No. 116 | July 2026

NTT DATA

# Radar

## The cybersecurity magazine

# Identity as the New Perimeter: Trust begins with every identity

By Hans Vigil Navas

For years, cybersecurity was built around a simple idea: protecting the perimeter. There was an internal network, known users, controlled systems and a relatively clear boundary between what was trusted and what lay outside. Firewalls, network segments and access controls appeared sufficient to protect what the organization considered critical. **But that boundary is no longer clear.**

Cloud computing, hybrid working, APIs, third parties, industrial automation and artificial intelligence have turned access into a continuous exchange between people, applications, machines and systems operating both inside and outside the organization**. Today, risk no longer arises only when someone attempts to cross a boundary.** In many cases, the risk is already inside, using a valid credential, an active token, a forgotten certificate or a service account with more privileges than necessary.

**In this new landscape, identity has become the new perimeter.** This is not merely a fashionable phrase. It is an operational reality. **Every identity represents a potential point of access, a trust decision and, at the same time, a possible gateway to the organization's critical assets**. Some identities belong to people. Others belong to applications, services, devices, automated processes or agents capable of performing tasks on behalf of someone else. Many of them do not appear in traditional inventories and are not reviewed with the same level of scrutiny as a human user.

The challenge is that digital trust has become more difficult to observe. An organization may have strong monitoring, encryption, incident response and network protection capabilities; but if it does not know who is accessing what, with which privileges, from where, for how long and on whose behalf, actions are being taken, its security posture remains incomplete. **Identity is no longer simply an administrative IT component; it has become a critical capability for governance, resilience and business continuity.**
**In banking, a compromised identity can lead to fraud. In insurance, it can result in the exposure of sensitive information. In mining, it can cause operational disruption. In manufacturing and industry, it can have a direct operational impact. In every case, the root cause is often the same: poorly governed trust.**

For the financial services and insurance sectors, this reality is particularly significant. Identity sits at the heart of fraud prevention, customer data protection, privileged access management, digital channel security, API usage and third-party relationships. In these environments, implementing controls is not enough; organizations must be able to demonstrate that those controls are effective, regularly reviewed, capable of generating evidence and sufficient to satisfy auditors, regulators and boards.

In mining and industrial environments, the impact can be even more tangible. A compromised identity does not always result in a data breach; it can also enable unauthorized remote access, shared accounts, persistent supplier credentials, engineering workstations or systems that support critical operations. In these sectors, identity does not only protect information. It also safeguards availability, operational continuity, physical safety and productive capacity.

This is why Identity as the New Perimeter is not simply about adopting a new IAM tool. It is about rethinking how the organization understands trust. Every access request should be explicit, verifiable, minimal, traceable and revocable. Every identity should have a defined purpose, an accountable owner, a lifecycle and associated controls. Every privilege should reflect a genuine business need. And every exception should be treated as a risk rather than an operational habit.

Leading international frameworks have been pointing in this direction from different perspectives. NIST approaches it through Zero Trust: never trust implicitly and continuously verify. ISO/IEC 27001 addresses it through risk management, access controls, third party relationships and continual improvement. OWASP highlights it through recurring weaknesses in authentication, authorization, API security and nonhuman identities. Although they start from different viewpoints, they all lead to the same conclusion: trust must be governed.

The management of nonhuman identities therefore becomes a critical priority. In many organizations, these identities already far exceed human identities in both volume and criticality. Digital certificates, secrets, tokens, automation accounts, platform integrations, cloud services, connected devices and automated processes operate in the background, supporting essential business functions. When one of these identities is compromised, an attacker does not need to breach the perimeter; they simply operate as though they already belong within it.

Adding to this landscape is a new layer of complexity: identity agents, or **ID Agents. As artificial intelligence evolves towards more autonomous models, agents are emerging that can act on behalf of a person, an application or a process.** They can consume APIs, execute tasks, make assisted decisions and operate with a degree of independence. The question is therefore no longer simply "who is accessing", but rather "on whose behalf is this agent acting, with what authority, within what limits and with what level of traceability".

**Autonomy without governance can turn identity into a blind spot.** Autonomy supported by effective controls, however, can improve efficiency without compromising security. This is the challenge facing CISOs: integrating access governance, privilege management, secrets protection, API security, third party oversight and continuous monitoring within a single risk management framework. In banking and insurance, this translates into fraud prevention, compliance, audit evidence and customer trust. In mining and industrial environments, it translates into continuity, availability and the protection of physical and digital environments. In both cases, identity ceases to be an isolated control and becomes a cross organizational pillar of defense and resilience.

**In this edition of Radar, we explore precisely this shift in mindset. Security can no longer rely on boundaries that the business has already moved beyond.** It must be built around verifiable identities, both human and nonhuman, managed throughout their entire lifecycle and aligned with standards, risk management and regulatory requirements.

The new perimeter is no longer the network; it is every identity capable of taking action. Some are human, some are machines and others will be autonomous agents. All require governance. In the age of hyperconnectivity, trust is no longer granted by default: it is verified, restricted, monitored and revoked.


**Hans Vigil Navas**
Cybersecurity Manager

# The keys to the kingdom: Identity as the primary attack vector

Cyber Chronicle by Nelson Andrés Barboza Landinez

For decades, corporate security was built on a simple premise: there was an inside and an outside. The firewall was the wall, the VPN the drawbridge, and antivirus solutions stood guard on every corner. It was a strong, predictable fortress designed for a world where threats came from outside and trusted users remained within. But that world has disappeared. Remote working opened side doors, and SaaS integrations handed the keys to dozens of external providers. Today, there is no inside. There are only identities.

According to Unit 42's 2026 Incident Response Report, 65% of initial access incidents in cyberattacks involved identity-based techniques, enabling unauthorized access, lateral movement and privilege escalation. Techniques such as phishing, stolen credentials, brute force attempts, IAM misconfigurations and insider activity continue to drive modern security breaches. In a world where significant investment is made in cyber defenses, attackers increasingly choose to walk straight through the front door. Verizon's 2025 Data Breach Investigations Report confirms this trend: 22% of breaches began with stolen credentials, representing a 34% increase compared with the previous year. They are not breaking in. They are logging in.

The rapid adoption of cloud infrastructure, SaaS platforms and accounts used by applications, services and automated processes has created a digital environment in which every integration represents a potential access path. The same Unit 42 report found that, across a sample of 680,000 cloud identities, 99% of users, roles and services had excessive permissions, including access rights that had not been used for more than 60 days.

Attackers no longer need to force their way in; they simply walk through corridors that no one has closed. Adding to this challenge is the growing threat that quantum computing poses to current encryption schemes, together with the anticipated reduction in the lifespan of TLS certificates. The clock is ticking, and the exposure surface continues to expand. CyberArk's 2025 report, based on a survey of 1,200 security leaders across organizations in the United States, the United Kingdom, Australia, France and Germany, revealed that most face significant challenges in effectively managing machine identities.

Real world incidents from 2025 illustrate this reality clearly. Marks & Spencer, the British multinational retailer, was the target of a cyberattack attributed to the group known as "Scattered Spider" in April 2025.

The company confirmed that multiple servers had been encrypted, significantly impacting its infrastructure.

The breach did not occur overnight; it was the result of a chain of events in which identity management proved to be the weakest link. During the intrusion, the threat actors gained access to an NTDS.dit file, enabling them to extract password hashes and facilitating privilege escalation across the network. Although the exact initial access vector has not been officially confirmed, multiple sources indicate that the Scattered Spider group routinely employs phishing campaigns, vishing techniques and MFA fatigue attacks to gain access to corporate accounts. The subsequent deployment of the DragonForce ransomware encryptor disrupted the continuity of multiple corporate and commercial services and resulted in unauthorized access to customer information, as confirmed by the organization.

Months later, between 8 and 18 August, another information theft campaign targeted the Salesloft sales automation platform, focusing particularly on Salesforce customer environments through the compromise of OAuth tokens associated with the Drift artificial intelligence agent. According to Cloudflare, the attack path involved object enumeration, reconnaissance of the compromised environment and the extraction of information through legitimate Salesforce interfaces.

Finally, as part of a carefully executed operation, the attackers deleted scheduled jobs to conceal their activities. The threat actor, identified by the Google Threat Intelligence Group (GTIG) as UNC6395, is believed to have affected approximately 700 organizations, including financial institutions, healthcare providers, technology companies and government agencies.

Cory Michal, CSO of AppOmni, stated that many of the affected organizations are themselves software and cybersecurity companies, suggesting that the campaign may represent an initial step towards future supply chain attacks.

This was not a technical failure involving endpoints or network infrastructure. It was a failure of agent identity governance. Long lived OAuth tokens, permissive scopes and a trusted agent that no one was monitoring created the perfect conditions for compromise. Organizations trust integrations in much the same way they trust employees, yet they rarely govern them with the same rigour. Agents are identities. And identities without governance are open doors.

Just a few weeks later, Jaguar Land Rover disclosed that it had suffered a devastating cyberattack on 31 August 2025, costing the company £196 million. In addition, according to The Cyber Monitoring Centre, the incident generated an estimated £1.9 billion impact on the United Kingdom economy due to the complete shutdown of global manufacturing operations for five weeks. The attack, attributed to the group Scattered LAPSUS$ Hunters, whose philosophy is "log in, not hack in", was enabled through the theft of credentials by an infostealer, a type of malware designed to extract passwords, session cookies and other sensitive information from compromised devices. In this case, the affected credentials belonged to a third party with access to JLR's Jira environment.

On 1 September, JLR's IT team detected an intrusion within its network and took the drastic step of shutting down all systems in an effort to contain the damage. As proof of access, the attackers published screenshots of internal systems on Telegram, exposing access to domains such as jlrint.com. Subsequent investigations, however, revealed that the intrusion was not the result of a zero-day vulnerability. Instead, it stemmed from a combination of social engineering, credential abuse, inadequate detection capabilities and weak segmentation between the corporate network and production systems.

Cases such as these do not occur in isolation. Artificial intelligence is playing a decisive role in accelerating the speed and scale of identity theft campaigns. Analysis of 32 million phishing emails documented in the Darktrace Annual Threat Report 2026 revealed a clear trend: phishing attacks are becoming increasingly sophisticated and potentially more effective, particularly when those emails reach highly privileged users.

This is hardly surprising when considering that 70% of these emails successfully passed DMARC authentication checks, enabling them to evade monitoring and detection controls.

Nathaniel Jones, Vice President of Security and AI Strategy at Darktrace, notes: "The traditional security perimeter was built for a world where attackers had to break in." While threat actors have historically relied on technical exploits, advances in artificial intelligence have enabled them to operate with greater precision, adopting techniques such as vishing and deepfakes and targeting identities as their primary initial access vector rather than the infrastructure itself.

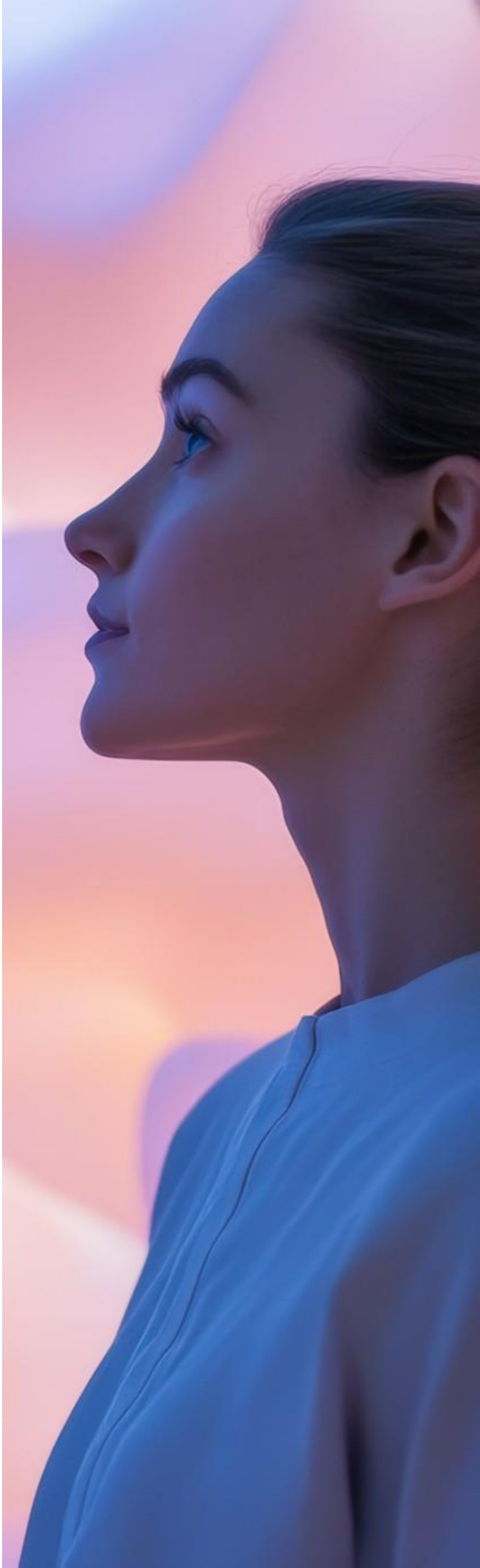
Effective mitigations such as the deployment of phishing resistant MFA, strong identity governance, the effective implementation and enforcement of the principle of least privilege, and AI enabled monitoring solutions capable of detecting anomalous behavior are fundamental components of a modern defense strategy. Examples include tokens being created for the first time from new geographic regions, unusual API consumption patterns and other indicators of suspicious activity.

A robust incident response capability is also essential, supported by playbooks that assume intruders may already be present within the environment. Equally important are controls to prevent password reuse and processes to identify exposed identities whose credentials are already circulating online. These practices are critical in a world where identities have become central to technological progress.

While it is true that passwords have never been inherently secure, the evidence now speaks for itself. In this new era shaped by artificial intelligence, passwords as a standalone authentication mechanism have proven insufficient against modern threats. The time has come to adopt stronger authentication methods. The confidentiality, integrity and availability of systems cannot depend solely on walls designed to withstand external attacks; they also require organizations to secure the front door and maintain visibility over who has access to the inside.

Over the years, millions have been invested in strengthening digital defenses, driven by the belief that danger would come from outside. Yet some of the most catastrophic incidents of recent months reveal a different reality: attackers no longer need to break down doors. They simply need to obtain the keys. In the era of cloud computing, intelligent agents and artificial intelligence, every user, service, token, application and machine possesses its own identity. That identity has become the new security perimeter.

**Nelson Andrés Barboza Landinez**
Cybersecurity Engineer



# Identity: The risk that has evolved alongside AI

Article by Jaime Andrés Tovar Prieto

How many AI agents are currently operating within your organization with broad access and no verifiable identity? Do you know which identity they are using? How long have they been operating under that assigned identity? In recent years, artificial intelligence has firmly established itself within the enterprise technology ecosystem and has evolved beyond standardized generative or conversational models designed to interpret context and generate responses under the constant supervision of a human operator, an approach known as Human in the Loop (HITL). The next stage in this evolution is the rise of AI agents: autonomous software components that not only interpret inputs and plan strategies but also execute tangible tasks through communication with APIs (Application Programming Interfaces), interact with databases, other agents and subagents within coordinated workflows, all with minimal or no human intervention at each individual step of the process.

Conventional AI governance has largely focused on mitigating risks associated with model outputs, assessing whether they are accurate, fair, ethical and free from bias or hallucinations, based on the assumption that a human will review the results before making a decision or taking action. However, the governance of agentic AI requires a structural and conceptual shift: risk management must move beyond outputs and focus on actions. An autonomous agent may initiate complex financial transactions, update customer records within corporate systems or apply configurations to security devices protecting critical infrastructure without waiting for any interactive human approval. Consequently, the absence of strict, dynamic runtime controls can lead to unintended privilege escalation, large scale data exposure and systemic disruptions that threaten business continuity.

## The New Risk Frontier: From Response to Action

These developments have raised significant concerns across the industry. Gartner projects that by 2027, 40% of organizations will be forced to scale back or completely dismantle their autonomous agent deployments due to weaknesses in governance models. Organizations that fail to distinguish between an agent's technical capability to perform an action and the legitimate scope of the permissions granted to it face an imminent and unsustainable operational risk.

Against this backdrop, it is imperative to examine the new frontier of risk, where Identity is emerging as the critical component still evolving within the broader context of artificial intelligence.

Okta notes in its article "What Is AI Agent Identity? Securing Autonomous Systems" that, on average, an organization manages 45 machine identities, or NHIs (Non Human Identities), for every human user. However, while traditional NHIs operate within predictable parameters and predefined scripts without awareness of their environment, AI agents are capable of reasoning, adapting their strategies iteratively according to context, retaining information to improve decision making and executing autonomous actions with real world impact on the environments in which they operate. Applying today's rigid identity models to agentic AI can create significant security vulnerabilities.

## Standard IAM vs. Agentic Identity: Fundamental Differences

The structural differences between conventional identity management and the unique requirements of agentic identity become evident across three critical dimensions that fundamentally reshape the identity lifecycle:

- **Lifespan:** A human user identity may remain active for days, months or years and requires interactive validation through biometrics, passwords, tokens or multifactor authentication mechanisms. Agents, by contrast, operate continuously and without constant human intervention; their identities may be ephemeral, existing only for the few seconds required to complete a transaction.

- **Delegated Authorization:** Human accounts act on their own behalf. AI agents, however, operate on behalf of (OBO, On Behalf Of) a human, a system or a service. This requires cryptographically robust delegation chains and token exchange mechanisms that preserve accountability and forensic traceability, maintaining an inseparable link to the original delegating entity.

- **Access Control:** Static role assignment is incapable of keeping pace with an agent that chains together complex tasks and makes thousands of access decisions per minute. Agents require continuous evaluation of context, environmental risk and task specific attributes, enforced through Policy as Code.

## Risk Vectors in Ungoverned AI Environments

When the pace of deployment outstrips the maturity of AI governance, a highly likely scenario in today's environment, organizations become exposed to structural risks arising from unmanaged NHIs. The principal risk vectors include:

- **Ungoverned Persistent Access:** Agents operating with permanent credentials or long lived access tokens become high value targets. If a model is compromised, for example through a malicious prompt injection attack, the attacker inherits all of the agent's persistent access and can operate freely within the corporate environment.

- **Privilege Escalation and Authority Drift (Privilege Drift):** In dynamic environments, an agent may invoke tools or assume roles that accumulate permissions never explicitly approved by a security administrator. This drift often manifests as a gradual expansion of authority over time rather than as an abrupt or immediately visible change in the outcomes produced.

- **Lack of Attribution and Audit Evasion:** When an agent modifies a database using a generic or shared service account, the action loses its delegation context. The inability to algorithmically distinguish a human action from a synthetic one eliminates accountability and undermines compliance with stringent regulatory requirements.

## Governance Framework for Agentic Identities

The first step towards effective governance is the establishment of a risk measurement framework for AI agents.

It is essential to avoid implementing a uniform security model for all agents. Such an approach can lead either to excessive operational restrictions that hinder productivity or to increased risk exposure through underestimating an agent's actual capabilities. Security policies must be proportionate to the context and the specific capabilities of each agentic entity.

Traditional IAM was designed to manage human identities with predictable lifecycles and interactive authentication. In agentic AI environments, this model is structurally inadequate: agents do not possess credentials in the conventional sense, operate through delegated authority and function at speeds that exceed any human review process. To bridge this gap, the architecture requires a higher level abstraction layer known as an Identity Fabric. Advanced enterprise platforms act as this Identity Fabric, connecting applications, identity providers (IdPs) and hybrid and multicloud environments without requiring existing applications to be rewritten.

The orchestration provided by an Identity Fabric goes beyond simply connecting systems; it centralizes identity management across six operational dimensions:

- **Authentication:** Provide modern, adaptive sign in services that move beyond legacy protocols with known vulnerabilities.

- **Access Control:** Enforce granular and consistent policies at the individual, group and machine level through a single unified control plane.

- **Authorization:** Establish precise rules that determine which specific functions an agent may perform and under exactly which environmental conditions.

- **Attributes:** Provide dynamic user data from any IdP at runtime to support contextualized and personalized security decisions.

- **Administration:** Deliver centralized and visual policy management across the entire ecosystem.

- **Auditing:** Provide deep observability into actual activity compared with granted permissions, enabling continuous demonstration of regulatory compliance.

## Towards an Authentication Framework for Agents: SPIFFE

Traditional authentication mechanisms used in web environments, including JWTs, OAuth, static credentials and API keys, are insufficient for managing authentication within agentic AI ecosystems. To address this gap, a key architectural component has emerged: **SPIFFE** (Secure Production Identity Framework for Everyone).

**SPIFFE** specifically addresses a layered security risk often described as the “Russian doll” effect. If an attacker compromises a subagent deep within a processing chain through prompt injection, they may inherit the extensive privileges granted to the primary agent, potentially causing catastrophic damage through a technique known as “Agent Session Smuggling”.

**SPIFFE** provides a standardized mechanism for issuing cryptographically verifiable identities to software based on its provenance and execution context, without requiring human intervention for credential provisioning. Its core element is the **SVID** (SPIFFE Verifiable Identity Document), an ephemeral credential that is cryptographically signed as an identity assertion.

**SVIDs** are managed through **SPIRE** (SPIFFE Runtime Environment), which ensures their automatic rotation throughout the entire lifecycle of an agent. This mechanism effectively eliminates the persistence vector commonly exploited by attackers and embodies a pure Zero Trust approach.

## Conclusion

Identity in agentic AI environments is not a minor technical challenge; it is the central pillar upon which an organization's operational trust is either built or undermined. As long as agents continue to proliferate without verifiable identities, governed lifecycles and cryptographic traceability, every autonomous automation represents an open risk vector. The path towards a mature AI security posture requires organizations to adopt Zero Trust principles not as theoretical static guidelines, but as executable architecture: ephemeral identities, provisioned Just in Time, operating with least privilege and supported by continuous auditability.

**Jaime Andrés Tovar Prieto**
Cybersecurity Architect

# The Invisible Risk: How nonhuman identities are redefining cybersecurity

Article by César Vega Calderón

Non-Human Identities are currently one of the fastest growing risk vectors. Their effective management will be critical to the cyber resilience of organizations in the era of cloud computing, automation, digital transformation and artificial intelligence.

The accelerated adoption of cloud services, automation, DevOps and artificial intelligence has driven exponential growth in Non-Human Identities (NHIs). These identities, used by applications, APIs, service accounts, containers, IoT devices and AI agents, are essential to modern organizational operations, but they also represent one of the fastest growing attack surfaces.

## The Explosion of Non-Human Identities

For years, Identity and Access Management (IAM) strategies focused primarily on human users. Today, that reality has changed. Modern organizations operate thousands of identities associated with automated systems that must continuously authenticate in order to access data, services and critical resources.

Industry research shows that Non-Human Identities significantly outnumber human identities, with an average ratio of 50 to 1 across many enterprise environments. Okta, one of the leading Identity and Access Management providers, highlights that modern organizations manage entire identity ecosystems distributed across users, applications and workloads. This expansion increases both operational complexity and the attack surface.

## What Are Non-Human Identities?

They are digital credentials assigned to machines, applications and automated processes that typically operate autonomously and continuously. They use certificates, API keys, tokens and cryptographic secrets rather than passwords, biometrics or mobile device based multifactor authentication (MFA) to authenticate and interact with other systems.

## Where Are They Used?

They are primarily used in automated cloud workloads, where roles enable secure service to service access; CI/CD pipelines that automate deployments; communication between microservices using OAuth and certificates; API driven SaaS integrations; connected IoT devices; advanced analytics platforms; and artificial intelligence agents that automatically consume and process data. Across all of these use cases, credentials are required to operate, making them a new and increasingly significant source of cybersecurity risk.

## The Invisible and Expanding Risk

Every service account, token or certificate represents a potential entry point into an organization. Because Non-Human Identities often operate autonomously, with elevated privileges and limited oversight, the compromise of a privileged identity can enable attackers to access sensitive data, escalate privileges and move laterally throughout the organization's technology environment.

## Five Critical Risk Factors

- Excessive Privileges
- Long Lived Static Credentials
- Lack of Inventory and Limited Visibility into Existing Identities
- Poor Secrets Management
- Insufficient Monitoring of Automated Behaviour

## Artificial Intelligence Accelerates the Challenge

Agentic AI introduces new autonomous identities capable of consuming APIs, querying data and executing actions. Every agent requires authentication, authorization and continuous monitoring.

## Towards an NHIM Strategy

Non-Human Identity Management (NHIM) enables organizations to discover, inventory, govern, protect and monitor these identities throughout their entire lifecycle. Key capabilities include automated discovery, least privilege, secrets rotation, continuous monitoring, anomaly detection and unified governance.

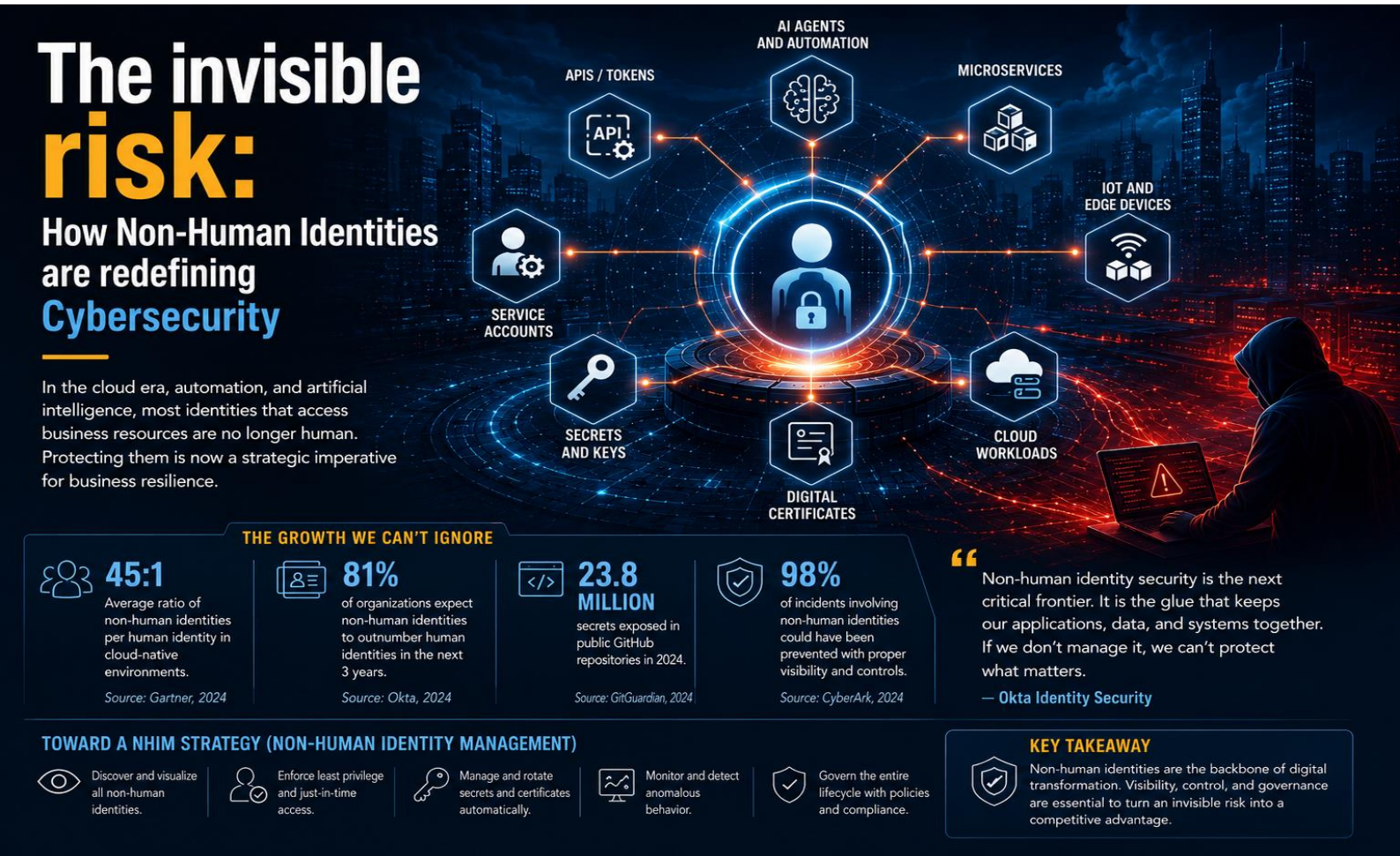
## Recommendations for CISOs

Implement automated discovery of Non-Human Identities, strictly enforce the principle of least privilege, conduct regular privilege reviews, adopt Zero Trust models, automate secrets management, monitor anomalous behaviour and unify the management of human and nonhuman identities, ensuring that every Non-Human Identity has a clearly assigned owner.

## Conclusion

Non-Human Identities are no longer solely a technical concern. They have become a strategic component of modern cyber resilience, and organizations that govern them effectively will be better positioned to reduce the risks associated with cloud computing, automation, digital transformation and artificial intelligence, while strengthening their cybersecurity posture to protect their most critical digital assets.

**César Vega Calderón**
Cybersecurity Manager



# Security without a perimeter: The rise of identity as the core of protection

Trends by Whendy Oré Crisostomo

The traditional perimeter-based cybersecurity model is now a thing of the past. In cloud based, distributed and highly dynamic environments, identity has emerged as the new centre of control. This shift affects not only users, but also systems, applications and automated processes. Today, protection means continuously verifying who, or what, is accessing resources, even in everyday scenarios such as connecting from home, using a corporate application or automating processes between systems.

## Identity as the Core of Control

Security no longer depends on being "inside" or "outside" the network. Every access request must be evaluated based on identity, device, context and risk level. This approach, aligned with Zero Trust principles, eliminates implicit trust and requires continuous verification. In this new model, identity becomes the true point of defense. Managing it accurately and dynamically is now the foundation of any modern security strategy.

## The Growth of Machine Identities

Beyond human users, the digital ecosystem is increasingly driven by interactions between systems. APIs, microservices, containers and automated processes rely on **machine identities** for authentication. These identities, including certificates, tokens and keys, enable applications, services and automated workflows to communicate with one another without human intervention, for example when one application retrieves data from another or executes scheduled tasks. However, their numbers are growing exponentially and they often lack adequate visibility and control, making them a critical source of risk within organizations.

## Machine Identity Management: Control and Visibility

To mitigate these risks, organizations need to know exactly which identities exist, where they are being used and for how long. This is where Machine Identity Management (MIM) becomes essential. Its objective is to establish comprehensive control through:

- Continuous Inventory and Discovery
- Credential Automation
- Enforcement of Least Privilege
- Continuous Monitoring
- A mature MIM strategy helps reduce the attack surface and strengthen organizational resilience.

A mature MIM strategy helps reduce the attack surface and strengthen organizational resilience.

## Why Does It Matter Now?

This shift towards identity centric security is not accidental. It reflects the natural evolution of digital environments, where users no longer work from a single location and applications no longer reside in one place. Today, it is common for organizations to rely on multiple cloud environments, external applications and personal devices, increasing the number of access points while reducing the effectiveness of traditional controls. In this context, relying solely on the network is no longer sufficient.

At the same time, attackers have adapted their strategies and increasingly seek to compromise credentials rather than infrastructure. This makes protecting both human and machine identities the decisive factor in preventing unauthorized access. Failing to address this challenge can lead to difficult to detect unauthorized access, exposure of critical data and a significant increase in operational risk. This shift reflects a clear trend: the transition from an infrastructure based security model to one centred on identity management.

## Identity Agents (ID Agents): Security at the Point of Execution

In distributed environments, **ID Agents** bring security directly to the point where execution takes place. These components enable:

- Local Access Validation
- Credential Protection Without Exposure
- Real Time Policy Enforcement
- Security Telemetry Generation
- Their implementation reinforces the concept of identity as the perimeter, embedding security into every layer of the digital environment.
- In modern environments, these agents ensure that security does not depend on a single central control point, but instead accompanies every system and application wherever it operates.

## From Control to Dynamic Trust

More than a technological evolution, this shift represents a transformation in how organizations understand trust. It is no longer about assuming that everything inside the organization is secure, but about continuously validating every identity, every access request and every interaction.

This approach not only strengthens security, but also enables organizations to operate with greater flexibility in increasingly distributed environments.

## Conclusion

The traditional perimeter has disappeared. In its place, identity has emerged as the core of cybersecurity. Understanding this shift is no longer solely a technical matter; it has become an operational necessity for every organization. This evolution is not temporary, but a structural transformation in the way organizations approach and understand security.

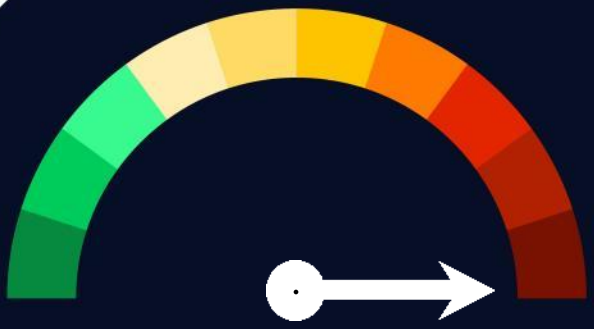
**Whendy Oré Crisostomo**
Cybersecurity Analyst

# Vulnerabilities

## OneUptime Sandbox Escape

**Date:** 27 May 2026
**CVE:** CVE-2026-45102



**CVSS: 9.9**

**CRITICAL**

## Description

CVE-2026-45102 is a critical Remote Code Execution (RCE) vulnerability in OneUptime. The issue stems from the insecure use of Node.js's "vm" module as an isolation mechanism.

A low privileged authenticated attacker can exploit this flaw to execute arbitrary code on the server, access sensitive information and compromise the application. Due to its severe impact, the vulnerability has been assigned a CVSS score of 9.9.

## Solution

- Upgrade to OneUptime version 10.0.98 or later, where the issue has been resolved.

## Affected Products

- OneUptime versions prior to 10.0.98.

## References

- nvd.nist.gov
- github.com

# Vulnerabilities

## WordPress WP Maps Pro

**Date:** 29 May 2026
**CVE:** CVE-2026-8732

**CVSS: 9.8**

**CRITICAL**

## Description

The WordPress plugin WP Maps Pro, an interactive mapping plugin based on Google Maps, is vulnerable to privilege escalation through the creation of an administrator account.

When an attacker visits a public page, they can extract a nonce, a temporary access token exposed within the JavaScript code. They then send a background AJAX request containing the nonce.

The system does not verify whether the user has administrator privileges; it only checks whether the nonce is valid, allowing the attacker to obtain administrator level access.

## Solution

Recommendations:

- Review and uninstall any recently installed unauthorized plugins.
- Update the plugin to version 6.1.1 or later.

## Affected Products

Affected products include:

- WP Maps Pro versions prior to 6.1.0.

## References

- thehackernews.com
- wordfence.com
- incibe.es

# Android Fixes an Actively Exploited Privilege Escalation Vulnerability

**Date:** 2 June 2026
**CVE:** CVE-2025-48595

**High**

## Description

Google has addressed CVE-2025-48595, a vulnerability identified in the Android Framework component. The flaw is an Integer Overflow vulnerability (CWE-190) that can lead to local privilege escalation and allow code execution with higher privileges than intended.

Exploitation of this vulnerability does not require prior elevated privileges and may compromise the security of the affected device. Google stated that there was evidence of limited and targeted exploitation before the release of the security update.

The vulnerability affects multiple Android versions and is included in the June 2026 Android Security Bulletin.

## Affected Products

- Android 14
- Android 15
- Android 16
- Android Framework
- Android devices that do not have the 2026-06-05 security patch level or later installed

## Solution

- Update devices to the 2026-06-05 security patch level or later.

## References

- android.com
- nist.gov
- cisa.gov

 | 

# Cisco Patches Vulnerabilities in Unified CM

**Date:** 4 June 2026
**CVE:** CVE-2026-20230

**High**

## Description

The CVE-2026-20230 vulnerability in Cisco Unified Communications Manager (Unified CM) could allow an unauthenticated remote attacker to carry out Server-Side Request Forgery (SSRF) attacks through a vulnerable device.

This vulnerability is caused by improper validation of certain HTTP requests by the SSRF handling mechanism.

An attacker could exploit the flaw by sending a specially crafted HTTP request to an affected device. Successful exploitation would allow the attacker to write files to the underlying operating system, which could subsequently be used to gain administrator privileges.

## Affected Products

Affected products include:

- Cisco Unified CM up to version 14 and Unified CM SME up to version 15 when the WebDialer service is enabled.

## Solution

Recommendations:

- Administrators should disable the WebDialer service.
- Install the latest security patch.

## References

- thehackernews.com
- sec.cloudapps.cisco.com
- incibe.es

# Events

### GITEX AI Europe 2026
*30 June– 1 July*

GITEX AI Europe 2026 will take place from 30 June to 1 July in Berlin, Germany, as a forum dedicated to exploring the role of artificial intelligence in Europe's digital transformation. The event will bring together technology companies, public sector organizations, research centres and industry leaders to share insights on AI adoption, regulatory challenges and the innovation opportunities this technology is creating across a range of sectors. The program will feature conferences, demonstrations and discussions on the development of AI driven solutions, as well as their impact on areas such as cybersecurity, business productivity and digital competitiveness.

**Link**

### RAISE Summit 2026
*7 July– 9 July*

RAISE Summit 2026 will take place from 7 to 9 July in Paris, France, bringing together thousands of business leaders, investors, entrepreneurs and technology executives to discuss the future of artificial intelligence. The event will feature more than 2,000 companies and hundreds of leading speakers from the global technology ecosystem, including representatives from organizations such as Google, OpenAI, Anthropic, Meta and AWS. Throughout the program, participants will explore the challenges associated with enterprise AI adoption, from infrastructure and governance to business value creation, making it a key forum for understanding the strategies shaping the next generation of digital innovation.
**Link**

### Gartner Security & Risk Management Summit
*22 July – 24 July*

The Gartner Security & Risk Management Summit will take place from 22 to 24 July in Tokyo and will bring together CISOs, risk leaders and cybersecurity executives to discuss the challenges reshaping the security function within organizations. The program will be structured around six specialized tracks: cybersecurity leadership and innovation, risk management and resilience, infrastructure and cloud security, application and data security, security operations and incident response, and the exclusive CISO Circle program for senior executives. Through these sessions, attendees will gain insights into the latest trends in artificial intelligence, cyber resilience, data protection, cloud security and the alignment of security strategies with business objectives.

**Link**

# Resources

- **ENISA NIS360**

Published by the European Union Agency for Cybersecurity (ENISA), the NIS360 2026 report provides a comprehensive assessment of the cybersecurity maturity and criticality levels of sectors considered essential under the NIS2 Directive. The study examines the preparedness of key sectors including energy, transport, finance, healthcare, digital infrastructure and public administration, identifying strengths, gaps and priority areas for improvement. It also offers a comparative view of how cyber resilience is evolving across Europe and highlights those sectors where strategic importance exceeds current security maturity levels, making it a key reference for cybersecurity leaders, regulators and critical infrastructure operators.

Link

- **NIST IR 8374r1: Ransomware Risk Management – A Cybersecurity Framework 2.0 Community Profile**

Published by the National Institute of Standards and Technology (NIST), this document provides practical guidance to help organizations manage ransomware related risks using the NIST Cybersecurity Framework (CSF) 2.0. The profile identifies the most relevant security objectives for governing, preventing, detecting, responding to and recovering from ransomware incidents, providing a structured reference for assessing an organization's level of preparedness against this type of threat. In addition, the document supports the identification of security gaps and the development of resilience strategies aimed at reducing the operational and financial impact of an attack.

Link

Subscribe to RADAR

**Powered by the cybersecurity NTT DATA team**

es.nttdata.com