German-American IT Security Forum

San Francisco, 23.03.2026

The Identity Crisis: Mitigating Modern Identity-Based Cyber Threats

Nick Terkay, Unosecur

The Identity Crisis: Mitigating Modern Identity-Based Cyber Threats

Agenda

01. The Identity Crisis

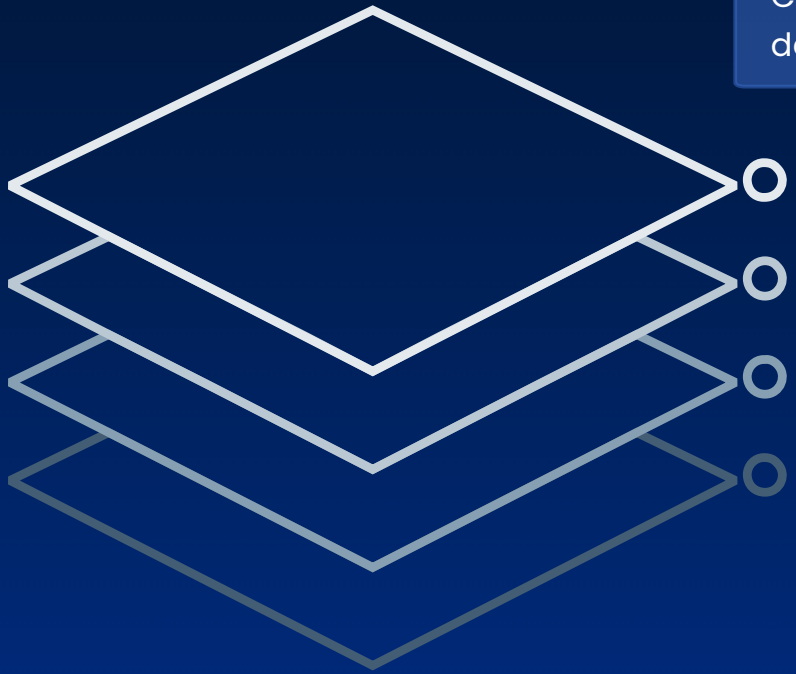
02. An Evolving Threat Landscape

03. Key Pillars of Identity Security

04. Recommendations

05. Wrap-up

01.
The Identity Crisis



Cybersecurity is a form of **economic warfare** where success depends on understanding and countering adversaries. source

Adversary Incentives: Adversaries are driven by rational self-interest, motivation, and purpose (whether ideological, financial, or geopolitical)

Objective: Shift the balance of time and money against the adversary by raising the marginal cost, making the attackers' approach unattractive

The Innovation/Reuse Cycle: Adversaries follow the path of least resistance, repeating successful techniques until defenders make them uneconomical

Defender success forces attackers to change course, facing four choices:

- **Stop** and abandon the tactic
- **Focus** on softer targets by shifting to easier victims
- **Innovate** and refine tooling or combine methods to overcome defenses
- **Migrate** to a different vector where barriers are lower/rewards are greater

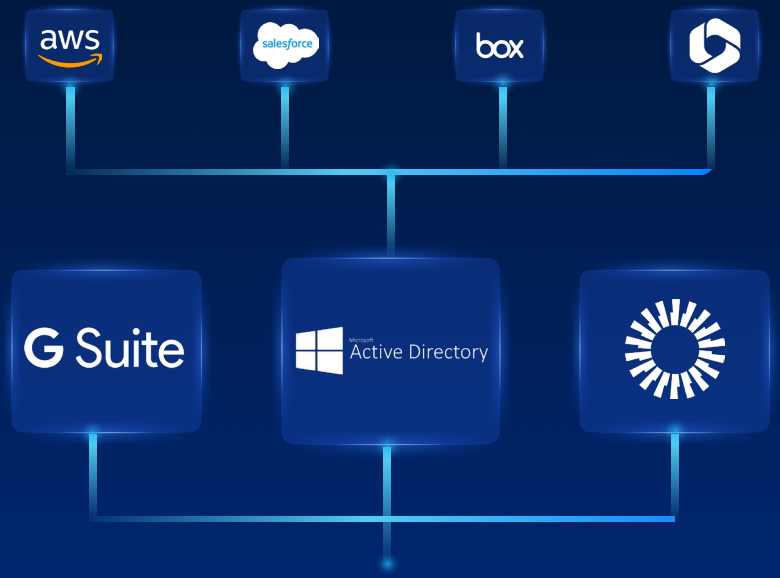
	Attacker Strategy	Defender Response
Human Speed (Manual)	Attacks are done by hand, limited by the time and attention of one person (e.g., manually checking for an open port).	Defenders fix issues manually, one at a time (e.g., applying a patch after reading an advisory).
Standardized Tools (Repeatable)	Attackers codify their methods into simple scripts and tools (e.g., Autohack, Metasploit) to repeat the process across many targets consistently.	Defenders use standardized processes like default-deny firewalls, network segmentation, and the first generation of vulnerability scanners.
Mass Automation (Scale)	Attackers use global connectivity and automation to launch campaigns against millions of systems simultaneously using a few known vulnerabilities. **Ransomware** flourishes here because of scalable, anonymous monetization (Bitcoin).	Defenders struggle to keep up due to the sheer volume of assets and vulnerabilities. Defense requires moving beyond old signature models to new **machine learning (ML)-based detection**.
Intelligent/Adaptive Warfare (Complexity)	Attackers layer high sophistication onto their scaled attacks, using complex chains and possibly using ML/LLMs to **generate brand-new vulnerabilities**.	Defenders cannot win by patching alone. The strategy shifts from "patch-and-prevent" to **"contain-and-constrain,"** focusing on stopping attacks in real-time and limiting the damage (blast radius).

source

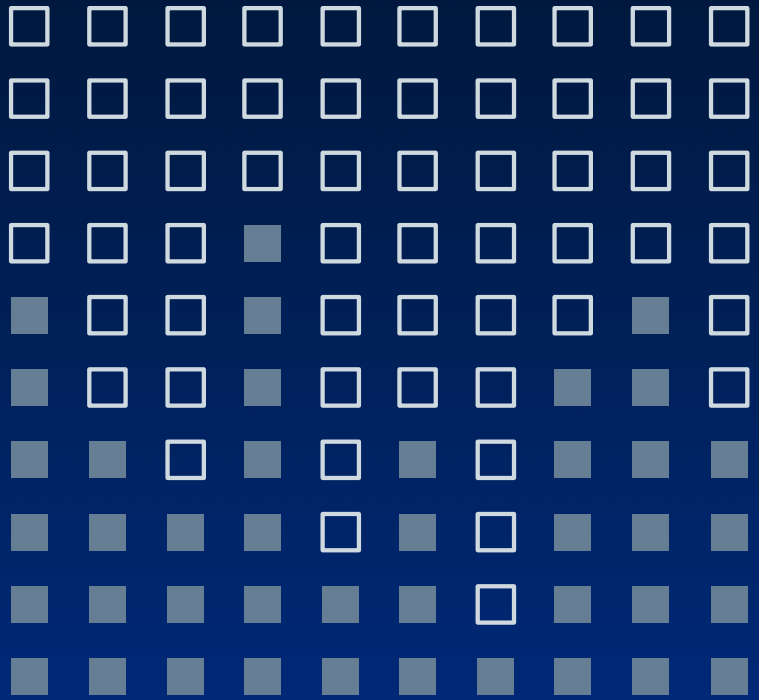
You can't secure what you can't see

- Having hundreds of disparate systems and providers makes identity security opaque, leaving governance a major challenge - and the result - many thousands of human and non-human identities become soft targets

- 4 of every 5 actual data breaches are linked to compromised credentials - whether from social engineering, supply chain compromise, or insider threats - identity continues to be the top and most successful attack vector every year



Security must start with Identity



Identity cuts deep

Organizations understand the criticality of identity, but its security is often overlooked and under budgeted. A breach of identity systems grants attackers virtually unrestricted access, making identity a high-value target.

02.

An Evolving Threat Landscape

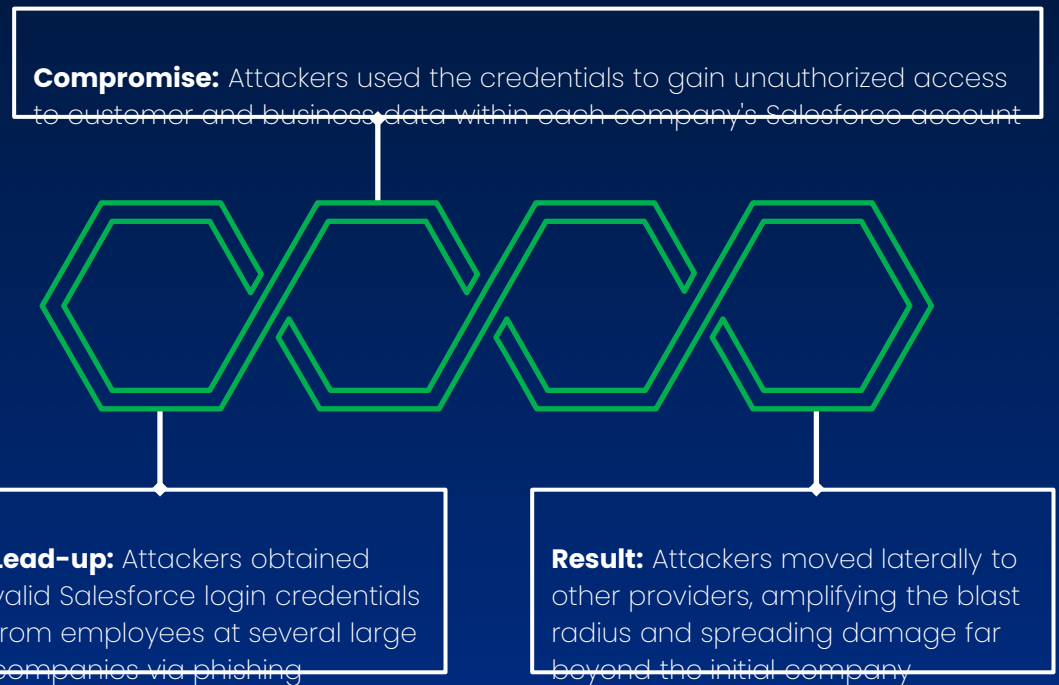
2.1 / Primary Threats

- **Credential Theft & Unauthorized Access**: Attackers relentlessly target employee and system credentials to gain initial footholds into networks, bypassing traditional perimeter defenses.
- **Ransomware & Malware Attacks**: Malicious software is frequently used to cripple critical systems, leading to operational disruption, data breaches involving millions of customer records, and severe reputational damage.
- **Software Supply-Chain Attacks**: Vulnerabilities within the software we rely on are being exploited, allowing attackers to compromise systems through trusted third-party vendors.
- **Social Engineering (e.g., Phishing)**: Deceptive tactics remain a highly effective method for tricking employees into divulging credentials or executing malicious code, serving as a primary entry point for broader attacks.

2.2 / Case Study of Third-Party Identity Compromise

The tangible risk of third-party identity compromise cannot be overstated.

A well-documented 2025 case involving Salesforce credentials illustrates this danger. Attackers, using credentials obtained via phishing, not only accessed sensitive customer data within Salesforce but also **leveraged API connections to move laterally into integrated partner systems**.

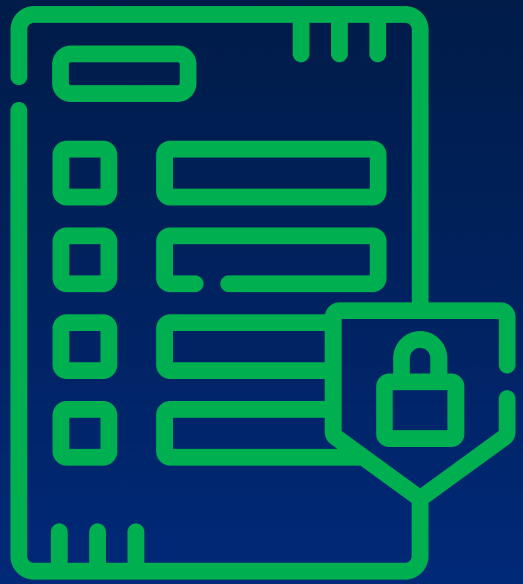


03.
Key Pillars of Identity Security

3.1 Never trust, always verify

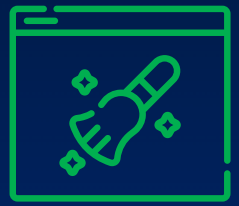
To combat modern identity-based threats, a fundamental shift in security philosophy is required. We must move away from less sophisticated defender responses and embrace Zero Trust. Not as a specific technology, but as a strategic security principle to focus directly on securing our users, assets, and resources.

- Access must be determined by dynamic policies
- Decisions can not be static; they should be based on real-time signals, including user identity, device security posture, geographic location, and deviations from normal behavior patterns



3.2 / Three Pillars of a Modern Identity Security Program

Proactive Defense
Shrink the attack surface before an attack occurs



Real-Time Response
Neutralize active threats in progress

Comprehensive Governance
Secure automated non-human foundation of our operations

3.3 / Proactive Defense => ISPM

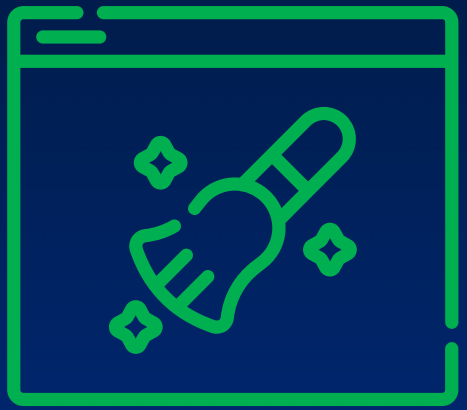
Identity Security Posture Management (ISPM) is the foundational practice of proactively discovering, analyzing, and hardening the entire identity landscape. Its primary goal is to enforce the **Principle of Least Privilege** ruthlessly, ensuring that every user and application has only the absolute minimum level of access required to perform its function.

By continuously removing excessive/unused permissions, ISPM helps organizations adhere with strict protocols, functionally serving as the digital enforcement of **Segregation of Duties,** dramatically limiting the potential blast radius of a compromised account.

3.4 / Real-Time Response => ITDR

Identity Threat Detection and Response (ITDR) provides the real-time monitoring and response capabilities necessary to stop active attacks as they happen. It detects malicious activities like privilege escalation, lateral movement, and credential misuse in progress.

The strategic value of ITDR is its ability to reduce our **Mean Time to Detect and Respond (MTTD/MTTR)** to a 5-minute benchmark. This speed is critical to disrupting an attack chain before significant data exfiltration or operational damage can occur, effectively neutralizing the threat in its earliest stages.



3.5 / Comprehensive Governance => NHI

Non-Human Identity (NHI) Management is the critical function of governing the digital identities of our automated tools, including service accounts, API keys, and bots. Especially in the era of AI.

The sprawl of these identities, driven by our deep integrations with SaaS platforms and cloud services, creates significant risk. These identities often possess elevated privileges, yet they are rarely inventoried or rotated. A dedicated NHI management program ensures these powerful identities are discovered, governed by least privilege, and monitored for compromise.

04.
Recommendations

4.1 / Prioritize Full Identity Visibility

Discovery and Inventory of every Human and Non-Human Identity

- ✓ Multi-Cloud
- ✓ On-Premise
- ✓ SaaS Apps

4.2 / Champion a "Least Privilege" Culture

Non-Negotiable Adherence to Safety Protocols in the Digital Environment

- ✓ Continuously Reduce Permissions
- ✓ Significantly Limit Blast Radius
- ✓ Maintain Operational Continuity

4.3 / Invest in Real-Time Threat Disruption

Allocate Dedicated Resources to Implement a Modern ITDR Capability

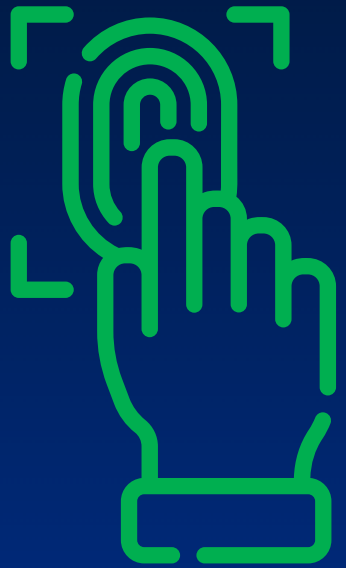
- ✓ Shift from Reactive to Active
- ✓ Disrupt Attacks in Real-Time
- ✓ Protect Data & Avoid Interruptions

05.
Wrap-up

5.1 / Identity is the New Battlefield

The most important takeaway is that in modern cybersecurity, **identity is now the perimeter**. The old model of protecting a company by building a strong wall around its network is no longer enough. This is where the real fight is: **80% of data breaches involve misused credentials**.

Protecting the full spectrum of digital identities is the most critical challenge to overcome to defend against the most common and damaging cyber threats facing your company.



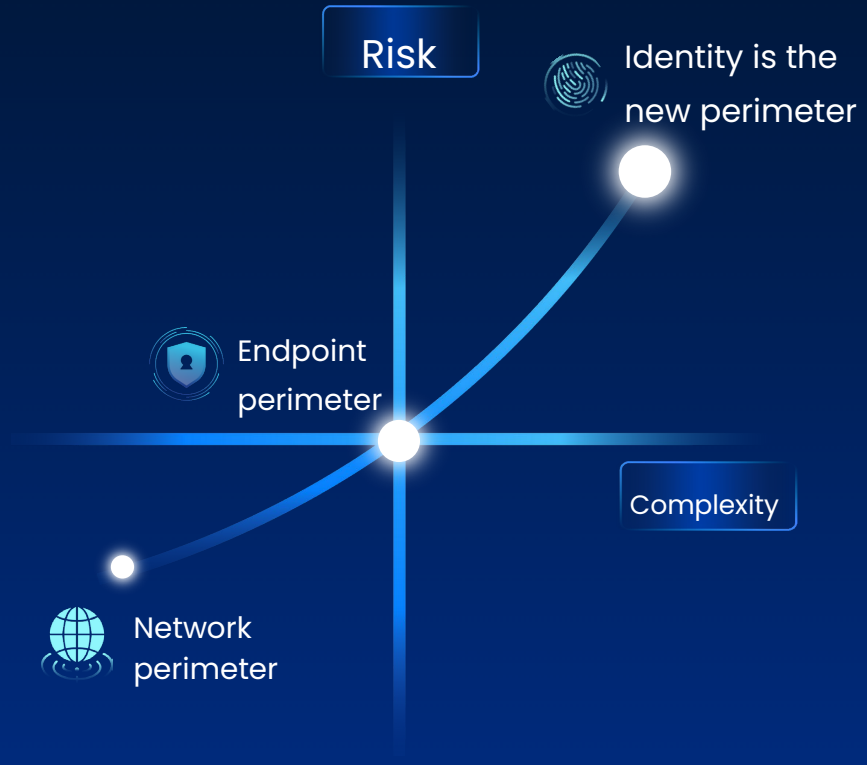
Identity-first security is at the cusp of exponential necessity and soaring complexity

312%

Rise in data breach notices YoY in the US (2024 ITRC Annual Breach Report).

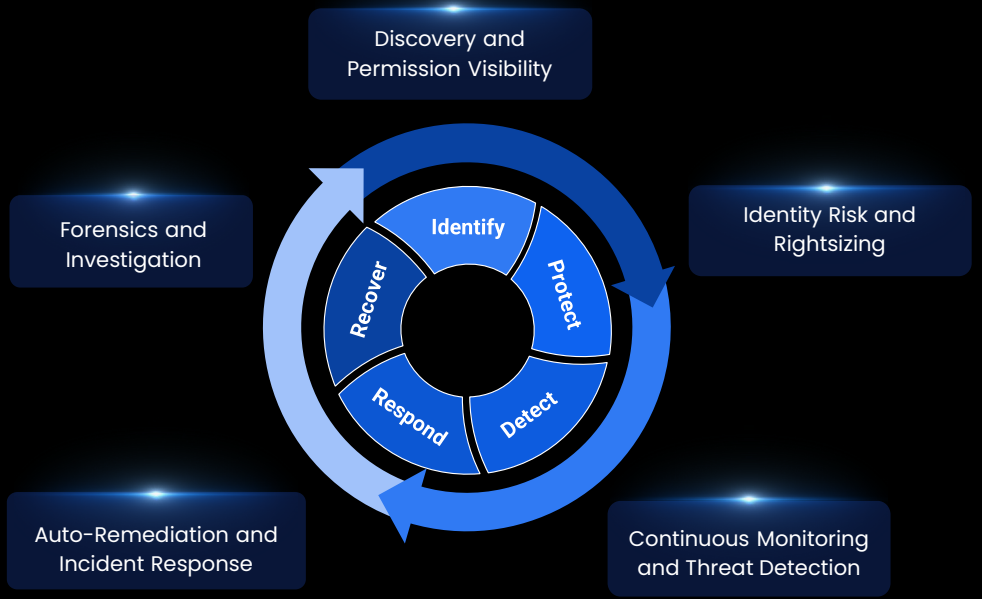
1/92

For every human identity there are 92 non-human identities exposed to 3rd parties.



What is a Unified Identity Fabric?

Imagine every identity in your organization, human and non-human, as threads. **Unosecur's Unified Identity Fabric** weaves those threads together into a single, adaptable framework for managing and monitoring every identity across disparate identity systems, cloud service providers, as well as SaaS and legacy applications. It stitches together your current tools, workflows, and teams into a cohesive whole. Rather than replacing existing systems, it connects them, adding a layer of insight and control across your identity ecosystem.



How it works

1: Effortlessly onboard your Cloud, IdP, On-prem and SaaS providers

2: Actionable identity and access issues are available in minutes

3: Unified identity workflows provide quantified outcomes continuously

Platform features

JIT + JEP Policy Builder

AI-based NLQ Forensics

Simplified Permissions

Auditing and Reporting

Visual Attack Paths

Bonus: The AI Slide – a new breed of NHI – Agentic AI

Coding Agents
Enterprise SaaS Agents
Custom-built agents

Booth / Event Details

- Booth [xyz] with TeleTrusT
- Tues nite - High Stakes. Least Privilege.
  - Luma link
  - Hotel Zeppelin
- Tues/Wed @ The Hive @ Yerba Buena Bar
  - Nick speaking
  - Pranav speaking

unosecur

Identity threat defense for modern enterprises

Unified runtime coverage of access controls and activity across Cloud, IdP, on-prem and SaaS for human & non-human identities

get in touch

Nick Terkay

Field CTO

unosecur.com | linkedin.com/in/terkay

nick@unosecur.com