VARONIS

Securing AI Starts with data



Robert Elferink

Sales Engineering Leader Northern Europe

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.


VARONIS

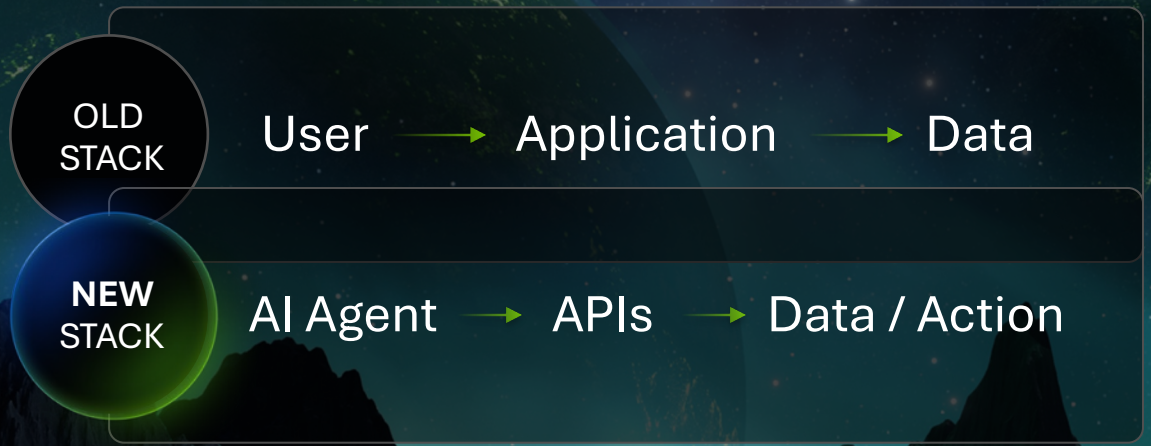
“IT SUCKS, BUT YOU HAVE TO LIVE WITH IT... IT’S CERTAINLY NOT LIKE IT WAS LAST YEAR.”

Lando Norris

McLaren Formula 1 Driver



The Application Collapse



VARONIS


THE AGENTIC REVOLUTION
VARONIS

Every app is reduced to a data store,

Whether they like it or not

BEFORE: MANUAL

1. Log into Rippling
2. Log into Gusto
3. Log into Jira
4. Log into QuickBooks
5. Export 4 spreadsheets
6. Cross-reference Excel
7. Reconcile to GL
8. Send for CFO approval

Time: 5 hours

Quality: Error Prone

AFTER: AGENTS

"Run our payroll process and reconcile to GL. Send final to CFO for approval."

+ Queries 4 APIs
+ Asks 2 clarifying questions
+ Produces clean Excel
+ Sends Excel to CFO

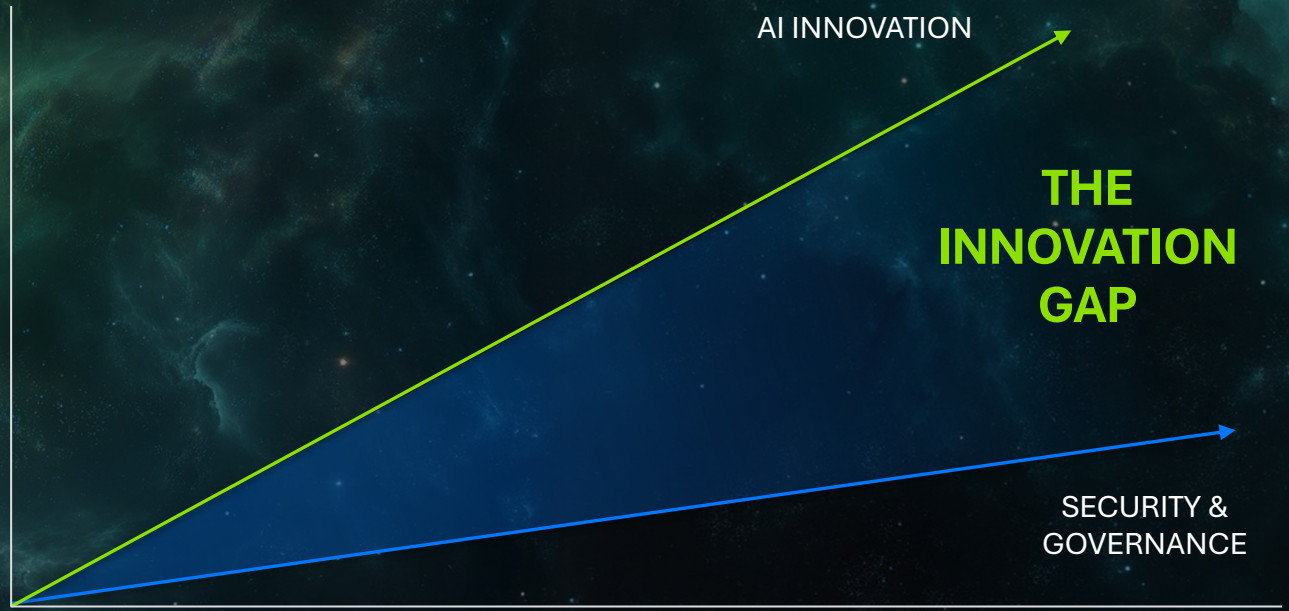
Time: 5 mins.

Quality: Excellent

VARONIS

The stack used to change every 6 years.

Now it changes every 6 days.



VARONIS

The AI train has left the station.




“We need to accelerate AI transformation!”
VARONIS

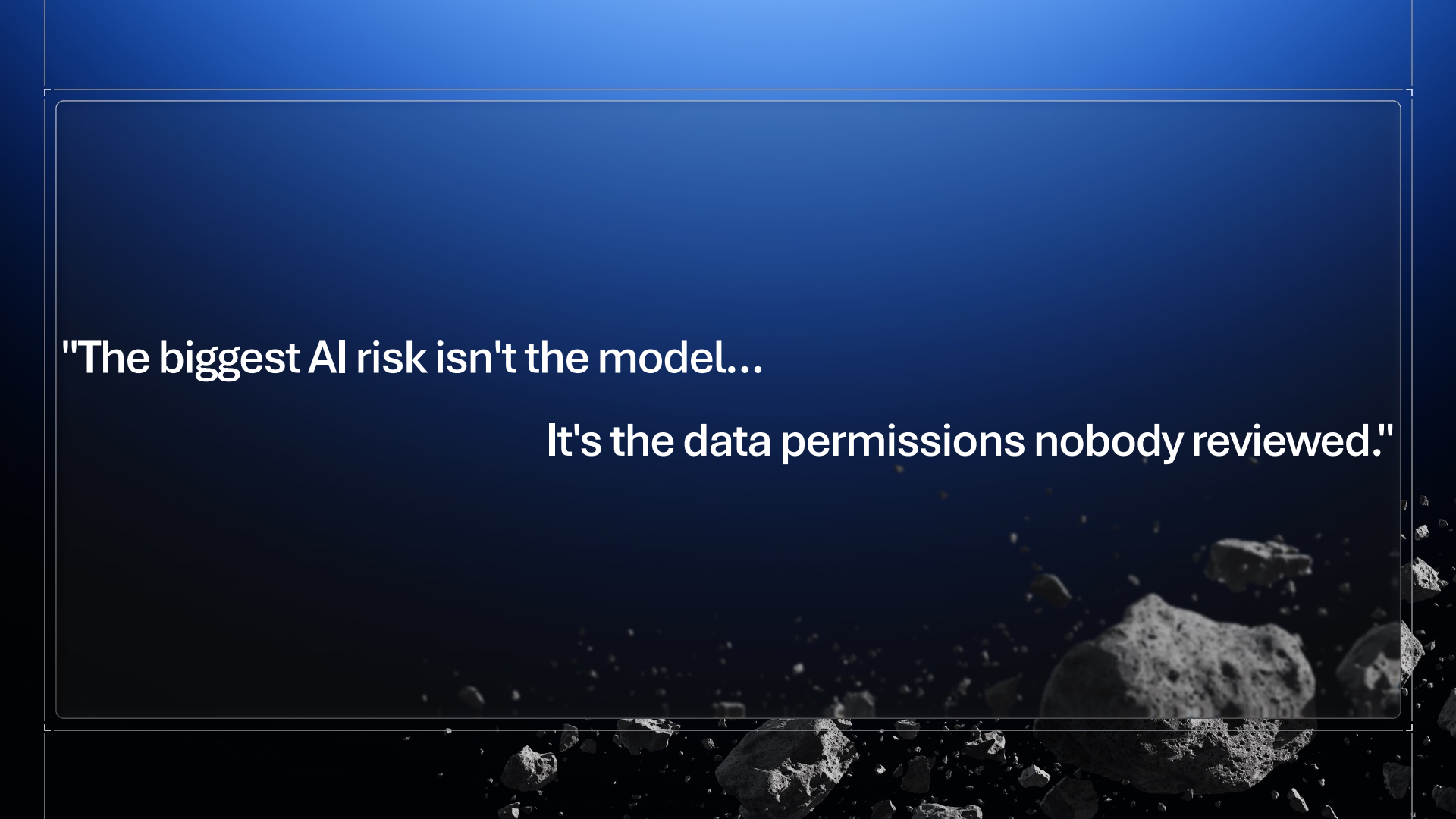
THE CHALLENGE

How do we connect our company’s universe of knowledge to LLMs & agents without compromising security & trust?

VARONIS

"The biggest AI risk isn't the model...

It's the data permissions nobody reviewed."





We don’t know what we don’t see.

- Everyone

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

VARONIS

[Redacted] Critical Findings

1. 455,397 PII records and 210 GB of HR data exposed enterprise-wide
2. 124,498 PII records including birthdates, SIN, gender open enterprise-wide
3. 91k PII records, benefits info, and stale sensitive data within IT department folders
4. 502k birthdates and 1.1 million student ids mixed and accessible to at least 1,000 employees
5. Over 78,000 Personal Health Numbers stored in OneDrive and shared with a Gmail account
6. Medical information, email addresses, counsellor name and more in MS Teams available enterprise-wide



The biggest AI breach in your organization probably won't start with a hacker.

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

AI AS A

TOOL



AI AS AN

EMPLOYEE

VARONIS

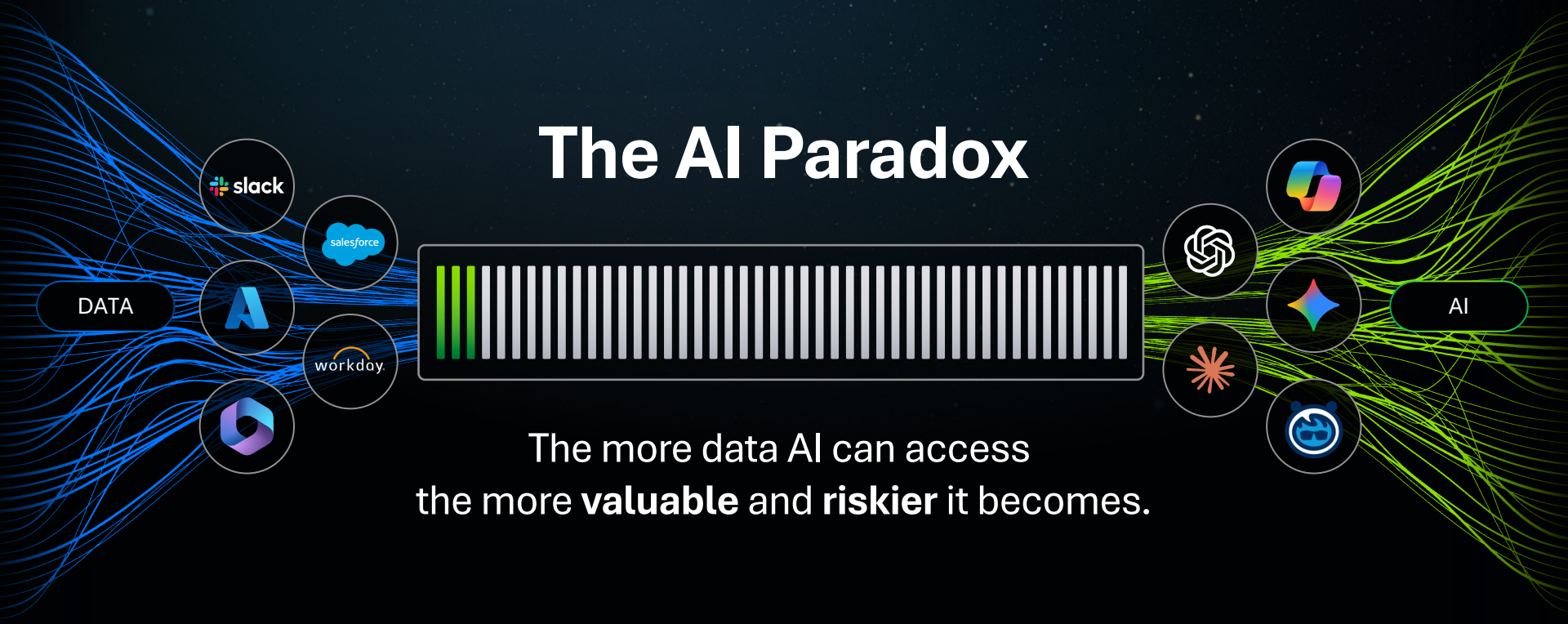
83%

of organizations report have strong visibility into how AI interacts with data using AI



Source: Cyber Insiders, State of AI Data Security, 2025

The AI Paradox



The more data AI can access
the more **valuable** and **riskier** it becomes.

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

VARONIS

BARRIER 1

Securing Your Data

BARRIER 2

Securing Your AI Systems & Agents

BARRIER 3

Fighting AI-Powered Adversaries

VARONIS

The Varonis Approach

Data & AI Security Platform

- Fast setup
- SaaS deployment
- AI-Native

Find

Real-time visibility of your AI and data security posture and runtime activity at petabyte scale.

Fix

Continuously reduce your blast radius, apply labels, and enforce policies without breaking anything.

Alert

Always-on, data-centric UEBA with 24x7 managed data detection and response.

Available on the marketplace: aws Microsoft

8K+
customers

VRNS
Nasdaq

Forrester WAVE LEADER 2025 Data Security Platforms — #1 DSP

Gartner Peer Insights Customers' Choice 2025 — #1 DSPM vendor

G2 SPRING 2026 Leader — DSPM Leader

E*TRADE · BlueCross BlueShield · e+ · Lowe's · Cintas · Nasdaq · Aflac · ING · Penguin Random House

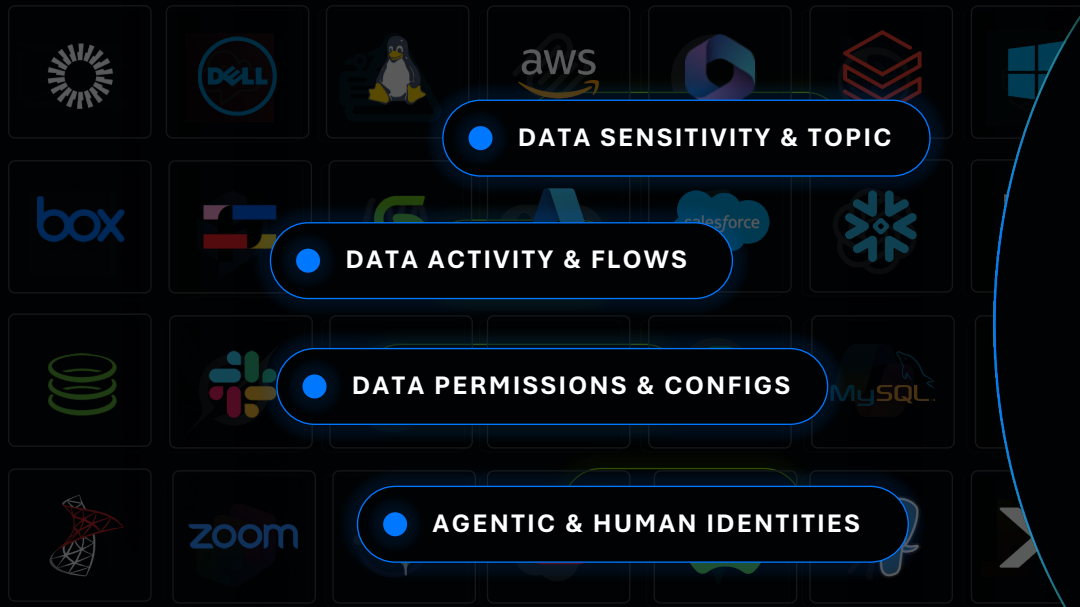
VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

VARONIS

FIND | FIX | ALERT

Real-time visibility

Understand your AI and data security posture and activity in real-time.



Contextual

Understand exposure, usage, lineage, and business context.

Current

We know what's changed and created, so visibility is always up-to-date.

Complete

Full scans on huge data stores.
No blind spots.

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

VARONIS

FIND | FIX | ALERT

Automated prevention

Continuously reduce your blast radius and auto-enforce least agency.

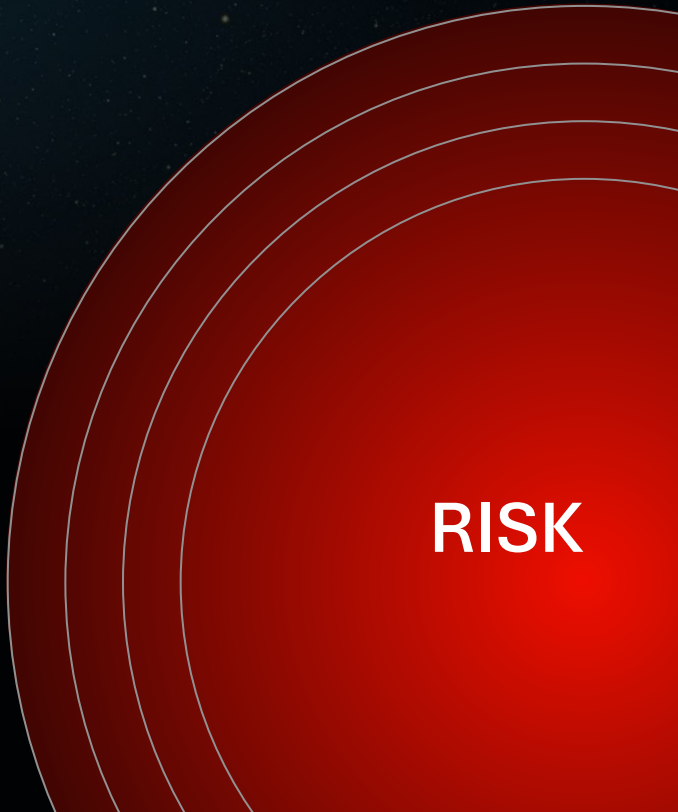
SECURE AI SYSTEMS

- Patch vulnerable code
- Fix misconfigurations
- Block malicious prompts
- Filter sensitive data

PROTECT YOUR DATA

- Right-size permissions
- Apply labels
- Mask and encrypt data
- Archive stale data

...and many more



FIND FIX ALERT

Proactive detection

- We monitor everything
- We respond within minutes
- Fully integrated with your stack



Median Time To Respond

5 Min.

Hours Saved

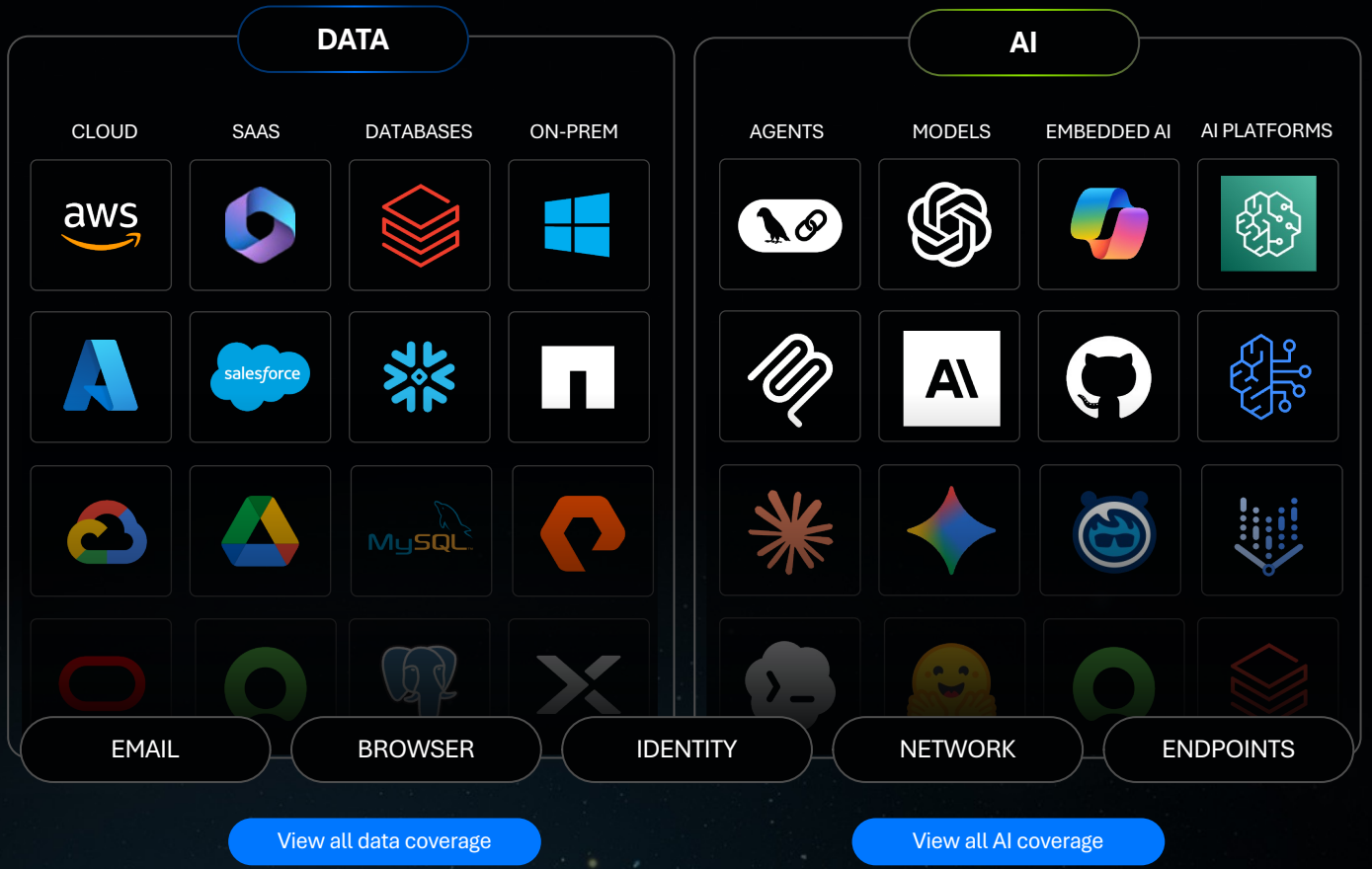
860 Hrs.

Raw Events	Alerts Analyzed	Alerts Escalated	Confirmed Threats
966,507,371	8,951	7	1

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

VARONIS

Secure AI & the data that powers it



VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

VARONIS


The winners won't be the organizations that adopt AI first.
They'll be the organizations that can trust it at scale.
VARONIS


VARONIS