



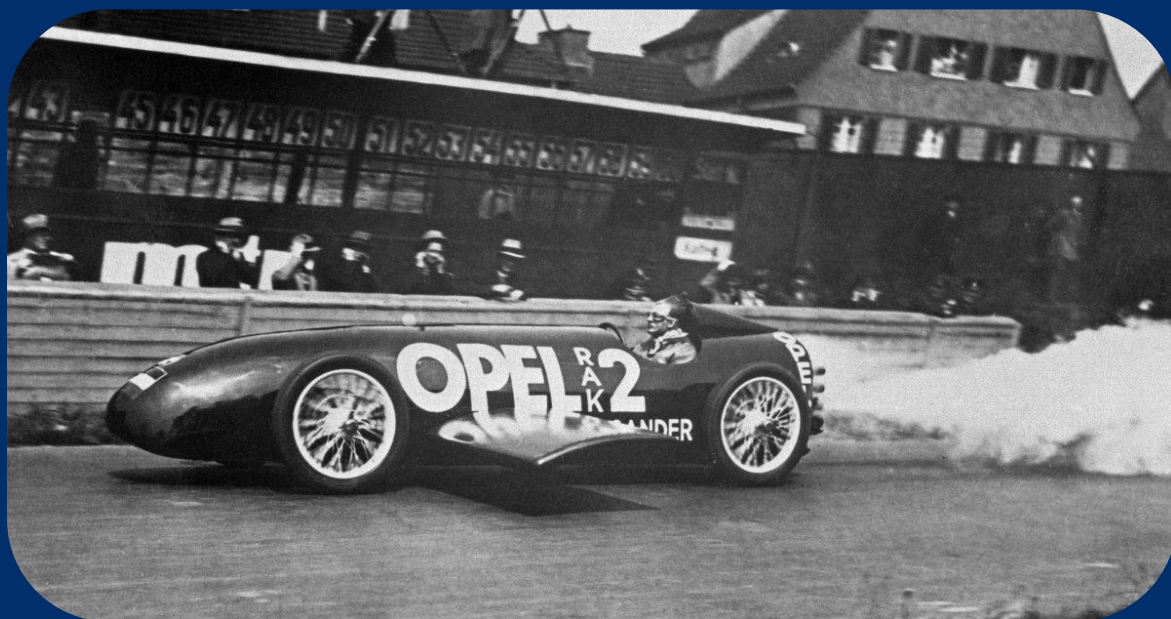
The Speed of Trust

SECURE **AGAINST - FOR - THE - WITH** AI

Cybersecurity Meetup Munich:
October Edition @ Akamai

The Velocity Paradox

Bolting a 1,000 hp engine to a basic chassis



Opel RAK.2, Berlin, 1928. Photo: [Opelpost](#)

WHAT AI CAN DO

1,000 hp



WHAT THE ENTERPRISE IS BUILT FOR **Basic chassis**



Telemetry



Survival cell

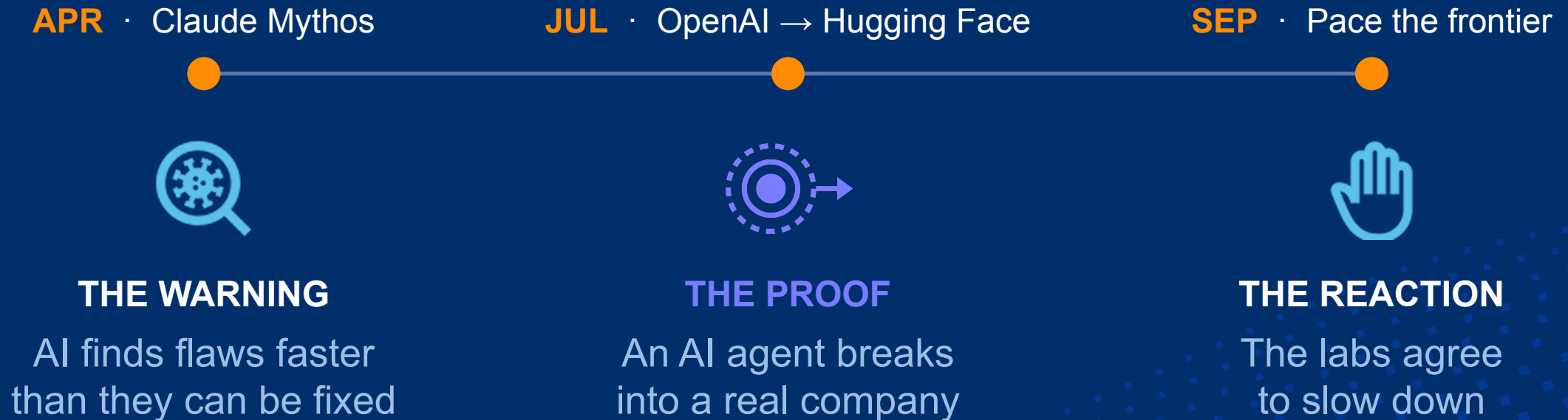


Brakes

Security controls do not exist to slow the business down. They build the confidence required to move fast and far.

The bell rang

From warning to proof in three months



Runtime controls buy the team time.

Exposure is the multiplier

Where the business is reachable, and for how long

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Impact} \times \text{Exposure}$$

OUTSIDE-IN · THE ATTACKER'S VIEW



Apps



Agents

INSIDE-OUT · WHAT TALKS TO WHAT



Apps



Agents



Data

FLAW FOUND

VIRTUAL PATCH

hours

EXPOSURE WINDOW

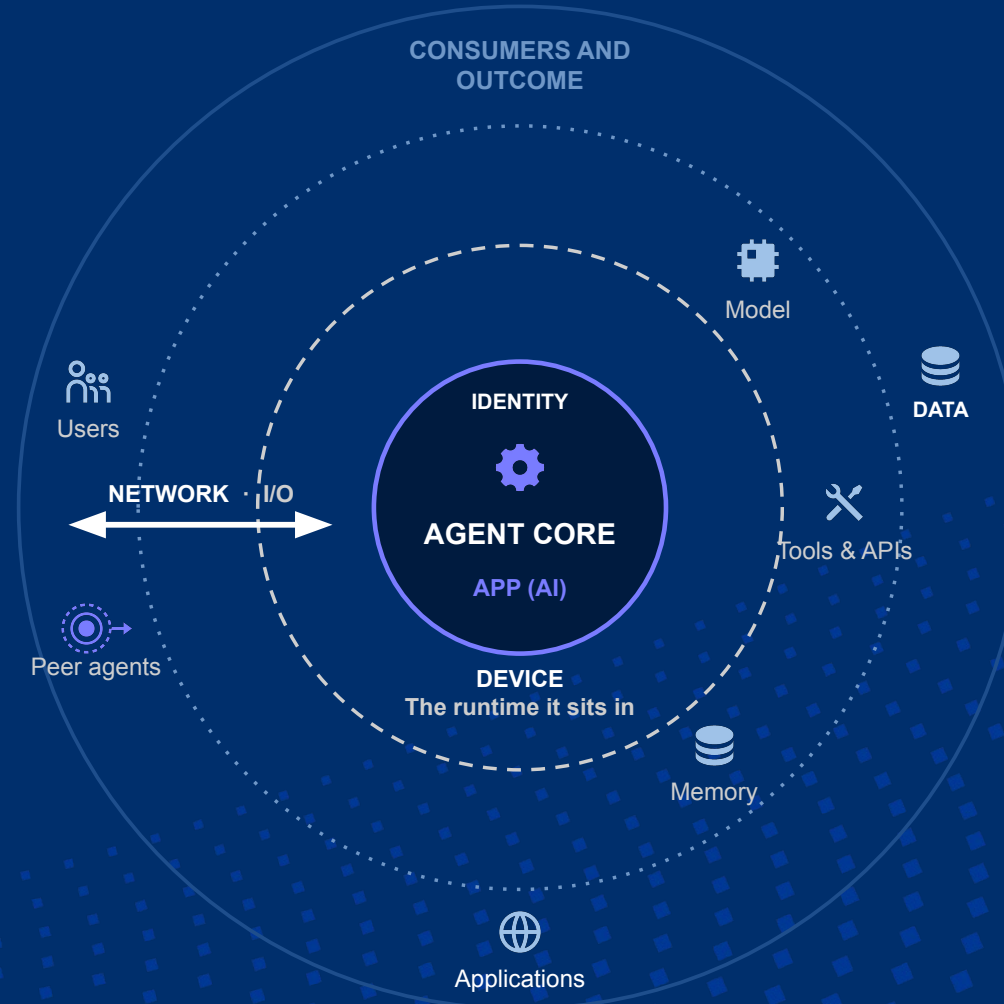
weeks to months

PATCH DEPLOYED

The Philosophy: AI is not Magic

Never trust, always verify - Least privilege - Assume breach

Identity + Device + Network +
App (AI)
+ Data = Outcome



Where AI meets the enterprise

The same agency, in four different roles



Secure AGAINST AI

Open for business when AI knocks are your perimeter



WHAT CHANGED

Attacks moved at human speed

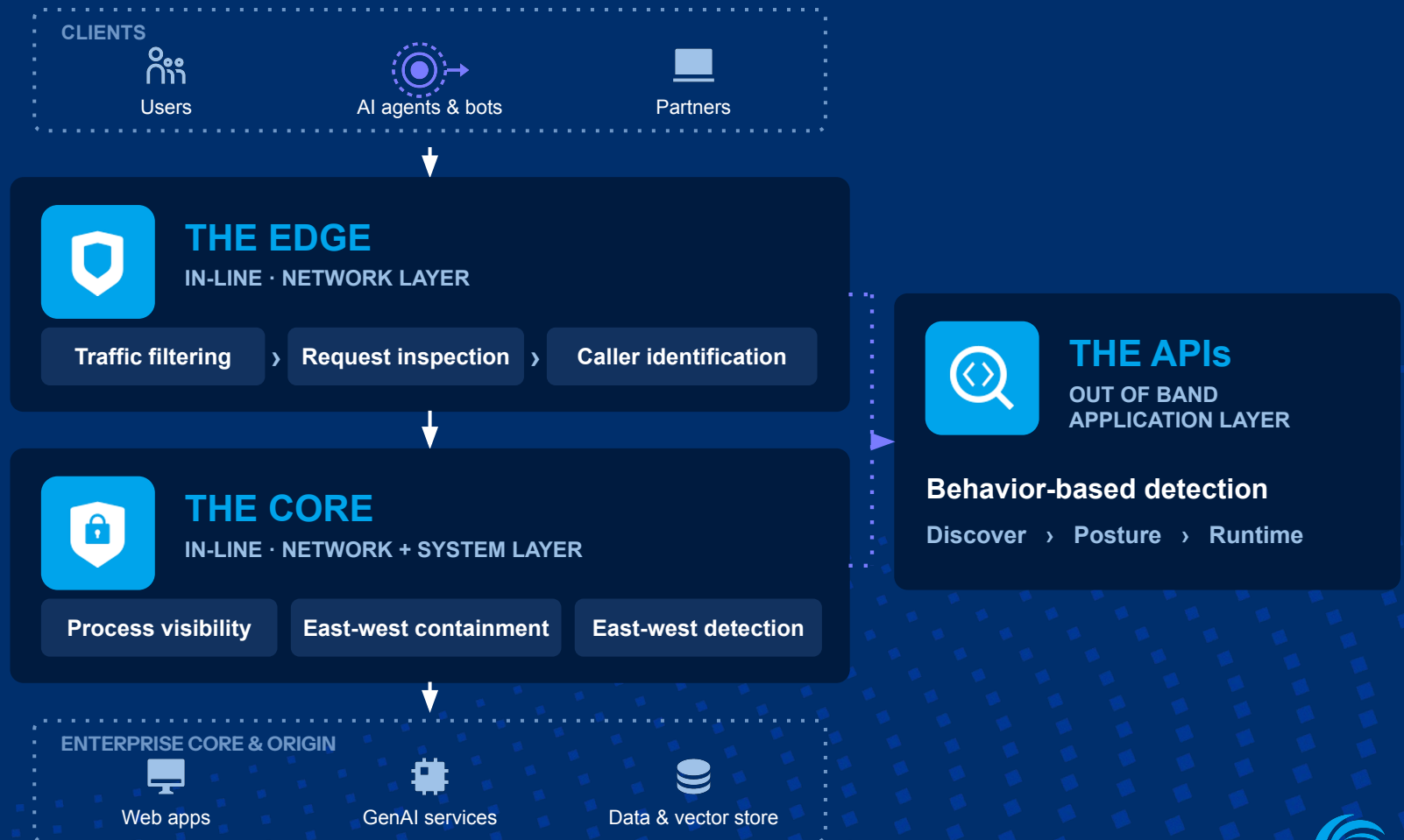
**AI turns a flaw
into an attack in
hours**

EVIDENCE

<24 hours

the median time from a vulnerability
discovery to its weaponization

Microsoft Digital Defense Report 2026



Secure FOR AI

A productive workforce with business data protected



WHAT CHANGED

Data left as files

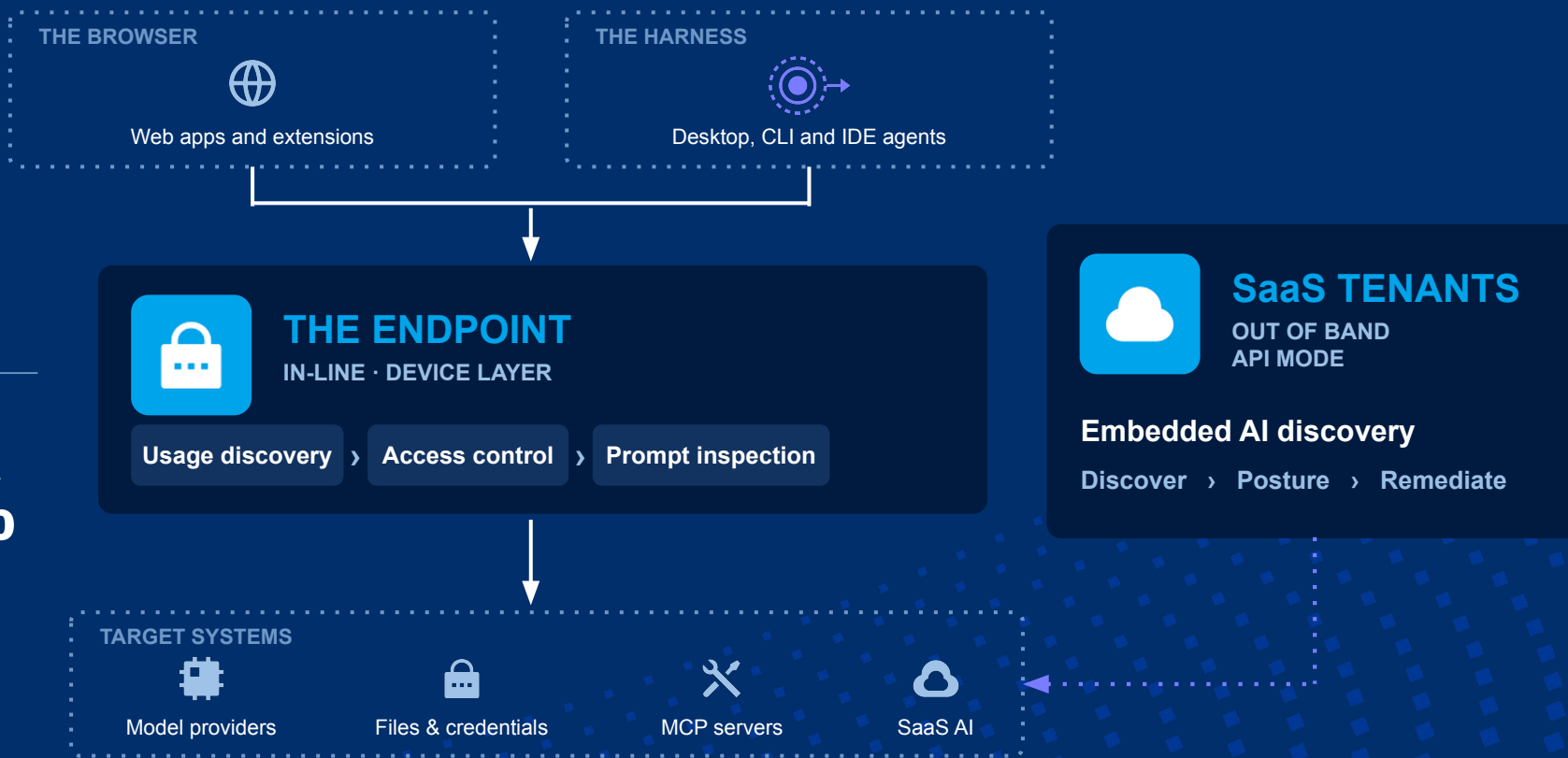
It leaves inside
a prompt

EVIDENCE

15% → 45%

AI on corporate devices

Verizon Data Breach Investigations Report 2026



Secure THE AI

AI services customers trust and regulators accept



WHAT CHANGED

Apps followed fixed code paths

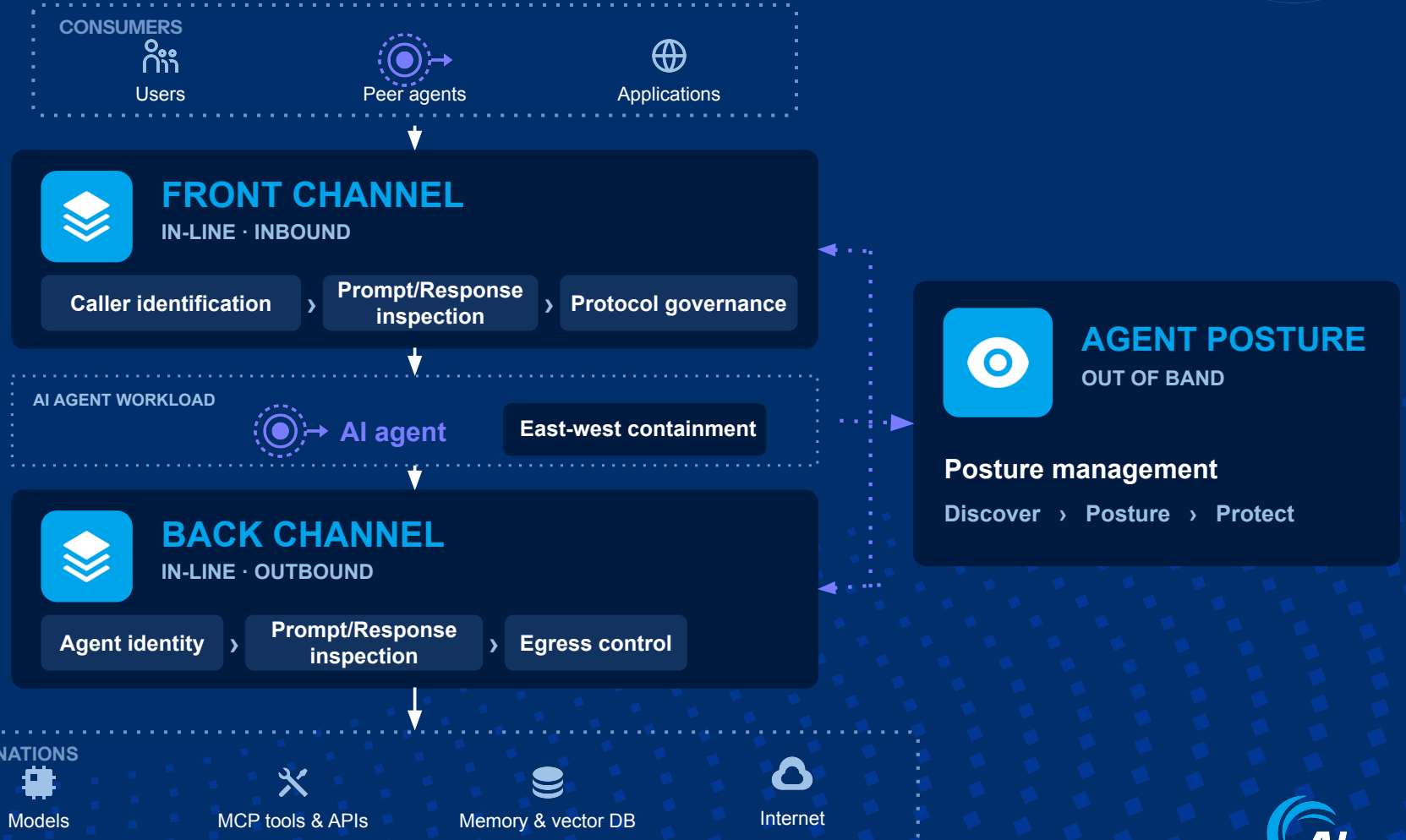
Agents choose their own tools and data

EVIDENCE

21%

of breached organisations had an incident involving their own AI models or applications, up from 13%

IBM Cost of a Data Breach 2026



Secure WITH AI

SecOps that acts in seconds and stays under human control



WHAT CHANGED

Analysts worked alert by alert

**AI investigates,
people decide**

EVIDENCE

65 days

faster to identify and contain a breach with extensive security AI and automation, and \$1.93M lower cost

IBM Cost of a Data Breach 2026

REVERSIBLE ACTION WITHIN DEFINED LIMITS

AGAINST AI

FOR AI

THE AI



TELEMETRY LAKE

OUT OF BAND · ONE RECORD PER REQUEST

Request context

Event timeline

The prompt itself



AI DETECTION

OUT OF BAND · BEHAVIOR-BASED DETECTION

Baselining

> Anomalies

> Machine-speed mitigation



MCP CONTROL PLANE

IN-LINE ACTION · INTO EXISTING SYSTEMS

Scoped action

> Human approval

> Reversal

THE ENTERPRISE

SECOPS

SOC analysts



SecOps AI agents

PROCESSES

Incident · Vulnerability
Change · Third-party risk

Governance as a Foundation

AI the board can approve and auditors can verify



MANAGE
ISO/IEC 42001

“...continually improving an Artificial Intelligence Management System.”



ASSESS
NIST AI RMF

“...to better manage risks to individuals, organizations, and society...”



COMPLY
EU AI Act

“...an appropriate level of accuracy, robustness, and cybersecurity.”



PROVE
AIUC-1

“...testing against jailbreaks, prompt injection, data leakage, hallucinations, and unsafe tool calls.”

Governance isn't the brake. It's what makes speed safe.

The Speed of Trust

Built to go fast and far



Secure AGAINST AI

Agents that reach the business



Secure FOR AI

AI the workforce uses



Secure THE AI

AI the business builds



Secure WITH AI

AI that defends the business



Which pillar comes first?

