IAM & SECURITY BRIEFING

IAM & Security Weekly Briefing

WEEK OF 2026-05-10 to 2026-05-16

Reporting window: Sunday–Saturday of the prior calendar week (does not include the current in-progress week).

---

1. Executive Summary (TL;DR)

- **Identity breaches are now near-universal.** Sophos's *State of Identity Security 2026* (May 12, n=5,000 IT/security leaders in 17 countries) found **71% of organizations suffered at least one identity-related breach in the past year**, averaging three attacks per affected org and a **$1.64M global mean recovery cost**. Two-thirds of ransomware victims (67%) traced their incident back to an identity attack. (Sophos press release, Help Net Security)
- **Patch Tuesday hit identity hard.** Microsoft's May 12 release shipped fixes for **137 CVEs** (no zero-days, a first since June 2024), including **CVE-2026-41103** — a CVSS 9.1 "Exploitation More Likely" bug in the Microsoft SSO plug-in for Jira & Confluence that lets an attacker **sign in with a forged identity, bypassing Entra ID authentication entirely** — and a CVSS 9.8 Netlogon RCE on Windows Server. (Tenable, BleepingComputer)
- **NHIs are the new attack surface.** Sophos pinned **41% of successful identity breaches on weak non-human identity (NHI) management** — static credentials, hard-coded API keys, orphaned service accounts — with NHIs outnumbering humans by ratios as high as **100:1**. Only **34%** of orgs regularly audit or rotate them. (ASIS International recap)
- **SailPoint launches Agentic Fabric.** On May 11, SailPoint unveiled an identity governance platform purpose-built for **autonomous AI agents and other non-human identities**, including agent discovery, runtime policy controls, and lifecycle governance from creation through decommission. (Help Net Security)
- **Strategic signal: agent governance is not catching up.** Cisco/CrowdStrike data circulating this week shows **85% of enterprises are running AI-agent pilots while only 5% have reached production — an 80-point governance gap.** Most agents still exist in an "identity gray area," not managed as either humans or first-class machine identities. (VentureBeat, Dark Reading)
- **CISA tightens identity-edge patching.** Federal agencies hit a **May 12 KEV remediation deadline** for two actively-exploited bugs — **CVE-2026-32202** (Windows Shell NTLMv2 credential-leak, residual issue from the February CVE-2026-21510 patch) and **CVE-2024-1708** (ConnectWise ScreenConnect). On May 15 CISA added **CVE-2026-42897**, a Microsoft Exchange Server XSS, to KEV. (CISA KEV, CISA alert — May 15)
- **Microsoft makes Entra passkeys-first.** Microsoft confirmed **passkeys for Entra External ID reach GA at the end of May** and signaled removal of security questions as a password-reset option in Entra ID in

January 2027. The shift is occurring alongside Entra SCIM moving off OAuth 2.0 Authorization Code grant onto client-credentials / workload identity federation. (Microsoft Entra blog — May 2026)

- **Instructure / Canvas extortion lands.** On May 12 Instructure publicly confirmed an "agreement" with a decentralized extortion crew (UNC6040 / ShinyHunters lineage) after the breach disclosed the prior week — closing the loop on the largest identity-led SaaS extortion event of the year so far. (Recent breaches index)

---

2. Top IAM & Security News

1. SOPHOS *STATE OF IDENTITY SECURITY 2026* — 71% OF ORGS BREACHED, $1.6M MEAN RECOVERY

Published May 12. Vendor-agnostic survey of 5,000 IT and cybersecurity leaders across 17 countries and 14 industries. Headline numbers: **71% suffered at least one identity-related breach** in the prior 12 months (Switzerland 89%, Mexico 83% leading by geography); average of **three identity attacks** per affected org; **67% of ransomware victims** said the incident was directly tied to an identity attack; **$1,637,363 mean / $750K median recovery cost**; only **24% continuously monitor for unusual login attempts**. - **Why it matters:** The report quantifies what 2025's incident trail already implied — identity is now both the dominant breach vector and the dominant ransomware on-ramp. The 24% continuous-monitoring stat is the actionable one: most orgs still treat identity telemetry as a quarterly audit, not a live signal. - **Source:** Sophos press release, Full report PDF, Help Net Security recap

2. CVE-2026-41103 — MICROSOFT SSO PLUG-IN (JIRA/CONFLUENCE) AUTHENTICATION BYPASS, CVSS 9.1

Microsoft's May 12 Patch Tuesday disclosed an elevation-of-privilege flaw in the Microsoft Single-Sign-On Plug-in for Atlassian Jira & Confluence. An unauthenticated attacker can send a crafted response during the sign-in handshake to **forge an identity and bypass Microsoft Entra ID authentication entirely**, gaining read/write access to Jira and Confluence content. Rated "Exploitation More Likely" in Microsoft's Exploitability Index. - **Why it matters:** This is exactly the failure mode CISOs have been warning about — a single bridge component between Entra and a downstream SaaS becomes the weakest link in the identity chain. Patch, audit Jira/Confluence audit logs for anomalous SSO assertions over the past 60 days, and confirm that conditional access policies actually require interactive MFA, not just a valid token. - **Source:** Tenable — May 2026 Patch Tuesday, CrowdStrike analysis, BleepingComputer summary

3. SAILPOINT AGENTIC FABRIC — FIRST DEDICATED IDENTITY-GOVERNANCE PLATFORM FOR AI AGENTS

Announced May 11. SailPoint extends its Atlas/Identity Security Cloud foundation with a layer purpose-built for autonomous agents: agent discovery and registration, runtime policy enforcement, **least-privilege scoping per task**, automated credential rotation, and agent-aware threat detection. The platform integrates with major agent runtimes (LangChain, Bedrock AgentCore, Azure AI Foundry, Vertex Agent Builder) and exposes a unified inventory across human, machine, and agent identities. - **Why it matters:** Until now, AI-agent governance has been bolted onto IGA or PAM products as a feature. Agentic Fabric is the first product launch positioning agents as a **first-class identity class with their own governance lifecycle** — and it lands a week before Cisco's Astrix-based offering is expected to ship. Procurement timelines for 2026 RFPs are about to compress. - **Source:** Help Net Security, SailPoint corporate blog (Adaptive Identity context)

4. CISA ADDS CVE-2026-42897 (MICROSOFT EXCHANGE XSS) TO KEV

On May 15 CISA added an actively-exploited Exchange Server cross-site scripting vulnerability to the Known Exploited Vulnerabilities catalog. Federal agencies were already racing a **May 12 deadline** for two earlier KEV adds — **CVE-2026-32202** (Windows Shell, NTLMv2 hash leak residual from a partial February patch) and **CVE-2024-1708** (ConnectWise ScreenConnect). - **Why it matters:** Exchange remains a high-value identity-context target — XSS in OWA can be chained to harvest session tokens, OAuth scopes, and delegated mailbox access. The May 12 deadline also illustrates the **partial-patch problem**: Microsoft's February fix for the NTLM relay path left a residual flaw that still leaked credentials, requiring a second patch and a second remediation sprint. - **Source:** CISA alert — May 15, CISA KEV catalog

5. INSTRUCTURE / CANVAS — EXTORTION AGREEMENT CONFIRMED (MAY 12)

Instructure (parent of the Canvas LMS) publicly confirmed it had reached an "agreement" with the decentralized extortion group behind the breach disclosed the prior week. The campaign — attributed to UNC6040 / ShinyHunters lineage — threatened to publish stolen records from thousands of K-12 and higher-ed institutions, with reported initial access via vishing of help-desk staff to compromise an SSO account. - **Why it matters:** The pay-or-leak resolution closes the largest identity-led SaaS extortion event of the year. Operationally it sets a precedent — and an unwelcome one — for how an SSO-mediated SaaS breach gets resolved when downstream stakeholders are millions of students. Re-validate help-desk identity-reset workflows; vishing → SSO reset → OAuth abuse remains the dominant kill chain. - **Source:** BrightDefense breach index, SharkStriker May 2026 breach roundup

6. MICROSOFT ENTRA MODERNIZATION: SCIM AUTH MIGRATION + PASSKEYS FOR EXTERNAL ID GA

Microsoft's May 2026 *What's New in Entra* recap (covering changes landing this month) confirms **passkeys for Entra External ID reach GA at the end of May**, lets customers migrate SAP SuccessFactors provisioning from basic auth to **workload identity federation** in place (no reconfiguration required), and forces **SCIM provisioning apps off OAuth 2.0 Authorization Code grant onto client-credentials or workload identity federation**. Entra Global Secure Access now supports network-based file-type filtering for transfers to generative-AI and SaaS apps. - **Why it matters:** SCIM is the silent identity backbone of most enterprise SaaS provisioning; pushing it onto modern auth materially reduces credential-theft blast radius. The External ID passkey GA also de-risks the consumer-facing identity surface most often abused in account-takeover attacks. - **Source:** Microsoft Entra blog — May 2026, Microsoft Learn — Entra What's New

7. QUEST RESEARCH: NHI SPRAWL NOW OUTPACES EVERY OTHER IDENTITY DISCIPLINE

Quest Security published *Non-Human Identity Security in the Age of AI and Automation* on May 14, restating what's becoming the consensus picture: NHIs (service accounts, API keys, agent credentials) are the **fastest-growing identity class** and the **least-governed**. The recommended modern stack: automated discovery, clear human ownership per credential, automated rotation, least-privilege scoping, and ITDR for behavioral baselines. - **Why it matters:** Pairs with the Sophos 41% NHI-root-cause stat. The "clear ownership" recommendation is the under-discussed one — most NHI inventories list credentials without naming a responsible human, which is what kills rotation programs at week six. - **Source:** Quest Security blog, Token Security NHI guide (May 13)

8. GRAFANA GITHUB-TOKEN EXPOSURE (DISCLOSED MID-WINDOW)

Grafana disclosed that an "unauthorized party" obtained a token granting access to its GitHub environment, with the source-code download attempted. Disclosure landed at the close of the reporting window; investigation and downstream-impact details are still developing. - **Why it matters:** Yet another reminder that

long-lived **GitHub PATs and OAuth app tokens** are first-class identities with prod blast radius. Audit your org for tokens with `repo` scope older than 90 days, especially on bot accounts where rotation discipline tends to lapse. - **Source:** The Hacker News — recent disclosures, BreachSense breach feed

---

3. AI, Identity & Emerging Tech

PING IDENTITY / KUPPINGERCOLE — *FROM AI AGENTS TO TRUSTED DIGITAL WORKERS*

Released this week. Core finding: **AI agents are being deployed into production faster than enterprises can govern them**, exposing gaps in identity systems originally designed for human users. The report calls out a specific failure mode — agents combining **individually legitimate permissions in unintended ways**, producing actions that bypass established controls and cannot be fully traced. - **Implications:** Coarse-grained role assignment to agents is the immediate risk. Move toward **per-task scoped credentials** (just-in-time, minimum scope, short TTL) and require human-in-the-loop checkpoints for any agent action that crosses a privilege boundary. - **Source:** Biometric Update — AI agents breaking IAM

CISCO / CROWDSTRIKE: 85% PILOT, 5% PRODUCTION — THE 80-POINT GOVERNANCE GAP

Data referenced across multiple this-week reports from Cisco and CrowdStrike: **85% of enterprises are running AI-agent pilots, only ~5% have reached production.** The blocker is governance, not capability — most agents lack distinct identities, durable audit trails, or behavioral baselines, and live in an "identity gray area" between human and machine. - **Implications:** The gap is closing fast as agent-identity platforms (SailPoint Agentic Fabric, Cisco/Astrix, IBM Vault 2.0, Microsoft) ship. Architects should treat the 5%-to-mainstream transition as a 12–18 month window and plan inventory + policy work now. - **Source:** VentureBeat — agent identity maturity model, Dark Reading — real-time identity for agents

MICROSOFT DEFENDER FOR CLOUD CIEM EXPANDS TO AWS CLOUDTRAIL SIGNALS

Released this week. CIEM recommendations in Defender for Cloud now ingest **AWS CloudTrail management-event activity** alongside Access Advisor, and extend the inactivity lookback window from 45 to **90 days**, evaluating unused role assignments rather than just sign-in activity. - **Implications:** Tighter signal for detecting dormant identities and silent privilege escalation paths in AWS workloads. Re-run least-privilege reviews using the new 90-day window — orgs with quarterly review cycles will catch identities they were previously missing. - **Source:** Microsoft Learn — Defender for Cloud release notes

IBM VAULT 2.0 + UNIFIED VERIFY/VAULT FOR THE AGENTIC ERA

Restated at industry events this week. IBM positions Vault 2.0 as identity-based security at scale for AI agents, with the unified Verify+Vault stack covering **both human and non-human identities under one policy plane**. - **Implications:** Combined with SailPoint Agentic Fabric and Cisco's Astrix acquisition, this is the third Tier-1 vendor staking a unified human+agent identity platform inside three weeks. Expect aggressive bundling and competitive procurement pressure in late 2026. - **Source:** IBM Think 2026 — identity recap, IBM — identity problem at the heart of agentic AI

---

4. Cyber Threats & Attack Trends

A) "LOG IN, DON'T BREAK IN" — CREDENTIAL-LED INTRUSION NOW DOMINATES

Multiple this-week sources converge on the same point: **stolen credentials, not unpatched vulns, are the dominant initial-access pathway.** Sophos puts identity in **80%+ of ransomware operations**; threat-intel firms tracked nearly 2.9B compromised credentials globally in 2025, with ~347M originating from infostealers on ~3.9M infected machines. - **Source:** SecurityWeek — stolen logins fueling ransomware and nation-state, Morphisec — fileless attacks to identity abuse

B) SAAS-EXTORTION VIA HELP-DESK VISHING (SHINYHUNTERS LINEAGE CONTINUES)

The Instructure resolution this week is one bookend. The kill chain — voice phishing → help-desk-mediated SSO reset → OAuth scope abuse → mass SaaS export → leak-site extortion — remains the highest-yield identity-led attack pattern of 2026. Help-desk identity verification is the single point of failure. - **Source:** SharkStriker May 2026 breach list

C) AUTHENTICATION-BYPASS SURFACE AREA IN IDENTITY MIDDLEWARE

CVE-2026-41103 in the Microsoft SSO plug-in for Jira/Confluence is the marquee example this week, but the broader pattern is identity-middleware (SSO plug-ins, federation bridges, SCIM connectors) becoming the soft underbelly between hardened IdPs and downstream SaaS. The flaw allowed an attacker to forge identity assertions and skip the Entra MFA challenge entirely. - **Source:** Tenable — May 2026 Patch Tuesday, Qualys Patch Tuesday review

D) IDENTITY-EDGE APPLIANCES UNDER SUSTAINED PRESSURE

KEV additions over the trailing month — PAN-OS User-ID portal (CVE-2026-0300, prior week), Ivanti EPMM RCE, Cisco Catalyst SD-WAN auth bypass (CVE-2026-20127), BeyondTrust RS/PRA (CVE-2026-1731) — all hit appliances that enforce identity at the perimeter or manage privileged sessions. These boxes authenticate everyone else; their compromise is the highest-leverage identity-context takeover available. - **Source:** Tenable — CVE-2026-20127 Cisco Catalyst SD-WAN, The Hacker News — BeyondTrust exploitation

E) NHI/SECRET LEAKAGE AT THE SDLC BOUNDARY

The Grafana disclosure (above) and ongoing infostealer harvesting both highlight that **GitHub PATs, CI/CD secrets, and OAuth app credentials are now identity-class assets** with prod blast radius — but few orgs govern them with the rigor applied to human SSO accounts. - **Source:** BreachSense breach feed

---

5. Product Updates & Vendor News

- **Microsoft Entra** — Passkeys for External ID hit GA at end of May. SCIM provisioning apps forced off OAuth 2.0 Authorization Code grant to client-credentials / workload identity federation. SAP SuccessFactors provisioning can migrate from basic auth to workload identity federation in place. Global Secure Access adds network-based file-type filtering for GenAI/SaaS transfers. (Microsoft Entra blog — May 2026)
- **Microsoft Defender for Cloud** — CIEM now ingests AWS CloudTrail management events. Inactivity lookback extended 45 → 90 days. (Microsoft Learn — release notes)
- **SailPoint** — Agentic Fabric launched May 11: identity governance platform for autonomous AI agents and other NHIs, with agent discovery, runtime policy enforcement, and lifecycle governance. (Help Net

Security)

- **IBM** — Vault 2.0 and unified Verify/Vault for the agentic era, covering humans + NHIs under a single policy plane. (IBM Think 2026 recap)
- **Google Cloud** — Wiz vibe-coding integration GA in May; Wiz security scanning runs inside the Lovable platform, surfacing vulnerabilities, secrets, and misconfigurations in Lovable's security view. Predefined roles catalog streamlining + IAM role picker UX changes. (Google Cloud / Wiz)
- **Ping Identity** — *From AI Agents to Trusted Digital Workers* research published with KuppingerCole, naming opaque delegation chains and prompt-injection exposure as the core agentic-IAM risks. (Biometric Update)
- **Cisco** — Continued integration of Astrix Security (announced May 4) into Cisco Identity Intelligence, Secure Access, and Duo IAM for NHI/agent discovery and governance. (VentureBeat — agent identity maturity model)
- **Microsoft (Patch Tuesday, May 12)** — 137 CVEs, no zero-days. Notable identity-relevant fixes: CVE-2026-41103 (SSO plug-in for Jira/Confluence, CVSS 9.1) and a Windows Netlogon RCE (CVSS 9.8). (CrowdStrike analysis, Lansweeper)
- **SAP** — 15 new security notes as part of May 2026 Security Patch Day, including critical S/4HANA and Commerce Cloud fixes. (SecurityWeek, BleepingComputer)

---

6. Notable Research & Reports

SOPHOS — *STATE OF IDENTITY SECURITY 2026*

- Sample: 5,000 IT/security leaders, 17 countries, 14 industries.
- 71% of orgs hit by ≥1 identity-related breach in the past 12 months; affected orgs averaged 3 incidents.
- 67% of ransomware victims tied the incident to an identity attack.
- 41% of identity breaches rooted in NHI mismanagement.
- Mean recovery cost $1.64M, median $750K.
- Only 24% continuously monitor for unusual login attempts.
- **Implication:** Identity attacks are no longer a category — they are the *default* breach mode. The continuous-monitoring gap is the single most actionable finding.
- Press release · Full report PDF

PING IDENTITY / KUPPINGERCOLE — *FROM AI AGENTS TO TRUSTED DIGITAL WORKERS*

- AI agents deployed faster than enterprises can govern them.
- Specific failure mode: agents combine individually-legitimate permissions in unintended ways, bypassing controls.
- Calls out opaque delegation chains, prompt-injection exposure, and the loss of human-consent and event-level auditability assumptions baked into IAM.
- **Implication:** Per-task scoped credentials and human-in-the-loop checkpoints for cross-boundary actions are the practical mitigations.
- Biometric Update summary

QUEST SECURITY — *NON-HUMAN IDENTITY SECURITY IN THE AGE OF AI AND AUTOMATION* (MAY 14)

- Modern NHI security stack: automated discovery → human ownership per credential → automated rotation → least privilege → ITDR for behavioral baseline.
- **Implication:** "Owner attribution" is the silently-critical step — without a named human owner, rotation programs stall and stale credentials accumulate.
- Quest blog

TOKEN SECURITY — *ULTIMATE NON-HUMAN IDENTITY SECURITY GUIDE* (MAY 13)

- Practitioner-oriented playbook covering API keys, service accounts, AI-agent credentials, and OAuth tokens across cloud-native + SaaS + agentic stacks.
- Token Security guide

---

7. Practical Security Takeaways

1. **Patch CVE-2026-41103 immediately.** Microsoft SSO plug-in for Jira/Confluence, CVSS 9.1, identity-forgery bypass. Then audit Jira/Confluence audit logs for anomalous SSO assertions over the past 60 days.
2. **Apply the May 12 KEV remediation set.** CVE-2026-32202 (Windows Shell NTLMv2 leak — partial-patch problem), CVE-2024-1708 (ConnectWise ScreenConnect), and now CVE-2026-42897 (Exchange XSS, added May 15).
3. **Run a help-desk vishing exercise.** Adversaries are walking through identity-reset workflows in production every week. Specifically validate that help-desk staff require **out-of-band re-auth + manager approval** before resetting MFA or password on any account with SaaS-admin or SSO-admin scope.
4. **Inventory non-human identities with named human owners.** Pair every API key, service account, OAuth app, and agent credential with a responsible engineer. Credentials without owners get rotated or revoked. This single change is what makes the next four items work.
5. **Continuous identity monitoring, not quarterly review.** Sophos found only 24% of orgs continuously monitor unusual logins. The fix is ITDR/UEBA-style behavioral baselines with **real-time alerting on credential reuse, impossible travel, MFA-fatigue patterns, and OAuth-scope changes**.
6. **Tighten SCIM and OAuth-app posture.** Microsoft is forcing SCIM off Authorization Code grant for a reason — long-lived bearer tokens are the most-exploited identity-class secret outside of SSO sessions. Migrate to workload identity federation or client-credentials where the IdP supports it.
7. **Phishing-resistant MFA is now the floor for privileged accounts.** Passkeys (FIDO2/WebAuthn) for admins, SaaS-admin, IdP-admin, and any role with cross-tenant scope. Number-matching push is no longer sufficient against MuddyWater-style live-coached MFA defeat.
8. **Treat AI agents as first-class identities.** Per-task scoped credentials, short TTL, behavioral baselines on agent actions, and human-in-the-loop for any privilege-boundary crossing. If you can't answer "which agent did this, with what permission, on whose behalf" — fix that first.
9. **Rotate GitHub PATs, CI/CD secrets, and OAuth-app credentials older than 90 days.** Grafana's disclosure is the third major incident in 2026 with GitHub-token blast radius. Bots and service identities tend to skip rotation policy entirely.

10. **Re-run AWS least-privilege reviews under the new 90-day window.** Defender for Cloud's extended lookback will surface dormant identities and unused permissions you previously kept — clean them up before an attacker logs in instead.

---

8. Trends to Watch

- **Identity middleware becomes the soft underbelly.** SSO plug-ins, federation bridges, and SCIM connectors between hardened IdPs and downstream SaaS are emerging as the highest-leverage authentication-bypass surface area (CVE-2026-41103 is the case in point).
- **Agent identity standards are about to land.** Between FIDO's *Trusted AI Agent Interaction* workstream, SailPoint Agentic Fabric, Cisco/Astrix, and IBM Vault 2.0, the long-lived API-key era ends in the next ~18 months. Start cataloging which workflows depend on bearer tokens — those are migration candidates.
- **NHI ratios will keep widening.** 100:1 NHI-to-human is the leading edge; in heavily-automated environments the ratio is already higher. Governance tooling needs to scale at machine speed, not human-review speed.
- **ITDR becomes table stakes.** Sophos's 24% continuous-monitoring gap, the Sophos $1.6M mean recovery cost, and the 80%+ ransomware-identity tie make Identity Threat Detection & Response the budget line that closes fastest in 2026.
- **Partial-patch incidents are recurring.** CVE-2026-32202 (residual NTLM leak after the February fix) is the latest example. Expect more "patch the patch" cycles, particularly on identity-context vulnerabilities where the attack surface has multiple paths.

---

9. Tool / Resource of the Week

Token Security — *The Ultimate Non-Human Identity Security Guide* (published May 13, 2026)

A practitioner-oriented playbook for inventorying, scoping, rotating, and monitoring NHIs across cloud, SaaS, containerized, and agentic stacks. Covers API keys, service accounts, OAuth tokens, secrets-manager hygiene, and agent credentials, with operational checklists and concrete owner-attribution patterns.

- **Why it's useful:** With NHIs sitting behind 41% of identity breaches and most orgs missing structured owner-attribution, this is the most practical, vendor-implementable artifact to come out of the week. Pair it with Quest's *Non-Human Identity Security in the Age of AI and Automation* (May 14) for a complete on-ramp.
- **Link:** Token Security NHI guide

---

10. Sources

- Sophos State of Identity Security 2026 — press release
- Sophos State of Identity Security 2026 — full report PDF
- Help Net Security — Over 70% of organizations hit by identity breaches
- ASIS International — Lax Security Management of AI Agents and Other Non-Human Identities Costs Companies
- Tenable — May 2026 Microsoft Patch Tuesday addresses 118 CVEs / CVE-2026-41103

- CrowdStrike — May 2026 Patch Tuesday updates and analysis
- BleepingComputer — Microsoft May 2026 Patch Tuesday fixes 120 flaws, no zero-days
- Qualys — Microsoft and Adobe Patch Tuesday May 2026 review
- Lansweeper — Microsoft Patch Tuesday May 2026
- Help Net Security — SailPoint Agentic Fabric expands identity governance to autonomous AI agents
- StockTitan — SailPoint redefines identity security with new adaptive identity
- Microsoft Entra blog — What's New in Microsoft Entra: May 2026
- Microsoft Learn — Microsoft Entra releases and announcements
- Microsoft Learn — Defender for Cloud release notes
- CISA — KEV catalog
- CISA Alert — CISA Adds One Known Exploited Vulnerability to Catalog (May 15, 2026)
- BrightDefense — List of Recent Data Breaches in 2026
- SharkStriker — May 2026 Data Breaches
- BreachSense — Data Breach News
- The Hacker News
- Biometric Update — AI agents operating continuously at machine speed are breaking human-centric IAM
- VentureBeat — AI agent identity: how to govern agentic AI in 6 stages (Cisco/CrowdStrike RSAC 2026)
- Dark Reading — AI Agents Are Forcing Identity Security Into Real Time
- IBM — What identity means in the age of agentic AI: Insights from Think 2026
- IBM — The identity problem at the heart of agentic AI security
- Google Cloud / Wiz — Redefining security for the AI era
- Quest Security — Non-Human Identity Security in the Age of AI and Automation
- Token Security — The Ultimate Non-Human Identity Security Guide
- SecurityWeek — Stolen Logins Are Fueling Everything From Ransomware to Nation-State Cyberattacks
- Morphisec — From Fileless Attacks to Identity Abuse: The Hard Truth About Ransomware in 2026
- SecurityWeek — SAP Patches Critical S/4HANA, Commerce Vulnerabilities
- BleepingComputer — SAP fixes critical vulnerabilities in Commerce Cloud and S/4HANA
- Tenable — CVE-2026-20127 Cisco Catalyst SD-WAN auth bypass
- The Hacker News — Researchers Observe In-the-Wild Exploitation of BeyondTrust CVSS 9.9 Vulnerability