HFS

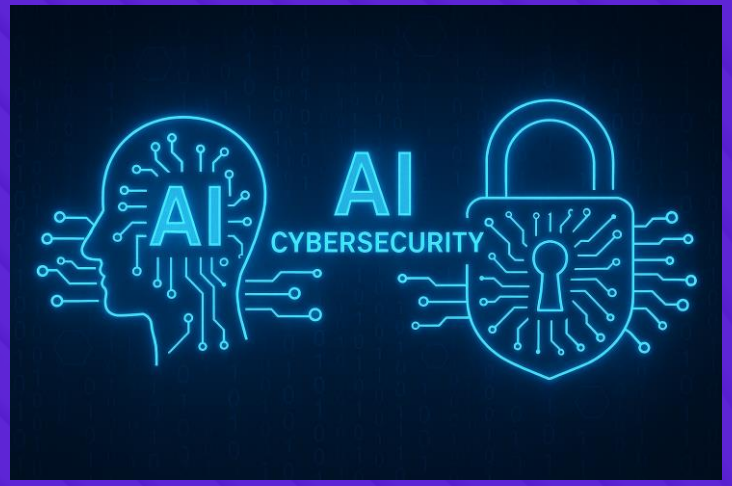
HFS RESEARCH FALL SUMMIT

THE SERVICES-AS-SOFTWARE ECONOMY: DISRUPT OR BE DISRUPTED

Encrypting your Agentic Enterprise

Joel Martin
Executive Research Leader, HFS Research

AI is shifting the security landscape



44%

Of Enterprises HFS surveyed in recent Pulse **lean on their Services partner** to provide robust cybersecurity solutions and management.

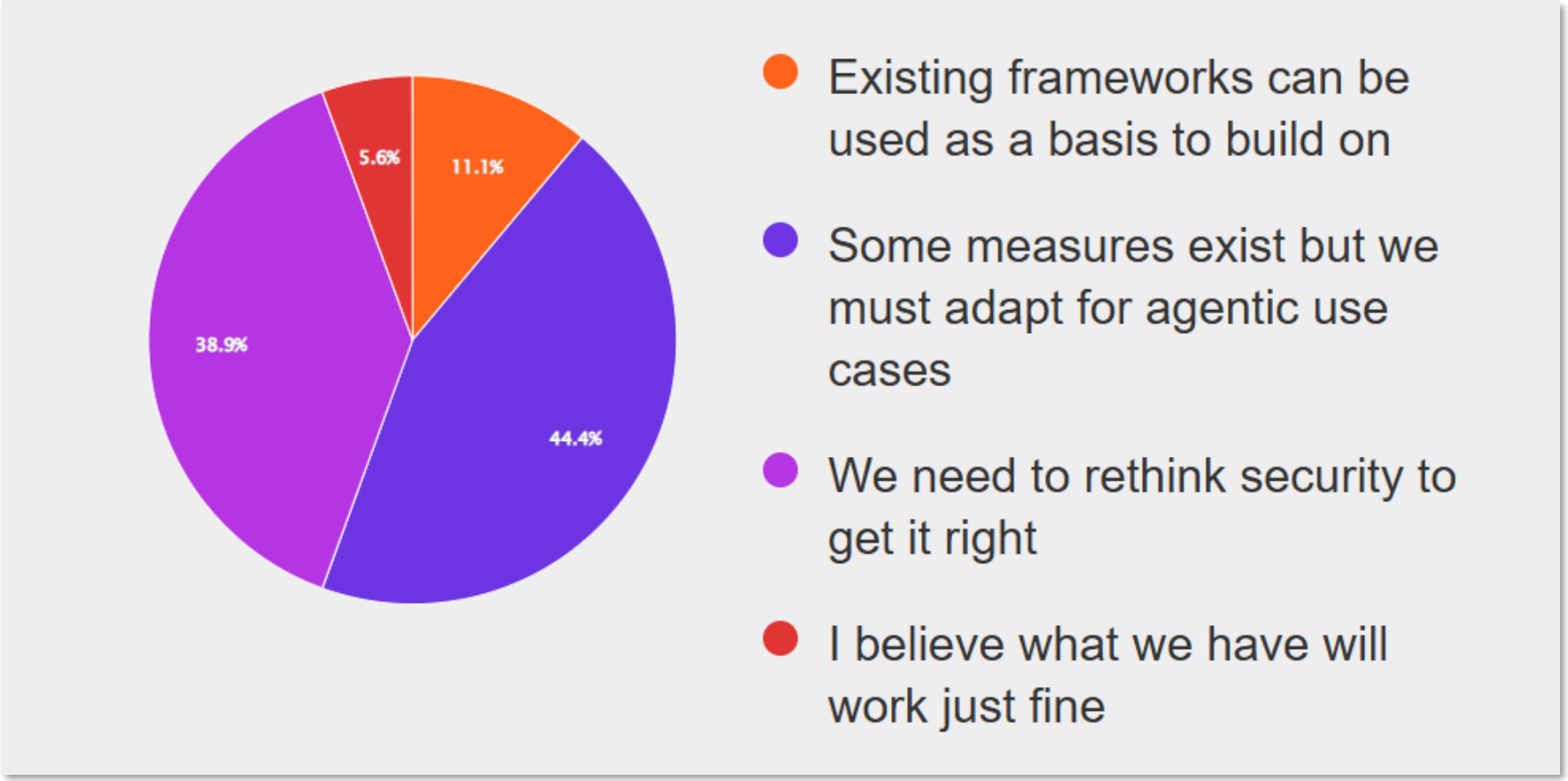
42%

Enterprises say **AI creates the most value in cybersecurity and threat detection**, making it the single biggest application of AI across IT, ahead of software engineering (35%) and infrastructure (30%)

40%

Enterprise decision-makers rank cybersecurity threats as one of **their top external barriers**, nearly at the level of geopolitical risks (48%) and economic factors (42%), highlighting why AI is being pulled into the security fight.

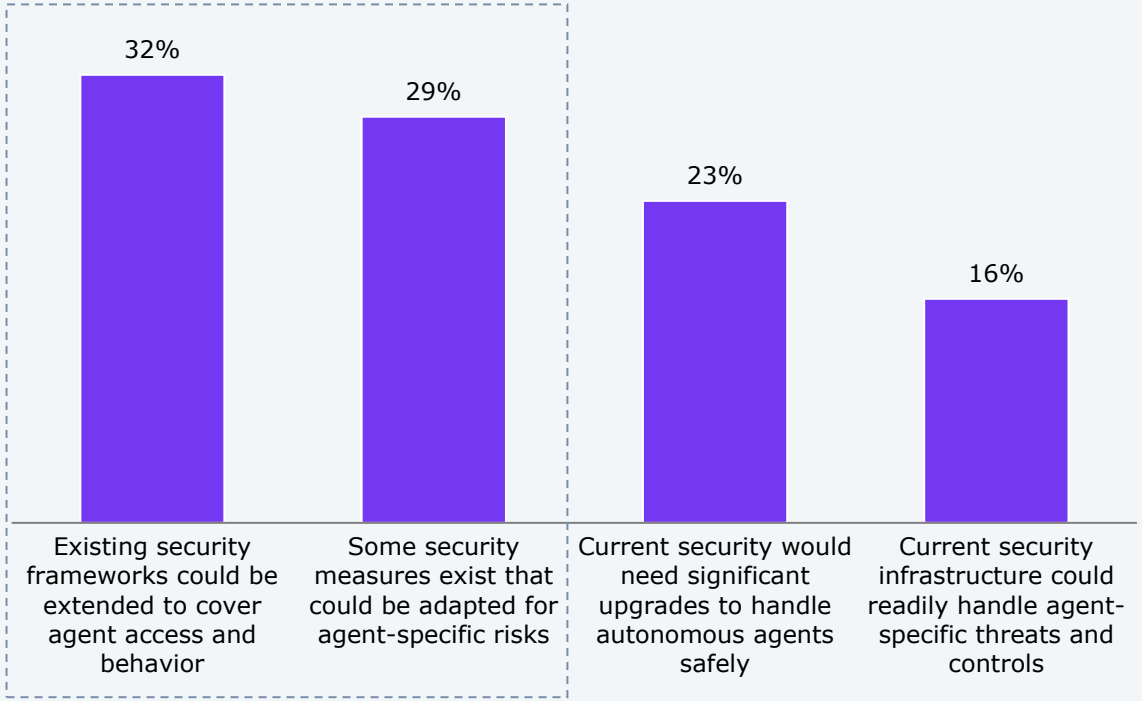
Poll Question 1: Which best describes your cybersecurity readiness for agentic AI?



Sample collected from HFS Summit attendees

Only 16% of enterprises have security infrastructure ready for agent-specific threats

Which best describes your cybersecurity readiness for agentic AI?



	Exploring	Emerging	Scaling	Pioneering
Existing security frameworks could be extended to cover agent access and behavior	17%	**51%**	29%	17%
Some security measures exist that could be adapted for agent-specific risks	32%	**34%**	17%	3%
Current security would need significant upgrades to handle autonomous agents safely	**51%**	5%	0%	0%
Current security infrastructure could readily handle agent-specific threats and controls	0%	10%	54%	**79%**

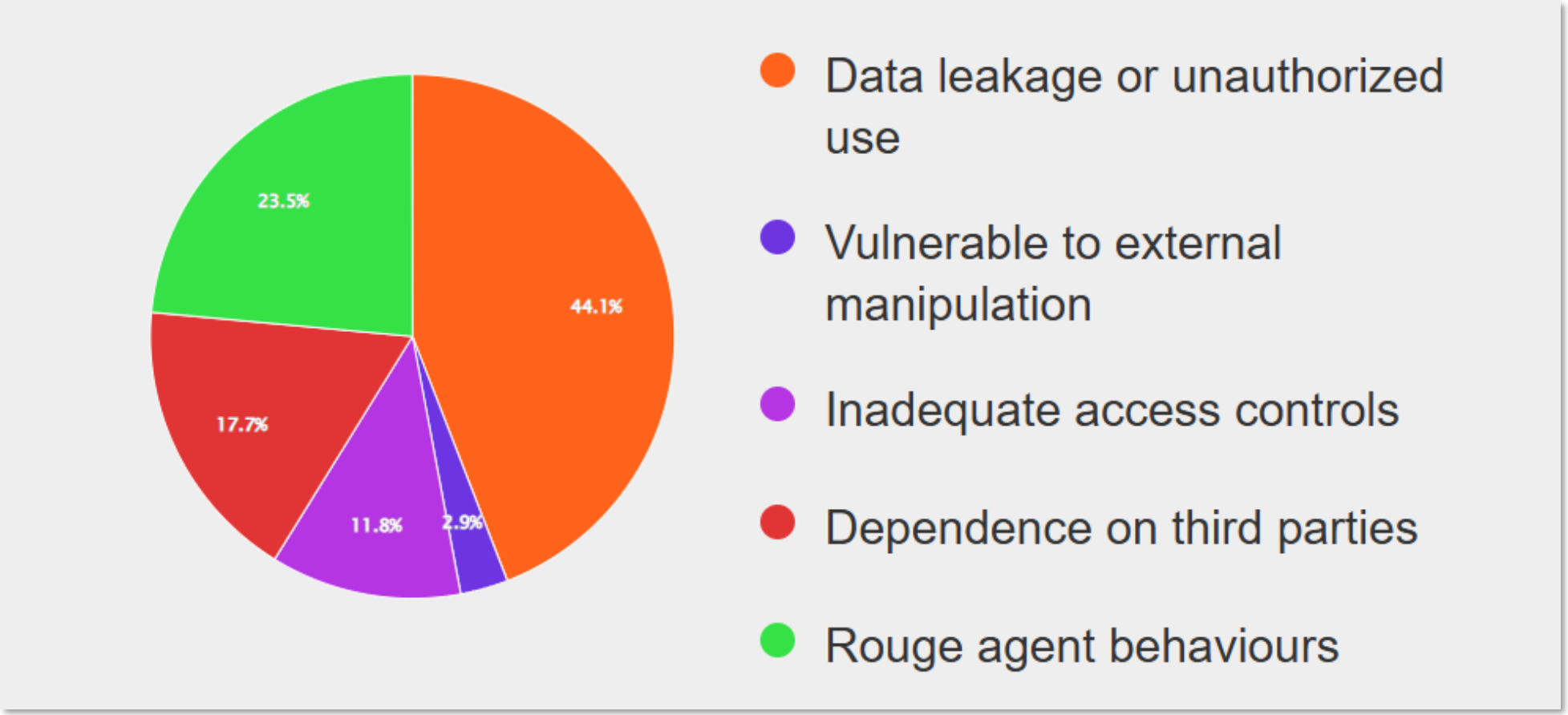
Most organizations are not fully equipped to defend against the unique risks introduced by agentic AI.

While 32% say existing frameworks could be stretched and 29% have adaptable controls, only 16% report having infrastructure that can already manage autonomous agent behavior securely.

The remaining third acknowledge that significant upgrades are needed. This highlights a widening readiness gap—enterprises are deploying autonomous systems faster than they're securing them, creating risk exposure that governance alone cannot contain.

Sample: 505 Global 2000 Enterprise Decision makers
Source: HFS Research, 2025

Poll Question 2: What are the most concerning risks your organization faces as it scales agentic AI?



Sample collected from HFS Summit attendees

Data exposure tops the list of agentic AI risks

What are the most concerning risks your organization faces as it scales agentic AI?

	Exploring	Emerging	Scaling	Pioneering
#1 risk	**Data leakage**	**Data leakage**	**Data leakage**	Inadequate access controls / escalation safeguards
#2 risk	Vulnerability to manipulation	Vulnerability to manipulation	Vulnerability to manipulation	Vulnerability to manipulation
#3 risk	Inadequate access controls	Inadequate access controls	Rogue agent behavior / unintended decision-making	Overreliance on vendors / third-party tools

Enterprises are focused on hard risks but underestimating soft ones.

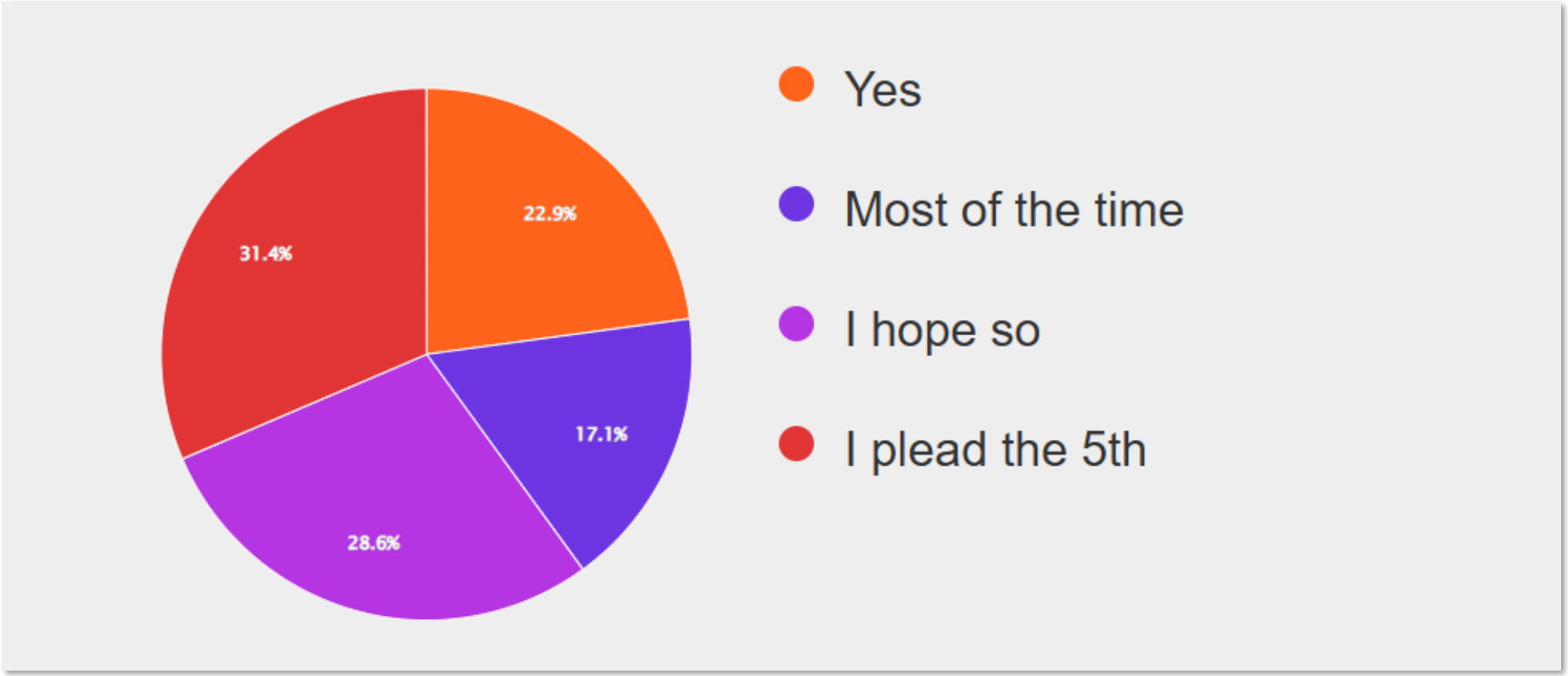
Security, access control, and vendor reliance dominate the conversation—but risks tied to transparency, ethics, and employee experience are deprioritized or ignored.

If enterprises only secure the perimeter and ignore the psychological, organizational, and behavioral risks, they'll build technically safe systems that fail to gain workforce trust or sustain real value.

The real threat may not be rogue agents—it may be rolling out agents in environments not designed to govern or absorb them.

Sample: 505 Global 2000 Enterprise Decision makers
Source: HFS Research, 2025

Poll Question 3: Do you balance security concerns with the need for AI innovation?



Sample collected from HFS Summit attendees

Innovation can’t be strangled by security, but it can be a wild west either…

AI and Cybersecurity are inseparable

AI and cyber aren’t separate conversations anymore. Each leap in AI adoption opens new vulnerabilities, forcing stronger cyber defenses. Governance steps in to steady the system, which only drives more adoption. That’s the **AI-cyber risk flywheel**.

AI–Cyber Risk Flywheel:

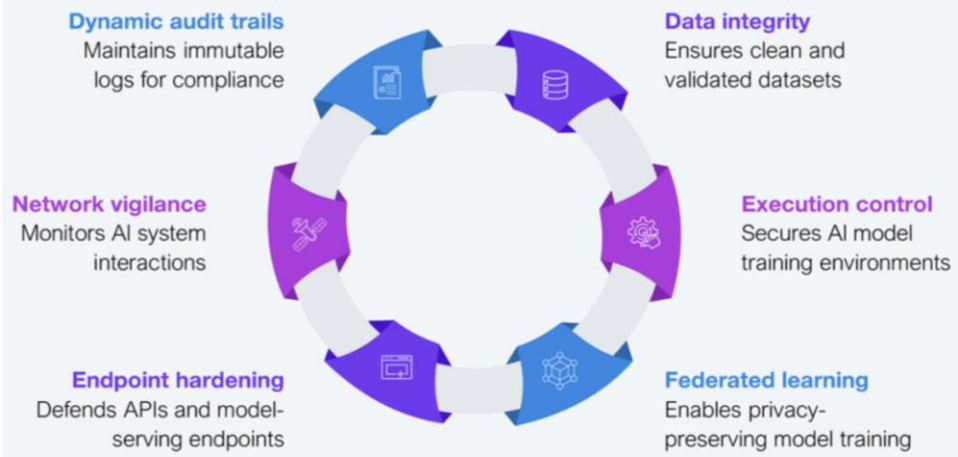
- More AI adoption expands the attack surface and introduces new risks.
- Rising risks demand AI-powered defenses to detect, respond, and adapt faster.
- New defenses trigger governance, compliance, and oversight requirements.
- Governance enables responsible AI adoption, which again fuels the cycle.

The bottom line: AI and cybersecurity now reinforce each other in a continuous loop. The moment you treat them separately, resilience breaks down.

Cyber for AI frameworks

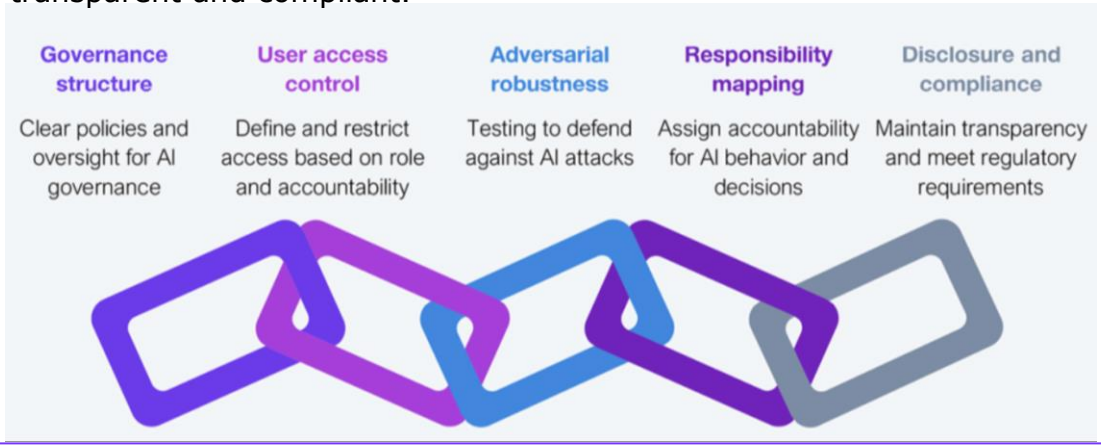
DEFEND: Six pillars of technical security for AI systems

AI itself is now an attack surface. DEFEND lays out the core technical controls that keep it from being compromised. It's about ensuring data can't be poisoned, execution environments can't be hijacked, APIs can't be abused, and every action leaves a trace you can audit.



GUARD – Governance for responsible AI

AI does not just need technical defences, it needs guardrails on how it is used. GUARD captures the governance layers that make AI responsible in practice. It means setting clear policies and ownership, controlling who has access, testing for adversarial risks, defining accountability when things go wrong, and keeping systems transparent and compliant.



Thank you.

www.hfsresearch.com

hfsresearch

www.horsesforsources.com

www.horsesmouthpodcast.com