2026 Predictions

The Evolution of Cyber Defense: Embracing Dynamic Trust

John Swanson, Global Security Portfolio Lead, Uvance, at Fujitsu

Organizations have long struggled to keep up with the increasing complexity of cyber threats, often depending on reactive, perimeter-based defenses that trust access once granted. However, a fundamental shift is occurring. The principles of Dynamic Trust are becoming possible through advanced artificial intelligence (AI), continuous exposure management, and real-time risk assessment, which are changing the way we approach cybersecurity.

Currently, many organizations have security blind spots, deploying technologies without proper governance frameworks and lacking sufficient visibility into where their data is stored or how their systems are exposed. By 2026, advances in AI-driven defense, proactive risk management and integrated information and operational technology (IT/OT) security will transform the cybersecurity landscape, turning it from a technical task into a strategic priority that shapes corporate integrity.

1. AI Governance Will Become a Board-Level Imperative

The promise of generative and agentic AI is outstripping organizational ability to govern it effectively, creating a perfect storm of security vulnerabilities. In 2026, this governance gap will no longer be acceptable. Organizations will face mounting pressure from regulators, investors, and insurers to demonstrate AI accountability.

We will see the emergence of AI Governance-as-a-Service solutions and integrated compliance platforms designed to enforce policy, monitor model behavior, and mitigate risks such as data leakage, prompt injection attacks, and tackle the dangers of granting agentic systems too many access privileges. These platforms will provide continuous visibility into AI model deployments, data flows, and decision-making processes.

Inevitably, the rush to deploy agentic AI will also expose organizations to novel attack vectors. In 2026, we expect to see significant breaches where attackers compromise networks through prompt injection from unexpected sources such as SIEM logs, DNS records or other infrastructure data that AI agents process automatically.

Expect AI security to dominate boardroom discussions as new regulatory mandates, such as the EU AI Act, will require explainability, auditability and ethical AI usage. Organizations that establish robust AI governance frameworks early will gain a competitive advantage, while those that play catch-up will face compliance penalties and reputational damage.

2. Data Sovereignty Will Reshape Cloud Strategy

As geopolitical tensions intensify, organizations will demand greater transparency about where their data resides and who controls access to it. The fear of losing critical information “at a stroke" will drive a shift in thinking related to cloud strategy throughout 2026.

Recent disruptions have exposed a disturbing reality: Many businesses do not truly understand where their data resides until an audit forces uncomfortable truths into the open. This knowledge gap represents unacceptable risk in an era where data access can be restricted through political decisions with no technical recourse.

Organizations will prioritize cloud and service providers who guarantee jurisdictional clarity and resilience against political interference. Multi-cloud sovereignty strategies will accelerate, with enterprises distributing data across trusted regions to mitigate single-point geopolitical risks. We expect to see organizations repatriate critical workloads to on-premises infrastructure for situations where data sovereignty concerns outweigh the benefits of the cloud.

The result: Procurement decisions will weigh data location and legal jurisdiction as heavily as technical capabilities and cost. Vendors and other suppliers unable to provide clear answers about data residency will lose business to competitors offering sovereignty guarantees**.**

3. Continuous Exposure Management Will Replace Periodic Assessments

The security paradigm will shift from periodic vulnerability assessments to continuous exposure management throughout 2026. Organizations will deploy platforms that provide real-time visibility into their attack surface, automatically identifying and prioritizing risks based on exploitability, business context and threat intelligence.

These systems will integrate data from vulnerability scanners, configuration management databases, threat intelligence feeds and business impact analyses to create dynamic risk scores that reflect current exposure. Unlike traditional tools that generate static reports, continuous exposure management platforms will track how risks evolve as systems change, patches are applied and monitor emerging new threats.

Most importantly, these platforms will enable proactive risk mitigation rather than reactive patching. This means security teams identify and address exposures before they can be exploited, and in doing so, shift from a firefighting mode to a strategic risk management approach.

The impact: Security leaders will present boards with clear, quantifiable metrics about cyber risk exposure and demonstrate how security investments reduce business risk. Cybersecurity transforms from a cost center into a value protection function with measurable return on investment.

4. IT and OT Security Convergence Will Accelerate

The artificial separation between IT and OT security will crumble in 2026 as organizations recognize that threats ignore these boundaries. Critical infrastructure operators will align OT security controls with IT security standards, implementing unified visibility and governance across both domains.

State-sponsored threat actors and wannabe hackers will continue targeting critical infrastructure, with attacks increasingly affecting secondary targets outside active conflict zones. The risk of collateral damage from weaponized cyber tools will grow, as sophisticated malware designed for specific targets spreads beyond intended victims, much like Stuxnet in the early 2010s.

Increasingly, organizations will deploy integrated platforms that provide a single pane view of security risks across IT and OT assets. These systems will apply consistent security policies while respecting the unique requirements of operational environments where availability and safety take precedence over confidentiality.

Compliance frameworks will evolve to mandate the integration of IT/OT security, with standards like NIS2 becoming table stakes for critical infrastructure operators. Organizations that demonstrate mature IT/OT security convergence will gain advantages in terms of insurance premiums, regulatory approvals, and customer trust.

The Cybersecurity Transformation in 2026 and beyond

AI / Gen AI etc isn't going to address all the issues in the very short term – this is an evolution rather than a revolution. Next year and beyond, the convergence of AI-driven defense, robust governance frameworks, data sovereignty strategies, continuous exposure management, and IT/OT security integration will start to create cybersecurity ecosystems built more on Dynamic Trust rather than static perimeters.

We will move from an era where organizations are better able to react to breaches after they occur to one where AI and continuous monitoring enable better proactive threat prevention. Security needs to evolve from a technical function into a strategic differentiator, with cyber resilience becoming a key performance indicator that defines corporate value and reputation.

Companies that combine advanced AI capabilities with governance rooted in transparency and accountability will be best positioned to protect their assets and maintain stakeholder trust. Those that fail to adapt will face mounting risks from increasingly sophisticated threats, regulatory penalties, and loss of competitive position.

The future of cybersecurity is about transforming threat intelligence into actionable defense strategies that protect business value. As we approach 2026, that future has never been closer to reality.

John Swanson
Global Security Portfolio Lead, Uvance, at Fujitsu

John has fulfilled many Information Security leadership roles across Public and Private sectors including security program and capability leadership, consultancy (advisory and delivery), Security Operations Centers and Security Pre-sales functions.

He is responsible for developing Fujitsu's compelling Cybersecurity go to market propositions, which also underpin Fujitsu's wider Applications, Hybrid IT, Digital Workplace and Industry Sector aligned propositions. John focuses on the business aspects of Information Security and how Fujitsu can help clients enhance the strategic and operational maturity of the information security capabilities within their organizations.

