Issue 107 | October 2025

NTT DATA

Radar

The Cybersecurity Magazine

Identity is the New High-Security Zone

By Hans Vigil Navas

If 2024 was the year of consolidating Zero Trust, 2025–2026 will be the years of operationalizing identity as the true perimeter. Three forces are accelerating this shift: the maturity of NIST guidelines on digital identity, the pressure from APIs as the backbone of business, and the professionalization of attacks targeting weak authentication factors.

In our region (with multi-cloud ecosystems, expanding digital public services, and increasingly SaaS-driven supply chains), the cost of not modernizing IAM is no longer technical: it's strategic.

1. From "MFA Compliance" to Phishing-Resistant Authentication

NIST released revision 4 of SP 800-63 (August 2025), updating identity proofing, authentication, and federation requirements — now incorporating privacy and user experience considerations.For CISOs, this means raising the bar toward phishing-resistant MFA and standardizing assurance levels across the entire digital journey (onboarding, recovery, third-party federation).

2. Passwordless for Real (with Metrics)

The global momentum behind passkeys (FIDO2/WebAuthn) is no longer "the future": over 15 billion accounts can now use them, and corporate adoption continues to grow, guided by public metrics and best practices from the FIDO Alliance.By 2025, nearly half of the top 100 websites already support passkeys.For Latin America, this means planning for: Gradual migrations, recovery and portability policies and user education to avoid friction.

3. Zero Trust in the Identity Layer

NIST SP 800-207 and its companion 800-207A reposition access controls toward continuous, contextual access decisions, decoupling the network from the resource. Putting this into practice requires: Application-level policies, device posture signals, adaptive re-authentication and the goal isn't to "lock down the network," but to authorize every request using real-time context.

4. APIs: Where Access Control Is Broken — or Won

While the OWASP Top 10 for Web continues to list Broken Access Control as a critical risk, the OWASP API Security Top 10 (2023) highlights that the most exploited vulnerabilities are BOLA /BOPLA and broken authentication.

The recommendation for 2025–2026 is explicit: Policy-as-code for object/property-level authorization, API inventory and classification, security testing within the CI/CD pipeline, and token governance — including rotation, minimal scopes, and anomalous usage detection.

5. ISO/IEC 27001:2022 as a Management Anchor

The current standard remains ISO/IEC 27001:2022 (with the 2024 amendment), which aligns controls with cloud and identity realities.For CISOs, it provides a framework to integrate IAM with risk, audit, and vendor management, ensuring that IAM is not seen merely as "technology," but as a process tied to continuous improvement.

6. New Frontiers: Machines, Agents, and Identity Threat Detection

The explosion of non-human identities (workloads, containers, service keys, and AI agents) demands visibility, just-in-time issuance, Zero Standing Privilege, and automated rotation. The market is already treating ITDR (Identity Threat Detection & Response) as a necessary category to detect token abuse, impossible travel, hijacked sessions and consent phishing.

Concrete Priorities for the Next 12–18 Months

- Hardening Authentication: Build a passkey roadmap for critical apps, deploy phishing-resistant MFA, implement SMS-free account recovery and track adoption and success by user cohort
- API Access Governance: create a unified API inventory, run authorization tests in CI/CD, enforce least-privilege scopes per client and enable token telemetry and real-time revocation
- Identity-First Zero Trust: Apply dynamic policies using device/location/risk signals, continuously revalidate sessions and privileges
- Non-Human IAM: Issue ephemeral credentials, enable automatic rotation, maintain a cryptographic usage log and implement separate guardrails for AI agents

- Align with ISO 27001:2022: Define IAM KPIs within the ISMS, conduct third-party audits (federation, IDaaS), and address identity risk management at the security committee level.

- ITDR: Identity-centric anomaly detection and integrated “kill-switch” for compromised tokens/sessions within the SOC.

Ultimately, modernizing Identity & Access Management (IAM) is not a project — it's a business operating model. Adopting NIST SP 800-63-4, hardening APIs with OWASP, and anchoring governance in ISO/IEC 27001:2022 will enable organizations in Peru and across Latin America to: Sustain digital growth, meet regulatory requirements, reduce fraud, intrusion, and privilege abuse risks in a measurable way throughout 2025–2026.

Hans Vigil Navas
Cybersecurity Manager

Digital Identity: The Master Key

Cyber chronicle by Marlon Santiago Nivia Devia

Between mid-2024 and August 2025, the cybersecurity landscape made one thing clear: even the most prepared organizations can fall if their Identity and Access Management (IAM) is compromised.More than any firewall or antivirus, digital identity has become the master key to infiltrate systems, escalate privileges, and compromise critical infrastructure.In less than a year, a series of chained attacks revealed that the weakest link isn't always the code — it's often the credentials, the tokens, and the people who manage them.

The first alarm bell rang in mid-2024, when the ShinyHunters group carried out one of the largest data thefts in recent times. Armed with credentials stolen via infostealer malware, they gained access to Snowflake customer accounts that lacked multi-factor authentication.

The attack was silent and surgical: they identified compromised credentials on infected machines, tested them against Snowflake's cloud, and once inside, downloaded entire databases without triggering critical alerts.

Without needing to exploit platform code or compromise internal employees, they used the absence of a second factor as the entry point, exposing millions of records belonging to companies such as Ticketmaster, Santander, Advance Auto Parts, LendingTree, and AT&T.

The breach was so massive that much of the data ended up circulating in underground forums like BreachForums, where it was resold and shared among various criminal groups. This episode not only highlighted the growing threat of infostealers, but also how fragile security can be when an external provider centralizes critical information without enforcing strong authentication.

The industry was still processing the fallout of this blow when, in December 2024, another incident raised alarms at the heart of the U.S. government. The Department of the Treasury suffered what it called its "largest cybersecurity incident", after being attacked by an advanced persistent threat (APT) group allegedly linked to the Chinese state. By exploiting two zero-day vulnerabilities in the BeyondTrust privileged access management (PAM) support service, the attackers broke into the network and stole a highly privileged API key. With it, they not only reset passwords for critical accounts, but also obtained remote access to workstations containing classified information about financial operations and sanction policies.

Although BeyondTrust immediately revoked the compromised secret and disabled suspicious instances, the incident made one thing clear: in IAM and PAM environments, a single poorly protected token can become the master key that opens every door. The political dimension of the attack was equally significant: while the United States formally accused China, Beijing denied any involvement, escalating the incident into the realm of diplomatic tension.

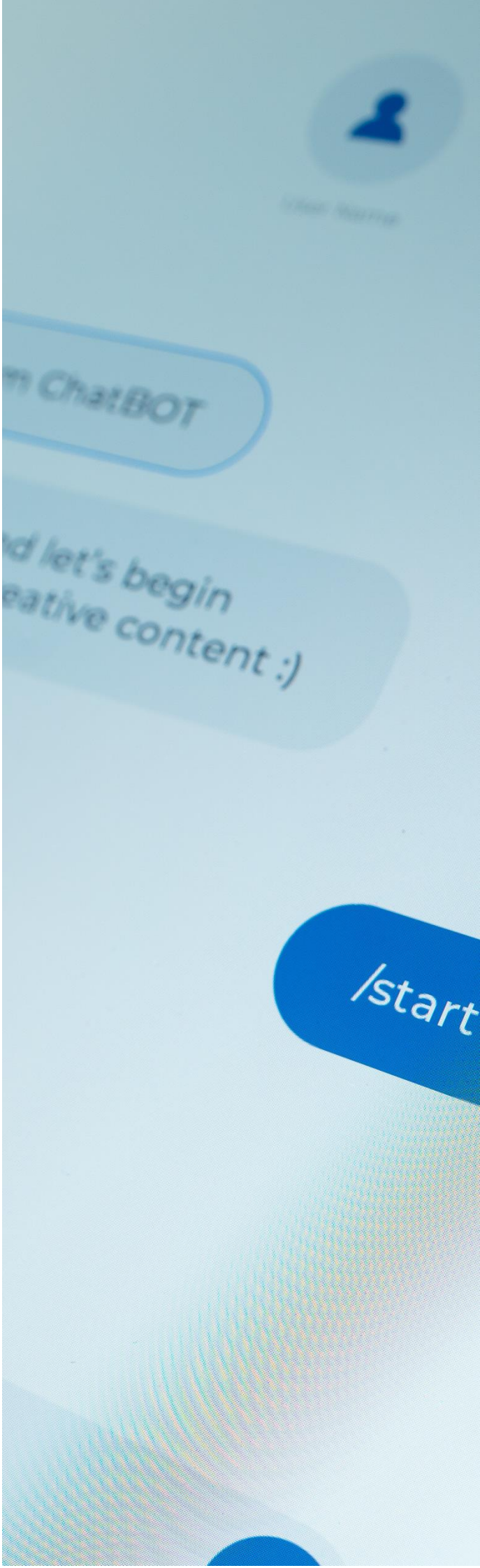
With no time to absorb that lesson, in April 2025, two British retail giants — Marks & Spencer and Co-op — found themselves at the center of what the Cyber Monitoring Centre called a "combined cyber event." Within just a few days, the same group carried out near-identical attacks, not through sophisticated technical exploits, but via psychological manipulation. Through fake calls and forged internal emails, attackers impersonated IT department staff to trick help desk operators into resetting privileged credentials. Once inside, they accessed internal systems for logistics, inventory, and sales, causing disruptions and leaking commercial data. The impact was severe: two major targets were seriously damaged, with a domino effect that spread to suppliers and partners whose operations depended on those supply chains. Shortly afterward, the Google Threat Intelligence Group warned that the group Scattered Spider was reusing the same technique against U.S. insurers — confirming that the method had proven profitable and difficult to stop.

And just when it seemed the year couldn't deliver another bitter lesson, in August 2025, Cisco became the latest victim. This time, the attack didn't rely on software vulnerabilities, but on human persuasion. A malicious actor carried out a vishing (voice phishing) campaign, which involved multiple calls, trust-building, and a meticulously crafted script designed to convince a support representative to grant access to an external CRM.

In addition, AI systems can learn from past incidents, continuously improving their ability to recognize new threats and reduce false positives. This results in a faster and more effective incident response, as AI can prioritize alerts and recommend corrective actions.

Finally, these techniques enable the integration of multiple information sources, providing a more comprehensive view of the threat landscape and helping analysts make better-informed decisions. Taken together, these capabilities make SOCs more proactive and efficient in defending against cyberattacks.

Marlon Santiago Nivia Devia
Cybersecurity Junior Analyst



CIAM: Security and Customer Experience in the Digital Age

Article by Alicia Lara Herrera

In a world where customer experience is as important as digital security, Customer Identity and Access Management (CIAM) has become a fundamental pillar for organizations seeking to deliver personalized, secure, and efficient services.Unlike traditional Identity and Access Management (IAM), which is focused on employees and internal resources, CIAM is designed to securely manage the identities of millions of external customers, combining security, scalability, and user experience.

IAM vs CIAM: Understanding the Differences

Corporate IAM is designed to control access for employees, partners, and devices to an organization's internal resources. Its focus is on operational efficiency, regulatory compliance, and internal privilege management. CIAM, on the other hand, is oriented toward the end customer. Its priorities are usability, scalability, security, and compliance with data protection regulations (such as GDPR). In addition, it incorporates key features such as: Social login, consent management, personalized experiences and multi-channel support (web, mobile, kiosks, etc.).

The Strategic Importance of CIAM for Businesses

In an increasingly digitalized environment, where customer interaction takes place across multiple channels such as mobile applications, web portals, social networks, and call centers, effectively managing customer identity has become a key competitive advantage. Beyond being just a security layer, Customer Identity and Access Management (CIAM) positions itself as a strategic platform that directly impacts customer experience, regulatory compliance, operational efficiency, and business growth.

1. Seamless Customer Experience (CX)

Well-implemented CIAM allows users to:

- Register quickly and securely.
- Log in using social identities (Google, Apple, Facebook, etc.).
- Authenticate without passwords (passwordless).
- Manage their profile, privacy preferences, and consent through a self-service dashboard.

This translates into more seamless interactions, reduced drop-offs during registration processes, and greater customer loyalty.In today's context, where customers expect a smooth and personalized experience, CIAM is a fundamental enabler.

2. Security and Trust

The rise of digital fraud, identity theft, and data breaches has made security a critical priority.CIAM provides:

- Strong, multi-factor authentication (MFA).
- Anomaly detection and behavioral intelligence to identify unusual access attempts.
- Session management and real-time token revocation.

Protecting customer identity also means protecting the company's reputation. A security incident can lead to loss of trust, reputational damage, and regulatory penalties.

3. Regulatory Compliance

Current regulatory frameworks require strict control over:

- Explicit user consent.
- Traceability and security of personal data.

A modern CIAM includes native tools to manage consent, log audits, and enable customers to exercise their rights autonomously.

4. Reliable Data for Analysis

CIAM is the gateway to valuable insights into customer behavior: Where are they accessing from? What devices are they using? How frequently do they log in? Which channels do they prefer?

Key points of the customer journey

Throughout the customer lifecycle, CIAM plays a role in critical moments:

1) **Registration:** Integration of options such as social login, email, and SMS. Consent capture.
2) **Authentication:** Secure authentication via MFA, biometrics, or adaptive authentication.
3) **Identity Management:** Self-service for updating data and privacy preferences.
4) **Resource Access:** Authorization based on roles, attributes, or policies.
5) **Logout and revocation:** Secure mechanisms to log out and revoke tokens.

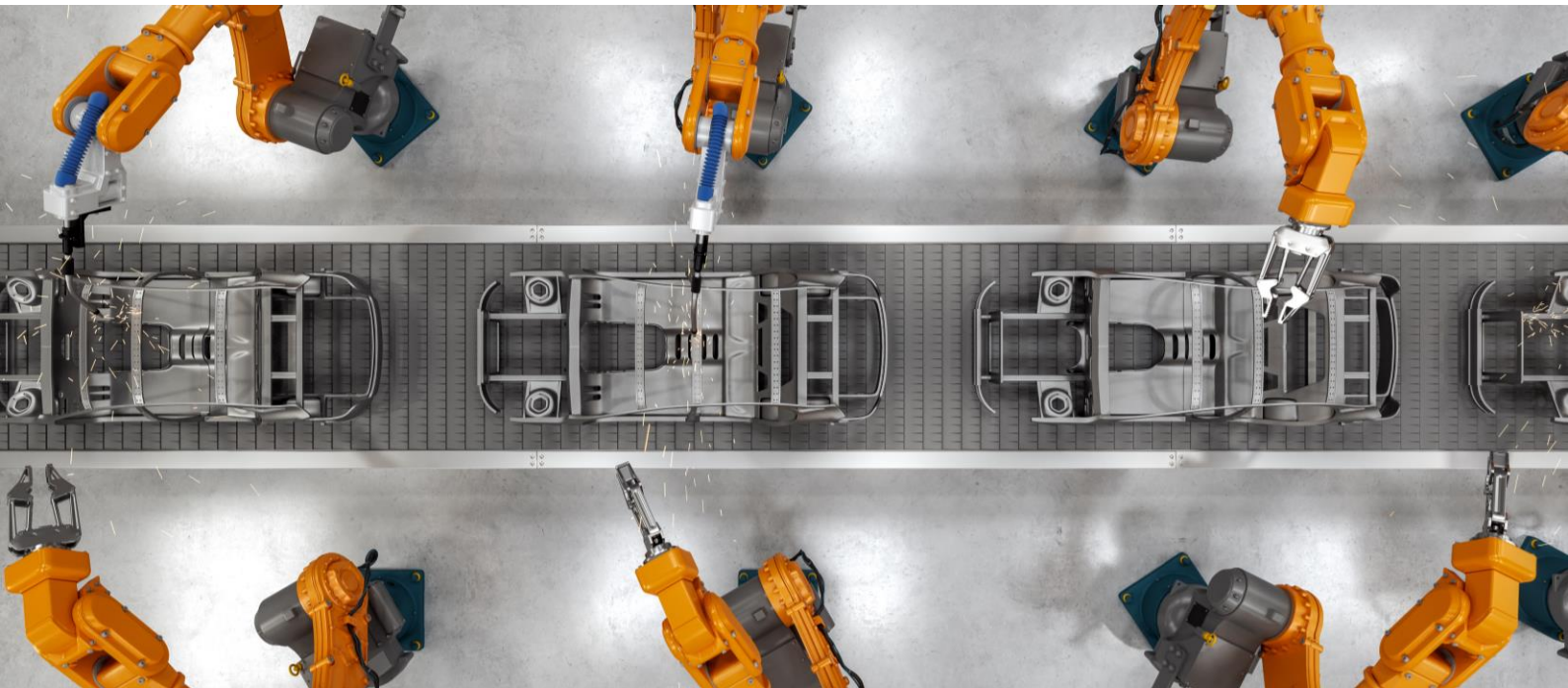
Authentication and authorization protocols

CIAM relies on open standards to ensure interoperability, security, and scalability:

- OAuth 2.0: An authorization protocol that allows applications to access resources on behalf of the user without sharing credentials.Key features include: delegated access, support for short-lived access tokens, and adoption across modern APIs and services.
- OpenID Connect (OIDC): Extends OAuth 2.0 to incorporate authentication. It allows applications to recognize the user's identity, retrieving additional information through an ID Token (JWT).
- JSON Web Token (JWT): OpenID Connect (OIDC): Extends OAuth 2.0 to incorporate authentication. It allows applications to recognize the user's identity, retrieving additional information through an ID Token (JWT).

In summary, adopting a modern CIAM not only strengthens an organization's cybersecurity but also radically enhances the customer experience.Integrating robust authentication, consent management, open standards, and a user-centered approach is essential to compete in an increasingly demanding digital environment.In this sense, CIAM is more than just technology — it is a key enabler of growth, trust, and business innovation.

Alicia Lara Herrera
Cybersecurity Expert Engineer



The world of PAM (Privileged Access Management)

Article by Mijail Muñoz Loja

In the context of cybersecurity, one of the most significant risks is the mismanagement of privileged access, since users with elevated permissions can reach critical information and sensitive systems that, if compromised, could cause irreparable damage. Privileged Access Management (PAM) is a set of policies, tools, and security practices designed to control and monitor privileged access, with the goal of minimizing the risks associated with these highly sensitive permissions. PAM plays a crucial role in protecting an organization's digital infrastructure, ensuring that privileges are granted and used appropriately.

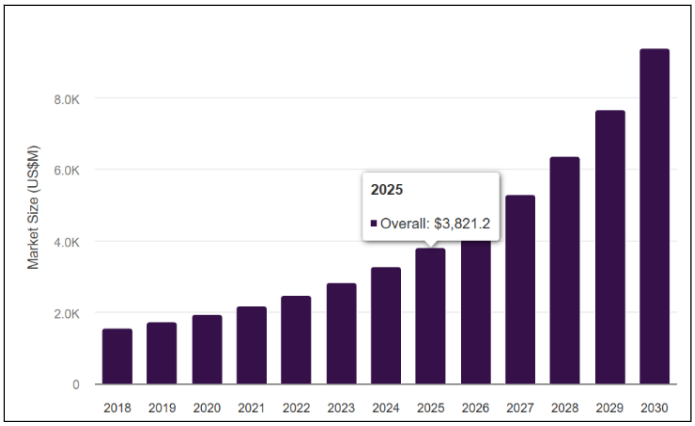
1. What is Privileged Access Management (PAM)?

PAM refers to the strategies and tools implemented to manage, secure, monitor, and audit privileged access within an organization.Privileged access grants a user, administrator, or application the ability to perform critical tasks, such as configuring systems, managing databases, or controlling networks and servers. Because these accounts have the potential to make significant changes to the IT environment, mismanagement of them can become the perfect entry point for cyberattacks.The main objective of PAM is to limit, manage, and monitor access to critical resources, ensuring that users only have the necessary privileges to perform their tasks, and that such access is continuously monitored and audited to detect any suspicious activity.(CyberArk, n.d.) (Fortinet, n.d.) (Techopedia, n.d.)

2. The size of the PAM market

i. Global Market Size and Outlook for Privileged Access Management

The global PAM market was estimated at USD 3,285.7 million in 2024 and is projected to reach USD 9,385.6 million by 2030, growing at a CAGR of 19.7% from 2025 to 2030.The rise in cybersecurity threats, including data breaches and insider attacks, is driving organizations to adopt more secure access management practices. Additionally, strict regulatory requirements and compliance mandates such as GDPR and HIPAA are further accelerating the need for secure PAM systems.(Global, n.d.)



Global Privileged Access Management (PAM) Market, 2018–2030 (US$M)

Global Privileged Access Management (PAM) Market Highlights

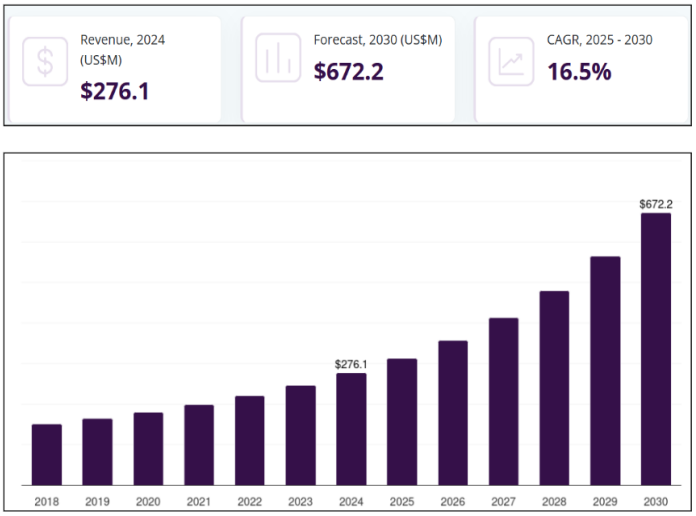
- The market is expected to grow at a CAGR of 19.7% (2025–2030), reaching 2030.
- By segment, Privileged Access Management software generated USD 2,407.2 million in revenue in 2024.
- Privileged Access Management software is the most lucrative type segment, recording the fastest growth during the forecast period.
- By region, North America was the highest revenue-generating market in 2024.
- By country, South Korea is expected to record the highest CAGR from 2025 to 2030.

Other Key Industry Trends

In revenue terms, North America accounted for 35.1% of the global PAM market in 2024. By country, the U.S. is expected to lead the global market in revenue by 2030. By country, South Korea is the fastest-growing regional market and is projected to reach USD 326.7 million by 2030.(Global, n.d.).

ii. Latin America PAM Market Size and Outlook

The Privileged Access Management market in Latin America is expected to reach USD 672.2 million by 2030.In addition, the Latin American PAM market is projected to grow at a compound annual growth rate (CAGR) of 16.5% from 2025 to 2030.(Latam, n.d.)



Latin America Privileged Access Management (PAM) Market, 2018–2030 (US$M)

Latin America Privileged Access Management (PAM) Market Highlights

- The Latin American PAM market generated USD 276.1 million in revenue in 2024.
- The market is expected to grow at a CAGR of 16.5% from 2025 to 2030.
- By segment, Privileged Access Management software was the highest revenue-generating type in 2024.
- Privileged Access Management software is also the most lucrative type segment, recording the fastest growth during the forecast period.
- By country, Brazil is expected to record the highest CAGR from 2025 to 2030.(Latam, n.d.).

3. Benefits of implementing PAM

Implementing a PAM solution in an organization provides several key security benefits::

- Reduced Risk of Unauthorized Access.
- Minimization of Potential Damage in Case of Compromise.
- Regulatory Compliance.
- Improved Visibility and Control over administrator activities.
- Automation of Account Management Processes.

4. Conclusions

Privileged Access Management (PAM) is one of the cornerstones of any modern cybersecurity strategy.Given the large number of attacks targeting privileged accounts, proper implementation significantly reduces risks and ensures the protection of an organization’s critical infrastructure.With growing threats and an increasingly complex digital environment, implementing PAM is not just an option — it is a necessity to protect the most valuable assets of any organization.

Mijail Muñoz Loja
Cybersecurity Lead Engineer

Quantum batteries

Quantum Space by María Gutiérrez

The energy transition depends on one essential element: batteries. From mobile phones to electric vehicles and smart grids, efficient and secure energy storage is a key challenge. However, understanding and improving batteries requires venturing into a field where classical physics (the world of electrons and chemical interactions) begins to fall short, while quantum computing emerges as a transformative tool.

The limit of classical simulation

Today, researchers use computational chemistry and molecular dynamics to predict the behavior of battery materials. These methods allow, for example, the estimation of how a lithium ion moves through an electrolyte or how a molecule reacts in the cathode.But as complexity increases — as in the case of the formation of the so-called solid–electrolyte interphase (SEI), which determines a battery's lifespan — classical algorithms become prohibitively expensive in time and cost. The problem is intrinsic: accurately simulating the electronic states of a system grows exponentially with the number of particles.

The Quantum leap: The dicke battery

Quantum computing promises to overcome this wall. These computers can directly tackle problems that classical systems can only approximate.Specifically for the case of batteries — and due to its experimental feasibility — the NTT DATA team has proposed a research project around the Dicke battery, which within quantum thermodynamics and quantum energy storage technology, is considered one of the most promising designs for quantum batteries.

It is based on the model proposed in 1954 by Robert Dicke, which describes how a set of atoms or quantum emitters (such as qubits, ions, or molecules) interact collectively with an electromagnetic field. Instead of behaving independently, the atoms couple collectively to the same radiation mode. This coupling can generate phenomena such as superradiance, where all atoms discharge their energy synchronously and much faster than they would individually.Applied to batteries, the idea is to charge and discharge energy collectively and ultra-fast at the quantum level.

In the NTT DATA research project, reinforcement learning (RL) is used to optimize the charging process of a Dicke battery, focusing on designing the policy function algorithm of an RL agent, supported by Quantum Approximate Optimization Algorithms (QAOA).The goal is to test whether extractable energy (ergotropy) and quantum mechanical energy fluctuations (charging precision) can be improved compared to standard charging strategies.Additionally, the study includes an analysis of the value map based on the strategies used, comparing them to the "Ground Truth". This aims to quantify the impact at the business level and determine the economic relevance of such strategies.

What benefits does it offer?

These remain small-scale lab prototypes (at most, dozens of qubits). There is no operational Dicke battery yet in the classical sense (storing and retrieving electrical energy for devices).What has been demonstrated is the physical feasibility of collective charging, which forms the basis of its potential.

Rather than replacing conventional chemical batteries (lithium, sodium, etc.), quantum batteries are expected to have applications in: Nanodevices, sensors and quantum technologies.

Here, ultra-fast recharging and quantum efficiency could make a decisive difference.

Broken Identity: A Call to Action in the Age of AI

Trends by Jordy Javier Ruiz Sánchez

I've spent years working on the frontlines of digital security, and I've witnessed an uncomfortable truth: the way we conceive identity is fundamentally broken.For decades, we clung to the idea of the username and password as if they were an impenetrable fortress. Today, that fortress is made of sand, and the tide of Artificial Intelligence (AI) is rising at a speed that forces us to act.

AI is not just another tool in the technological arsenal; it is the agent of change redefining the rules of the game. It has become a duality we must learn to live with: on one hand, it is the greatest threat identity management has ever faced, and on the other, it is our most powerful defense.This is not just another technical analysis, but a call to action, grounded in the Cloud Security Alliance's guidance on Identity Management in Agentic AI as well as independent research. It's time to stop talking about "doors" and start talking about "trust."

When "Being" and "Doing" Are no longer enough

At its core, identity management has always tried to answer two simple questions: "Who are you?" (authentication)"What are you allowed to do?" (authorization).

I often use simple analogies to explain this: identity is like entering the building where you work. You show your badge to the guard, who checks your photo and your name on the list. That's authentication. Once inside, your card only gives you access to your floor and parking lot, but not to the CEO's office or other departments. That's authorization. This model served us for a time; however, AI has made it obsolete. The challenge is no longer verifying a static identity, but understanding a dynamic context and answering much deeper questions: Under what chain of delegation is this AI agent acting? What permissions does it need for this specific task — and only for the next five minutes? How can I cryptographically trust that it has not been impersonated?

The AI Paradox: Both Arsonist and Firefighter

AI has now placed incredibly powerful tools in the hands of both attackers and defenders. From my perspective, it's a technological arms race in which we simply cannot afford to fall behind.

The Threat: The industrialization of deception

Generative AI has democratized fraud; phishing emails full of typos have evolved into flawlessly written, personalized messages, crafted through prompt engineering, making them indistinguishable from real communication.Then come the notorious deepfakes and synthetic identities. Processes once considered safe — such as Know Your Customer (KYC) verification — have become a minefield. An attacker no longer needs to steal a credential; they can fabricate a biometrically perfect identity capable of fooling our systems..

The Defense: Toward Adaptive Trust

Fortunately, the same AI also gives us the solution. The old dream of "preventing the breach" is dead. We must assume the attacker is already inside and focus our efforts on detecting and responding quickly.This is where Identity Threat Detection and Response (ITDR) comes in — a discipline that uses AI to learn how each identity (human or not) behaves and detect any anomaly in real time.

Imagine a developer who always works from Madrid, 9 to 5. Suddenly, their account tries to access a code repository from a server in Eastern Europe at 3 a.m. The system doesn't block it blindly. Instead, it triggers adaptive authentication: requiring a second factor that can't be faked, such as a physical FIDO2 key.It's not about building taller walls, but about having an intelligent immune system.

The New Workforce: Governing Non-Human identities

If you ask me what the biggest blind spot in today's security is, my answer is clear: we treat machines as second-class citizens.

On most companies, the number of APIs, microservices, containers, and AI agents already far exceeds the number of human employees. They are our new digital workforce, and the biggest strategic mistake is trying to manage them with yesterday's tools.

These identities don't use passwords. They operate with tokens, certificates, and API keys. The challenge is to manage their lifecycle at machine speed, not human speed. Embedding a secret key in application code is, bluntly, negligence.

The solution is to abandon static, long-lived credentials in favor of ephemeral, short-lived ones. An application should be able to prove its identity to obtain a valid token for just a few minutes, for a specific task — and then disappear.

As the Cloud Security Alliance rightly points out, traditional protocols are insufficient for the dynamic nature of AI. The frontier now lies in Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), which allow an agent to cryptographically prove who it is, what it can do, and who granted that authority. We are building an economy of trust for machines.

A lifecycle for every identity: Principles for action

A modern IAM approach must be relentless at every stage of the lifecycle, for both humans and machines.

- Provisioning (Onboarding): The first step is an inventory. Assign a human owner to every non-human identity to eliminate "orphan accounts." For employees, require phishing-resistant MFA such as Passkeys (FIDO2) from day one. For now, it's the most effective measure you can adopt.
- During Life (Management – Modification – Change): Governance must be continuous. Periodic access reviews, assisted by AI that recommends removing unused permissions (role engineering), are critical to maintaining the principle of least privilege.
- Deprovisioning (Offboarding): This phase is critical. When an employee leaves or an application is retired, their access must be revoked instantly and completely. Orphaned credentials are backdoors waiting to be discovered. We need systems capable of executing a global, immediate revocation of all active sessions for a compromised identity.

Conclusion: Identity is the new perimeter

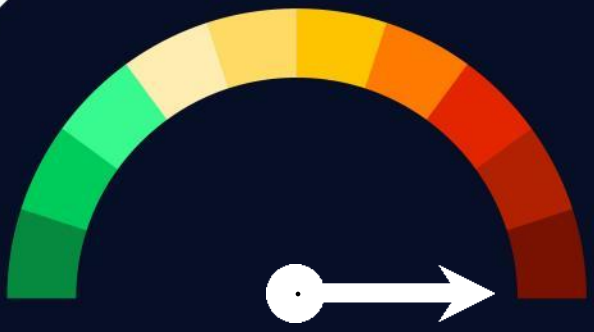
We have moved beyond the era when identity management was seen as an IT support function. Today, it is the strategic core that either enables or hinders secure innovation with AI. We no longer just manage people accessing systems; we govern a living ecosystem of humans, machines, and autonomous agents.
Adopting these strategies is not optional — it is imperative. In a world where identity can be fabricated, the only defense is trust that is never assumed and always verified. Zero Trust is not just an architecture; it is the philosophy that will allow us to navigate this new frontier. And AI, with all its risks, is the most viable option we have to do it at scale.

Jordy Javier Ruiz Sánchez
Cybersecurity Analyst

Vulnerabilities

Critical Vulnerability in SAP NetWeaver

Date: September 8, 2025
CVE: CVE-2025-42944



CVSS: 10

CRITICAL

Description

The CVE-2025-42944 vulnerability represents a critical threat for environments running SAP NetWeaver, as it allows remote command execution without authentication.

This flaw is rooted in insecure deserialization (CWE-502) due to the vulnerable RMI-P4 module, which acts as an entry point for attackers to manipulate serialized objects and execute arbitrary code on the server.

The lack of prior authentication significantly amplifies the risk, enabling external malicious actors to interact directly with the vulnerable system.

Solution

SAP's recommendations are as follows:

- Immediate update to the latest available version.
- Implementation of additional access controls for the tool.

Affected products

This critical vulnerability affects:

- SAP NetWeaver ServerCore version 7.50

References

- nvd.nist.gov
- zeropath.com

Vulnerabilities

WhatsApp Vulnerability Exploited on iOS and macOS

Data: August 29, 2025
CVE: CVE-2025-55177

CVSS: 5.4

MEDIA

Description

The CVE-2025-55177 vulnerability in WhatsApp, classified as a zero-click exploit, affects iOS, iPadOS, and macOS.

It is caused by insufficient authorization in device synchronization, allowing attackers to execute code or install spyware simply by sending a crafted message.

The flaw exploits the way WhatsApp processes objects and multimedia files, leading to memory corruption.

Although detected in only a few cases, it highlights the high risk of invisible attacks and exploit chains for espionage.

Solution

It is recommended to immediately apply the official patches from WhatsApp and Apple:

- iOS and iPadOS: Version 2.25.21.73 or later
- macOS: Version 2.25.21.78 or later

Affected Products

The vulnerable versions are as follows:

- iOS: from 2.22.25.2 up to 2.25.21.73
- macOS: up to 2.25.21.78

References

- incibe.es
- nvd.nist.gov

TLP:WHITE

Citrix Fixes Vulnerabilities in NetScaler ADC and Gateway

Date: August 26, 2025
CVE: CVE-2025-7775 and 2 more

Critical

Description

Recently, several vulnerabilities have been detected in Citrix NetScaler:

CVE-2025-7775 (Critical): A memory overflow vulnerability that could allow remote code execution or cause a denial of service (DoS). This occurs when NetScaler is configured as a Gateway or AAA virtual server, linked with IPv6 services or an HDX-type CR virtual server.

CVE-2025-7776 (High severity): Also a memory overflow, which may cause erroneous behavior or denial of service. It requires NetScaler to be configured as a Gateway with a linked PCoIP profile.

CVE-2025-8424: An improper access control vulnerability in the management interface, which could allow unauthorized actions if the attacker has access to NSIP, cluster management IP, local GSLB site IP, or SNIP with administrative privileges.

Affected products

- NetScaler ADC and NetScaler Gateway: Versions earlier than 13.1-59.22 and earlier than 14.1-47.48.
- NetScaler ADC FIPS/NDcPP: Versions earlier than 13.1-37.241 and earlier than 12.1-55.330, respectively

Solution

Cloud Software Group recommends that affected customers install the latest available versions

References

- nvd.nist.gov
- support.citrix.com

Google Fixes a Vulnerability in Android Runtime

Date: August 29, 2025
CVE: CVE-2025-48543

High

Description

Google has patched the privilege escalation vulnerability CVE-2025-48543.This vulnerability exploits a use-after-free flaw in Android Runtime to escape the Chrome sandbox and compromise the system_server process on Android devices.

It can then lead to local privilege escalation without requiring any user interaction.

Successful exploitation of CVE-2025-48543 could allow attackers to gain elevated privileges on the Android device.

Affected products

Some of the affected products include:

- Google Android 16
- Google Android 15
- Google Android 14
- Google Android 13

Solution

Google has strengthened the security of Android Runtime (ART), distributing the patch via Google Play to immediately protect devices with GMS, even before operating system updates are rolled out.

References

- nvd.nist.go
- source.android.com

Events

Cyber Security World Asia
8 – 9 October

On October 8–9, 2025, at the Marina Bay Sands Expo & Convention Centre in Singapore, this key cybersecurity event will take place. The event will bring together leaders and experts to address topics such as Zero Trust, AI applied to cyber defense, identity management, cloud security, network protection, quantum cryptography, and incident response, establishing itself as the most relevant gathering in the region within Tech Week Singapore.

Link

Forum InCyber Canadá
14 – 15 October

On October 14–15, 2025, at the Palais des Congrès in Montreal, Canada, this international forum on cybersecurity and digital trust will be held.The event will cover topics such as emerging threats, ransomware, cloud security, artificial intelligence, quantum cryptography, critical infrastructure protection, and smart mobility, establishing itself as the leading meeting point in North America for industry leaders and experts.

Link

InfoSec World 2025
27 - 29 October

From October 27–29, 2025, at Disney's Coronado Springs Resort in Florida, this leading cybersecurity conference will take place. It will address topics such as threat intelligence, cloud security, identity management, Zero Trust, resilience, incident response, and supply chain risks, establishing itself as a key space for professionals and industry leaders.

Link

Resources

➢ EU Cybersecurity Index 2024

The EU Cybersecurity Index, published by ENISA, assesses the cybersecurity posture of EU Member States, measuring key areas such as policies, technical capabilities, market and industry, and operations.The report identifies strengths and gaps, highlighting challenges in the adoption of AI, CSIRT certification, cybersecurity investments, and access to innovation funds.It serves as a reference tool to improve digital resilience and harmonize strategies at the European level.

Link

➢ Technical Implementation Guide for NIS2

ENISA has published this guide to support digital infrastructure entities, ICT service providers, and digital platforms in the implementation of the NIS2 Directive.It provides practical guidance on:Risk managementSecurity policiesIncident handlingBusiness continuitySupply chain securitySecure developmentThe guide aims to facilitate the adoption of cybersecurity measures and strengthen digital resilience in critical sectors.

Link

➢ Cyber Threat Landscape Methodology

ENISA has updated its methodology for developing the Cyber Threat Landscape, with the goal of providing a more practical and structured approach to the production of horizontal, thematic, and sectoral reports.The methodology defines key processes, stakeholders, tools, and content elements, promoting transparency and consistency in the analysis of cyber threats across Europe.

Link

Subscribe to RADAR

Powered by the cybersecurity NTT DATA team

es.nttdata.com