



CASE STUDY

Unifying Identity Security Across Hybrid Environments to Protect Systems & Data at Scale

EXECUTIVE SUMMARY

Autodesk unified identity visibility and observability across its cloud and on-premises environments using Permiso, gaining end-to-end visibility into all human and non-human identities. Prior to implementing Permiso, the Autodesk team had to manually stitch visibility and observability together across disparate point solutions. As their cloud footprint continued to expand, it was challenging to maintain integrations and continually develop ways to evaluate the identity fabric for exposures and threats.

Permiso enabled the security team to centrally manage and reduce identity risk, accelerate onboarding of new environments for risk analysis during M&A, and proactively protect critical infrastructure and intellectual property. With a single view across hybrid infrastructure, Autodesk transformed fragmented identity data into actionable insights. After implementing Permiso, they transformed their security posture: detecting identity threats faster, reducing alert fatigue significantly, and gaining complete visibility across their entire hybrid infrastructure. This transformation didn't just improve metrics; it protected their critical intellectual property and accelerated M&A integrations from weeks to minutes.



Company Overview

Autodesk is a multinational software company that develops and sells software for design, engineering, and entertainment. Their products are used in various industries, including architecture, engineering, construction, manufacturing, and media and entertainment. They have a complex environment spanning cloud platforms, on-premises systems, and dozens of SaaS applications. Its security challenges were magnified by rapid growth and a series of acquisitions, which introduced new identity sources, fragmented observability, and increased risk to intellectual property.



Challenges

Limited visibility into human and non-human identities across hybrid environments

Disjointed offboarding processes for privileged users

Visibility gaps in cloud-hosted and on-premises code collaboration tools

Difficulty onboarding and rapidly securing newly acquired entities

What Autodesk Needed

Centralized Comprehensive Inventory of all human, service, and machine identities across all environments

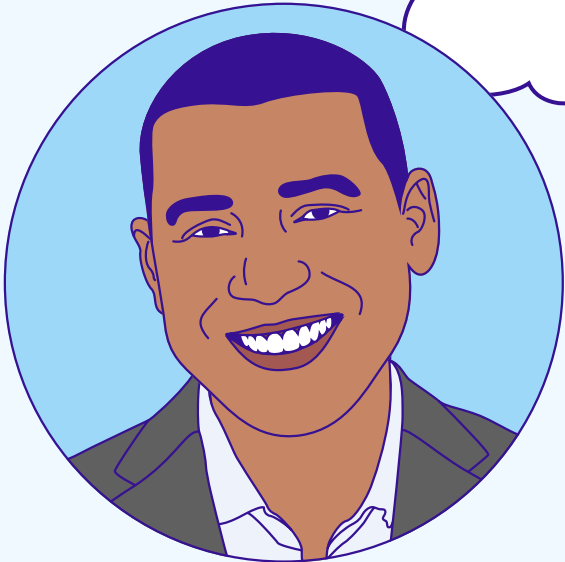
Continuous Posture Assessment to evaluate and reduce the identity attack surface

Threat Detection to monitor for identity misuse and compromise in real time with low noise and false positives

Automated Response to integrate identity alerts into SOAR/SIEM workflows

"Permiso gives us a unified view across all identities—human, non-human, on-premises, and cloud. That visibility is critical to securing our most sensitive data."

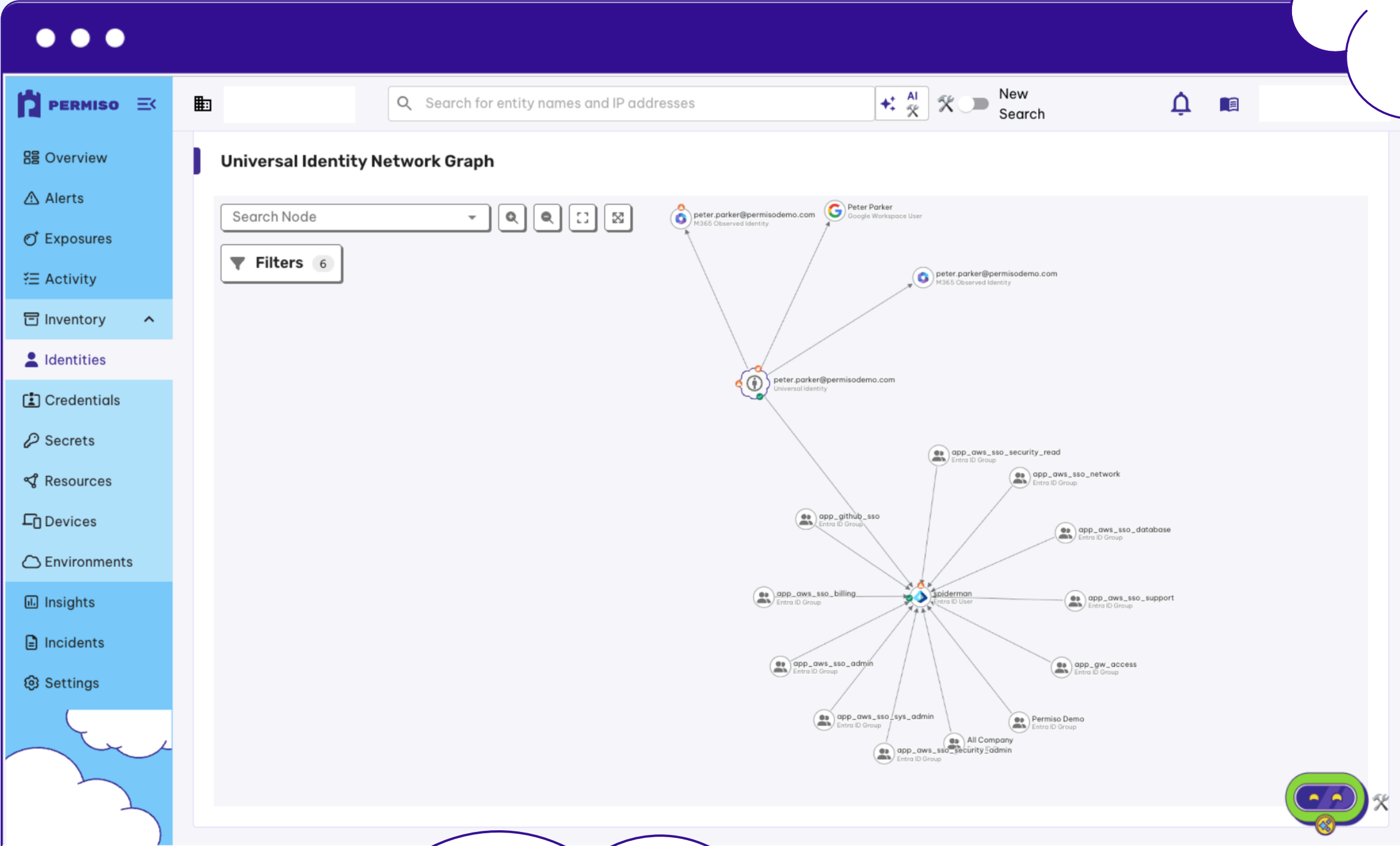
Sebastian Goodwin,
Chief Trust Officer, Autodesk





The Solution: Permiso Identity Security Platform

Challenge	Permiso Capability	Business Benefit
Siloed identity observability	Unified Identity Graph	End-to-end visibility across hybrid systems
IP data protection	Monitoring of SaaS and code platforms	Prevented unauthorized access and data theft
Risk-prone access & privilege sprawl	Posture scoring + privilege and key hygiene	Reduced attack surface & eliminated blind spots
M&A onboarding complexity	Rapid identity mapping + integration	Onboarded new entities in minutes
Insider threat and exit risk	Behavioral monitoring and offboarding insights	Prevented post-exit credential misuse





Why Autodesk chose Permiso

- ✓ **Specialized IP Protection:** Direct integrations with code repositories and collaboration tools to monitor critical collaboration platforms.
- ✓ **Unified Identity View:** Tracks human and non-human identities across IdPs, SaaS, cloud, and on-prem in a single console as opposed to point solutions for each.
- ✓ **Rapid Acquisition Support:** Enabled immediate risk visibility for newly acquired environments. Rapid onboarding allows for ease of deployment into new environments.
- ✓ **Dashboards for Identity Hygiene:** Delivered real-time views into posture, MFA usage, and privilege analysis.
- ✓ **Proven Expertise and Innovation:** Leading edge research in identity threats stemming from Mandiant heritage also served to augment their threat detection and engineering teams.
- ✓ **Low False Positive Rates:** Higher detection efficacy created lower false positive rates was a testament to Permiso's unique approach to correlating through identity attribution and sessions across layers.
- ✓ **Seamless Ecosystem Integration:** Integrated with existing SIEM and SOAR tooling to automate response workflows.

Results

- ✓ **Reduced risk of Intellectual Property exposure in applications**
- ✓ **Accelerated M&A identity integration from a period of weeks to matter of minutes**
- ✓ **Proactive detection of insider threats and credential misuse**
- ✓ **Implementation of key identity controls like configuration and use of phishing resistant MFA for admins**

"Whether it's credential compromise, account takeover, or insider threats, Permiso gives us the confidence to both detect and prevent identity-based attacks."

Raymond Winder,
Director of Information Security, Autodesk





PERMISO

Permiso discovers, protects, and defends human, non-human, and AI identities across cloud and on-premise environments, providing a comprehensive platform solution for your identity attack surface. Built on the Universal Identity Graph, the platform ingests data from across customer environments to deliver actionable insights and contextual alerts that help security teams understand their complete identity footprint. Permiso continuously identifies cross-environment exposures, visualizes identity attack paths, and prioritizes remediation actions to minimize risk. With over 1,500 built-in alert rules and advanced detection capabilities, the platform helps organizations monitor high-risk activities, prevent data loss, and respond effectively to modern identity-based attacks.

Clear the Clouds of Confusion

TRY PERMISO NOW

www.permiso.io