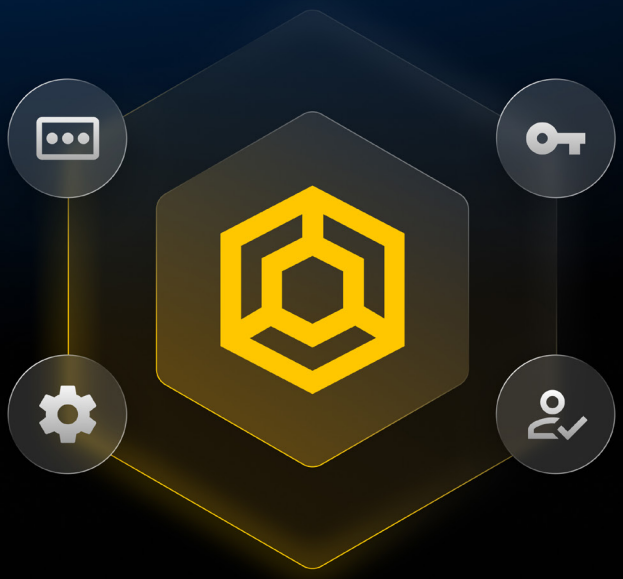
Case Study

Asite Secures Company-Wide Credentials, Secrets and Privileged Access With KeeperPAM®



Background

Asite is a SaaS company serving the construction industry, helping organisations manage complex projects — from 3D models and digital twins to document control and supplier collaboration — across global teams and regions. Asite operates across multiple geographies with data centres in nine locations and a workforce of 500+ employees.

Industry
Construction Technology (SaaS)

Employees
500+

Solutions
KeeperPAM

The Challenge

For a global SaaS business supporting major construction programmes, including customers operating in critical infrastructure and defence-adjacent environments, secure management of credentials and privileged access is essential. Asite needed a more centralised and enforceable approach to passwords, secrets and Privileged Access Management (PAM) across the organisation.

Legacy Tools With Fragmented Visibility - Reliance on browser-based password managers limited visibility and control, increasing risk through password reuse, weak credentials and a reduced ability to enforce security controls for compliance and customer assurance. The organisation's previous secrets management and PAM providers were costly and difficult to deploy.

Beyond securing internal users, Asite needed to extend the same level of protection to external partners and suppliers collaborating on complex construction projects, ensuring they met customer expectations and contractual obligations. The organisation sought a secure, easy-to-use solution that could support all its cybersecurity needs within a centralised platform.

> **"The (security) architecture and the flexibility with KeeperPAM is second to none."**
>
> **Tiago Rosado | Chief Information Security Officer**

The Keeper Solution

Asite selected **KeeperPAM** as its unified platform to secure privileged access, credentials, connections and secrets across the organisation. By consolidating its cybersecurity tech stack into a single zero-trust, zero-knowledge platform, Asite reduced complexity while enhancing security and compliance.

Centralised Privileged Access With Low Operational Overhead - KeeperPAM provides secure, auditable privileged access to servers, infrastructure and sensitive systems without exposing credentials. Session activity is centrally logged and recorded, supporting investigations, accountability and compliance across customer and regulatory environments. KeeperAI automatically terminates high-risk sessions and generates activity summaries with precise forensic detail for audit and incident response.

With fast deployment and a flexible architecture, KeeperPAM replaced both Asite's legacy PAM and secrets management tools while expanding privileged access coverage to additional systems without increasing cost or complexity.

> **"The deployment of KeeperPAM was extremely easy, one of the best in my experience. I wish other tools were as easy to deploy."**
>
> **Tiago Rosado | Chief Information Security Officer**

Enterprise Password Management, Built Into KeeperPAM - As part of the KeeperPAM platform, Asite standardised enterprise-wide **password management** for all employees, replacing browser-based password managers and establishing a centralised, enforceable approach to credential security.

This enabled admin-controlled password policies for length and complexity, and prevented credential reuse across applications. The IT team can now identify compromised credentials using Keeper's dark web monitoring tool, BreachWatch®, further strengthening the organisation's security posture. Accessing password management within the same vault as KeeperPAM ensures consistent governance across both end-user and privileged credentials, along with a simple user experience.

Modern Secrets Management With Keeper Secrets Manager - To protect application and infrastructure secrets, Asite deployed **Keeper Secrets Manager** as a native component of the KeeperPAM platform, replacing its previous secrets management tool. Keeper Secrets Manager automates the creation and rotation of passwords, keys and secrets, removes long-lived or manually managed credentials and integrates easily through **clear APIs and robust documentation**, all with minimal operational overhead for IT and security teams.

> **"The overhead is minimal ... the automation and rotation of passwords and keys is fantastic."**
>
> **Tiago Rosado | Chief Information Security Officer**

Managing secrets alongside passwords and privileged access within KeeperPAM enabled consistent governance across both human and non-human identities.

Best-in-Class Security - Keeper's zero-trust, zero-knowledge security architecture is unmatched at safeguarding information and mitigating the risk of a data breach. Keeper combines device-level, Elliptic-Curve Cryptography (ECC) with **multiple layers of encryption** (at the vault, folder and record levels), multi-factor and biometric authentication, as well as FIPS 140-3 validated AES 256-bit encryption plus PBKDF2. Keeper is **SOC 2 and ISO 27001 compliant** — with the longest-standing compliance in the industry — as well as FedRAMP High and GovRAMP Authorised.

Organisation Impact

By deploying Keeper's full PAM platform to enable password, secrets and privileged access management, Asite established a unified, scalable security framework that enhances protection while reducing operational complexity for its IT and security teams.

Improved Security Posture With Measurable Outcomes - Centralising credential and access management enabled Asite to significantly strengthen its overall security posture. Stronger password hygiene, automated secrets rotation and controlled privileged access reduced exposure to both external threats and insider risks. Credentials are no longer manually created, shared or reused, supporting consistent enforcement of security policies across the organisation.

Crucially, these controls are measurable and auditable, helping meet regulatory and contractual requirements across geographies and customer environments.

> **"The key benefits to the KeeperPAM platform would be reducing costs, reducing management of systems overhead, increasing compliance with security requirements and definitely increasing security posture."**
>
> **Tiago Rosado | Chief Information Security Officer**

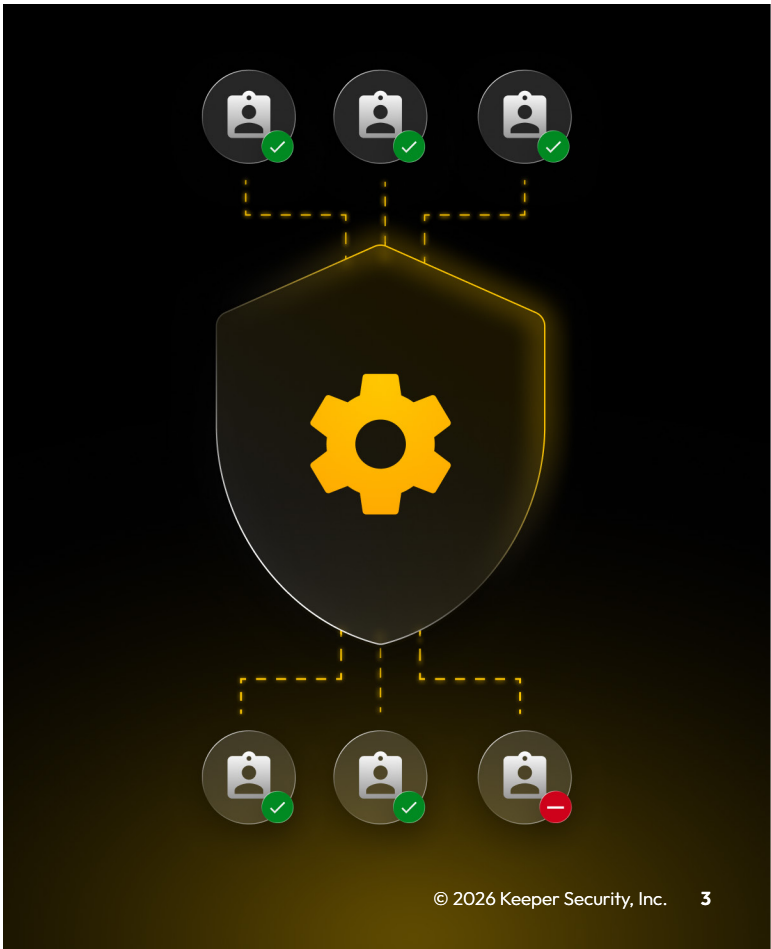
Reduced Operational Overhead and Tool Consolidation– By consolidating password management, secrets management and PAM into a single platform, Asite reduced tool sprawl and simplified administration, lowering operational overhead. This approach enabled lean IT and security teams to manage access controls more efficiently without increasing headcount or operational burden while scaling coverage to protect a broader range of systems and environments.

Lower Insider Risk Exposure and Stronger Accountability - With privileged access centrally governed and monitored, Asite strengthened its ability to detect, investigate and respond to high-risk activity. Session monitoring and audit trails support accountability and reduce the likelihood of misuse, whether intentional or accidental.

Ongoing Partnership and Enablement - Beyond technology, Asite highlighted the importance of dependable support and enablement throughout deployment and adoption. Keeper's support and enablement teams played a pivotal role in ensuring the platform was implemented effectively and aligned with the organisation's operational needs.

> **"The quality of support — even if it is the most technical question, they will do a deep dive [...] The training team [was] absolutely pivotal, tailoring the training to adapt to our reality."**
>
> **Tiago Rosado | Chief Information Security Officer**

KeeperPAM became the foundation of Asite's access security strategy, delivering centralised control over human and non-human identities across global environments. By bringing privileged access, password management and secrets management into a single platform, Asite strengthened security, improved operational efficiency and established a scalable foundation to support future growth.



KeeperPAM

KeeperPAM is a next-generation privileged access management platform that secures and manages access to critical resources, including servers, web apps, databases and workloads. Built on a zero-trust and zero-knowledge security architecture, KeeperPAM helps organisations of any size protect privileged accounts, enforce least privilege, secure remote infrastructure and meet compliance requirements, with unmatched ease of use and fast deployment.

Keeper is intuitive and easy to deploy, regardless of business size. KeeperPAM uses a zero-trust gateway service to access each environment. No firewall updates or ingress changes are needed, enabling seamless, secure access without complexity. With remote session capabilities, the user never has access to the credentials or SSH keys. Access to a resource can be time-limited, and credentials automatically rotate after access has been revoked, providing just-in-time (JIT) access without ever exposing credentials.

Keeper is designed to scale for organisations of any size. KeeperPAM centralises access in a single User Interface (UI) across multiple cloud providers, on-premises workloads and client environments, enabling multi-cloud management.

Business Use Cases: KeeperPAM

- Control and monitor all privileged accounts
- Provide JIT access without exposing credentials
- Consolidate development tools in one platform with an intuitive UI
- Enable seamless management of cloud, hybrid and multi-cloud environments
- Record multi-protocol sessions with AI threat detection and automated session termination
- Automate password rotation
- Enforce MFA protection on every system
- Deploy seamlessly via web or desktop app with automated SCIM provisioning

Protect your organisation with Keeper

To learn more about how Keeper can protect your organisation with an easy-to-use platform, **contact our sales team** for a free trial or personalised demo.

About Keeper

Keeper Security is one of the fastest-growing cybersecurity software companies that protects thousands of organisations and millions of people in over 150 countries. Keeper is a pioneer of zero-knowledge and zero-trust security built for any IT environment. Its core offering, KeeperPAM®, is an AI-enabled, cloud-native platform that protects all users, devices and infrastructure from cyber attacks. Recognised for its innovation in the Gartner Magic Quadrant for Privileged Access Management (PAM), Keeper secures passwords and passkeys, infrastructure secrets, remote connections and endpoints with role-based enforcement policies, least privilege and just-in-time access.

Keeper is trusted and loved by thousands of companies and millions of people globally.

Gartner

KeeperPAM® recognized in the 2025 Gartner Magic Quadrant™ for PAM

Cybersecurity Excellence Award **Privileged Access Management**

Cyber Defense Magazine **Editor's Choice – Privileged Access Management (PAM)**

Newsweek **#1 Cybersecurity Platform**

Enterprise Management Associates **KeeperPAM® recognized for product strength**