Digital Transformation in an ‘Always-on’ Era

Building foundations for continuous compliance and avoiding critical service disruptions

Bruno Azenha
Global FSI Technology Strategist

v1 | 25-Jun-2026

Red Hat

What will keep us busy...

- The new reality
- Building always-on FSI
- Recap
- Open discussion

The New Reality in Financial Services

The "Always-On" era isn’t just about uptime anymore... it’s about surviving the collision of 24x7 market demands, aggressive regulatory oversight, and non-human scale AI threats.

Where the FSI industry is heading

Major always-on trends driving transformation in the technology landscape

Banking

24x7x365 Real-Time Execution

Instant payment rails (FedNow, Pix, SEPA Instant) completely removing traditional "off-hours" and requiring new patterns

Financial Markets

Compressed Settlements

Compressed cycles (T+1 to instant settlement). Zero tolerance for micro-latency across global 24/5 markets.

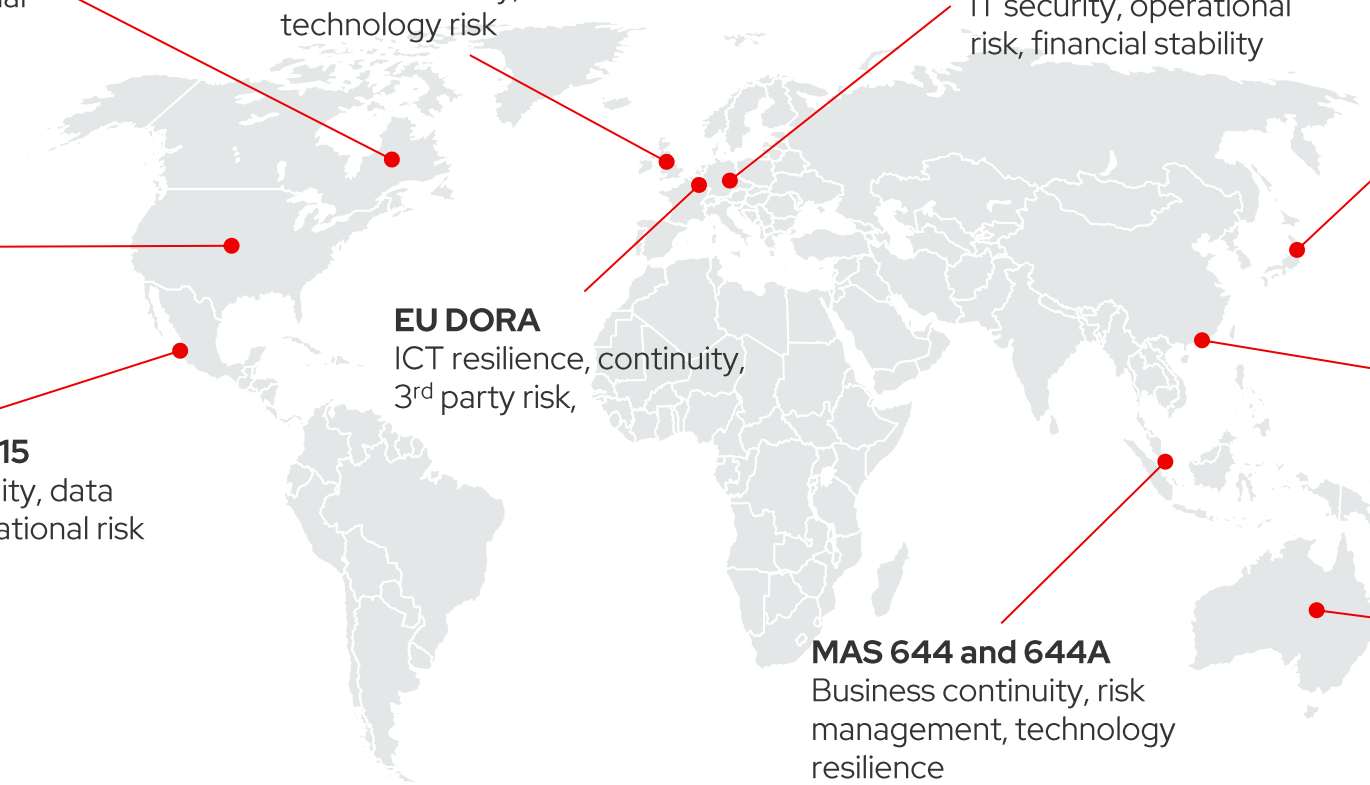
Insurance

The 24/7 Digital Claims Era

Instant automated triage and digital claims processing. Shifting from static policies to real-time responsive models.

The macro picture: Different Acronyms, Single Focus

Fragmented global regulations are converging on automated, continuous service resilience



OSFI's E-21
3rd party risk, operational resilience, data privacy

FSA PS21/3
Operational resilience, financial stability, technology risk

MaRisk and BAIT
IT security, operational risk, financial stability

JFSA Guidelines
Financial stability, cyber risk, operational resilience

FFIEC and FIDIC
Cybersecurity, depositor protection, financial system stability

EU DORA
ICT resilience, continuity, 3rd party risk,

HKMA OR-2
Operational continuity, 3rd party risk, technology resilience

CNBV Circular 115
Business continuity, data protection, operational risk management

MAS 644 and 644A
Business continuity, risk management, technology resilience

CPS 230
Organizational culture, business continuity, service resilience

Source: https://www.resolver.com/blog/global-operational-resilience-compliance

The regulatory direction: Global Mandates & New Threats

Regulation shifting from policies to demonstrability that effectively reduces systemic risks

Operational Resilience & Cloud Portability

Cross-sector regulations like DORA (EU), the FCA (UK), and federal insurance frameworks are mandating that a failure at a cloud provider cannot halt a critical service. Firms must actively demonstrate "stressed exit" capabilities.

Consumer & Market Integrity Focus

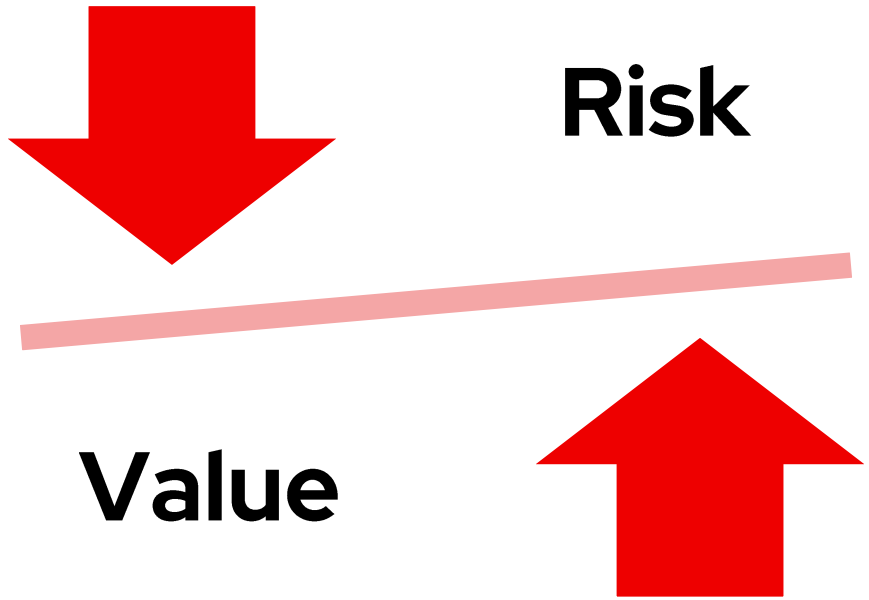
Regulators demanding automated proof that system outages do not disadvantage vulnerable retail banking customers, freeze capital market liquidity, or halt critical insurance claim payouts during natural disasters.

Cyber Resilience & Post-Quantum Security

Beyond standard security, regulators are focusing on Agentic AI security threats and Post-Quantum Cryptography (PQC) to protect data from "Harvest Now, Decrypt Later".

AI adoption dilemma: Business Value vs. Scaled Risk

- Legal/compliance liabilities of agentic hallucinations
- Token costs are exploding due to agentic expansion
- Business continuity plans when agentic AI becomes core



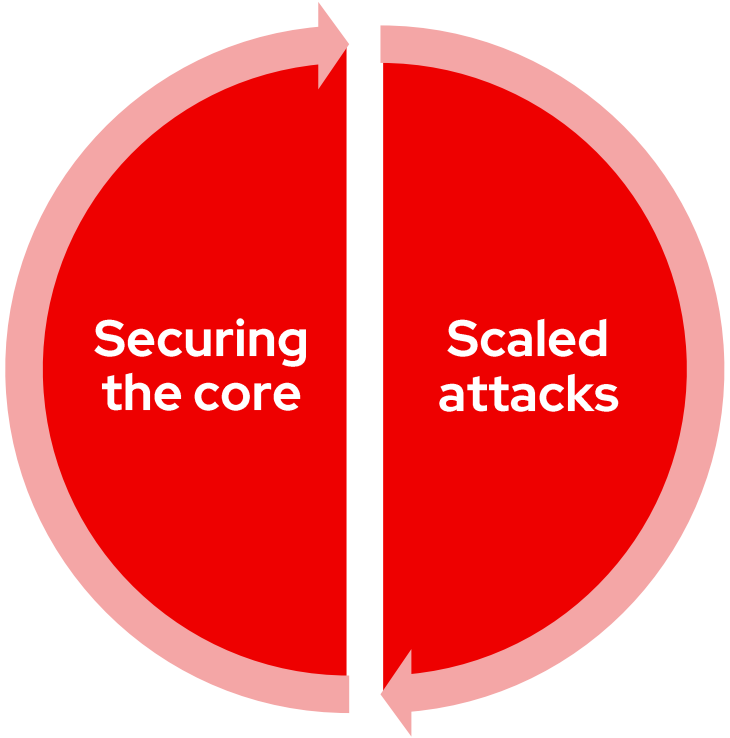
- AI RAG and guardrails enables reliable business scalability
- Intelligent routing, specialized models and private cloud allow AI right-sizing
- Everything-as-code, immutable infrastructure and agentic IT Ops unlock resilience and recoverability

External threat landscape

Preventing vulnerabilities and respond to AI-augmented threats in an always-on world

Legacy Code Risk
Tracking hidden vulnerabilities within decades-old application source code

The Retro-Patching Challenge
Securely backporting critical fixes into old, unsupported applications and open-source software



Agentic AI Weaponization
AI agents that probe infrastructure, find 0-day exploits, and execute breaches in seconds

Cascading Network Risks
Automated, hyper-targeted attacks capable of jumping cross-sector lines between banking, trading, and insurance networks at machine speed

Building an Always-On FSI Organization

Key Architectural guidelines to be successful in an interconnected, always-on era

The "Minimum Viable Core"

15m

Recovery Time Objective (RTO)

Institutions must define an "MVC" that quickly recovers from major disruptions and covers all essential capabilities and services

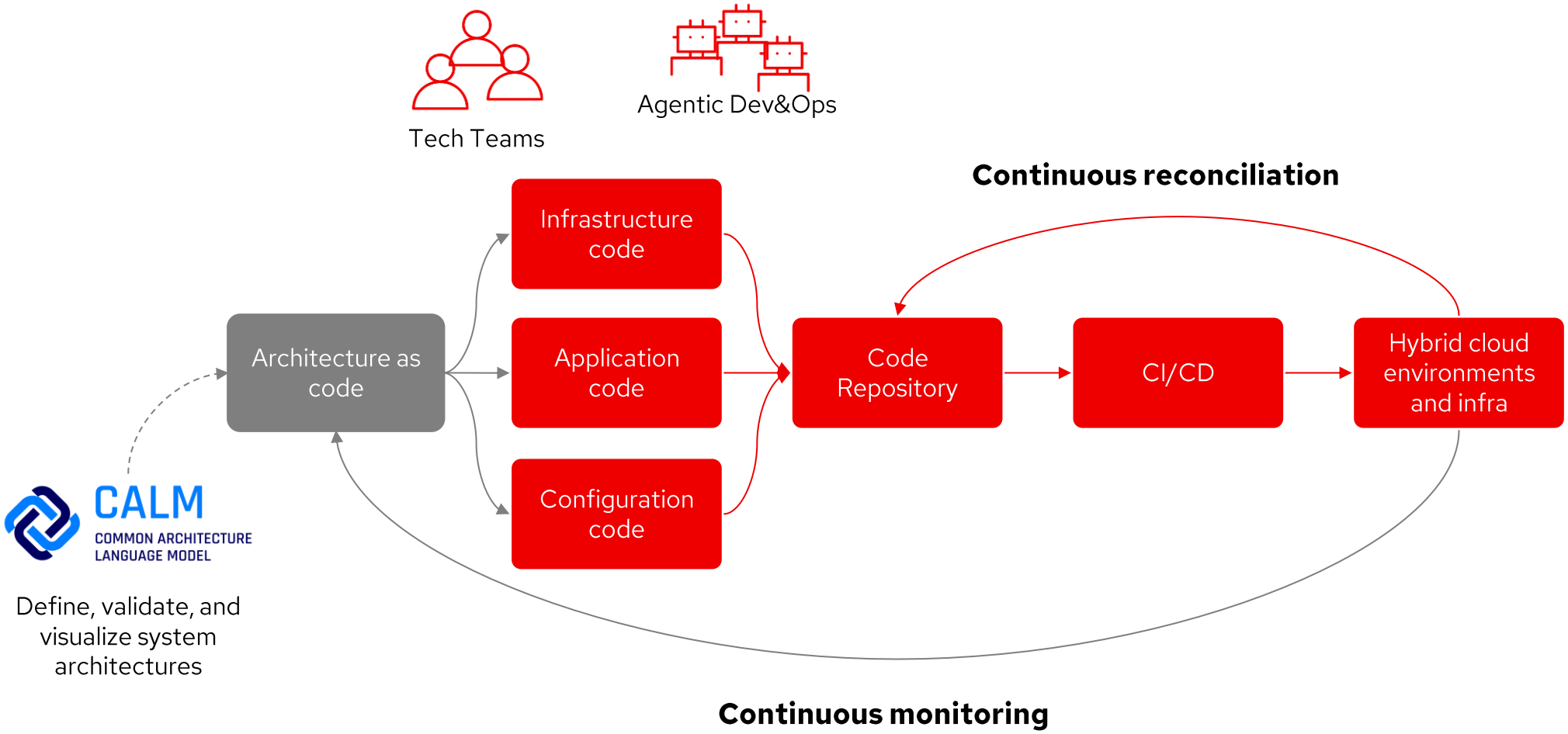
Core Data: Deeply secured, cross-region replicated data vaults operating with near-zero RPO

Business systems: essential services with HA and automated DR, requiring minimal RTO

Technical operations: critical platform utilities designed with the same rigorous HA/DR standards as customer-facing applications

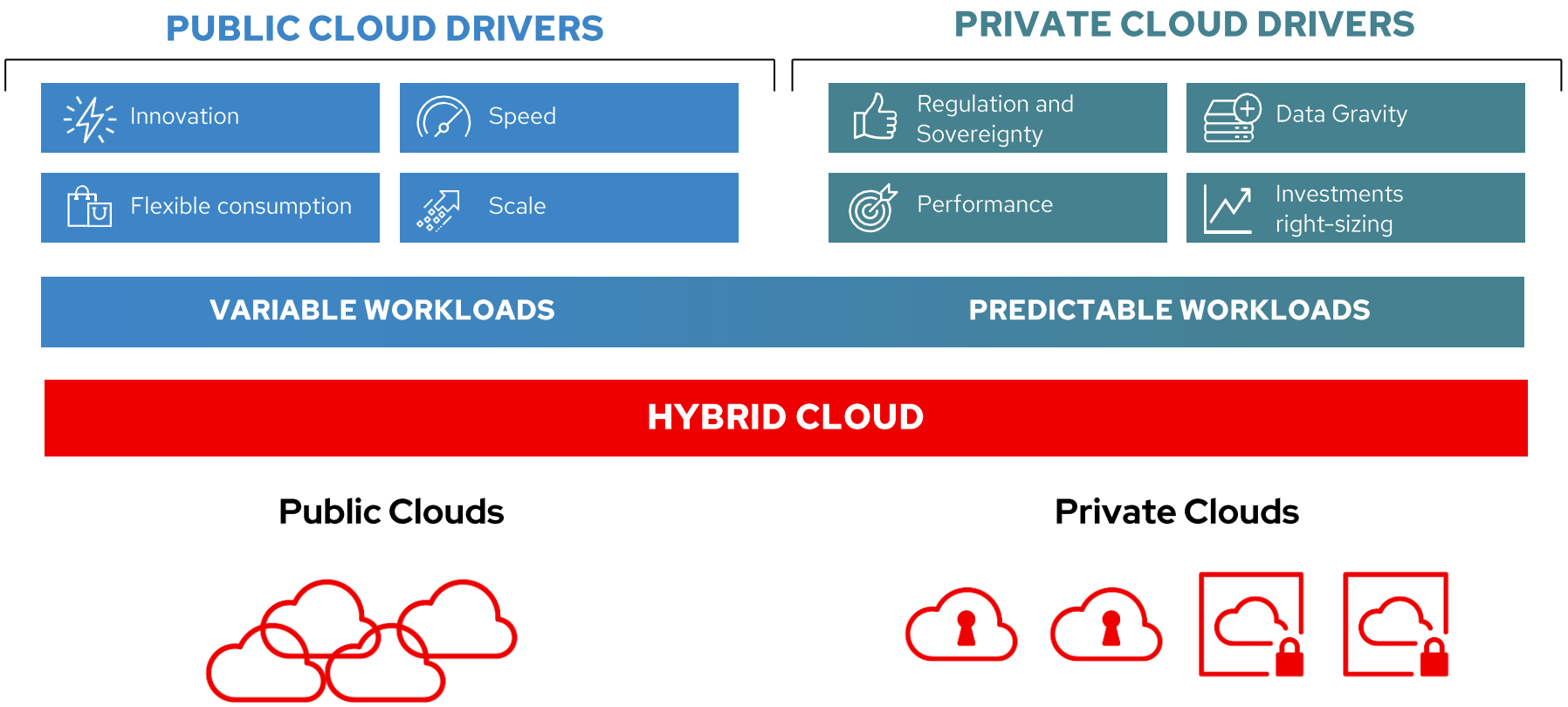
Architecture as code

Moving from static architecture to GitOps-embedded architecture



Composability of Public and Private Cloud

A hybrid cloud that unlocks flexibility, resilience, sovereignty and cost control



Three pillars of resilient AI engineering

Operationalized Trust, Economics, and Continuity

Economic Guardrails

- TCO modelling beyond token counts and that considers realized business value
- Tiered Unit Economics to prevent runaway costs

Trust & Governance

- Monitoring context, behaviour, and objective drift
- Hard guardrails to isolate and neutralize unauthorized or unvetted agentic actions

Operational Continuity

- State checkpointing for cross-cloud failover
- Graceful degradation Patterns like rerouting to SLM or human-in-the-loop queues

The Hybrid Cloud Advantage: Sovereign fallbacks

Proactive vulnerability management and avoidance

Phase 1: Secure Source

Inventory components and dependencies

Phase 3: Retro-Patching

Backporting security fixes to legacy application cores

Phase 2: Build Integrity

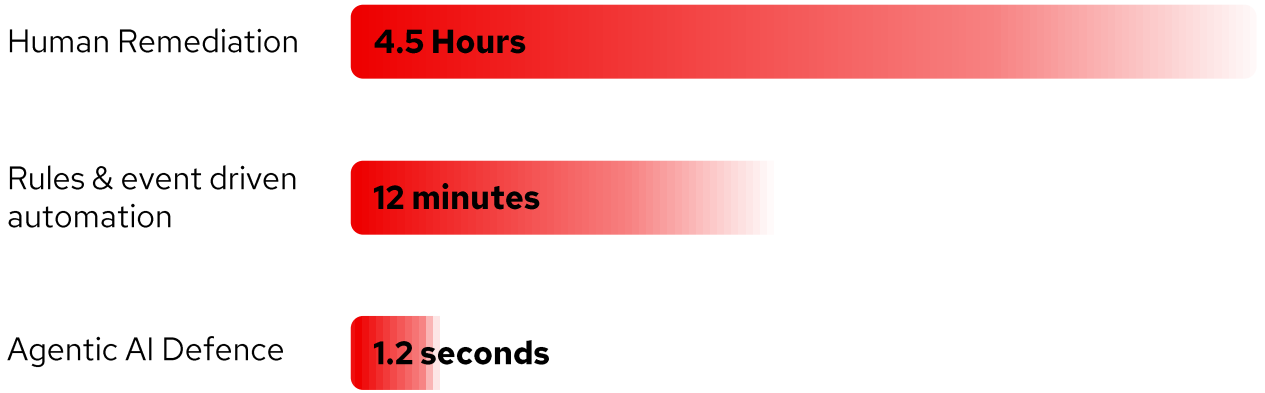
Automated scanning and provenance verification

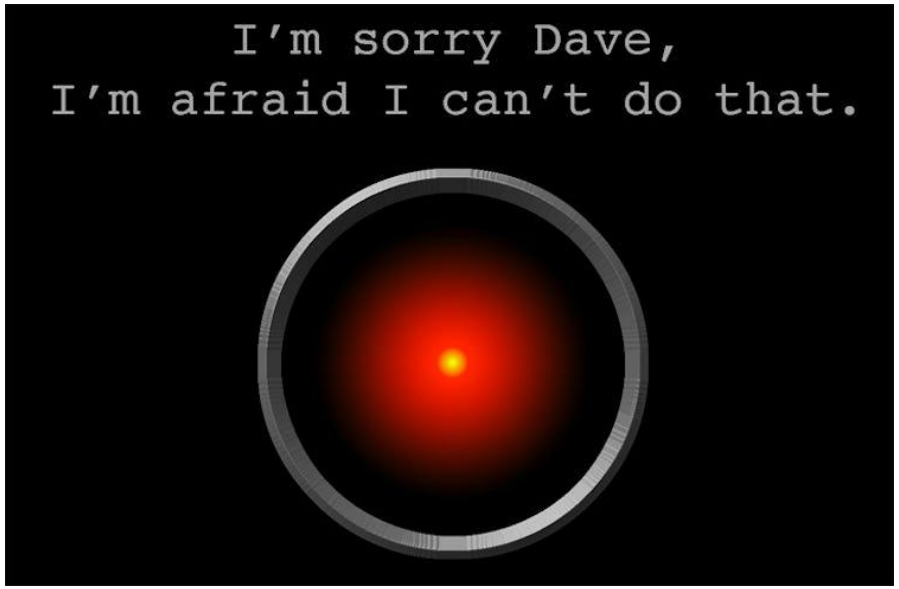
Phase 4: Continuous Ops

Real-time vulnerability monitoring across the lifecycle.

Agentic AI as a counter-defense for scaled attacks

Defeating AI-augmented threats requires autonomous, intent-based infrastructure response





Recap

The Always-On Challenge	The Resilient Response / Strategic Blueprint
Compressed Velocity (24x7/24x5)	Minimum Viable Core (MVC)
Regulatory shift from Policy to Proof	Everything-as-code & Hybrid Cloud
Exploding AI Economic & Operational Risk	Resilient AI Engineering
Machine-Scale External Threats	Proactive Secure Software Supply Chain and Agentic Counter-Defenses

Open discussion time

What other challenges do you see around always-on, regulation, resilience and sovereignty?

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.


linkedin.com/company/red-hat


facebook.com/redhat


youtube.com/@redhat


x.com/RedHat

Red Hat