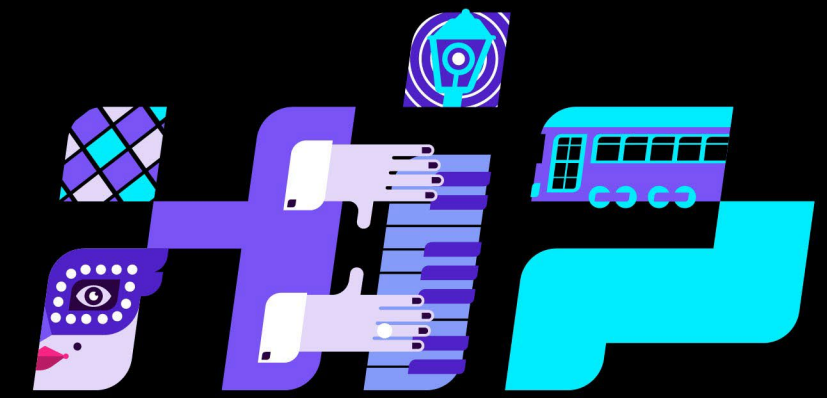
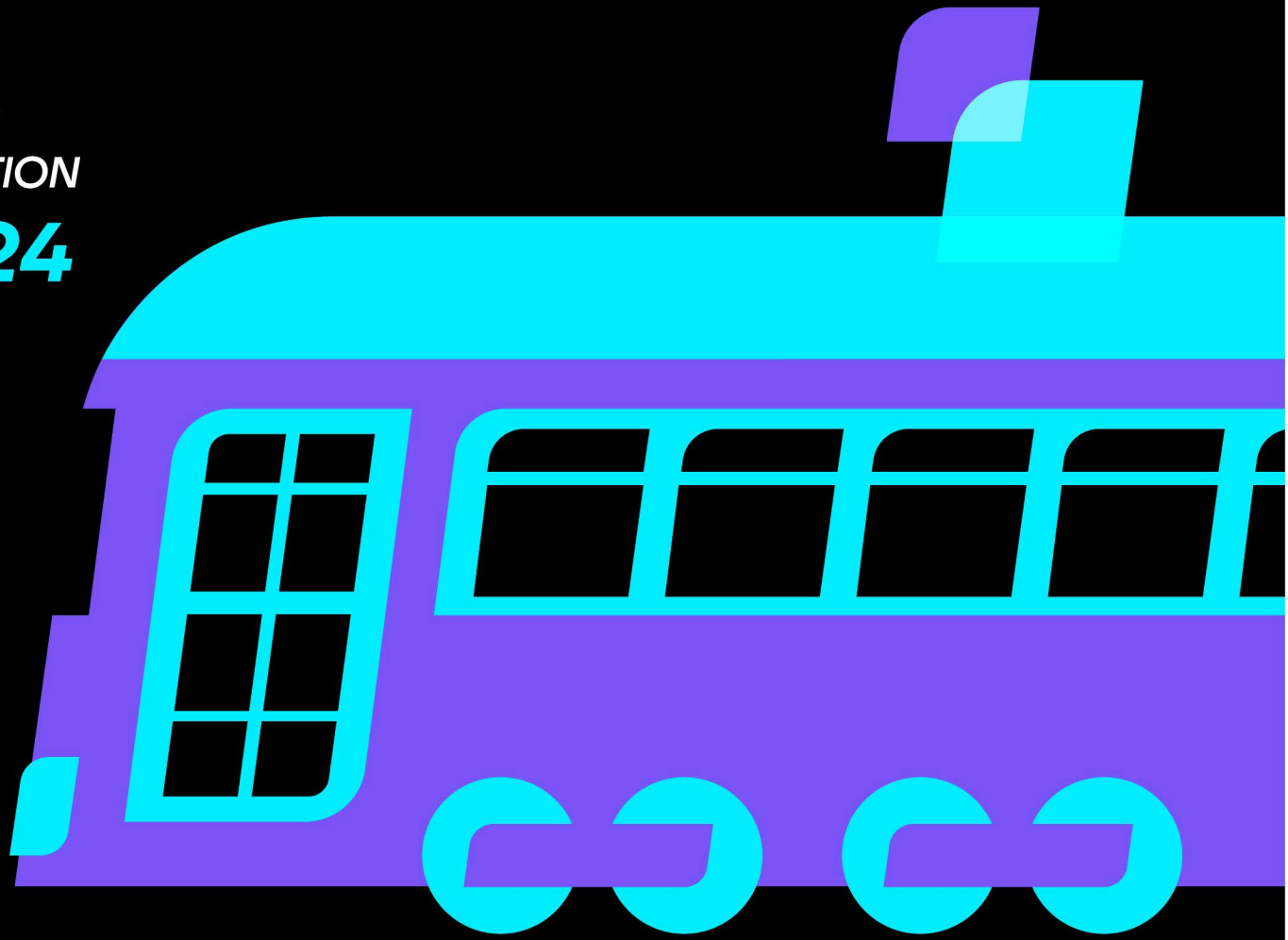
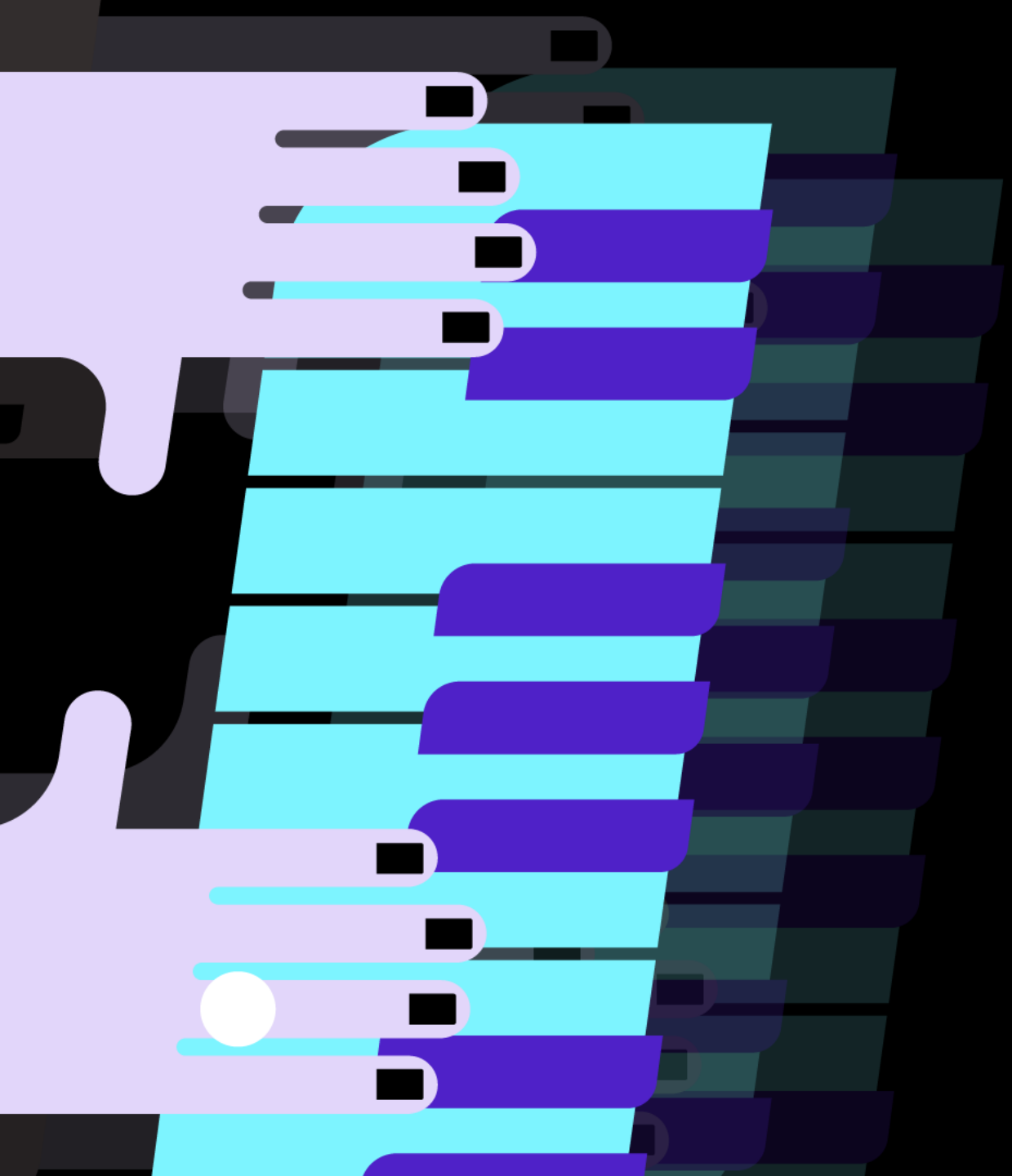


HYBRID
IDENTITY
PROTECTION

conf24

NEW ORLEANS





HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

Revolutionizing Workforce Identity with Data Engineering

From Access Control to Proactive Identity Intelligence

Rob Fry
CTO/Co-Founder of *aka identity*

The Workforce Identity Challenge

Workforce Identity Complexity

MULTIPLE DATA SOURCES

IDPs, HRIS, apps, directories, clouds

FRAGMENTED AND DISORGANIZED DATA

No single source of truth for identity data

OVER-PROVISIONING

Find me a company on planet earth who doesn't have an over-provisioning problem. A near-universal problem for companies.

Identity Hygiene Issues

"HYGIENE" AS A CONCEPT

Lack of trust in the data due to inconsistency & data getting out of 'sync.' Analytics can help pinpoint stale or duplicate identities, ensuring data stays clean.

MULTIPLE IDPS & TENANTS WITHIN EACH IDP

The challenge of complexity as companies grow and the need for centralized insights through identity data analytics.

STALE ACCOUNTS, OVER-PROVISIONED IDENTITIES, ORPHANED USERS OVER-PROVISIONING

Without comprehensive identity data analytics, it's nearly impossible to detect patterns in stale accounts or over-provisioning, contributing to security vulnerabilities and operational inefficiency.

COMPLIANCE CHALLENGES

The challenge of complexity as companies grow and the need for centralized insights through identity data analytics.

Business Drivers

SECURITY

Poor configuration, over-provisioning, poor identity hygiene, and lack of usage data make for a large attack surface.

OPERATIONAL INEFFICIENCY

IT teams spend time increasing rights while Security teams manage excessive or unnecessary access rights. (Boat with 10k holes)

COMPLIANCE BURDEN

Manual processes and unreliable usage data for UARs increase non-compliance risks.

BUSINESS ENABLEMENT

Identity is at the core of operating today's business. Any issue or risk can affect the business.

Where Are You in the Maturity Journey?

INITIAL/BASIC STAGE

Manual processes, high risk, no visibility, and no oversight.

STANDARDIZED TO OPTIMIZED STAGES

Gradual introduction of automation, governance, SSO/MFA, and regular audits.

MANAGED TO ADVANCED STAGES

Fully automated IAM processes, continuous monitoring, proactive risk identification, and strong governance models.

Lessons from Business-Side Data Expertise

Data Fragmentation Isn’t New

- Business-side teams have historically dealt with fragmented data.
- The transference of data engineering concepts like identity data fabric to the identity domain is already happening, allowing identity data to be unified and analyzed holistically.

The Power of Usage Data for the Business

- Business teams rely on usage data to gain insights into behaviors and product effectiveness.
- Key Insight: Identity management can leverage usage data analytics to optimize how users interact with systems and identify active vs. unused permissions.

Applying Data Engineering Techniques to Identity

1. **Normalization**
   Normalizing identity data across disparate sources for actionable insights.
2. **Cross-domain Correlation**
   Using analytics to understand relationships between different datasets.
3. **Data Pipelines**
   Automating data flow and reducing manual processes.
4. **Analytics**
   Leveraging identity data analytics to track access patterns, spot inefficiencies, and predict potential security risks.
5. **Automation**
   Automating access reviews, compliance checks, and policy violation/enforcement processes.
6. **Improving Identity Hygiene**
   Apply identity data analytics to detect and remediate stale accounts and over-provisioned identities. (get idea over to Alina)
7. **Identity Data Fabric**
   Creating an interconnected data fabric to seamlessly integrate identity data from various sources, ensuring visibility, automation, and governance.

The Modernization of Identity Through Analytics

Transforming Chaotic Identity Data

From silos to actionable, unified data. Identity data analytics transforms fragmented data into insights that streamline operations and reduce risks.

Key Benefits for IT and Security Teams

1. **Proactive Intelligence**
   With identity data analytics, organizations can detect hidden risks and usage patterns that manual reviews often miss.

2. **Efficiency**
   Automate identity lifecycle management, like provisioning, de-provisioning, and access reviews.

3. **Stronger Security**
   Reduce the attack surface by proactively identifying vulnerabilities in real-time.

4. **Boosted Productivity**
   Simplified workflows, freeing up IT and Security teams to focus on strategic initiatives.

5. **Improved Identity Hygiene**
   Maintaining clean, accurate data by monitoring access patterns and identifying unused accounts.

6. **Identity Data Fabric**
   A modernized approach that integrates identity data analytics into a unified fabric, continuously adapting to meet business and security needs.

Real-World Examples:

Data-Driven Identity Solutions

Example 1

Risk Management Through Identity Analytics

An enterprise used identity data analytics to detect anomalous access patterns and over-provisioned accounts, automating access revocation to prevent future incidents.

Example 2

Automating Identity Processes

A company leveraged identity analytics to track user behavior, allowing for real-time adjustments to access rights and reducing over-provisioning.

Example 3

Implementing an Identity Data Fabric

A company built an "identity data fabric" to centralize, automate, and provide real-time visibility into identity data. This fabric improved their security posture, compliance, and operational efficiency.

Implementing Business-Side Data Solutions in Identity Management

In a Perfect World

Sure, in a perfect world, IT and Security teams could just walk over to the business side, grab a cup of coffee with the data engineering team, and solve all their identity woes together. But let's be honest-that's not going to happen. You're not getting their resources, and they're not suddenly going to become identity experts overnight.

The Real World

In the real world, you've got two options:

- Hire Your Own Data Engineers: If you have the budget (and the luck to find them), build your own data engineering team. They'll help you apply the same techniques business-side teams have been using for years.
- Expect More from Your Vendors: If hiring a team isn't realistic, it's time to start demanding these capabilities from the products you buy. The days of vendors selling you a shiny dashboard and calling it "analytics" are over. Expect real, data-driven solutions that integrate identity hygiene, usage analytics, and automated remediation. If they can't deliver, well, maybe it's time to find someone who can.

The Lesson

IT and Security can't afford to sit back and wait for miracles. You need to adopt the same rigor in identity that the business side uses for customer data. Whether that's through building teams or holding vendors accountable, it's your move.

The Future of Identity Management:

From Reactive to Proactive

01

Proven Techniques, Proven Tools

- The same tools and methodologies that have worked in business-side data can solve identity issues today.

02

Identity Data Fabric as a Vision

- A fully interconnected identity data fabric enables seamless, proactive identity management, making data retrieval seamless for faster decision-making.

03

Next-Gen Capabilities

- Generative Agents: purpose-built algorithms that can dynamically analyze identity datasets, providing intelligent recommendations and automating complex decision-making processes, transforming how organizations manage and secure identities
- Identity Autopilot: Continuously monitor for anomalies and suspicious behavior, instantly responding with pre-defined actions that neutralize risks.

Conclusion

Key Takeaways

Identity challenges are complex, but data engineering techniques can provide immediate and impactful solutions

Collaboration between data and identity teams is the key to moving from reactive to proactive identity management

Maturity stages provide a guide for where your organization should focus to make meaningful progress

The identity data fabric is a practical, achievable framework for unifying and automating identity data

Call to Action

Partner with data experts, if possible, but expect this type of capability for identity in the near-future.

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

Questions?