HushSecurity | Customer Success

Kiloverse extends IAM for machines, governing all agents and NHIs with Hush Security

> What drew us to Hush was the vision, moving away from secrets to identity-based access. But you can't govern what you can't see. Hush's runtime detection gave us complete visibility into our NHI and agentic AI systems, surfacing exploitable risks other tools completely missed."

Arturas Kesleris
Head of Security

Kiloverse

The Challenge

Kiloverse faced growing risk and operational overhead due to :

01 No centralized visibility and fragmented insight into non-human identities and secrets across the organization

02 Growing NHI blind spots that expanded the attack surface and violated compliance requirements

03 Secrets dispersed across cloud services, CI/CD pipelines, runtime environments, and AI workloads

04 Manual and time-intensive remediation workflows and rotation paralysis

05 Reliance on long-lived, secret-based access for databases such as PostgreSQL

Existing tools provided partial coverage and static snapshots, but lacked runtime context and actionable remediation.

The Solution

Kiloverse deployed Hush to control their NHI and agentic access and extend identity-based access to all critical systems for more secure and controlled access.

The deployment started with comprehensive, deep visibility and discovery across AWS, GCP, GitLab, Jira, Confluence, Slack, and AI workloads. Hush combined runtime detection with static analysis to validate exploitable risks across environments, allowing security teams to focus on what truly mattered, secrets and credentials actively in use that posed real threats.

With clear visibility established, Kiloverse began replacing secret-based access models with identity-based access policies, starting with PostgreSQL databases. By eliminating long-lived credentials and implementing just-in-time access, Kiloverse established a more secure, compliant, and scalable access model across its infrastructure.

Customer Overview

Kiloverse is a cloud-native technology company operating across AWS and Google Cloud, with a modern DevOps stack that includes AWS, GCP, GitLab, Kubernetes, Jira, Confluence, and Slack. The company also runs AI-driven workloads using Google Vertex AI, Mastra, and multiple LLM providers, including OpenAI and Anthropic.

As their modern environments scaled, the risk from rapidly evolving infrastructure grew. Kiloverse needed a fundamentally different approach to secure non-human identities and agentic systems at scale, one that wouldn't slow down engineering delivery.

Industry
Professional Services

Apps

Use cases

- Detect Leaked Secrets
- Gain NHI Runtime Visibility
- Apply Identity-Based Governance

Results and Business Impact

Kiloverse's security team was drowning in alerts from fragmented tools, unable to distinguish real risks from noise. Credentials were stored but not monitored or governed, rotation was challenging, and compliance audits required weeks of manual evidence gathering.

The Transformation:

Within 24 hours of self-deploying Hush Security

01 **From Blind to Visible**

Full inventory of non-human identities and secrets, the first complete view across AWS, GitLab, Kubernetes, and AI workloads.

02 **From Sprawl to Control**

Reduced exposed and stale secrets by 60%, with runtime validation ensuring every flagged risk was real and actionable.

03 **From Secrets to Identity**

Eliminated all long-lived PostgreSQL credentials, replacing them with just-in-time, identity-based access that reduced blast radius by ~ 90%.

04 **From Reactive to Proactive**

Shifted from investigating false positives to maintaining continuous compliance with real-time evidence generation.

Key Capabilities Deployed

Complete NHI inventory

Across cloud infrastructure, CI/CD pipelines, and agentic AI workloads

Runtime-validated risk detection

Surfaces only exploitable threats based on live usage

Identity-based access implementation

Beginning with PostgreSQL, to remove credential attack vectors

The Outcome

Kiloverse transformed its NHI security from a big blind spot into its strongest control. The security team moved from fighting fires to enforcing policy, engineering maintained velocity, and the company established a scalable foundation for secure cloud and AI innovation. By cutting the secret-based attack surface, eliminating operational burden, and dramatically reducing blast radius, Kiloverse saved significant security and engineering effort while lowering the risk of costly security incidents.

Securing AI-Driven Workloads

Hush Security provided visibility into the non-human identities and secrets used by Kiloverse's AI and LLM workloads, ensuring least-privilege, just-in-time access across Vertex AI, Mastra AI, OpenAI, Anthropic, and related services.

Executive Summary

Hush Security enabled Kiloverse to move from fragmented, static controls to a unified, real-time approach for securing non-human identities and secrets. By combining API-based integrations with runtime intelligence, Kiloverse reduced risk, improved operational efficiency, and established a scalable foundation for secure cloud and AI innovation.

> We eliminated all PostgreSQL credentials and replaced them with just-in-time policies. Our security posture improved dramatically while operational burden dropped 70%. Identity-based access for machines isn't just better security, it's the only scalable path forward."

Arturas Kesleris
Head of Security

Kiloverse