- Products

PRODUCTS

Security Global Networking Wireless Connectivity Managed Services Voice

SECURITY

- Edge Protection
- Endpoint Security
- Identity Security
- AI Security
- Security Management

GLOBAL NETWORKING

- Internet
- Private Networking
- Cloud Connect
- Managed SD-WAN
- Managed Network Services

WIRELESS CONNECTIVITY

- Wireless Networking
- LEO Satellite
- IoT Connectivity
- SIM Management

MANAGED SERVICES

- Managed Network Services
- Security Management

- Managed Intelligence

VOICE

- SIP Trunking
- Hosted PBX
- POTS Replacement

- Solutions

SOLUTIONS

- Securing AI
- Security, Simplified
- Wireless Everywhere
- Secure From the Network Up

- Resource Center

RESOURCE CENTER

- Resources
- Press Releases

- Our Company

OUR COMPANY

- About Globalgig
- Careers
- Leadership

- Contact Us



- Products 
  - Security 
    - Edge Protection
    - Endpoint Security
    - Identity Security
    - AI Security
    - Security Management
  - Global Networking 
    - Internet
    - Private Networking
    - Cloud Connect
    - Managed SD-WAN
    - Managed Network Services
  - Wireless Connectivity 

SECURITY

# Why Fragmented Identities Are Holding Your Business Back, and How To Fix Them

By Globalgig

July 30, 2026



Content

**Identity is the foundation for modern enterprise security. But most organizations have hundreds of thousands of human and machine identities, and effectively managing them across a sprawl of siloed IAM tools is virtually impossible. An identity fabric ties these disparate tools together within a single framework, boosting security defenses and creating a platform for strategic initiatives to play out quickly and safely.**

It’s Friday afternoon and Jeremy, a sales rep, is firefighting an issue with a customer’s order. He’s on the phone trying to get things sorted out before the weekend when he gets a phishing email asking him to verify his Office 365 account. Because he’s distracted, he clicks on the link

and enters his credentials.

A cyber attacker now has a way in. But the sales role isn't the only job Jeremy's had with his company. The intruder discovers Jeremy still has access to an AWS environment, technical documentation, and a customer database from when he was a technical support engineer.

Now the attacker can steal more credentials, bypass security measures, escalate Jeremy's privileges, and move laterally through corporate resources. And because the systems asking for authentication aren't joined together, the company is too slow to spot that Jeremy's credentials are being used in a suspicious manner.

This kind of scenario isn't unusual – in fact, 9 out of 10 organizations have faced a successful identity-related breach in the last year, and silos add an average of twelve hours to identity-related incident response times.

So how have we ended up with this situation?

## The Security Environment Has Changed Beyond Recognition

The legacy castle-and-moat security approach worked well enough when corporate networks had a distinct perimeter.

Most people worked in an office, and devices, servers, and databases were generally either on-premises or in a data center, so there was a clear boundary between everything inside the network and everything outside. An Active Directory environment was usually enough to authenticate the identities of users and authorize access to these centralized corporate resources.

But cloud, SaaS applications, and AI integrations moved data outside of these clear physical locations, and remote working moved people away from the office. BYOD and IoT devices – often poorly configured and badly secured – added to the infrastructure complexity.

## Digital Identity Is the Sharp End of Security - But IAM Tools Don't Talk to Each Other

Without a defined network perimeter, digital identity has become the front line of enterprise security. Virtually all enterprise tools, services, and systems rely on some form of Identity and Access Management (IAM) to let the right people in and keep the bad guys out.

But these resources rely on a wide variety of IAM systems for access and authorization. So there may be different IAM solutions for cloud-based services, apps and resources hosted on-premise, and legacy applications – and they all work differently.

These identity systems are usually siloed, leaving gaps in security and accountability and creating blind spots and vulnerabilities. It's difficult to manage these complex, disparate systems too.

Trying to enforce consistent, centralized policies and governance is a major headache for time-poor security teams. And it's almost impossible to see who has access to what, because there's no overview to show how permissions have accumulated over time.

**Non-Human Identities Are an Even Bigger Problem Than People**

It's not just human identities that need to be managed these days, either. In many companies, non-human identities or NHIs – digital identities used by applications, AI agents, or other software – outnumber people by 109 to 1.

NHIs are usually undermanaged and overprivileged, and are often given static and long-lasting credentials. They can accumulate even more access permissions than human users do, but they're not compatible with human-centric security controls like multi-factor authentication (MFA).

As a result, they represent a huge security risk and an increasingly attractive vector for attack.

# Disparate Identity Tools Derail Zero Trust Programs

To secure a remote workforce and distributed corporate resources, many organizations are making the move to zero trust. This approach is based on the principles of 'never trust, always verify' and involves continuous authentication, principles of least privilege, and context-based access controls rather than broad network-level access.

Identity is central to this model, so zero trust breaks down if IAM tools are fragmented and human and NHI credentials are poorly managed. This is why some enterprises are beginning to look at a new approach – the identity fabric.

# What's an Identity Fabric?

An identity fabric is an architectural approach designed to overcome identity silos. It uses APIs to link together the different identity, privilege, and access management solutions that are used to authorize connections between people, applications, systems, clouds, and devices. It doesn't replace them, but merges them into a single cohesive framework with centralized visibility, orchestration, and policy management.

An identity fabric provides universal control for how people, devices, and NHIs can interact with enterprise resources across all environments. So instead of being a layer of security, identity can now become the control plane for securing networks, devices, clouds, and AI.

This creates the foundation for frameworks that rely on zero trust – like SASE and SSE – and feeds into stronger threat detection, effective microsegmentation, and robust AI governance.

## *Unified Policies and Access Controls*

Because each user has a single digital identity, an identity fabric allows organizations to create and enforce uniform policies and access permissions irrespective of what application, system, or resource is being used.

Revoking access becomes more straightforward, so when a user changes role or leaves, or an NHI becomes defunct, permissions are removed and don't accumulate. A single digital identity also simplifies things for users, since they don't have to manage different login details and passwords.

## *Compliance and Scalability*

This approach helps organizations meet regulatory compliance standards and provides a single source of truth for easier auditing and reporting.

New apps, AI agents, and resources can easily be integrated into the identity fabric, making it simple for enterprises to scale or introduce changes.

## *Human and Non-Human Identities Under a Single Security Model*

By bringing NHI credential systems – like secrets, tokens, and vaults – into this framework, identity fabrics allow enterprises to extend more rigorous security models to all identities, whether human, machine, or AI.

This approach helps enterprises to move away from the static, long-lived credentials and excessive privileges that attackers can harness during a breach. It also improves accountability by tying NHIs to human owners.

By bringing NHI credential systems – like secrets, tokens, and vaults – into this framework, identity fabrics allow enterprises to extend more rigorous security models to all identities, whether human, machine, or AI.

## *Tighter Management of Privileges*

Privileged accounts are a top target for cybercriminals because they provide very high levels of access and control, and the consequences can be devastating if they're hijacked.

An identity fabric incorporates privileged account management (PAM), helping to tighten governance of these accounts, mitigate identity sprawl, and identify issues before a breach becomes a catastrophe.

## *Clearer Visibility Boosts Threat Detection*

With a single digital identity, it's possible to monitor and inspect user and NHI behavior across different apps and systems to make breach detection quicker and easier. According to Palo Alto, organizations that use identity-driven security controls can accelerate breach response times by up to 80%.

Going back to the scenario we started with, an identity fabric would provide an overview that would allow the threat to be identified much faster. The fact that Jeremy's credentials were being used to access systems he no longer needed, and that he appeared to be logging in to different resources from more than one location at once, would raise red flags immediately.

# Identity Fabrics Feed Business Agility

The advantages of an identity fabric go beyond tying fragmented IAM systems together.  Its value is increased exponentially when it feeds into the wider security architecture, so that identity-level events provide the intelligence to drive threat detection, breach response, vulnerability mitigation, and increased resilience across the whole enterprise infrastructure.

This isn't just a technical goal – it has implications for the whole business. For most organizations, competitive strategy is built on digital foundations, like AI agents, automated workflows, SaaS platforms, cloud workloads, and IoT devices.

For these initiatives to drive revenue and realize business goals, enterprise security must be able to flexibly support the timely roll-out of digital projects while minimizing risk. An identity fabric streamlines access controls across these immensely complex enterprise environments, providing the foundation for safer, faster innovation.

**Related to your reading**



SECURITY

## Refreshing Network Hardware? Don’t Overlook Connectivity and End Up Doing the Work Twice.

Read more →



SECURITY

## Endpoint Security: Are You Scrutinizing Your AI Add-Ons as Closely as Your Agents?

Read more →



SECURITY

## Scary Cybersecurity Stats: Alarming Findings from 2026 Research

Read more →

- 
- 






- Products
  - Security
  - Global Networking
  - Wireless Connectivity
  - Managed Services
  - Voice
- Solutions
  - Securing AI
  - Security, Simplified
  - Secure From the Network Up
  - Wireless Everywhere
- Our Company
  - About Globalgig
  - Careers
  - Leadership
  - Channel Partners
- Customer Support
  - Contact Us
  - Network Operations
  - Service Advantage Team
  - Orchestra Login

© 2026 Globalgig. Globalgig is a trading brand of iGEM Communications.

- Privacy Policy
- Acceptable Use Policy