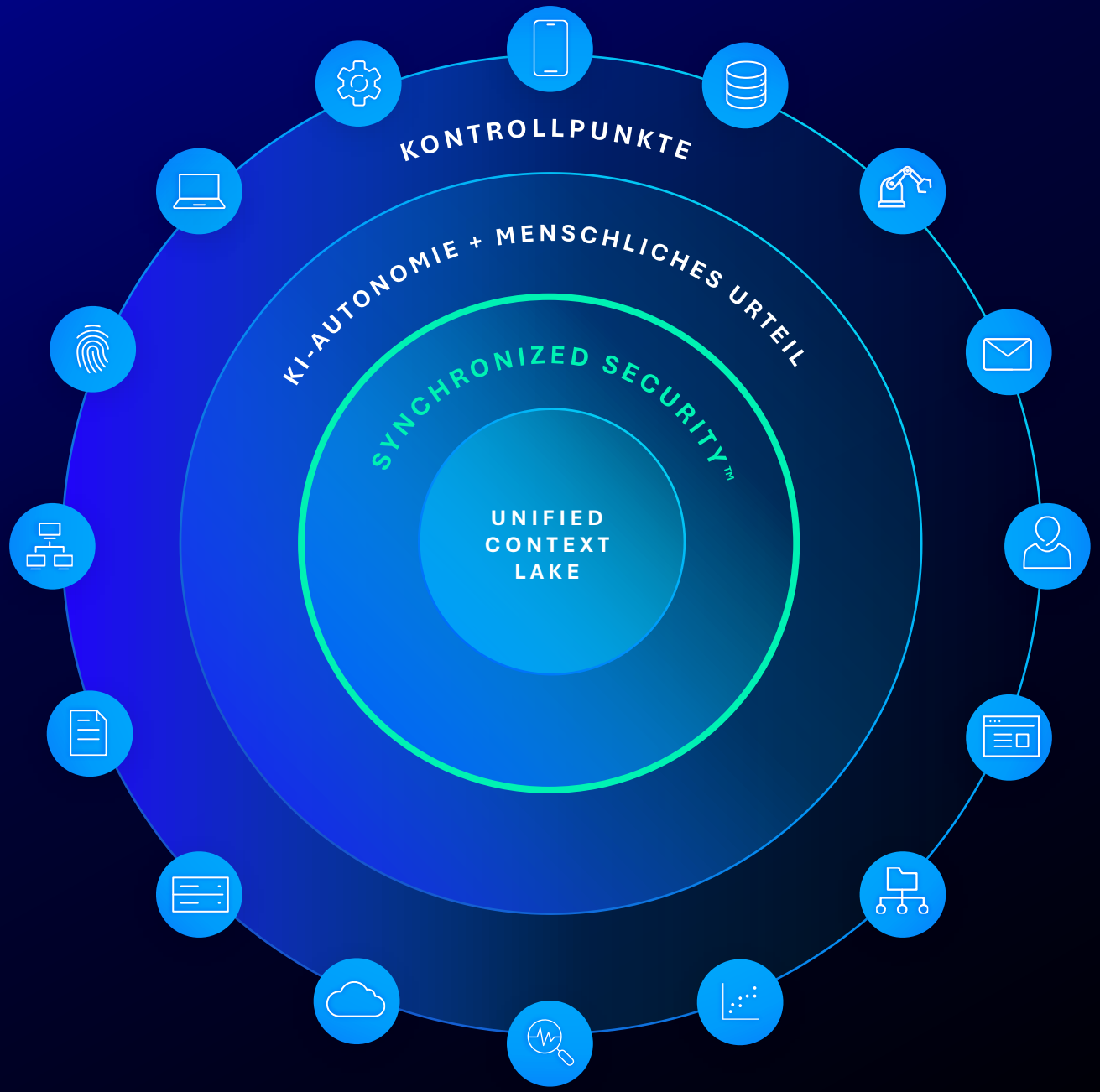
AI-Native Cybersecurity Defense System



FUSION

SOPHOS

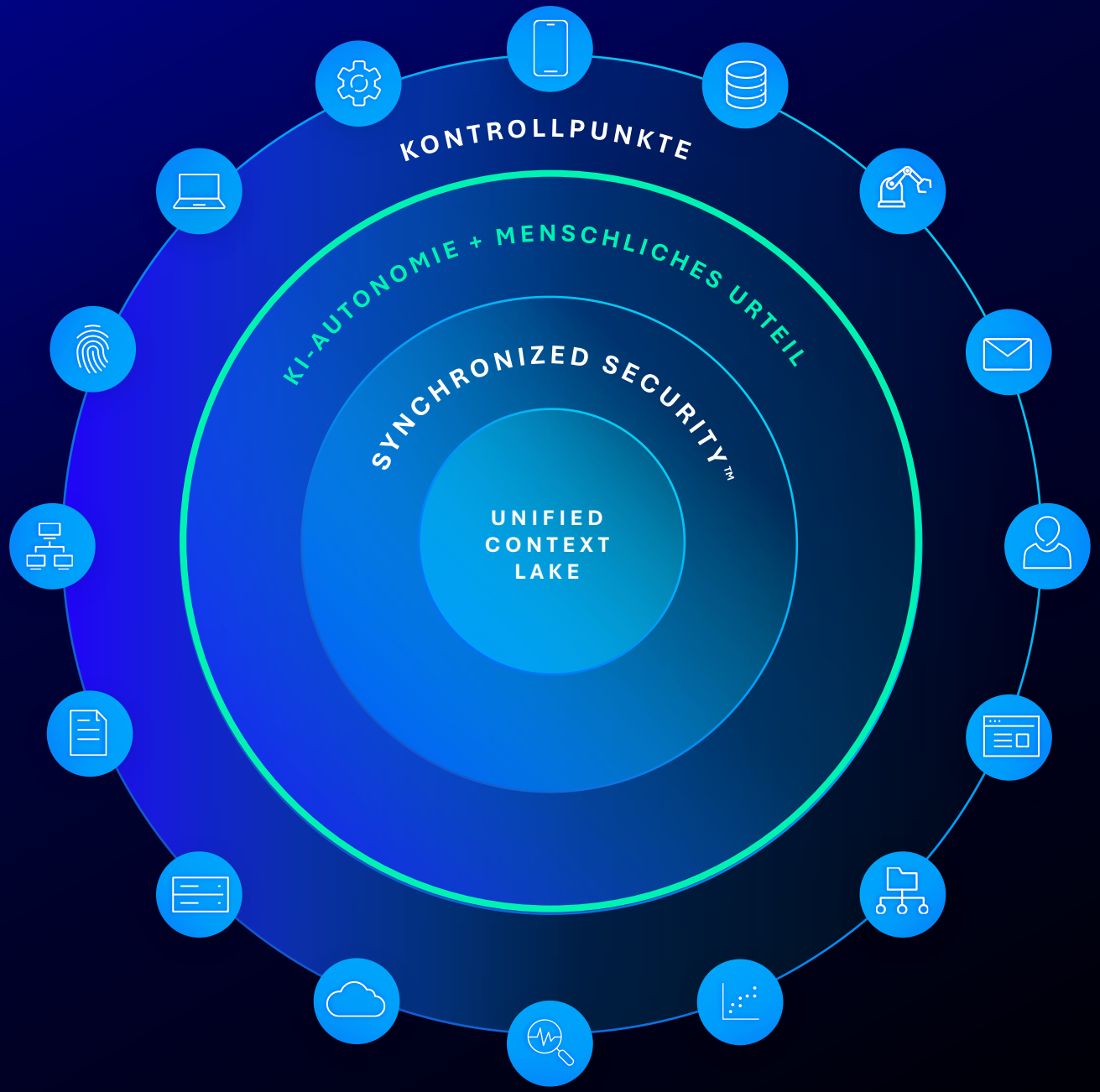
AI-Native Cybersecurity Defense System



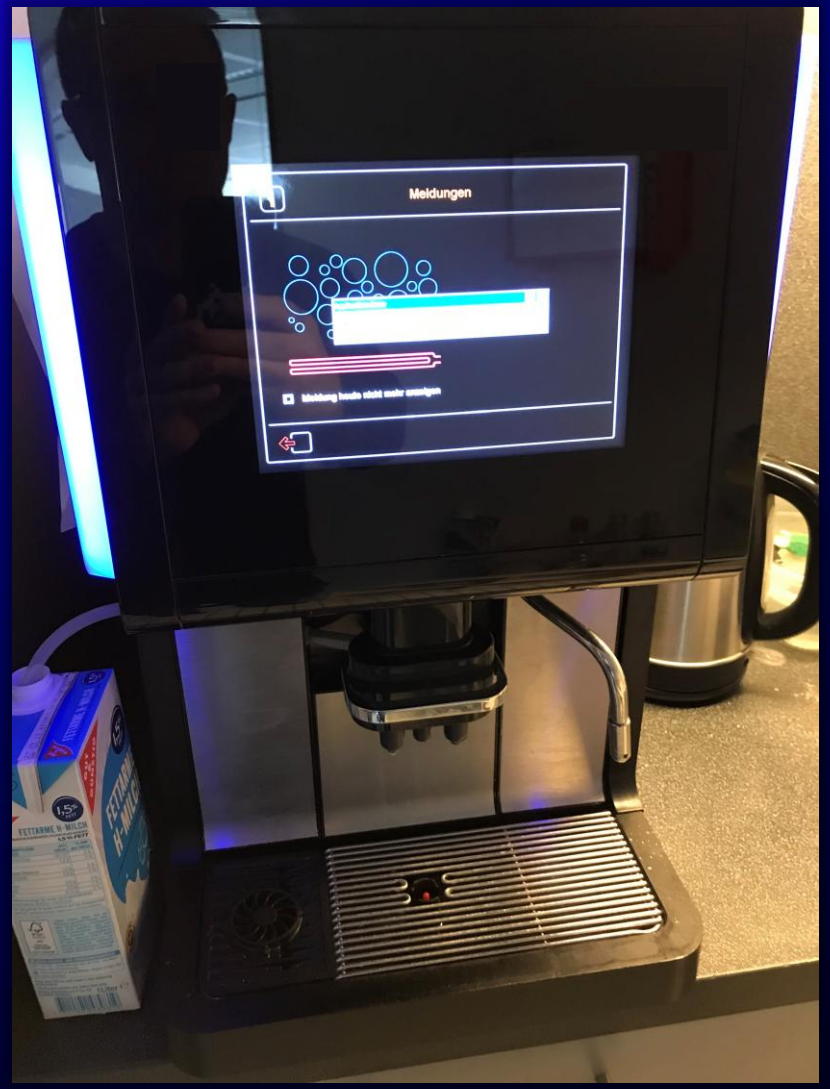
FUSION

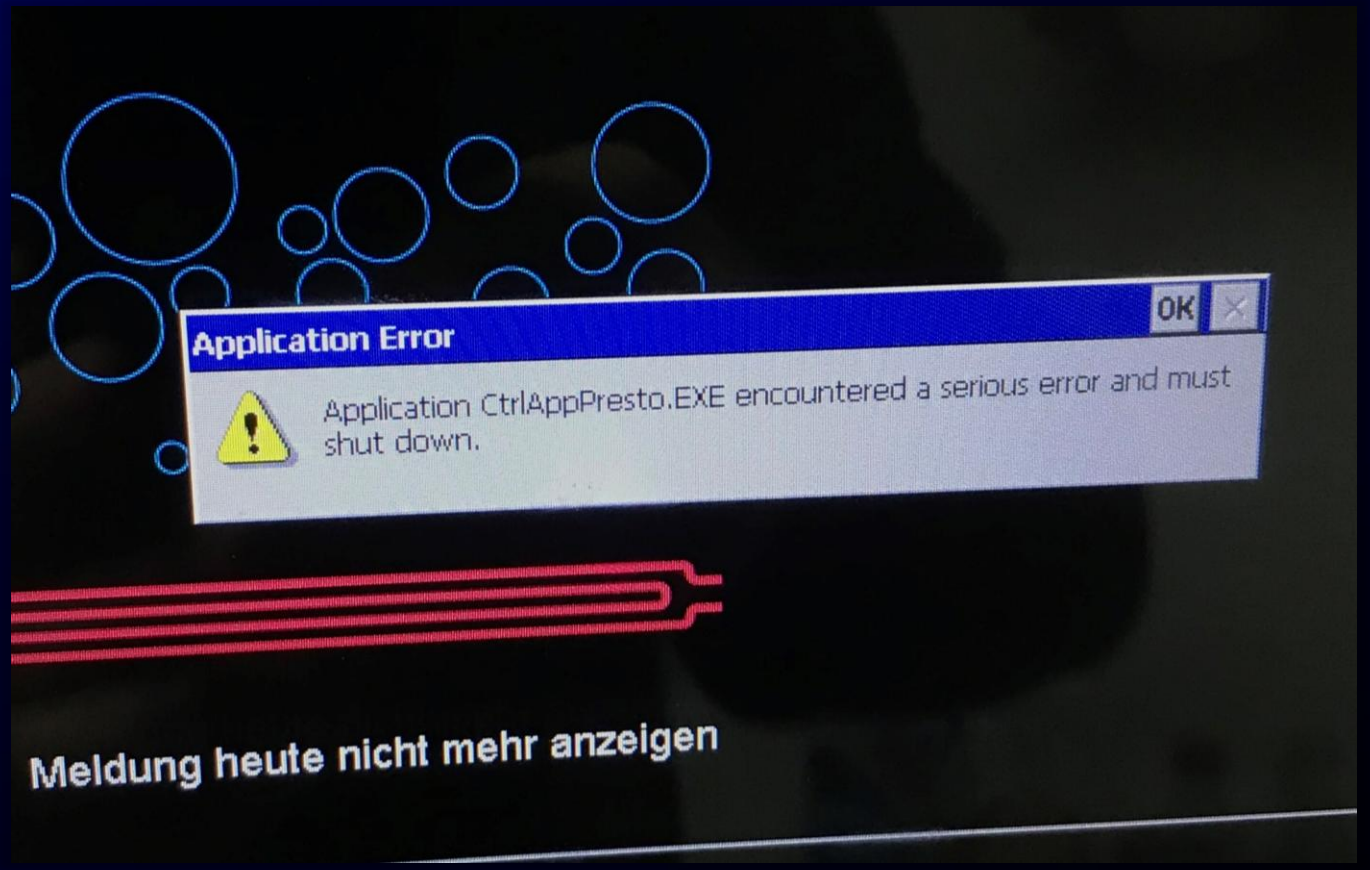
SOPHOS

AI-Native Cybersecurity Defense System



Telemetrie ist wichtig





Offen konzipiert.

500+ Sicherheits- und IT-Integrationen



SOPHOS FUSION

A real attack – and how a defense system responds

The anatomy of a real customer attack, traced step by step

CONTROL POINTS · UNIFIED · OPEN

- CONTROL POINT **Sophos Email** connected
- CONTROL POINT **Microsoft Entra ID** connected
- CONTROL POINT **MS Graph Security** connected
- CONTROL POINT **Sophos Endpoint** connected
- CONTROL POINT **Fortinet Firewall** connected
- CONTROL POINT **Sophos Firewall** connected

UNIFIED CONTEXT LAKE

One data model · one timeline · one detection across every vendor

AI CORRELATION
Signals from every source into one attack chain

→ **AUTOMATED CONTAINMENT**
Block, isolate and revoke sessions

→ **HUMAN ACCOUNTABILITY**
Analyst reviews, cleans up and releases

→ **CONTINUOUS IMPROVEMENT**
Every lesson protects all customers

SOPHOS

SOPHOS FUSION

Sophos protection in place

Endpoint, email and an internal segmentation firewall at the customer

CONTROL POINTS · UNIFIED · OPEN

- SOPHOS — **Sophos Email** — protected
- CONTROL POINT — **Microsoft Entra ID** — connected
- CONTROL POINT — **MS Graph Security** — connected
- SOPHOS — **Sophos Endpoint** — protected
- CONTROL POINT — **Fortinet Firewall** — connected
- SOPHOS — **Sophos Firewall** — segmentation

UNIFIED CONTEXT LAKE

One data model · one timeline · one detection across every vendor

AI CORRELATION
Signals from every source into one attack chain

→ **AUTOMATED CONTAINMENT**
Block, isolate and revoke sessions

→ **HUMAN ACCOUNTABILITY**
Analyst reviews, cleans up and releases

→ **CONTINUOUS IMPROVEMENT**
Every lesson protects all customers

SOPHOS

SOPHOS FUSION

Open to third-party technology

Microsoft 365, Entra ID and the gateway firewall are connected in the same way

CONTROL POINTS · UNIFIED · OPEN

- CONTROL POINT — **Sophos Email** — connected
- MICROSOFT — **Microsoft Entra ID** — connected
- MICROSOFT — **MS Graph Security** — connected
- CONTROL POINT — **Sophos Endpoint** — connected
- THIRD PARTY — **Fortinet Firewall** — connected
- CONTROL POINT — **Sophos Firewall** — connected

UNIFIED CONTEXT LAKE

One data model · one timeline · one detection across every vendor

AI CORRELATION
Signals from every source into one attack chain

→ **AUTOMATED CONTAINMENT**
Block, isolate and revoke sessions

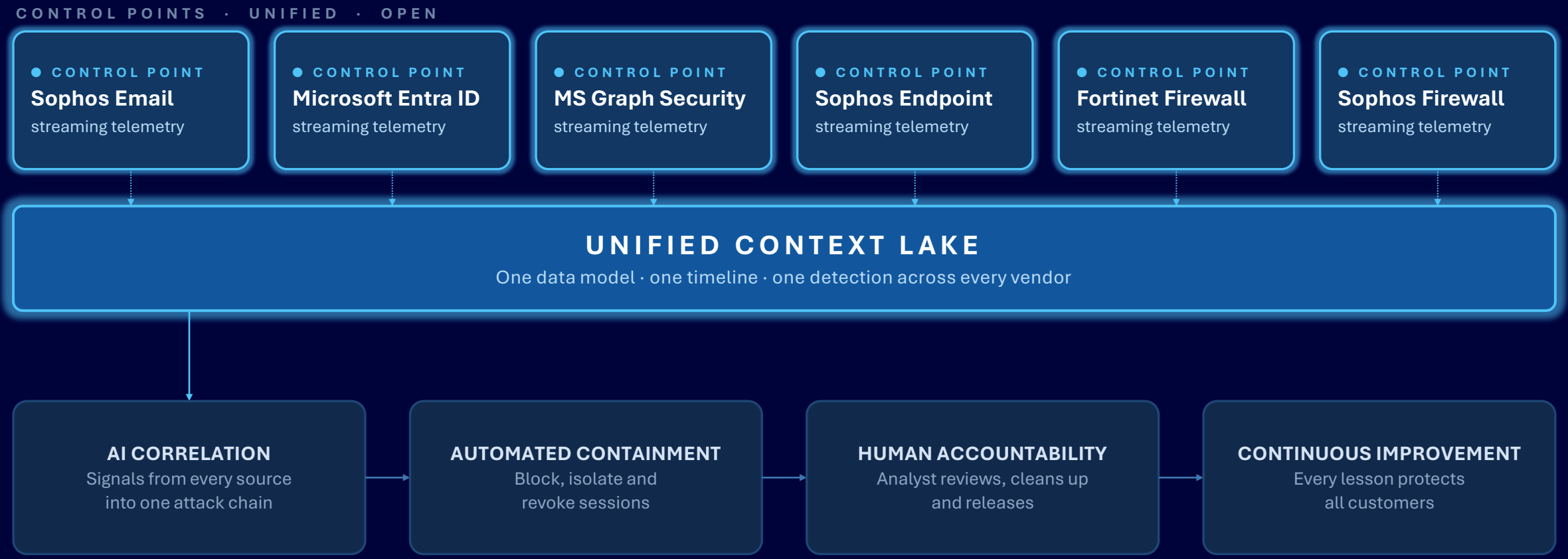
→ **HUMAN ACCOUNTABILITY**
Analyst reviews, cleans up and releases

→ **CONTINUOUS IMPROVEMENT**
Every lesson protects all customers

SOPHOS

Telemetry in real time

Every control point streams continuously into the Unified Context Lake



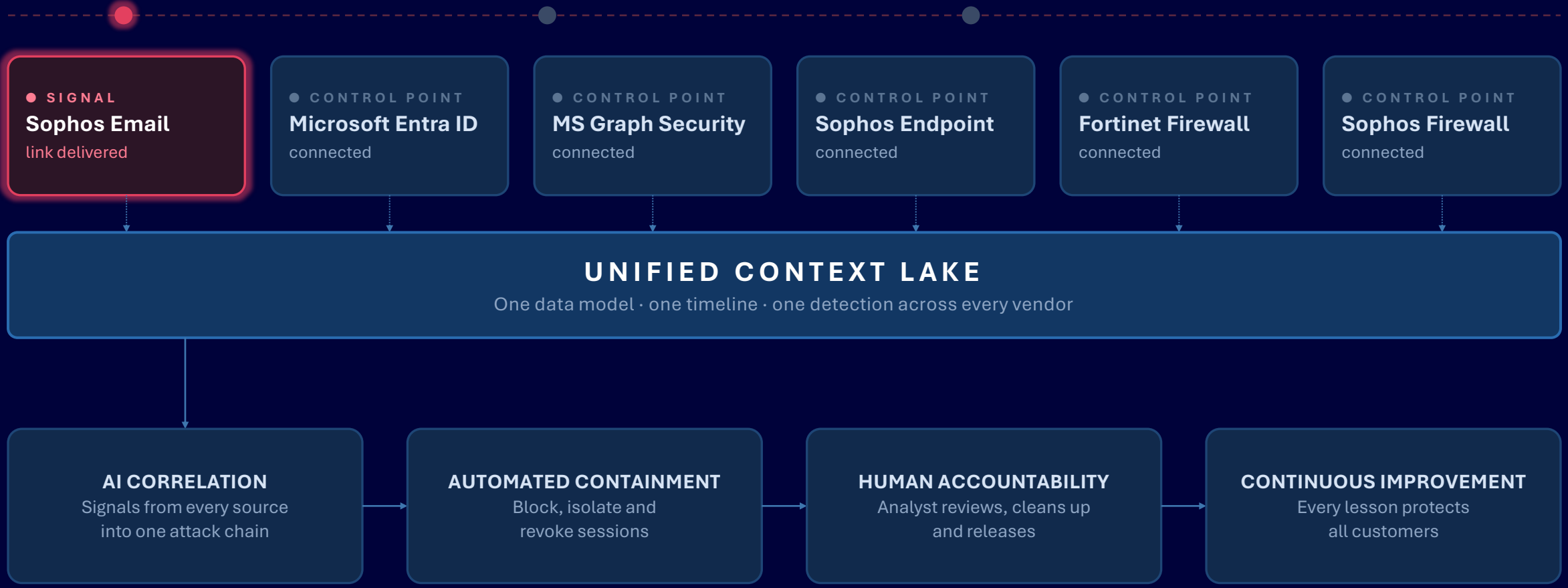
SOPHOS

SOPHOS FUSION

The attack begins

A phishing email carries a link to a convincing fake M365 sign-in page

Phishing email delivered



1 weak signal – no alert on its own

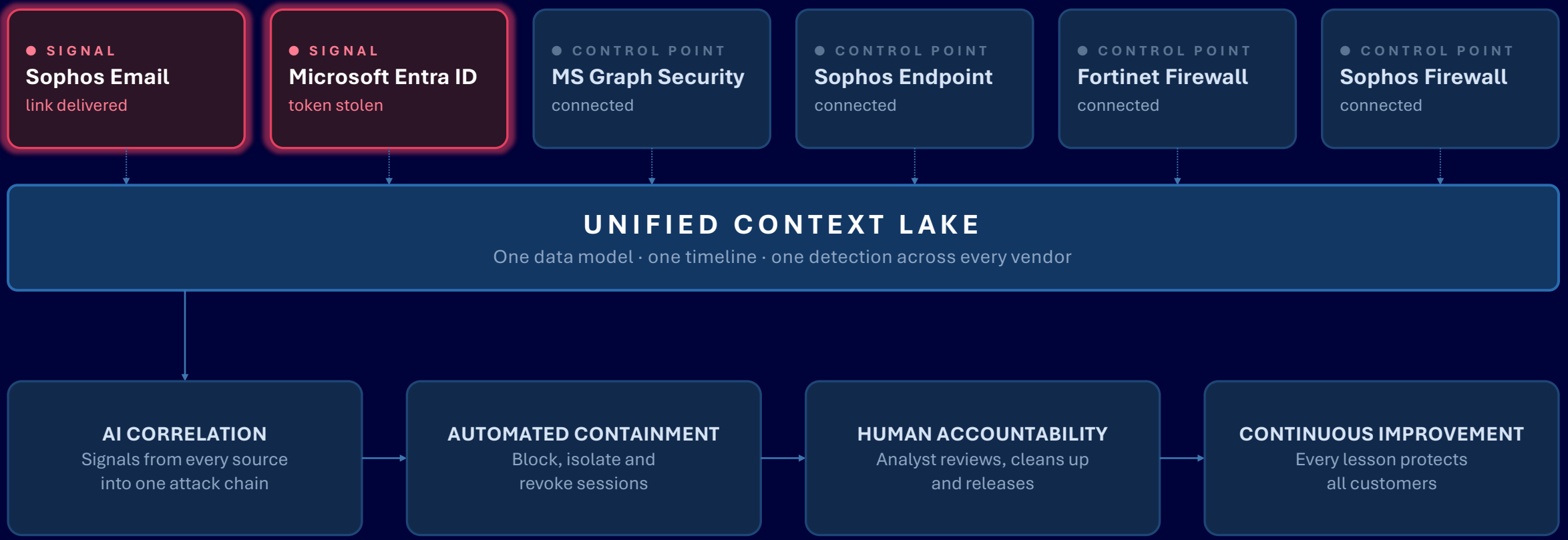
SOPHOS

SOPHOS FUSION

Sign-in intercepted

An adversary-in-the-middle steals the session token – MFA alone does not stop this

Phishing email delivered — **AiTM: token intercepted**



2 weak signals – no alert on their own

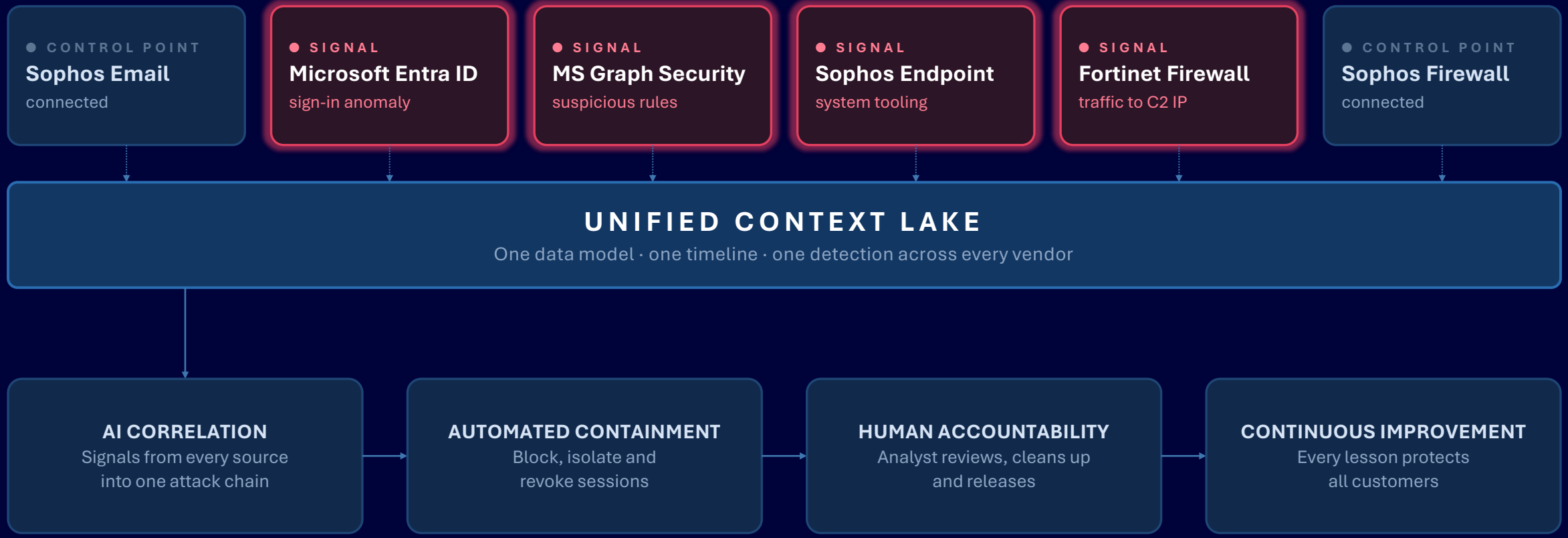
SOPHOS

SOPHOS FUSION

Four control points, four weak signals

Inbox rules for business email compromise, system tooling and C2 traffic

Phishing email delivered — **AiTM: token intercepted** — **Inbox rules & lateral movement**



With other vendors: four consoles, not a single alert

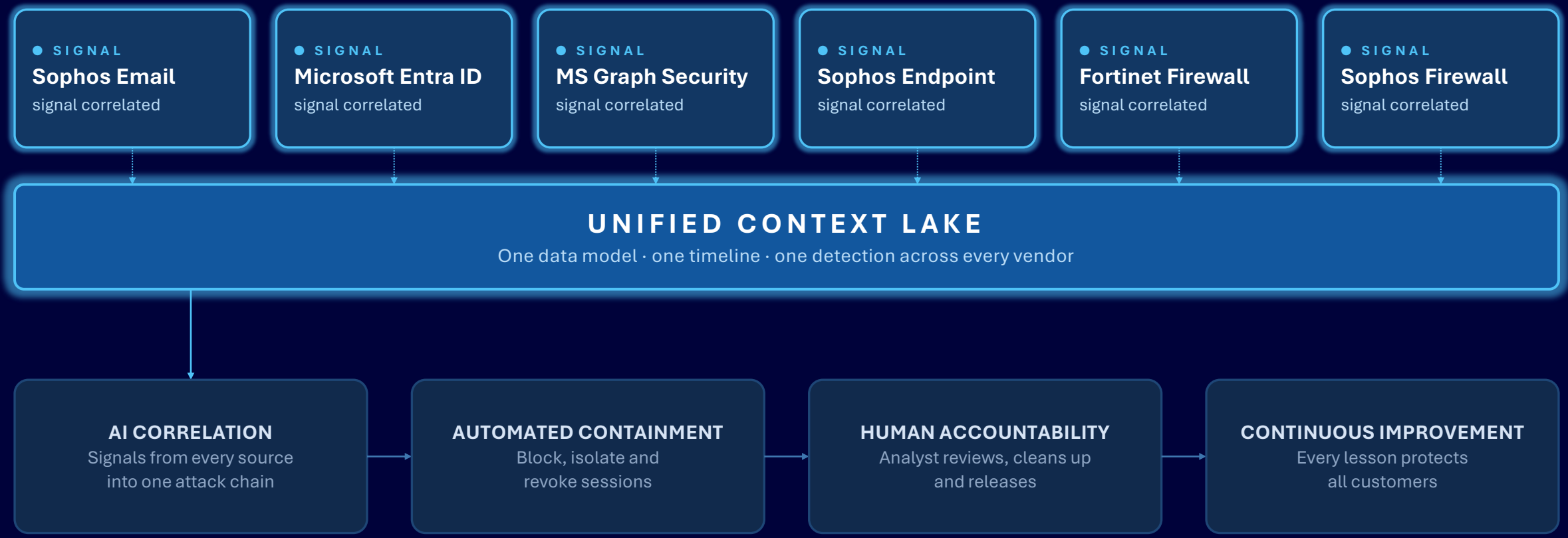
SOPHOS

SOPHOS FUSION

A system, not separate products

Every event lands in the same Unified Context Lake and triggers the detection together

Phishing email delivered — **AiTM: token intercepted** — **Inbox rules & lateral movement**

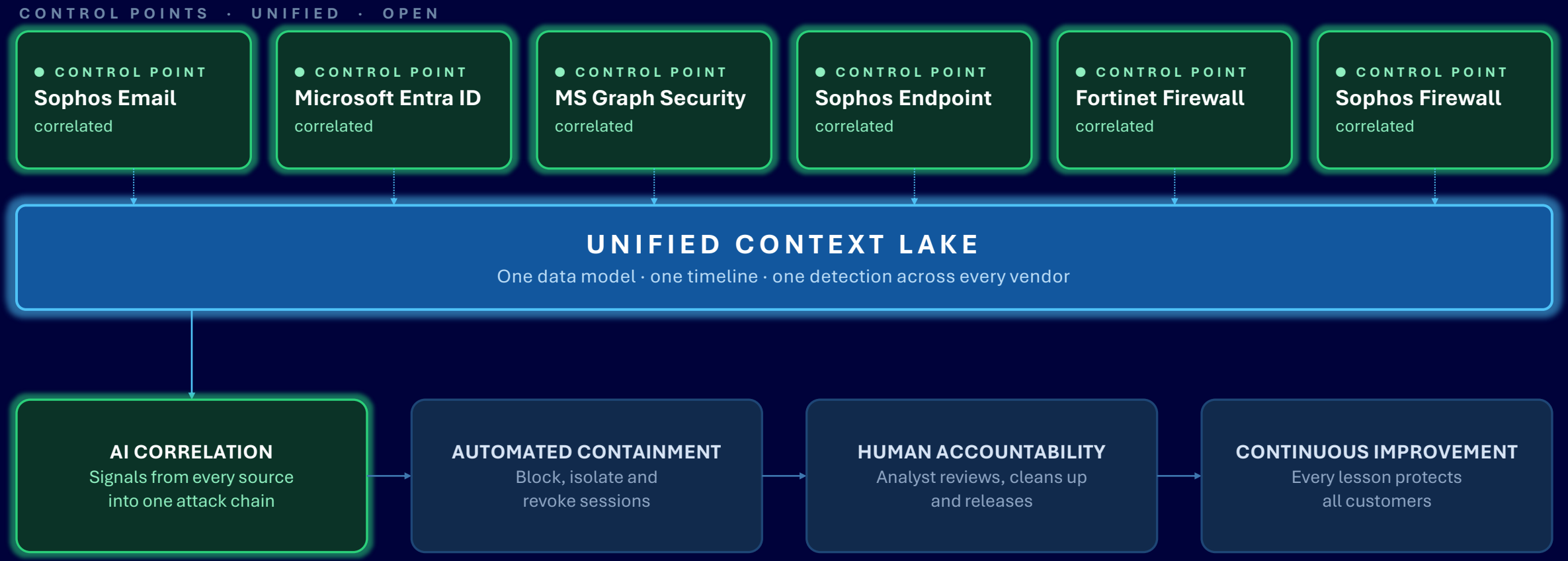


No single event is enough – only the shared context reveals the attack

SOPHOS

Seconds later: the full picture

Six signals, one attack chain, one console



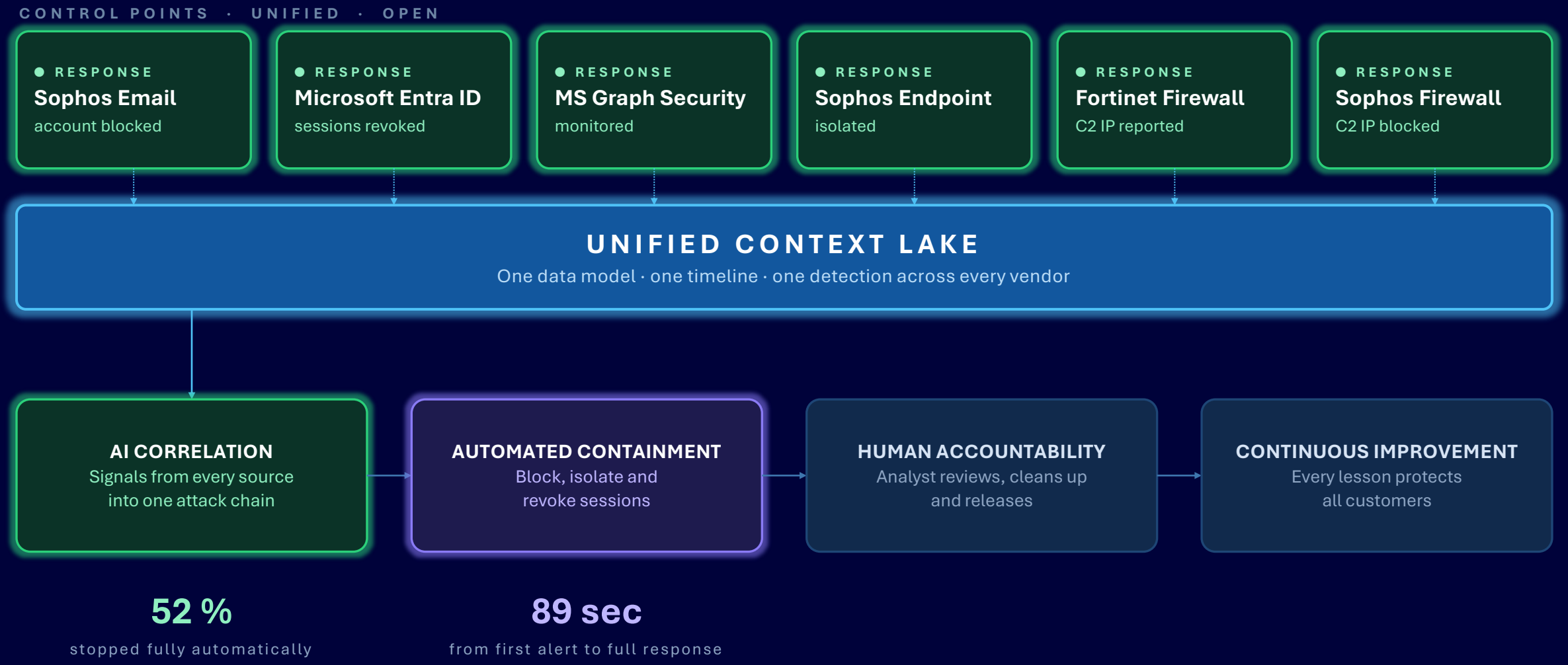
52 %

of attacks stopped fully automatically

SOPHOS

Automated response

Account blocked, sessions revoked, endpoint isolated, C2 IP blocked



52 %
stopped fully automatically

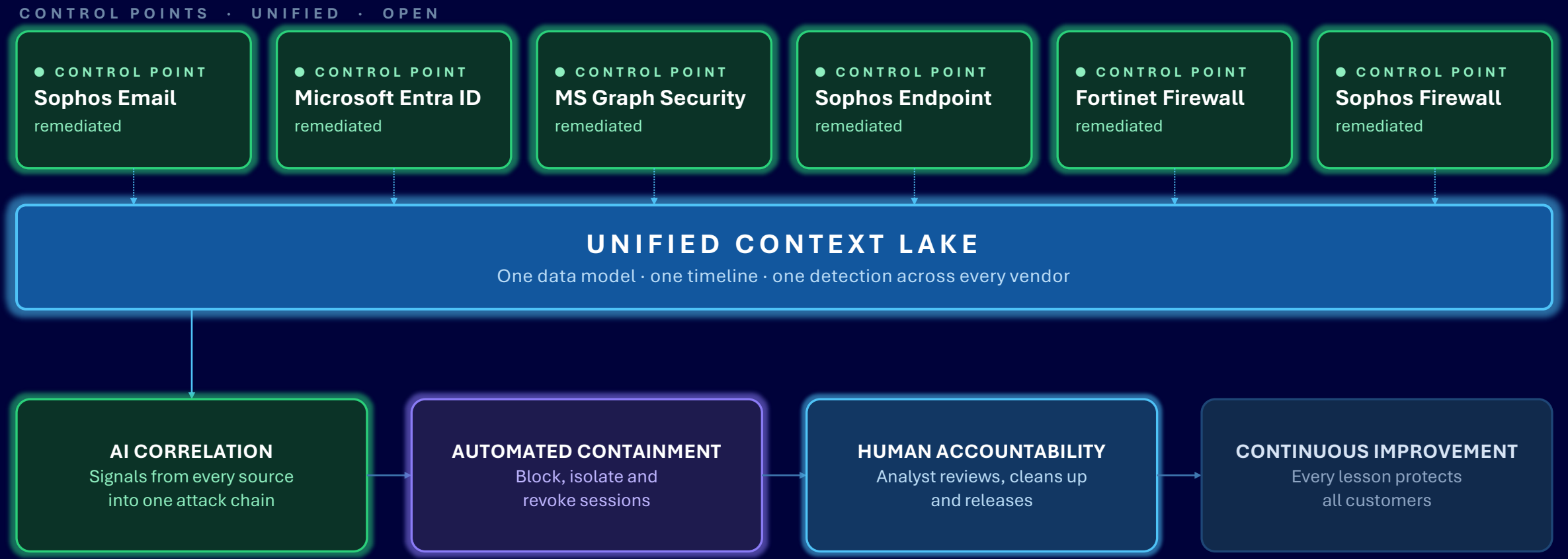
89 sec
from first alert to full response

SOPHOS

SOPHOS FUSION

Humans stay accountable

The analyst reviews the inbox rules, cleans up, resets the password and closes the case



89 sec
from first alert to full response

48 %
reviewed and closed by analysts

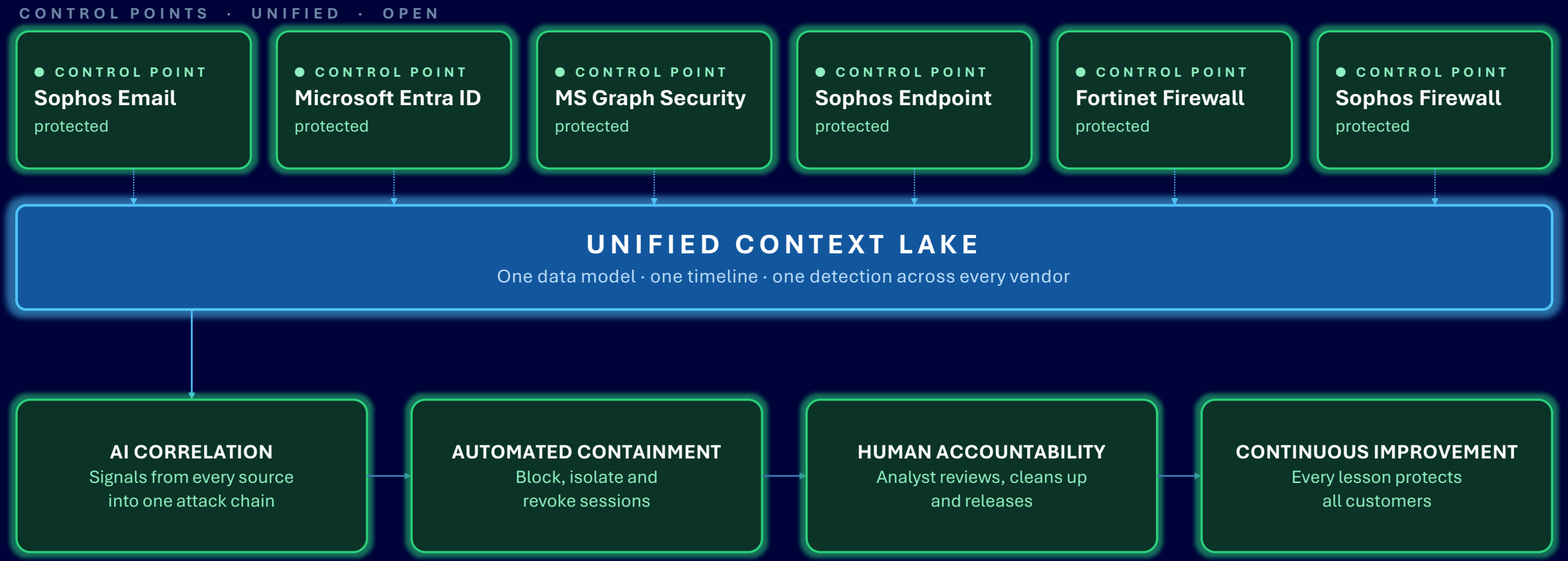
AI acts autonomously – humans set the boundaries

SOPHOS

SOPHOS FUSION

The system learns – for everyone

What was learned in this case now protects every organization in the network



625,000+

organizations protected instantly

SOPHOS

This case happened exactly like this

Sophos MDR at a glance

40K+ MDR customers globally

A vast, diverse customer base provides unparalleled intelligence and proactive threat defense.

1K+ Investigations completed daily

Our highly skilled experts monitor, triage, investigate, and respond to threats on your behalf.

200+ Advanced attacks stopped every day

Learnings from attacks stopped by Sophos MDR drive enhancements to proactive protection.

Global analyst coverage



Tested. Recognized. Trusted.

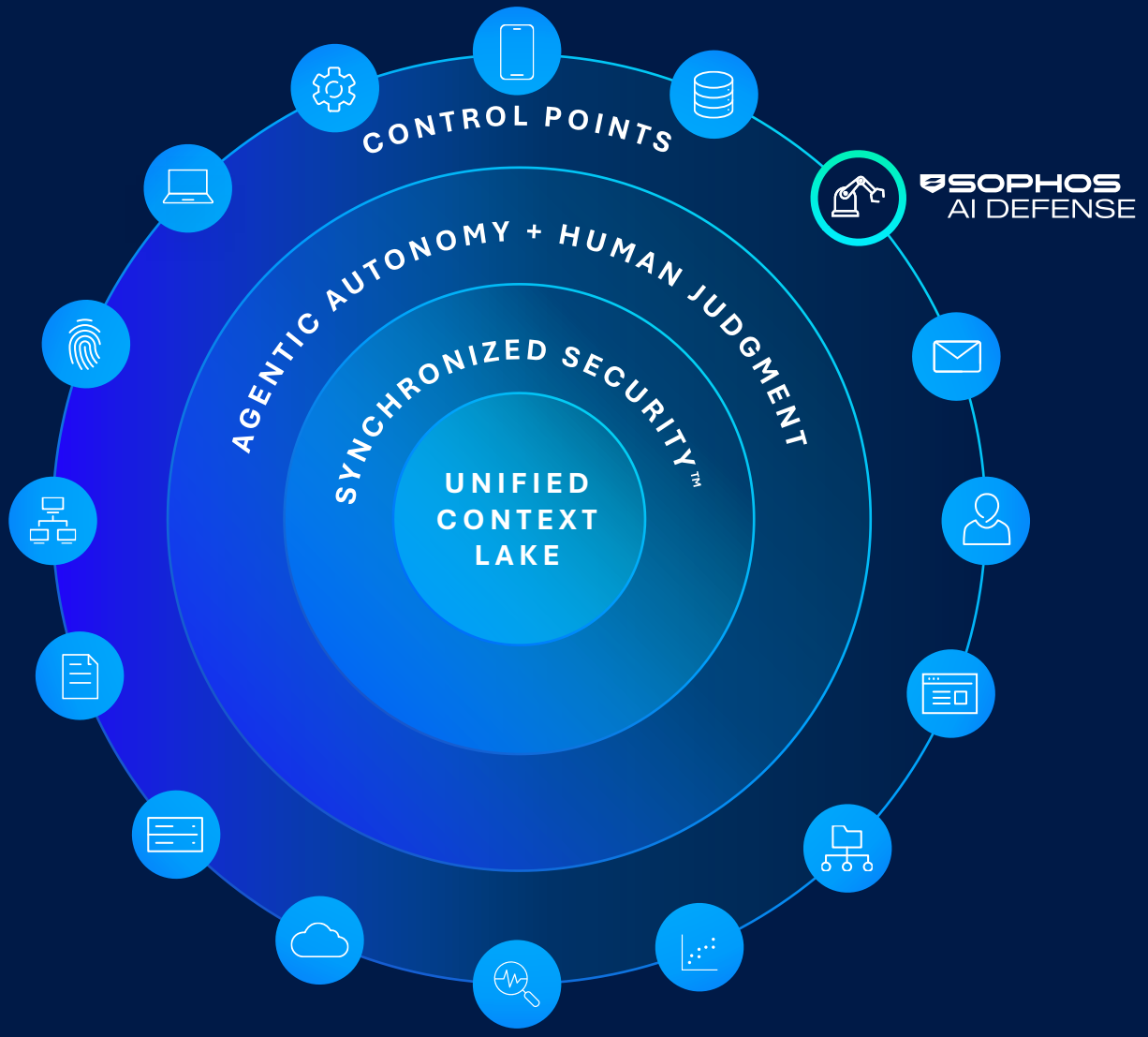
- Gartner Peer Insights Customers' Choice 2026 — Customers' Choice
- MITRE ATT&CK® — 100% detection
- FROST & SULLIVAN — Leader
- G2 Grid® Reports — Highest-rated
- kuppingercole ANALYSTS — Leader

SOPHOS

FUSION

SOPHOS

AI-Native Cybersecurity Defense System



SOPHOS

Coordinated action across the AI lifecycle

SEE → CONTROL → SECURE



Discover: See AI usage in customer environment

Reveals sanctioned, shadow, and embedded AI across users, agents, and workflows so nothing runs beyond customer visibility.



Assess: Focus on customer's AI risk

Evaluates identity, data exposure, location, and behavior in context to separate acceptable use from activity that warrants action.



Enforce: Apply AI policy as adoption grows

Applies continuous guardrails on prompts, data sharing, and agent behavior — keeping AI use aligned with policy and regulation without slowing innovation.



Respond: Contain AI risk before impact

Detects, investigates, and contains AI-driven risk through proven MDR workflows, handling AI incidents as first-class security events, not exceptions.

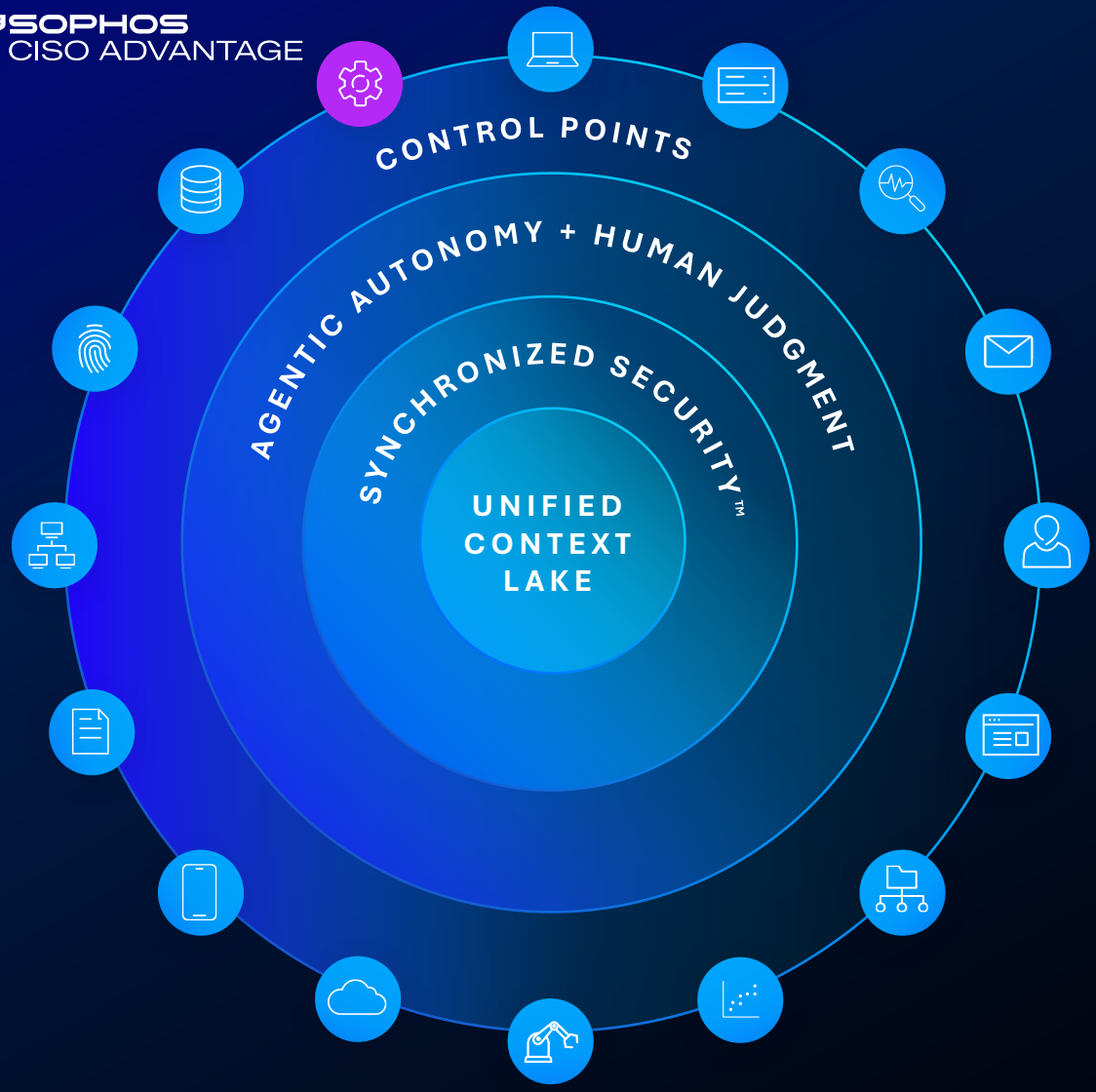
SOPHOS

SOPHOS

FUSION

AI-Native Cybersecurity Defense System

SOPHOS
CISO ADVANTAGE



Security leadership is not scaling fast enough



Global CISO Shortage

35,000 CISOs serve 359 million businesses worldwide

10,000 : 1 coverage ratio

Source: 2026 CISO Report, Cybersecurity Ventures



Rising Cost of Cyber Crime

The global cost of cyber crime will more than double between 2021 and 2031

$12.2T bill by 2031

Source: 2026 CISO Report, Cybersecurity Ventures



Disproportionate SMB Impact

90% of companies worldwide are small businesses

~0% of SMBs have a CISO

Source: World Economic Forum; 2026 CISO Report, Cybersecurity Ventures

SOPHOS

Compliance Challenges

Multiple Obligations	**5**	compliance standards adhered to on average
Resourcing Overhead	**39%**	of IT/cyber team's time spent on compliance activities
Lack of Visibility	**82%**	of leaders are concerned they are not fully compliant
Difficulty Keeping Up	**79%**	find it challenging to keep up with compliance changes
Disproportionate SMB Impact	**16%**	more of IT team's time spent on compliance by companies with $10M-$50M annual revenue

Source: Independent survey of 5,000 IT and cybersecurity leaders across 17 countries commissioned by Sophos and conducted in Q1 2026

SOPHOS

Introducing Sophos CISO advantage

A structured approach that helps organizations assess risk, prioritize action, simplify compliance, and demonstrate measurable improvement



SEE YOUR SECURITY POSTURE CLEARLY

Visibility, not assumptions

Understand what is working, where the gaps are, and where to focus first — based on live data, threat intelligence, and business context.



MAKE EVERY SECURITY DECISION COUNT

Decisions backed by evidence.

Translate complex security data into clear, business aligned priorities so leadership can act with confidence.



PROVE PROGRESS, NOT PROMISES

Measurable improvement over time.

Track risk reduction, show framework alignment, and give leadership, auditors, and insurers validated evidence of progress.

SOPHOS


SOPHOS
DEFEAT CYBERATTACKS