ARMIS®

PREDICTIONS 2026

EBOOK

2026 Cybersecurity Predictions: The Future of AI-Driven Defense

Your Guide to the 2026 Cyber Landscape

Welcome to Armis Predictions 2026! This is your front-row view into a year where cybersecurity crosses a threshold and AI-driven adversaries rewrite the rules of engagement. From autonomous ransomware and synthetic identity epidemics to supply-chain poisoning, hybrid warfare, and the rise of individuals operating with nation-state-level capabilities, 2026 marks the moment when threat velocity, scale, and sophistication surge beyond anything traditional defenses can contain.

This report distills the most critical insights from Armis' top experts across threat intelligence, public sector, federal, healthcare, and OT/CPS security. Inside, you'll find concise executive summaries on everything shaping the year ahead: the operationalization of Continuous Threat Exposure Management (CTEM), the convergence of IT/OT/IoT/medical environments, the evolution of critical infrastructure attacks, the new economics of cyber resilience, and the shift from reactive protection to strategic, AI-native defense.

If you want to dive deeper into agentic AI attacks, digital-twin-driven OT validation, unified vulnerability management, autonomous detection and response, or the new metrics that will define resilience, follow the link at the bottom of each page. Think of this summary as your fast, potent preview of the cyber landscape ahead and an invitation to explore the full depth of what 2026 will demand.

Securing the Next Era: How Armis Is Shaping the Future of Cyber Resilience

Yevgeny Dibrov,
Co-Founder & CEO, Armis

Cybersecurity has become a foundation of global trust as digital and physical systems increasingly intertwine. Cyber incidents now disrupt essential services, supply chains, and national stability, pushing governments and organizations to shift from reactive defense to demonstrable resilience. Expectations for transparency and continuity have never been higher.

Armis is leading this shift with a platform built for predictive intelligence, autonomous protection, and full-spectrum visibility across IT, OT, IoT, medical devices, cloud, edge, and AI systems. By combining real-time behavioral analytics, attack-path insights, and adaptive AI-driven intelligence, Armis helps organizations anticipate threats, close exposure gaps, and safeguard critical operations at scale.

As we enter 2026, Armis is committed to shaping a more resilient digital future where businesses, communities, and societies can operate with confidence in an increasingly interconnected world.

READ THE FULL ARTICLE

Securing the Next Frontier of AI-Driven Threats

Nadir Izrael
Co-Founder & CTO, Armis

In 2026, AI has transformed the cyber threat landscape, enabling everyone from lone actors to nation-states hackers, to conduct autonomous, highly sophisticated operations across IT, OT, IoT, and medical environments.

From AI-powered financial manipulation and synthetic identity epidemics to hybrid warfare, supply chain poisoning, and preemptive data blackmail, adversaries can now inflict systemic, real-world disruption at unprecedented speed and scale.

Organizations must respond with predictive, autonomous, and integrated security platforms that deliver continuous visibility, AI-driven detection, and orchestrated response across the entire attack surface.

By perationalizing intelligence, automating mitigation, and embedding defense into every layer of their ecosystems, organizations can shift from reactive protection to strategic advantage, staying ahead of AI-driven threats that traditional tools cannot stop.

READ THE FULL ARTICLE

From Resilience to Strategic Advantage

Alex Mosher
President and CRO, Armis

In 2026, cybersecurity will evolve from a defensive necessity into a strategic business advantage, with organizations leveraging intelligent, embedded security to accelerate innovation, strengthen trust, and gain competitive differentiation.

Escalating threats which include everything from self-evolving AI attacks, autonomous ransomware, and deepfake-enabled fraud to systemic supply chain compromises and IoT/OT-targeted disruptions, are converging with regulatory pressures, geopolitical volatility, and hyper-connected infrastructures to expand the attack surface exponentially.

Success will depend on unified, AI-driven security platforms that provide continuous asset intelligence, automated detection and response, and coordinated orchestration across IT, OT, IoT, and medical devices.

Organizations that operationalize security as a core enabler, rather than a compliance checkbox, will transform resilience into opportunity, turning proactive protection into measurable strategic advantage.

READ THE FULL ARTICLE

The Cyber Wake-Up Call: What Every Public Sector Leader Needs to Know

Michael Bimonte
Field CTO, Armis
(State, Local & Education)

By 2026, state, local, and education (SLED) organizations will face a defining cybersecurity reckoning: the era of “we’ll patch later” is over, and continuous, sophisticated threats demand resilience as the new measure of success.

Cyber exposure management (CEM) and Continuous Threat Exposure Management (CTEM) will become the operational baseline, shifting focus from technical metrics to mission-critical outcomes such as downtime avoided, data protected, and services maintained.

Threats are evolving from broad ransomware campaigns to precision extortion and supply-chain infiltration, exploiting trusted vendor relationships and poorly monitored SaaS ecosystems.

At the same time, federal and state funding will flow with accountability, requiring measurable results tied to operational continuity. Leaders who succeed will embrace exposure management as a strategic foundation, connecting every control, investment, and decision to the resilience of public services, translating cybersecurity achievements into tangible citizen impact, and ensuring the continuous delivery of essential functions in an increasingly hostile digital landscape.

READ THE FULL ARTICLE

Operational Resilience Reimagined: How CTEM, AI, and Access Control Redefine OT Security

Carlos Buenano
Field CTO, Armis

In 2026, operational technology (OT) and cyber-physical systems (CPS) security are entering a new era where visibility, context, and continuous risk management define resilience. AI-powered adversaries, supply chain fragility, and relentless digitization are driving organizations to adopt Continuous Threat Exposure Management (CTEM) as the operational center of gravity, transforming cyber risk from abstract metrics into measurable business outcomes that will be tracked financially, operationally, and safety-related.

Modern OT security now combines autonomous threat detection, least-privilege access enforcement, and automated remediation, while leveraging digital twins to safely simulate attacks, validate policies, and train teams.

Legacy systems are no longer ignored; virtual patching, micro-segmentation, and compensating controls protect unpatchable assets, while supply-chain accountability ensures vendors uphold transparency and risk controls.

By integrating CTEM, AI-driven insights, and dynamic access controls into daily operations, organizations can proactively reduce exposure, secure uptime, and maintain trust, making 2026 as the year OT security matures from reactive defense to strategic resilience.

READ THE FULL ARTICLE

Exposure Reckoning: Why 2026 Will Redefine Federal Cyber Defense

Christian Terlecki
VP Sales, Public Sector, Armis

As federal agencies enter 2026, the stakes in cybersecurity have shifted from reactive recovery to proactive prevention, demanding a continuous, mission-focused approach to threat exposure.

Accelerating adversary tactics, expanding supply-chain risks, and increasingly interconnected CPS/OT environments require agencies to embrace Continuous Threat Exposure Management (CTEM) as the foundation of defense, paired with Unified Vulnerability Management (UVM) that prioritizes risk in real-time rather than by patch schedules.

Success hinges on comprehensive situational awareness, automated response orchestration, and federated collaboration across the federal ecosystem, transforming exposures into actionable mitigation before they escalate into crises.

Agencies that operationalize CTEM and UVM, integrate CPS/OT discovery, and automate verification loops will be positioned not only to reduce mission-impact incidents but also to turn exposure visibility into measurable operational resilience.

READ THE FULL ARTICLE

Elevating Healthcare Cybersecurity Beyond Medical Devices

Moh Waqas
CTO Healthcare, Armis

In 2026, healthcare cybersecurity is evolving from a narrow focus on individual medical devices to a holistic, organization-wide strategy that embeds security into every operational and clinical process.

Forward-looking healthcare organizations are uniting IT security and HTM teams, adopting proactive device lifecycle management, and extending protection across all connected assets including smart technologies, operational systems, and patient-facing digital tools.

Regulatory pressure, public expectations, and the expanding threat landscape are driving a shift from reactive defense to prevention, where cybersecurity initiatives are measured by their impact on patient care, operational efficiency, and risk reduction.

By integrating strategy, collaboration, and comprehensive asset visibility, healthcare providers can safeguard patient safety, protect sensitive data, and build trust in an increasingly digitized healthcare environment.

READ THE FULL ARTICLE

The Year an Individual Operates Like a Nation-State

Michael Freeman
Head of Threat Intelligence, Armis

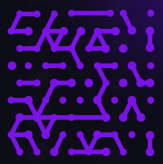
By 2026, the cybersecurity landscape is transforming as AI democratizes capabilities once reserved for nation-states, enabling individual operators to execute fully autonomous, multi-vector attacks at unprecedented speed.

Agentic AI, automated ransomware campaigns, and quantum-accelerated threats are converging to make traditional defense models obsolete, while critical infrastructure and supply chains face heightened exposure to stealthy, AI-assisted adversaries.

Organizations must adopt AI-native, unified security platforms that integrate continuous exposure management, crypto-agility, behavioral analytics, and autonomous response to detect, reason, and act at machine speed.

Success will depend on proactive, intelligence-driven resilience, where every system, workflow, and control is designed to stay ahead of adversaries who operate like entire nation-states.

READ THE FULL ARTICLE



ARMIS®

Discover new approaches to protecting your organization - then experience Armis firsthand.

Experience Armis Centrix™ Live

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

+1 888 452 4011

armis.com