The Airitos Identity & Access Management December 2025 Trends Report

The identity battlefield has transformed beyond recognition. What security leaders predicted just months ago has been obliterated by the relentless pace of change sweeping through enterprise environments in late 2025.

Artificial intelligence has become both the ultimate defender and the most sophisticated attacker, locked in an explosive arms race that's redefining security itself. Meanwhile, non-human identities have silently invaded every corner of enterprise infrastructure, outnumbering actual humans by a staggering 100 to 1 ratio. Traditional IAM frameworks are crumbling under pressure they were never built to withstand.

Autonomous AI agents have shattered every assumption about identity risk. These aren't just tools—they're independent actors making decisions, accessing systems, and creating vulnerabilities that didn't exist in any security playbook. Organizations are discovering that their carefully constructed identity architectures are suddenly obsolete.

This report cuts through the noise to deliver the hard truths security leaders need right now. Drawing from frontline researchers, battle-tested practitioners, and real-time threat intelligence, it reveals not just what's happening, but what you must do to survive the identity revolution reshaping enterprise security.

Table of Contents

Identity & Access Management: December 2025 Trends Report

Executive Summary

As we enter December 2025, the identity and access management landscape has evolved significantly from predictions made earlier in the year. What were emerging trends in spring and summer have now crystallized into operational imperatives, while new challenges have emerged that demand immediate attention. This trends report captures the current state of IAM developments, highlighting both the progress organizations have made and the critical gaps that remain.

The most striking development is the near-total convergence of artificial intelligence and identity security—operating as both defender and attacker simultaneously. Meanwhile, the explosion of non-human identities (now outnumbering humans by 100:1 in enterprise environments) has matured from a theoretical concern to a concrete crisis requiring fundamental shifts in how organizations architect their identity systems. Additionally, the proliferation of AI agents as autonomous actors has created an entirely new class of identity risk that traditional IAM frameworks were never designed to address.

This report synthesizes findings from leading security researchers, industry practitioners, and emerging threat data to provide actionable insights for security leaders navigating the complex identity landscape of late 2025.

---

1. The Non-Human Identity Crisis: From Theory to Emergency Response

The 100:1 Reality

By December 2025, the magnitude of the non-human identity problem has become impossible to ignore. OWASP's December 2025 release of the Non-Human Identities Top 10 crystallized what security researchers have been documenting: in enterprise environments, non-human identities now outnumber human identities by a ratio of 100:1, according to industry analysis. In some organizations, this ratio reaches 45:1 to 100:1 or higher depending on their cloud maturity and automation investments[1][128][131].

This exponential growth has profound implications. A large enterprise managing 5,000 employees now maintains potentially 500,000 or more non-human identities—service accounts, API keys, tokens, certificates, OAuth credentials, workload identities, and increasingly, AI agents. Traditional IAM tools, designed for managing hundreds or thousands of human users, simply cannot scale to provide the visibility, governance, and continuous monitoring these machine identities require[113].

The OWASP NHI Top 10: A Roadmap of Emerging Risks

OWASP's 2025 framework identifies ten critical risks unique to non-human identities, representing a fundamental shift from traditional IAM security thinking[131]:

NHI1:2025 – Improper Offboarding: The leading risk. When services, integrations, or applications are decommissioned, their associated machine identities often remain active and unmonitored. Analysis of AWS environments found that nearly 47% of organizations using AWS have at least one IAM Role connected to a third-party integration that hasn't been used in 90 days—yet remains active and exploitable[137][131].

NHI2:2025 – Secret Leakage: API keys, tokens, and certificates continue to appear in code repositories, configuration files, container images, and communication channels at alarming scale. This remains one of the most preventable yet most frequently exploited vectors[131].

NHI3:2025 – Vulnerable Third-Party NHI: As development teams integrate IDE extensions, GitHub Actions, and SaaS tools, they introduce third-party machine identities into their security perimeter. A single compromised GitHub Action or IDE extension can exfiltrate credentials or misuse granted permissions across thousands of developer workflows[131].

NHI4:2025 – Insecure Authentication: Many NHIs rely on deprecated or weak authentication methods. Organizations often maintain compatibility with legacy authentication protocols even as they migrate to cloud-native environments, creating inconsistent security postures[131].

NHI5:2025 – Overprivileged NHI: Similar to human privilege creep, machine identities frequently receive more permissions than necessary. Once compromised, these over-privileged accounts become high-value targets for lateral movement and data exfiltration[131].

NHI6:2025 – Insecure Cloud Deployment Configurations: CI/CD systems and cloud deployments often use static credentials or improperly validated OIDC tokens. Misconfigured trust relationships can allow unauthorized systems to obtain credentials for production environments[131].

NHI7:2025 – Long-Lived Secrets: Perhaps the most persistent problem. API keys, certificates, and tokens with no expiration or expiration dates years in the future remain standard practice in many organizations. When these long-lived credentials are compromised, attackers maintain access indefinitely[131].

NHI8:2025 – Environment Isolation Failures: Development, staging, and production environments often share machine identities or use credentials generated in one environment that remain valid across others. This blurs security boundaries and creates lateral movement paths[131].

NHI9:2025 – NHI Reuse: The same API key or service account used across multiple applications or services means a breach in one application compromises all connected systems[131].

NHI10:2025 – Human Use of NHI: Developers and operators misusing machine identities for manual administrative tasks—avoiding the need to request human access and audit

trails. This eliminates accountability and creates detection evasion opportunities[131].

Best Practices for NHI Governance

Organizations responding effectively to this crisis are implementing comprehensive NHI governance programs:

- **Automated Discovery**: Continuous scanning across all cloud providers, code repositories, container registries, and infrastructure-as-code to identify all machine identities and their characteristics[128]
- **Lifecycle Automation**: Automated provisioning, periodic validation of necessity, and automated revocation when services are decommissioned[128]
- **Least Privilege Enforcement**: Implementing fine-grained permissions policies and automatically detecting over-privileged identities[128]
- **Metrics and Monitoring**: Tracking secret age, cross-environment credential usage, privilege levels, and anomalous NHI behavior[128]
- **Secrets Rotation**: Implementing short-lived credentials where possible, or dramatically shortening rotation cycles for long-lived secrets (quarterly at minimum, monthly preferred)[128]

---

2. AI Agents: A New Class of Non-Human Identity Creates Unprecedented Risk

The Rapid Rise and Security Gap

AI agents represent perhaps the most disruptive identity development of 2025. Enterprises are rapidly deploying autonomous AI systems—GPT agents, autonomous LLM-powered bots, multi-agent systems coordinating across APIs—that require authentication, make authorization decisions, and access protected resources without human intervention. The CAGR for AI agents is forecasted at approximately 46%, meaning their population is doubling every 18 months[127].

Yet enterprises are deploying these autonomous systems without adapting their identity security frameworks. The result is a significant vulnerability: 89% of organizations acknowledge that AI agents are creating identity and security risks they're not adequately prepared to address[139].

Why AI Agents Break Traditional Identity Models

AI agents violate fundamental Zero Trust principles by maintaining long-lived credentials and executing non-deterministic actions. They require broad API access across multiple domains simultaneously—LLM provider APIs, enterprise SaaS services, cloud infrastructure, data stores—that traditional workload identity models were never designed to manage[127].

Consider a typical AI agent implementation: A GPT-4 powered business analysis bot needs access to Salesforce APIs to retrieve customer data, calls OpenAI's API for analysis, queries a Snowflake data warehouse for historical trends, and writes results to a company Slack channel. This agent requires valid credentials for four distinct services with different authentication protocols (OAuth, API key, managed identity, webhook token), different permission scopes, and different validation requirements. When the agent switches

between these execution contexts during operation, the complexity of maintaining consistent access control becomes exponentially harder[127].

The Unique Attack Surface of AI Agents

AI agents create entirely novel categories of identity vulnerabilities[127]:

Multi-Protocol Identity Confusion: Agents interact with multiple authentication providers and protocols simultaneously (enterprise APIs via OAuth, LLM services via API keys, cloud resources via managed identities). Federation attacks exploiting protocol transition points emerge as attackers attempt to spoof one authentication mechanism while actually authenticated via another.

Autonomous Identity Modification: AI agents often request permission escalation based on their analysis of task requirements—GPT-4 agents analyzing data requirements and auto-requesting additional database table access. Dynamic scope expansion occurs without human authorization or audit.

Agent-to-Agent (A2A) Protocol Risks: As agents begin directly communicating with other agents, ungoverned trust relationships form outside traditional identity provider oversight, lacking standard audit trails.

Cross-Protocol Token Substitution: Agents may reuse authentication tokens across different service boundaries, creating token substitution attack opportunities where tokens valid for one service are exploited to gain access to others.

Prompt Injection and Identity Manipulation: Malicious prompts can manipulate agents into revealing credentials, escalating permissions, or changing their own identity claims mid-execution.

Emerging Governance for AI Agent Identity

Security leaders implementing AI agent identity controls are adopting several strategies[127][129][130]:

- **Secretless Authentication**: Eliminating API keys from agent code entirely through transparent credential injection and identity-based access patterns
- **Agent Discovery and Inventory**: Maintaining comprehensive visibility into all deployed agents, their capabilities, their access requirements, and their current permissions
- **Unified Policy Framework**: Providing consistent access control across all AI integrations regardless of target service or authentication protocol
- **Real-Time Monitoring and Audit**: Tracking agent access across all API boundaries, maintaining comprehensive audit trails of agent decisions and actions
- **Segregated Agent Execution**: Isolating high-risk agent operations in sandboxed environments with limited blast radius
- **Automated Agent Offboarding**: When agents are retired, systematically removing their credentials and access across all connected services

---

3. Third-Party Identities: The Overlooked Attack Vector

The Ecosystem Inversion

A fundamental shift in risk topology is occurring: third-party identities now outnumber internal employee identities by an estimated 3:1 in large enterprises[111]. Contractors, service providers, technology partners, API integrations, and SaaS vendors have become primary participants in enterprise systems rather than peripheral accessors. Yet many organizations maintain legacy identity governance models designed for 90% internal employees and 10% external users[129].

The implications are significant. When 75% of your interactive identities are external and your IAM governance infrastructure was designed for the inverse, substantial security gaps emerge. Recent data indicates that the percentage of breaches involving a third-party has doubled in the past year, with 54% of firms experiencing a breach sourced at least partially by a third-party[129].

Where Third-Party Identity Governance Fails

Traditional identity governance treats external access as special cases requiring ad-hoc management. In practice, this creates systematic gaps[129][132]:

Identity Gaps and Stale Accounts: Third-party access requirements change frequently as projects evolve, shift, and conclude. But offboarding is often incomplete—contractors retain access long after their assignments end, leaving dormant credentials available for exploitation.

Overpermissioned External Access: When external parties onboard quickly, they often receive broad permissions as a convenience, rather than implementing strict least-privilege access. A vendor managing a single integration point may receive read access to an entire database or admin rights to an application.

Shared Accounts: Rather than creating individual credentials for each external user, many organizations use shared service accounts or vendor-supplied credentials. This eliminates audit trail clarity and makes permission revocation complex.

Weak Authentication and Reauthentication: Many third-party integrations rely on legacy authentication methods, weak credential storage, or absent re-authentication at sensitive touchpoints.

Unmonitored Sessions: External user activity often lacks real-time monitoring or comprehensive logging. While internal user access is increasingly monitored for suspicious behavior, external access may only be logged after the fact, if at all.

Inadequate Vendor Vetting: Organizations frequently partner with vendors who lack security certifications, haven't undergone SOC 2 audits, or have weak credential management practices themselves.

B2B Identity and Access Management: An Emerging Discipline

In response to this crisis, B2B IAM has emerged as a distinct discipline focused on managing external access at scale[129][132]. Leading practices include:

- **Continuous, Adaptive Trust**: Rather than granting access once and assuming it remains appropriate, modern B2B IAM continuously validates that external parties' access aligns with current business requirements
- **Real-Time Visibility**: Comprehensive dashboards showing active external users, their current permissions, last-access timestamps, and anomalous behavior patterns
- **Just-In-Time Access**: Provisioning external access only for the duration needed, automatically revoking upon task completion
- **Transitive Trust Management**: Monitoring not just direct external relationships but also understanding which other parties they're connected to (e.g., a vendor's subcontractors)
- **API-Driven Governance**: Enabling external partners to verify their own access status without requiring support tickets
- **Proof of Trust Mechanisms**: Vendors demonstrating current compliance status, security certifications, and breach history through continuous reporting rather than annual questionnaires[135]

---

4. AI-Powered Attacks: The Credential Stuffing Weaponization

The 160% Surge

Credential-based attacks have surged 160% in 2025 compared to 2024, making them the fastest-growing cyber threat on record[152]. The Verizon 2025 Data Breach Investigation Report found that 88% of breaches in 2024-2025 used stolen credentials as the initial access vector—not stolen data, not exploited vulnerabilities, but compromised identity credentials[155].

What has fundamentally changed is the automation and intelligence applied to credential attacks. Traditional credential stuffing was a blunt force instrument: attackers obtained leaked credential lists, ran mass login attempts against targets, and counted successful account takeovers. Success rates were low, measured in percentages[146].

AI-Driven Credential Optimization

In 2025, machine learning algorithms have transformed credential stuffing from spray-and-pray into precision targeting[146][152]:

Credential Prediction: AI models trained on billions of leaked credentials and behavioral data are now predicting which accounts are likely to reuse passwords, which users are susceptible to phishing, and which accounts are most likely to have high-value access. Rather than testing credentials sequentially, attackers use ML to prioritize likely successful attempts[152].

Dynamic Adaptation: AI-driven bots continuously adapt login flows, rotating IP addresses, spoofing device characteristics, and adjusting timing patterns to evade bot detection. Each

target's unique login security—CAPTCHA variations, rate limiting, behavioral signals—is analyzed and countermeasures adjusted in real-time[146].

Behavioral Mimicry: Attacks now closely mimic legitimate user behavior rather than executing obviously automated patterns. Login attempts are spaced appropriately, device fingerprints are simulated, and geographic patterns match likely user locations[146].

MFA Bypass Techniques: AI has made social engineering campaigns dramatically more sophisticated. Attackers now generate convincing deepfake videos to authenticate fraudulent account openings, use AI-generated voice to impersonate executives, and create pixel-perfect cloned login pages that prompt for MFA tokens in real-time[146][152].

The Credential Lifecycle Risk

The core problem is that passwords and static credentials remain embarrassingly easy to compromise through breaches, malware, and phishing—and once compromised, they're reused across multiple services. A 2025 analysis found that 36% of consumers admit to having been compromised due to weak or reused passwords[146], and attackers exploit that reuse through credential stuffing.

The result: when a low-security website is breached and its username-password pairs leaked, attackers immediately test those credentials against Netflix, Amazon, Gmail, corporate SaaS platforms, and banking portals, knowing that password reuse will yield valid accounts. A single breach spawns cascading compromises across unrelated services[146].

Defensive Responses Taking Shape

Security practitioners responding to this crisis are implementing several strategies[146][161]:

- **Advanced Behavioral Analytics**: Continuous analysis of user behavior patterns to identify login attempts that deviate from baseline activity (unusual locations, devices, times, or access patterns)
- **Device Intelligence**: Browser attestation APIs and device integrity verification that prove a login originates from a legitimate, non-compromised stack rather than from headless bots
- **Predictive Hardening**: Using AI to forecast credential stuffing spikes hours in advance, enabling organizations to automatically tighten authentication policies during peak attack windows
- **Invisible Security**: Applying step-up authentication and additional verification only when risk signals warrant it, maintaining smooth experience for legitimate users
- **Account Takeover Detection**: Monitoring for successful account takeover (legitimate credential use from unusual context) and immediately invalidating sessions or forcing re-authentication

---

5. The Third-Party Credential Explosion and Supply Chain Risk

From Theory to Reality

Third-party supply chain attacks have long been security concern. But 2025 has made them impossible to ignore. High-profile incidents demonstrate how compromise of a single vendor propagates across entire industries—a single vulnerable third-party integration, compromised API key, or misconfigured cloud deployment affecting hundreds of downstream customers[126][129].

What makes third-party credential risks uniquely challenging: enterprises often have minimal visibility into how third parties manage their own credentials. A SaaS vendor may have poor secrets management that goes undetected for months. A cloud deployment may store credentials in plain text configuration files. A GitHub integration may leak API keys to public repositories. By the time the breach is discovered and disclosed, lateral movement through the third-party into upstream customers is already underway[126].

The Shifting Risk Assessment Paradigm

Traditional third-party risk management relied on annual security questionnaires, occasional SOC 2 audits, and static certifications. In 2025, leading organizations are shifting toward continuous, real-time trust verification[135]:

Real-Time Proof of Trust: Vendors demonstrating current compliance, security posture, and breach status through continuous APIs and embedded dashboards rather than annual assessments. A prospective vendor can embed their TrustCloud profile directly into their sales pitch, allowing buyers' security and risk teams to verify current trust status before signing contracts[135].

Transitive Trust Analysis: Understanding not just direct third-party relationships but chains of dependencies. If a critical vendor uses a subcontractor for infrastructure management, and that subcontractor has weak identity governance, the risk propagates to you[129].

Secrets Scanning and Monitoring: Leading organizations are now monitoring their third-party vendors' public code repositories, configuration files, and cloud environments for exposed credentials—essentially auditing vendors' identity governance without permission[126].

---

6. The Deepfake Identity Verification Crisis

Biometric Authentication Under Assault

One of 2025's most alarming trends is the sophistication of deepfake attacks targeting biometric authentication systems. Fraudsters using AI-generated video have been successfully opening new accounts at financial institutions by fooling identity verification systems into accepting synthetic face videos as legitimate[111][31].

Organizations have responded with certified liveness detection and advanced biometric verification, but the arms race intensifies. For every new detection mechanism, research

groups develop more sophisticated deepfakes that evade it. The challenge is no longer "can we detect deepfakes?" but rather "can we maintain sufficient security margin while keeping authentication friction acceptable?"[111]

The Authentication Paradox

This creates a fundamental tension in identity security. Traditional authentication factors—passwords (weak), SMS codes (intercepted), one-time codes (phishable), biometric data (spoofable with deepfakes)—are all vulnerable to sophisticated attacks. Yet multi-factor authentication requirements that combine multiple vulnerable factors introduce substantial user friction, degrading adoption of online services.

The industry response is increasingly focused on possession-based authentication (physical devices you own and control) combined with biometric binding—passkeys being the primary example. But significant portions of the population still lack compatible devices, creating a migration challenge[111].

---

7. Digital Identity Wallets and eIDAS 2.0: The Regulatory Catalyst

Regulatory Mandate Accelerating Adoption

The EU's eIDAS 2.0 regulation has accelerated the deployment of digital identity wallets as a fundamental identity infrastructure component. With EU Digital Identity Wallets (EUDI Wallets) mandated to be available to all citizens and businesses within 24 months of technical specification finalization (with full rollout by 2026), the ecosystem is shifting rapidly[148][150][153][156].

eIDAS 2.0 establishes a framework for verifiable credentials (VCs) and decentralized identifiers (DIDs)—digital equivalents of physical identity documents. These credentials are issued by trusted authorities, stored in citizens' digital wallets, and presented selectively to service providers who verify them cryptographically[148][150][153].

Practical Implementation Beginning Now

By December 2025, financial institutions, government agencies, and major SaaS providers are beginning eIDAS 2.0 pilots. Banks are issuing verifiable credentials for account holders, reducing the need to store customer identity data in centralized databases. Governments are implementing citizen digital identity wallets for accessing public services. Universities are issuing blockchain-backed digital diplomas[150][153].

The business case is compelling: organizations no longer need to store customer personal data (reducing GDPR liability and breach risk), customers no longer need to re-enter identity information at every service (improving experience), and verification can happen without central intermediaries (improving privacy)[148][150][153].

The Enterprise Catch: Standards and Interoperability Challenges

However, significant challenges remain. The standards are maturing but not yet fully implemented. Wallet solutions from different vendors may not interoperate seamlessly. Legacy systems require integration efforts to accept and validate verifiable credentials[148][150][153].

Organizations beginning their eIDAS 2.0 journey in December 2025 are advised to:

- **Begin pilots with non-critical use cases**: Start with secondary authentication flows or lower-risk services to understand the technology
- **Participate in standards communities**: Contribute to W3C working groups and industry consortiums developing standards
- **Plan infrastructure investments**: Prepare for verifiable credential issuance capabilities and wallet integration
- **Design for interoperability**: Assume that wallet solutions from different vendors will need to work together

---

8. The Quantum Computing Timeline: Urgency Increasing

NIST Standards Published, Migration Planning Underway

The National Institute of Standards and Technology published its first post-quantum cryptography (PQC) standards in 2024, and by December 2025, organizations are beginning serious migration planning. The U.S. government's Quantum Computing Cybersecurity Preparedness Act mandate has accelerated timelines for federal agencies and their contractors[111][118].

What has changed since earlier in 2025 is that cryptographic migration is no longer theoretical—organizations are conducting cryptographic inventories, testing hybrid implementations of PQC and traditional algorithms, and developing transition roadmaps[111].

The Harvest Now, Decrypt Later Reality

The threat driving urgency is that adversaries are currently harvesting encrypted data with the assumption they'll decrypt it once quantum computers become available. Data with long-lived confidentiality requirements—medical records, financial information, state secrets, encrypted backups—are all potential targets for this "harvest now, decrypt later" attack. Organizations storing encrypted data that must remain confidential for decades cannot wait until quantum computers mature to begin their transition[111].

Practical Migration Strategies

Organizations conducting December 2025 assessments are following this approach:

Phase 1 (2025-2027): Discovery and Risk Assessment

- Inventory all cryptographic dependencies (TLS certificates, SSH keys, digital signatures, encrypted data, authentication tokens)
- Identify systems with the longest data lifetime requirements
- Prioritize highest-risk assets and long-lived data

- Begin testing hybrid PQC-traditional implementations in non-production environments

Phase 2 (2028-2030): Critical Asset Migration

- Replace vulnerable encryption for highest-priority systems with quantum-safe alternatives
- Implement hybrid cryptographic systems supporting both traditional and post-quantum algorithms
- Schedule regular audits of cryptographic usage
- Establish crypto-agility as an architectural principle for future systems

Phase 3 (2031-2035): Complete Transition

- Migrate remaining assets to PQC
- Deprecate non-quantum-safe algorithms in legacy systems
- Maintain crypto-agility for future adaptations

Organizations that haven't begun this assessment by December 2025 are falling dangerously behind the migration timeline[111].

---

9. Zero Trust Maturity: From Architecture to Operational Doctrine

The 91% Adoption Milestone

By December 2025, 91% of enterprises report having implemented Zero Trust principles to at least some degree—up from 48% earlier in 2025 for critical identities only[111][112]. However, there's a critical distinction between "implemented" and "operationalized."

Many organizations have deployed Zero Trust security technologies—identity verification, continuous authentication, microsegmentation—without fundamentally shifting their operational culture or access governance models. True Zero Trust requires "never trust, always verify" to become the operational default rather than an exception for high-security environments[111].

The Continuous Verification Challenge

The most challenging aspect of Zero Trust implementation is continuous verification throughout sessions rather than only at initial authentication. Many organizations have successfully implemented step-up authentication (requiring re-authentication at sensitive touchpoints), but scaling this to continuous verification across all sessions and all resource access remains difficult[111][112].

Technology challenges include:

- **Visibility gaps**: In hybrid and multi-cloud environments, achieving real-time visibility into all identity activities remains challenging
- **Inventory challenges**: Unknown or poorly documented applications and data stores make it difficult to apply consistent Zero Trust policies
- **Legacy system constraints**: Older applications may not support modern authentication protocols or continuous verification mechanisms

- **Performance impacts**: Some continuous verification approaches (re-authenticating every few minutes) create unacceptable user experience friction

---

10. Hybrid Work Identity Security: The Persistent Challenge

The Hybrid Model as Default

By December 2025, hybrid work has matured from an emergency response to organizational default. Yet identity and access security challenges persist[151][154][157]:

Distributed Attack Surface: With employees accessing corporate resources from home networks, personal devices, coffee shops, and coworking spaces, the traditional "corporate network perimeter" has completely dissolved. Each remote location represents a unique security context with different threat exposure[151][154].

Device Proliferation: Employees use multiple devices (laptops, phones, tablets), often personal devices (BYOD), with varying security postures. Maintaining consistent identity security policies across this device diversity remains challenging[151][154].

Network Vulnerabilities: Home Wi-Fi networks, personal ISPs, and public networks lack corporate-grade security controls. VPNs provide traffic encryption but don't address the growing sophistication of network-layer attacks[151][154].

Credential Exposure Risk: Remote workers use credentials from less-secure environments. Malware on personal devices can compromise credentials. Phishing attacks targeting remote workers remain highly effective[151][154].

Emerging Defensive Approaches

Organizations successfully securing hybrid workforces in December 2025 are implementing:

- **Device Posture Assessment**: Real-time evaluation of device security status (OS patches, endpoint protection, encryption status) as input to access decisions
- **Behavioral Analytics**: Continuous analysis of user behavior patterns to identify anomalies suggesting credential compromise
- **Network Intelligence**: Monitoring network traffic and connection patterns for signs of compromise or unusual access
- **Adaptive Authentication**: Dynamically adjusting security requirements based on device posture, location, time, and behavior analysis
- **Phishing-Resistant Authentication**: Implementing passwordless or multi-factor authentication that resists phishing attacks
- **Endpoint Detection and Response**: Deploying EDR tools to detect compromised endpoints and malicious activities

---

11. Identity Security Budget Reality: Underinvestment Despite Rising Risk

The Funding Gap

Despite escalating threats and regulatory requirements, many organizations continue to underinvest in identity and access management relative to overall IT security spending. A significant portion of identity budgets remain allocated to maintaining legacy IAM infrastructure rather than modernizing to address emerging threats like NHI governance, AI agent identity management, and third-party risk[111][118].

The skills shortage exacerbates the challenge. Organizations struggling to hire security professionals with IAM expertise find themselves unable to implement advanced identity programs, leading to reliance on external consultancies and vendors[111][118].

The Cost of Inaction

However, the financial incentives are shifting. Data breaches resulting from identity compromise continue to increase in cost, with average breach costs exceeding $4.4 million in 2025. Breaches caused by credential compromise (the majority of breaches) approach $5 million average cost, making the ROI case for identity security investments compelling[152][155].

Organizations investing in automated identity governance, AI-driven threat detection, and comprehensive NHI management are experiencing measurable risk reduction and operational efficiency gains.

Conclusion: The Identity Inflection Point

December 2025 represents an inflection point in identity and access management. The industry has moved decisively past the "is IAM important?" question. The challenges now are execution-focused: How do we rapidly scale non-human identity governance? How do we secure AI agents without stifling innovation? How do we manage third-party relationships at the scale they've reached? How do we implement truly continuous verification without creating unacceptable friction?

Key Imperatives for 2026 and Beyond

1. Non-Human Identity Governance is Now Essential: Organizations must implement automated NHI discovery, lifecycle management, and least-privilege enforcement immediately. The 100:1 NHI ratio means that security depends on automation more than any human-driven process.

2. AI Agent Identity Security Must Be Built In: As AI agents proliferate, organizations deploying them without comprehensive identity controls are creating high-risk security debt. The multi-protocol, autonomous nature of AI agents demands fresh thinking about identity architecture.

3. Third-Party Identity Risk Requires Continuous Management: The days of annual vendor questionnaires are ending. Continuous, real-time visibility into third-party access and verification of their security postures is becoming table stakes.

4. Credential Security and Stuffing Defense Must Evolve: Traditional passwords and static credentials are losing the security race against AI-driven attacks. Organizations must accelerate transition to passwordless authentication while implementing AI-driven threat detection and behavioral analytics.

5. Zero Trust Implementation Must Mature: While architecture-level Zero Trust adoption is nearly complete, operationalization remains challenging. Organizations must move from deploying Zero Trust technologies to living Zero Trust principles across access governance.

6. Digital Identity Wallet Integration Should Begin Now: Even for organizations outside the EU, digital wallets and verifiable credentials represent the future of identity verification. Early pilots and standards participation position organizations advantageously.

7. Quantum Readiness Cannot Delay Further: Migration timelines have compressed. Organizations that haven't begun cryptographic assessment and inventory in December 2025 are already behind schedule.

Final Thoughts

Identity and access management has become the foundational security capability—not just a compliance requirement or technical control, but a core business enabler that determines which organizations thrive in the digital economy and which become breach victims. The organizations that will lead in 2026 and beyond are those recognizing identity security as a strategic investment worthy of budget priority, executive attention, and sustained organizational commitment.

About Airitos

Airitos specializes in guiding organizations through complex identity transformations. Whether your challenge is securing non-human identities across hybrid cloud environments, architecting AI agent identity governance, modernizing third-party access management, or preparing for quantum-safe cryptography transition, Airitos brings proven methodologies and deep expertise to accelerate your journey.

Our approach emphasizes practical implementation, measurable outcomes, and alignment with your organization's unique context, risk profile, and maturity level. In 2025, organizations that partnered with Airitos have successfully implemented comprehensive NHI governance programs, deployed advanced ITDR capabilities, modernized customer identity experiences, and strengthened compliance postures across complex, multi-cloud environments.

The identity security challenges of late 2025 demand expert partnership. Contact Airitos to discuss your identity strategy.

References

[1] Identity Management Institute - "IAM Market Report 2025"
[31] Identity Management Institute - "Deepfake Risks to Identity and Access Management"
[111] Thales Group - "IAM Predictions for 2025: Identity as the Linchpin"
[112] Delana Technologies - "Cybersecurity Insights & Predictions: Q4 2025"
[113] Accesa - "Future Trends in Identity and Access Management"
[118] IBM - "Cybersecurity trends: IBM's predictions for 2025"
[126] SkyBlackBox - "Top Third-Party Security Risks in 2025 and How to Mitigate Them"
[127] Aembit - "How AI Agents Are Creating a New Class of Identity Risk"
[128] GitGuardian - "OWASP Top 10 Non-Human Identity Risks for 2025"
[129] CyberArk - "The life and death of an AI agent: Identity security lessons from the human experience"
[130] Okta - "What is AI agent identity? Securing autonomous systems"
[131] OWASP - "OWASP Top 10 Non-Human Identities Risks - 2025"
[132] iddataweb - "Understanding Third Party Risk In Identity Management"
[135] TrustCloud - "2025 Third-Party Risk Management: Emerging Trends and Technology"
[137] Orca Security - "OWASP Non-Human Identities Top 10"
[139] TechRadar - "AI agents are fuelling an identity and security crisis for organisations"
[146] Gibraltar Solutions - "Credential Stuffing in 2025"
[148] MiniOrange - "eIDAS 2.0-Compliant Digital ID Verification with EUDI Wallet"
[150] Luminess EU - "eIDAS 2.0: the digital wallet serving citizens and businesses"
[151] EmpMonitor - "How Hybrid Work Security Is Impacting Modern Workspace?"
[152] Saptang Labs - "AI-Powered Credential Theft Why 2025's 160% Surge is Only the Beginning"
[153] Partisia - "What is eIDAS 2.0? Digital Identity & EUDI Wallet explained"
[154] Darktrace - "Protecting Your Hybrid Cloud: The Future of Cloud Security in 2025"
[155] The Hacker News - "AI Agents Supercharging Credential Stuffing Attacks 2025"
[156] European Digital Identity - "eIDAS 2.0 | Updates, Compliance, Training"
[157] JD Supra - "[Webinar] Hybrid Work, Hybrid Risks"
[161] IDDataWeb - "Stopping credential stuffing account takeovers in 2025"

www.airitos.com