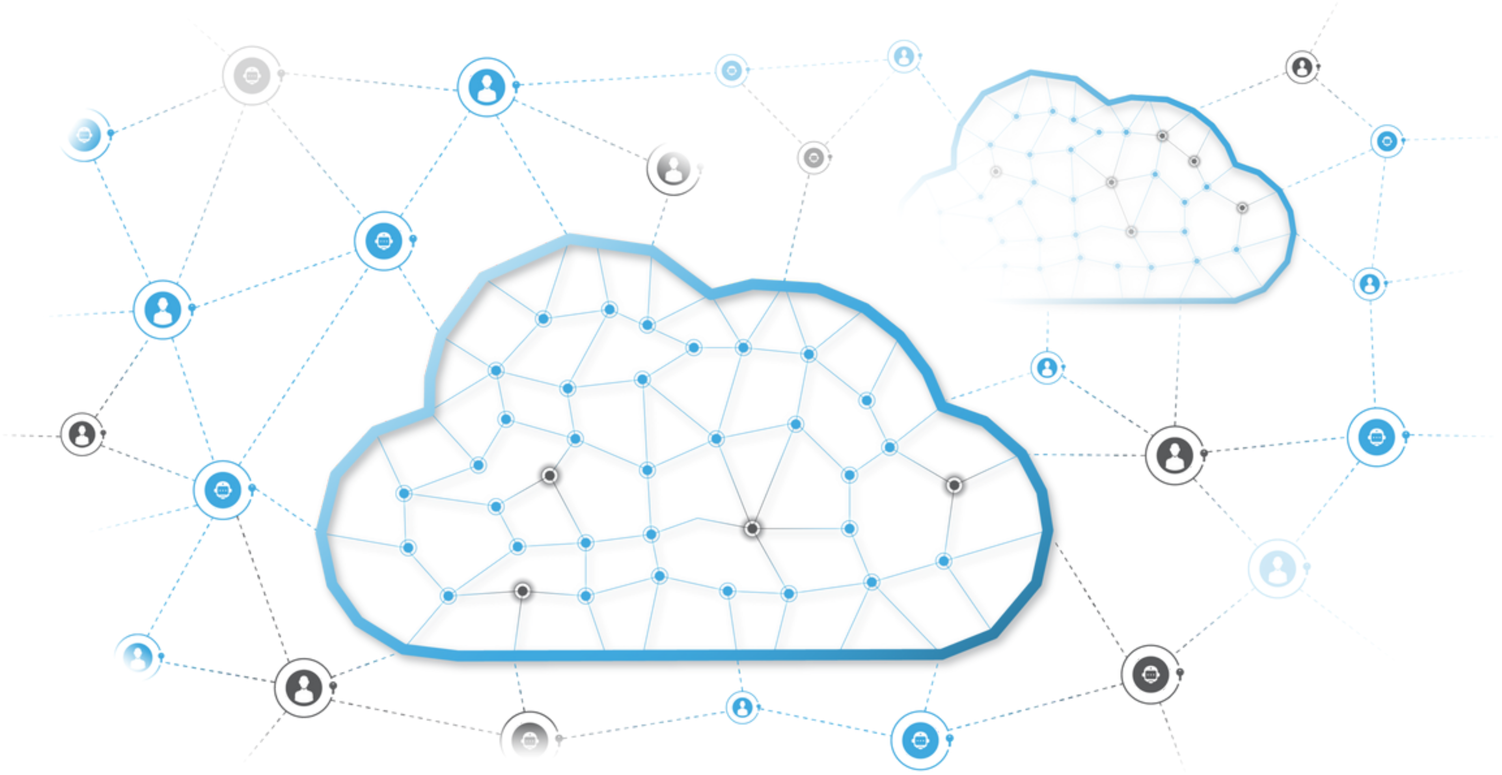
STACK IDENTITY

Securing Tomorrow’s Access: A Dynamic Journey Through Access Evolution

White Paper



Abstract:

This paper delves into the nuanced evolution of access control over time, introducing Stack Identity as an Identity Access Risk Management platform tailored for the challenges beyond day 1. Traditional IAM processes, centered around human identities and Joiner-Mover-Leaver practices, prove inadequate in addressing the dynamic nature of modern security. Stack Identity redefines Access Controls, offering real-time visibility, correlation, and automated identity and access intelligence across human and non-human entities, providing a unified solution for IAM, Security, and Cloud teams.

Introduction:

In contemporary cloud architectures, identity serves as the bedrock foundation for accessing infrastructure, applications, and data. This paper explores the challenges posed by evolving identities, particularly the 95% that are non-human in public cloud environments. Traditional Identity Governance and Administration (IGA) practices, including Joiner-Mover-Leaver (JML) processes, have proven effective for IT productivity but fall short in addressing the dynamic threat landscape and neglecting the crucial factor of time as a significant variable in the IAM process.

Navigating the Identity Lifecycle: Unraveling Day 1 Access and the Complexities Beyond

Day 1 Access stands as the threshold where employees are handed the keys to crucial corporate IT applications, guided by the principles of Birthright Access through the meticulous Joiner-Mover-Leaver (JML) process. This inaugural access is orchestrated seamlessly by Identity Governance and Administration (IGA) tools like Sailpoint, Saviynt, Entra ID (formerly Azure Active Directory), Okta, and others, forming the foundation of secure onboarding.

In the dynamic expanse of cloud environments, developers, on their day 1, may find access facilitated through Infrastructure-As-Code tools like Terraform or Cloud Formation Templates, introducing a new dimension to the traditional access paradigm. Simultaneously, business and analytics teams independently navigate their data assets, configuring local administrators and granting access to business and product users, fostering an environment of tailored permissions.

However, the initiation of an identity and the conferment of access mark the enterprise's entry into the intricate web of risks intertwined with identity and access. This realization serves as the bedrock of a dynamic identity lifecycle, where effective access unfolds over time, shaped by daily events and operational shifts.

Continuous deployment of new applications and assets, occasional access grants by exception, users elevating their access, human errors leading to unintended access, the sharing of access, and the explosive growth of LLM (Large Language Models) embedded applications all contribute to the evolving landscape.

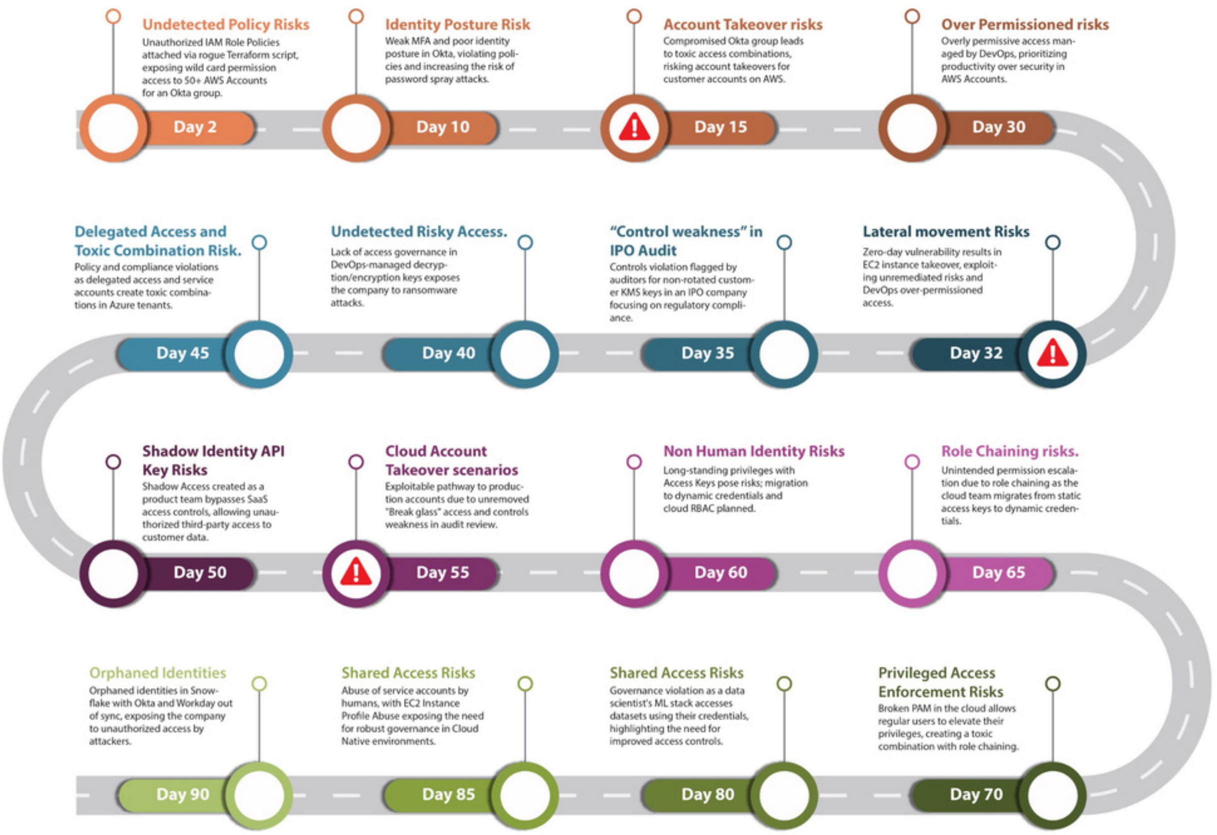
In cloud environments, infrastructure-as-code becomes a primary mode of access, often bypassing traditional Identity and Access Management (IAM) and IGA tools, adding layers of complexity.

The multifaceted risk landscape is compounded by programmatic or headless access, whether through static or API keys, and the looming specter of unauthorized data sharing. The stark contrast between access granted on day 1 and the actual effective access over time becomes evident in scenarios depicting day 2 and beyond.

Effectively addressing the intricate challenges posed by this evolving landscape demands a holistic reevaluation and reconstruction of security, risk management, compliance, and governance processes. In this dynamic scenario, Identity and Access emerge as the linchpin, requiring continuous fortification and adaptation to navigate the evolving contours of digital risk. As organizations navigate this complex journey, the narrative underscores the imperative for a robust and responsive Identity and Access Management strategy.

Dynamic Shifts: Unveiling the Evolution of Access Control Over Time

Let’s walk through how time impacts identity and access risks over a 90-day period. These scenarios reflect everyday changes in identity, access, and configurations that open up legitimate access as active conduits for threats, vulnerabilities, and data breaches.



Day 2

Undetected Policy Risks

Unauthorized IAM Role Policies attached via rogue Terraform script, exposing wild card permission access to 50+ AWS Accounts for an Okta group.

Day 10

Identity Posture Risk

Weak MFA and poor identity posture in Okta, violating policies and increasing the risk of password spray attacks.

Day 15

Account Takeover risks

Compromised Okta group leads to toxic access combinations, risking account takeovers for customer accounts on AWS.

Day 30

Over Permissioned risks

Overly permissive access managed by DevOps, prioritizing productivity over security in AWS Accounts.

Day 32

Lateral movement Risks

Zero-day vulnerability results in EC2 instance takeover, exploiting unremediated risks and DevOps over-permissioned access.

Day 35

“Control weakness” in IPO Audit

Controls violation flagged by auditors for non-rotated customer KMS keys in an IPO company focusing on regulatory compliance.

Day 40

Undetected Risky Access.

Lack of access governance in DevOps-managed decryption/encryption keys exposes the company to ransomware attacks.

Day 45

Delegated Access and Toxic Combination Risk.

Policy and compliance violations as delegated access and service accounts create toxic combinations in Azure tenants.

Day 50

Shadow Identity API Key Risks

Shadow Access created as a product team bypasses SaaS access controls, allowing unauthorized third-party access to customer data.

Day 55

Cloud Account Takeover scenarios

Exploitable pathway to production accounts due to unremoved "Break glass" access and controls weakness in audit review.

Day 60

Non Human Identity Risks

Long-standing privileges with Access Keys pose risks; migration to dynamic credentials and cloud RBAC planned.

Day 65

Role Chaining risks.

Unintended permission escalation due to role chaining as the cloud team migrates from static access keys to dynamic credentials.

Day 70

Privileged Access Enforcement Risks

Broken PAM in the cloud allows regular users to elevate their privileges, creating a toxic combination with role chaining.

Day 80

Shared Access Risks

Governance violation as a data scientist's ML stack accesses datasets using their credentials, highlighting the need for improved access controls.

Day 85

Shared Access Risks

Abuse of service accounts by humans, with EC2 Instance Profile Abuse exposing the need for robust governance in Cloud Native environments.

Day 90

Orphaned Identities

Orphaned identities in Snowflake with Okta and Workday out of sync, exposing the company to unauthorized access by attackers.

Emergence of Shadow Access and Shadow Identities:

As these scenarios illustrate, Access control is no longer a day 1 problem. Access control challenges, as illustrated by these scenarios, reflect the emergence of a phenomenon that Cloud Security Alliance describes as Shadow Access and Shadow Identities. Traditional Identity Governance and Administration (IGA) processes lack the adaptability needed for threats, time, and changes. Effective access to resources changes over time.

Introducing Stack Identity:

Stack Identity stands at the forefront of solving the evolving challenges in Identity and Access Management (IAM) highlighted earlier. We provide a comprehensive Identity Access Risk Management solution tailored for modern cloud-native and data-centric applications. Our platform equips enterprise customers to proactively assess, remediate, and govern their identity and access risks, staunchly preventing unauthorized access, policy violations, incidents, and data breaches.

Leveraging the power of AI, our platform generates intelligent resolutions, recommendations, and policies to effectively tackle Identity Access Risks across cloud environments, applications, databases, and data platforms. It boldly bridges critical gaps in traditional Access Management, IAM, IGA, and Identity Provider platforms that often overlook nuanced Identity and Access Risks - a must-have for secure and adaptive management in modern cloud-native and data-centric applications.

Central to our approach is the Open Identity Security Data Lake, forming the backbone of our platform. This infrastructure connects, correlates, and contextualizes Identity Access Risks, providing a unified and comprehensive view.

With the Stack Identity platform, enterprises gain comprehensive capabilities:

- Obtain a global view of their identity population, spanning humans, machines, and APIs, assessing their posture and associated risks.
- Visualize intricate access landscapes, gaining insights into who has access to what, and untangling complex data pathways.
- Map the progression of threats, illustrating how risky identities exploit permissions, resulting in unauthorized access and data exfiltration.
- Continuously monitor and mitigate over-privileged access, toxic combinations, and privilege escalations, ensuring a secure and least privileged environment. Investigate identity threats, account takeover risks, and permissions issues with precision.
- Automate real-time access reviews, streamlining permissions for enterprise systems.
- Bridge critical gaps by integrating and embedding resolutions, recommendations, and policies into AM (Access Management), IAM, IGA, and Identity Provider (IDP) platforms.

Technical Features

- Powered by the industry's first open Identity Security Data Lake
- Open Data model and schema supporting major cloud platforms, Applications, Databases, and Data Platform
- API first
- 80+ Out of the Box detections supporting Cloud Identity Entitlements Management, Identity Threat Detection and Response, and IAM Governance
- LLM-based "Remediation as Code"
- Integrations with Access Management, IAM, IGA, IDP and CNAPP providers
- Automated Notifications and workflows for early detection and prevent Incidents, policy violations, Identity, and Access baseline drift.
- Monitor and implement Granular Access Controls - applied at Table, Column, Query, schema and ObjectsIdentity and Access Analytics.

In essence, Stack Identity's solution is a proactive and dynamic response to the intricacies of day 2 and beyond, fortifying organizations against the multifaceted challenges presented by the evolving landscape of identity and access risks.

Conclusion:

The initiation of an identity and the bestowment of access on day 1 signifies the enterprise's entry into the intricate web of risks associated with identity and access. Day 2 and subsequent access and identity events usher in cumulative risks, manifesting in various forms such as toxic access combinations, privileged access pathways, account takeover, unauthorized account utilization, audit and compliance failures, and incidents leading to data breaches.

As the landscape of access control continually evolves, shaped by persistent threats, inadvertent misconfigurations, and the inherent challenges of fragmented tools and processes, Stack Identity stands resolute as a steadfast guardian. Our dynamic, threat-aware approach provides resilience in a landscape where security risks are ever-changing, ensuring organizations are not merely prepared but empowered to effectively address the diverse challenges of day 2 and beyond.

Now is the opportune moment to proactively fortify your identity and access management strategy. To experience the transformative capabilities of Stack Identity, schedule a demo, or explore a trial by visiting stackidentity.com. Empower your organization with a security solution that seamlessly adapts to the dynamic contours of the digital landscape.