EXECUTIVE BRIEF · STATE OF IDENTITY SECURITY

The identity perimeter is the only one that still exists.

The question is no longer whether identity is the new perimeter. The question is whether your IAM program can hold it against an attack surface that has grown by orders of magnitude in eighteen months.

22%	$10.22M	144 : 1	217%
of breaches start with stolen credentials	average US breach cost in 2025	non-human to human identity ratio	YoY rise in MFA fatigue attacks

DOCUMENT	Annual Identity Security Report
SERIES	2026 IAM Practitioner Papers · Vol. III
AUDIENCE	CISOs, Security Architects, IT VPs
AUTHOR	IdentityLogic Consulting LLC · Arlington, VA

§ 01 · WHAT CHANGED IN 2025

Three structural shifts that broke the 2024 playbook.

Last year's report argued for IAM, PAM, and IGA convergence. The data this year tells us convergence is no longer the leading edge of the conversation. Three new fronts have opened: non-human identity sprawl, agentic AI permissions, and adversary-in-the-middle attacks that bypass MFA without breaking it.

1. Credentials are still the front door, but the door multiplied.

Compromised credentials remained the leading initial access vector at 22% of breaches in the 2025 DBIR, and 88% of basic web application attacks involved stolen credentials. What is new is the *volume* of credentials in scope. The State of Machine Identity report measured 44% YoY growth in non-human identities, with cloud-native organizations now running between 40 and 100 machine identities per human user. In the most automated environments the ratio crosses 500 to 1.

The traditional IAM control plane was designed for human onboarding and offboarding cycles. It is not architected for the velocity at which CI/CD pipelines, microservices, and AI agents create credentials.

2. MFA IS BYPASSABLE, NOT BREAKABLE

The 2025 DBIR documented a 217% YoY rise in MFA fatigue attacks. Adversary-in-the-middle proxy techniques continue to intercept session tokens after MFA. Push-notification MFA in 2026 should be treated as a baseline, not an end-state defense.

3. Third-party access is now the median attack path.

Breaches involving external partners doubled to 30% of all incidents in the 2025 DBIR. Every SaaS integration, vendor connection, and OAuth application your organization authorizes creates non-human identities operating under your trust with someone else's security practices. The tj-actions GitHub Actions compromise in March 2025 illustrated the blast radius: a single stolen personal access token exfiltrated secrets from CI/CD logs across more than 23,000 downstream repositories. Supply chain compromise also became the most expensive vector to resolve in 2025 at **$4.91M average** and **267 days to contain**.

> **The 2024 playbook assumed humans were the attack surface. The 2025 data ended that assumption.**
>
> — PRACTITIONER FIELD NOTE · 2026

§ 02 · BREACH ANCHORS

What three years of headline incidents tell us.

The breaches that defined 2024 through early 2026 were not novel. They were repeated failures of the same handful of identity controls: missing MFA, dormant privileged accounts, third-party trust without scoped access, and help-desk processes that can be socially engineered. The pattern is the warning.

INCIDENT	YEAR	IDENTITY FAILURE	CONTROL THAT WOULD HAVE BLUNTED IT
Change Healthcare	2024	No MFA on Citrix; single compromised credential	Phishing-resistant MFA on every external-facing interactive login
Snowflake customer breaches	2024	Service accounts without MFA; credentials harvested by infostealers	MFA enforced for non-human identities; vaulted machine credentials
Conduent	2025	Supply-chain access into a payroll and benefits SaaS provider	Scoped third-party access; continuous session monitoring
tj-actions GitHub Actions	Mar 2025	Stolen PAT for a popular GitHub Action; secrets exfiltrated from 23,000+ repos	Short-lived workload identity tokens; secret rotation on detection
M&S / Co-op / Harrods (Scattered Spider)	Apr–May 2025	Help-desk social engineering reset privileged credentials at a vendor	Identity-proofing for credential resets; vendor-side privileged access governance
Yale New Haven Health	Mar 2025	Lightly secured demographic data segment outside core clinical IAM	Unified entitlement governance across shadow data surfaces
Hims & Hers (Okta SSO via Zendesk)	Q1 2026	Social engineering against a third-party support tenant; lateral move via SSO trust	ITDR with cross-tenant SSO anomaly detection; scoped Zendesk OAuth grants

PATTERN

Each incident maps to an IAM control that exists today. None required novel technology to prevent. The gap is consistently between known controls and operationalized controls.

§ 03 · THE 2026 FRONTIER

Non-human identities and AI agents are eating governance.

The single most cited shift at Gartner IAM Summit 2026 was the recognition that machine identity has overtaken human identity as the primary attack surface. Only 12% of organizations have high confidence in their ability to prevent attacks via non-human identities.

44%
YoY growth in non-human identities

50%
of enterprises breached via unmanaged NHIs

68%
of security incidents involve machine identities

18%
of NHIs in some orgs are "Super NHIs" with admin access

Why traditional IAM does not catch this.

IAM frameworks were designed for joiner-mover-leaver lifecycles measured in days or weeks. A Kubernetes cluster spinning up 200 pods per minute creates and destroys workload identities at a rate that no quarterly access certification can keep up with. An AI agent operating under a broad service principal can decide to provision new resources, escalate its own privileges in pursuit of a goal, or persist credentials beyond its task lifetime. Nearly half of NHIs in surveyed environments are over a year old. One in a thousand is over a decade old. They outlive the humans who created them and the projects they served.

WHAT A 2026-READY NHI PROGRAM LOOKS LIKE

Complete inventory of service accounts, workload identities, OAuth grants, certificates, and secrets — mapped to owner and access scope. Vault-backed credential storage with automated rotation. Just-in-time issuance for agentic AI workloads with bounded permissions and TTL. Continuous secrets-exposure detection feeding identity governance. Activity-based access certification, not calendar-based. Treating an unknown service account as a finding, not a feature.

Where investment is moving.

Five program shifts dominate 2026 budget conversations. Each closes a control gap the breach data has already named.

§ 03 · WHERE INVESTMENT IS MOVING

Five shifts CISOs are funding in 2026.

Phishing-resistant authentication

FIDO2 and passkeys are moving from privileged-only to default-everywhere. IBM's 2025 report explicitly recommends moving away from SMS-based codes. Credential breaches still cost an average of $4.67M and take 246 days to contain.

Identity Threat Detection & Response (ITDR)

Treating identity events as security telemetry. Highest-impact use case is cross-tenant SSO anomaly detection — the gap that the Hims & Hers Okta breach exploited. ITDR is now distinct from SIEM in mature programs.

Non-human identity governance

A new product category in 2025–2026 (Astrix, Entro, Oasis, Aembit) operating between traditional PAM, secrets management, and IGA.

Just-in-time and ephemeral access

Standing privileged access continues to migrate to JIT issuance with time-bounded sessions. For machine workloads and AI agents the pattern is being adopted via workload identity federation, particularly with SPIRE and cloud-native equivalents.

AI governance integrated with IAM

97% of organizations that experienced an AI-related breach lacked proper AI access controls. Shadow AI added an average **$670K** to breach costs. The 2026 CISO mandate is to bring AI tools, agents, and supply-chain integrations under the same identity governance framework that already covers human and traditional service identities.

§ 04 · HOW WE HELP

Four engagement models, mapped to the 2026 control gaps.

IdentityLogic Consulting fixes broken IAM programs across seven domains: **IGA, PAM, AM, CIEM, CIAM, PIAM, and vIAM**. The mapping below is how we line up against the issues this report identifies.

ENGAGEMENT MODEL	WHERE IT FITS	WHAT WE DELIVER
Advisory	Programs without a current architecture, strategy, or roadmap	Current-state assessment across the seven IAM domains; target architecture; platform selection; three-horizon roadmap with prioritized risk reduction
Implementation	Programs with strategy in place but execution stalled	End-to-end SailPoint, Saviynt, Okta, CyberArk, BeyondTrust, and Ping engineering by practitioners who have shipped at Fortune-500 scale
Managed Support	Live IAM platforms with operational drift, alert fatigue, or skills gaps	Steady-state run-and-improve: connector health, certification cycles, policy tuning, NHI inventory and rotation, monthly governance reporting
Fractional Leadership	Programs needing IAM ownership without a full-time hire	vIAM (virtual IAM leadership) covering strategy, vendor management, audit response, and stakeholder communication on a fractional basis

SCHEDULE A FREE 30-MINUTE IAM ASSESSMENT CALL

Practitioner conversations, not sales pitches.

We work primarily with security leaders and IAM architects who already know they have a program problem. IdentityLogic Consulting LLC is a Minority-Owned Small Business based in Arlington, VA.

IDENTITYLOGICCONSULTING.COM CONTACT@IDENTITYLOGICCONSULTING.COM

(703) 843-6787

SOURCES

Verizon, 2025 Data Breach Investigations Report, May 2025. IBM and Ponemon Institute, Cost of a Data Breach Report 2025, July 2025. Entro Labs, NHI & Secrets Risk Report H1 2025, July 2025. Cloud Security Alliance, State of Non-Human Identity and AI Security Survey Report 2026, January 2026. Gartner, Top 6 Cybersecurity Trends for 2026, February 2026. BeyondTrust, Cybersecurity Predictions for 2026 and Beyond, November 2025. Public reporting on Change Healthcare (2024), Snowflake customer breaches (2024), Conduent (2025), tj-actions (March 2025), Scattered Spider UK retail intrusions (April–May 2025), Yale New Haven Health (March 2025), and the Hims & Hers Okta-Zendesk incident (Q1 2026).