Securden

Case Study

How a Globally Distributed Technology Organization Transformed Privileged Access with Securden

From fragmented access to unified control: How Aspire Systems streamlined endpoint privilege management, credential management, and compliance with Securden Unified PAM.

Aspire Systems, a globally distributed technology organization, transformed its privileged access security by implementing Securden Unified PAM. Operating across isolated command centers in multiple regions, Aspire Systems required a unified, scalable, and secure solution to manage privileged access, enforce endpoint controls, and streamline compliance.

- Complete control over endpoint privileges
- Centralized visibility across distributed environments
- Streamlined IT operations and audit readiness
- Enhanced protection against credential misuse and unauthorized access

Over nearly four years, Securden has become a foundational component of Aspire System's IT security infrastructure.

aspire SYSTEMS

Chennai, Kochi, Poland, Mexico, Hyderabad

INDUSTRY

Technology-driven organization with globally distributed IT infrastructure

SOLUTION

Securden Unified PAM

KEY CHALLENGE

- Securing privileged access across completely isolated, geographically dispersed command centers

RESULTS

- Complete control over endpoint privileges
- Centralized visibility across distributed environments
- Streamlined IT operations and audit readiness
- Enhanced protection against credential misuse and unauthorized access

The Background

Aspire Systems is a globally distributed, technology services and consulting organization specializing in software engineering, digital transformation, testing, and infrastructure support. Founded in 1996, the company partners with enterprises and independent software vendors worldwide, helping them build, modernize, and

Globally Distributed Networks

Securing privileged access on endpoints in diversified networks with a unified solution.

manage business-critical applications and IT systems across industries such as banking, retail, insurance, and technology.

In its day-to-day operations, Aspire Systems teams are engaged in continuous software development, application modernization, cloud and infrastructure management, quality engineering, and round-the-clock support services. These functions require secure, seamless access to a wide range of systems, environments, and sensitive credentials across geographies. With a global customer base and a strong presence across multiple regions, ensuring consistent security and operational efficiency is critical to delivering reliable services.

The Challenge

To support its global delivery model, Aspire Systems operates a highly distributed IT ecosystem with command centers in Chennai, Kochi, Poland, Mexico, and Hyderabad. Each location functions as an independent operational hub, managing regional workloads, customer environments, and internal systems.

What makes AspireSys's infrastructure unique is the strict network isolation between these command centers.

"Kochi operates under a different command center, and Poland operates under a different command center," explains Arunachalam Shenkodi, a key stakeholder in the IT team. *"There is no network connectivity between these command centers. They function as completely separate entities from a network perspective."*

While this architecture enhances security and resilience, it also introduces complexity:

- Independent administrative teams per region
- Limited centralized visibility
- Hurdles in enforcing uniform security policies

The complexity created three major challenges:

Endpoint Privilege Control

Managing administrative rights across endpoints was a significant challenge. Users often had excessive privileges, leading to unauthorized software installations and increased exposure to security vulnerabilities.

"We had difficulty restricting the admin access in laptops and all endpoints, as well as controlling software installation," explains Arunachalam.

Security Gaps

The lack of centralized control created potential security gaps, making it difficult to enforce consistent password policies or maintain a clear picture of who had access to critical systems and when.

Compliance and Auditing Burden

Demonstrating compliance with internal security policies and external audit requirements was a manual, time-consuming process. The IT team spent countless hours compiling asset information and application access logs, often with incomplete data.

The Search for a PAM Solution

With clear goals in mind, Arunachalam and the AspireSys team began evaluating PAM solutions. Their requirements were specific and demanding:

- **A unified platform** that could address all their PAM needs—including endpoint privilege management—without requiring multiple disparate tools or complex integrations
- **Ease of use and implementation** to ensure quick adoption by IT teams and end-users across the organization
- **Robust security** with strong encryption, multi-layered access controls, and comprehensive audit capabilities
- **Asset management capabilities** to provide visibility into software details and hardware inventory

The team evaluated several enterprise-grade PAM solutions, carefully assessing each against their criteria. After a thorough evaluation, they concluded that Securden Unified PAM uniquely met all their requirements.

"We chose Securden because it offered all the features we needed in a single, cohesive package. The team also maintained excellent communication with us in every step of the evaluation. Other solutions we looked at required piecing together multiple components and had higher pricing which would have added complexity," points out Arunachalam Shenkodi.

"Securden has been with us for nearly four years, and it's been a positive experience throughout. The product works, the team is responsive, and we've never felt the need to look elsewhere."

ARUNACHALAM · IT TEAM · ASPIRE SYSTEMS

Finding the Ideal Solution in Securden Unified PAM

The decision to choose Securden was driven by its ability to deliver a comprehensive PAM experience out-of-the-box. The initial implementation was remarkably smooth and allowed the team to immediately take control of their privileged accounts and endpoints.

Comprehensive Endpoint Privilege Management

A key differentiator for AspireSys was Securden's robust endpoint privilege management capabilities. The solution provided granular control over admin access on all laptops and endpoints, effectively addressing their most pressing challenge.

"The endpoint control was a game-changer for us." Arunachalam emphasizes. *"Before Securden, we had significant difficulty restricting admin access and managing software installations. After implementing Securden, everything came under control. We can now precisely manage who can install software and what privileges users have on their endpoints."*

A Comprehensive and Unified Approach

Securden provided a single, integrated solution that combined all essential PAM capabilities—privileged account discovery, enterprise password vaulting, endpoint privilege management, session management and recording, access workflows, and detailed auditing. The ability to import existing credentials directly from disparate sources accelerated the onboarding process. *"We didn't have to start from scratch. The migration was straightforward, and we were up and running quickly with minimal disruption to our daily operations."*

Assets and Application Inventory

Another valuable capability that AspireSys leveraged was Securden's application control features. The solution automatically discovered and tracked software details across their environment, providing comprehensive visibility into their IT assets.

"It provides comprehensive reports on applications and assets, which is one of the key features," Arunachalam notes. *"We get detailed software information across all systems, which helps us maintain an accurate inventory and ensure compliance with licensing and security policies."*

Proven Reliability and Ease of Management

Over nearly four years, AspireSys has experienced firsthand the reliability and stability of the Securden platform. The solution has become an integral part of their daily operations, consistently delivering its promise of secure and efficient administrative access.

"Before Securden, we had significant difficulty restricting admin access and managing software installations. After implementing Securden, everything came under control. We can now precisely manage who can install software and what privileges users have on their endpoints."

The Securden Difference:

Enhanced Security, Operational Efficiency, Compliance Readiness and Full IT Visibility - All in One.

For AspireSys, Securden Unified PAM has been more than just a security tool—it has been a foundational component of their IT operations. Over the years, the benefits have been consistently realized across multiple dimensions of the business.

The most immediate and impactful benefit was gaining control over endpoints.

By centralizing and vaulting all privileged credentials, enforcing strong password policies, implementing granular access controls, and managing endpoint privileges, AspireSys has significantly reduced the risk of credential theft, unauthorized access, and potential insider threats.

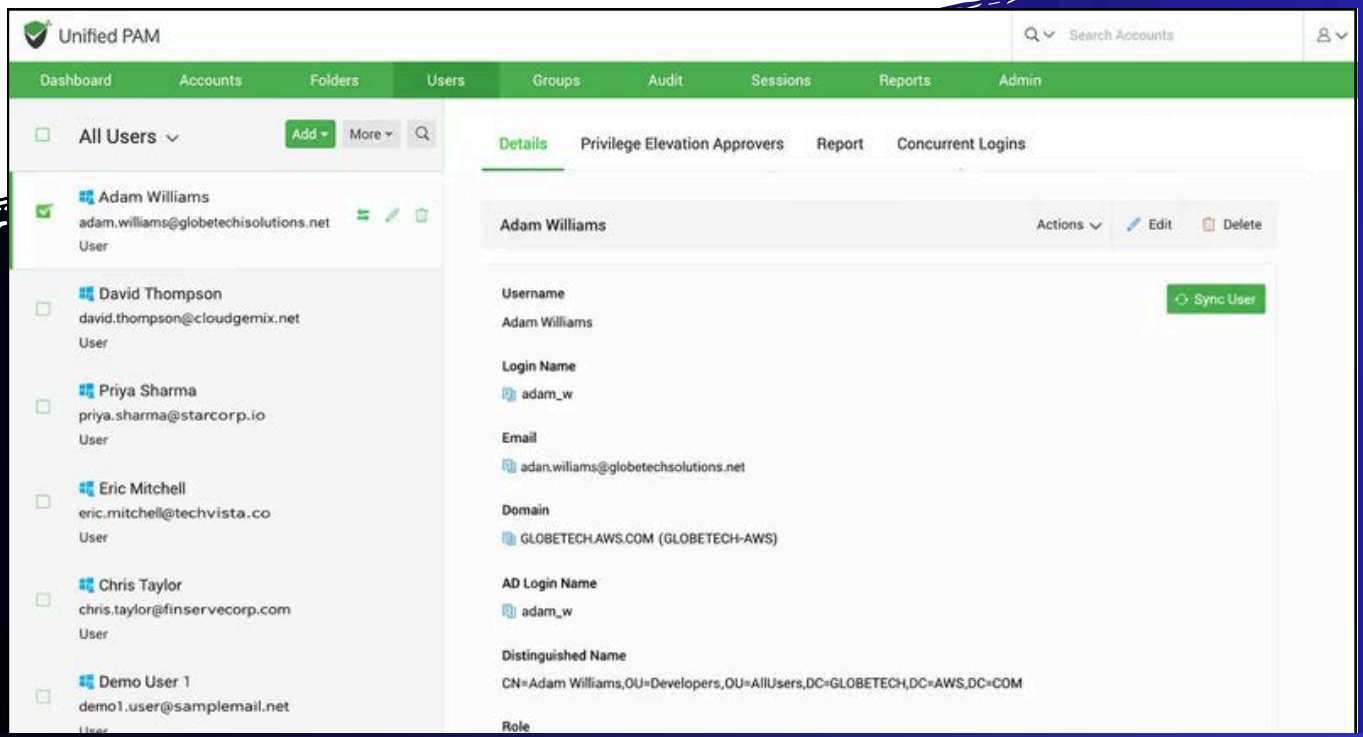
"What used to take hours now takes minutes. That efficiency gain has been tremendous," adds Arunachalam. Automated password management, simplified access request workflows, and a centralized interface have freed up valuable IT staff time.

Securden's comprehensive logging and detailed reporting capabilities have transformed AspireSys's approach to compliance and auditing —generating reports with just a few clicks.

The IT team now enjoys full visibility into all privileged activities across their infrastructure and endpoints, including exactly what software is installed and when.

Securden has helped AspireSys enforce consistent policies against password reuse, weak credentials, and unauthorized software installations.

"Everything that has been implemented in our environment works well. The features we use—endpoint privilege management, asset management, password vaulting—all deliver as expected. We're happy with the solution," points out Arunachalam.



A Partnership for the Long Haul

The Aspire System team's experience on using Securden has been overwhelmingly positive.

"The key point is that Securden has been with us for nearly four years, and it's been a positive experience throughout. The product works, the team is responsive, and we've never felt the need to look elsewhere," asserts Arunachalam Shenkodi.

Arunachalam also appreciates the opportunity to provide feedback for future enhancements. *"If there are any features that could be improved, we're happy to share our input,"* he mentions, highlighting the collaborative nature of the partnership.

"We found a solution that met our needs, and more importantly, a partner that has supported us consistently over the years. That's what makes the difference."

> *"Everything that has been implemented in our environment works well. The features we use—endpoint privilege management, asset management, password vaulting—all deliver as expected. We're happy with the solution"*

> *"The key point is that Securden has been with us for nearly four years, and it's been a positive experience throughout. The product works, the team is responsive, and we've never felt the need to look elsewhere."*