



CASE STUDY

Italian Digital Services Leader Streamlines Managed Services Workflows with Securden

By deploying Securden, Sanmarco Informatica established a secure, centralized, scalable foundation for managing enterprise and customer credentials, integrating access control into project workflows, meeting stringent compliance requirements, and improving managed services efficiency by more than 60%.

Background

Sanmarco Informatica is a leading Italian digital consulting and software solutions provider specializing in business process transformation and enterprise technology services. Serving over 2,500 customers with a workforce of more than 650 employees—including a dedicated R&D team of 200+ professionals—the company delivers secure, scalable, and high-performance digital services across industries

60%+

OPERATIONAL EFFICIENCY GAIN

3–5 hrs



Quick facts

COMPANY

Sanmarco Informatica

INDUSTRY

Digital Consulting, Enterprise Software, Managed IT Services

LOCATED IN

Italy

REQUIREMENT

- Centralized credential management across internal and customer environments
- Integration with internal project management workflows
- Stronger governance to meet ISO/IEC 27001 and NIS2 compliance

SOLUTION ADOPTED

Securden Password Vault for Enterprises

RESULTS

- 3–5 hours saved everyday through automated credential workflows
- 60%+ improvement in managed services operational efficiency
- Centralized visibility and control over credential usage
- Reduced human error with policy-based credential governance
- Improved audit readiness and compliance posture



Compliance with frameworks such as ISO/IEC 27001 and NIS2 is central to Sanmarco Informatica's operating model, placing heightened responsibility on the protection of credentials, access paths, and critical systems. As a provider of Managed IT services, Cybersecurity solutions, and B2B support, the company manages privileged access not only within its own infrastructure, but also across customer environments.

This dual responsibility—securing both internal operations and client environments—requires enterprise-grade credential governance at scale. As Sanmarco Informatica expanded its managed services portfolio, strengthening credential protection while preserving operational efficiency became a strategic priority.

The Challenge: Scaling Access Governance without Slowing Delivery

As Sanmarco Informatica's operations scaled, multiple teams—including managed services engineers, cybersecurity specialists, technical architects, and developers—needed access to an increasing number of privileged, service, and application credentials to perform their daily work. These credentials spanned internal infrastructure, customer environments, and third-party platforms.

“We were dealing with credentials every day—privileged accounts, service users, application access—across many teams and customer environments,” explains Elisabetta Viero Chief Information Officer (CIO) at Sanmarco Informatica. “The volume kept growing, and it was becoming harder to clearly track who had access to what.”

While credentials were stored securely, access governance processes remained largely manual. Provisioning, approvals, and revocation workflows operated separately from day-to-day service execution. As projects evolved and responsibilities shifted, access updates often required manual intervention resulting in delays and inconsistencies,

“In practice, work moved forward through our internal project management system (TWP), but access didn't,” the CIO adds. “Projects progressed, tasks changed hands, but credential access still had to be requested and cleaned up manually.”

As managed services engagements increased, this disconnect began affecting efficiency. Manual access handling introduced delays, increased the potential for errors, and limited centralized visibility into credential usage across customer environments.

Sanmarco Informatica needed a structured, scalable approach to credential governance—one that could improve visibility and control while aligning access more closely with how work was actually executed.

The Hunt for an Enterprise Grade Solution with Workflow Integration

Sanmarco Informatica's IT team evaluated multiple password and access management solutions to address growing operational and governance challenges across managed services and software delivery teams. Their evaluation was driven by a clear set of non-negotiable requirements shaped by their managed services model and compliance obligations.

The solution needed to:

- ✓ Support on-premises deployment, with flexibility for future cloud migration
- ✓ Be optimized for software companies and managed services workflows, rather than a password storage tool
- ✓ Enable secure, team-based credential sharing across departments
- ✓ Provide approval workflows with temporary and expiring access
- ✓ Offer ease of use for both technical and non-technical teams

Beyond core functionality, architectural strength and scalability were critical.

The team prioritized:

- ✓ A robust, secure database architecture suitable for enterprise use
- ✓ API-driven integration capabilities to embed credential workflows into internal systems
- ✓ Scalability to support continued managed services growth

- ✓ Strong price-to-value alignment without sacrificing capability

After a thorough evaluation, Sanmarco Informatica selected Securden as the best fit for its operational and compliance requirements. Securden met every core requirement while offering the flexibility, automation, and governance needed for large-scale managed services operations.

“The setup was straightforward, and the value was clear very quickly,” says Elisabetta. “The product was easy to deploy, the configuration was simple, and the support team worked closely with us on integrations and automation. That made leadership buy-in easy from the start.”

The Securden difference

Securden distinguished itself not only by meeting functional requirements, but by aligning credential governance with the realities of managed services delivery. The platform could operate on-premises or in the cloud, with the freedom to migrate as needs evolved—an important consideration for a growing managed services provider.

Custom Credential Models for Complex Environments

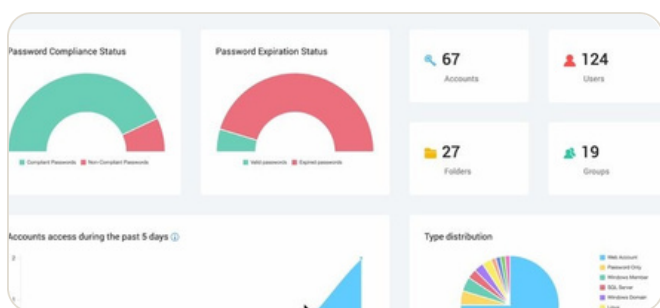
Sanmarco Informatica manages access across diverse systems and customer infrastructures, each with distinct authentication requirements. Securden's support for custom account types and application-specific credential models enabled the organization to standardize governance while accommodating varied platforms and use cases.

Rather than forcing rigid workflows, the platform adapted to existing operational structures.

Granular Access Control with Built-In Approvals

Securden's granular role-based controls and approval workflows strengthened governance across teams and engagements. Temporary and expiring access policies ensured credentials were granted only for the required duration, reducing risk while preserving agility.

This capability proved especially valuable for support teams operating across multiple customer environments simultaneously.



Centralised credential governance across internal and customer estates.

API-Driven Automation and Workflow Integration as Force Multipliers

Automation became a key force multiplier.

Using Securden's APIs, Sanmarco Informatica embedded credential workflows directly into its internal project management platform (TWP). Daily automation scripts streamlined provisioning, approvals, and revocation processes—eliminating repetitive manual tasks and ensuring access updates remained synchronized with project changes.

Access control became integrated into how work was executed, not managed as a separate administrative layer.

“What really worked for us was the platform's flexibility,” Elisabetta explains.

“We deal with many different systems and custom applications, and Securden allowed us to model access in a way that matched our environments. The API integrations helped us eliminate a significant amount of manual work—we weren't forced into rigid workflows.”

Strengthened Compliance and Audit Readiness

From a security perspective, Securden reinforced Sanmarco Informatica's compliance posture. Features such as LDAP integration, advanced authentication mechanisms, detailed audit logs, and strong database security architecture supported ongoing alignment with ISO/IEC 27001 and NIS2 obligations.

The availability of an on-premises deployment model, along with secure desktop applications, further enhanced control over sensitive credentials within regulated environments.

“The support experience made a real difference,” Elisabetta adds. “From setup to integrations and automation, the Securden team worked closely with us and responded quickly whenever we needed help. It felt like a partnership built around understanding our environment and priorities.”

Ease of Deployment and Rollout

From a deployment and adoption standpoint, Securden proved easy to implement and quick to deliver value. The installation and configuration process was straightforward, and Securden's support team worked closely with Sanmarco Informatica on integrations, automation scripts, and custom feature requirements.

This collaborative approach accelerated leadership buy-in, as tangible benefits were visible early in the rollout.

Securden serves Sanmarco Informatica as a centralized access governance and brokering platform, supporting custom applications, service workflows, and stringent compliance requirements.

Results and Impact: Efficiency, Security, and Compliance

By centralizing credential governance and embedding access control into operational workflows, Sanmarco Informatica achieved measurable improvements across managed services delivery:

- ✓ 3–5 hours saved per day through automated credential provisioning, approvals, and revocation
- ✓ Over 60% improvement in operational efficiency, driven by workflow-integrated access control

- ✓ Reduced risk of human error through centralized, policy-based credential governance

- ✓ Improved visibility and audit readiness, with detailed tracking of credential access and usage

- ✓ Strengthened compliance alignment with ISO/IEC 27001 and NIS2—without adding operational overhead

What was once a manual, fragmented process is now a centralized, automated governance framework aligned with how work is actually executed.

By integrating credential management directly into service workflows, Sanmarco Informatica established a secure, scalable foundation capable of supporting continued growth in enterprise and managed services operations—without compromising compliance, visibility, or efficiency.

60%+

EFFICIENCY GAIN

3–5 hrs

SAVED EVERY DAY

2,500+

CUSTOMERS SERVED

650+

EMPLOYEES



“

The support experience made a real difference. From setup to integrations and automation, the Securden team worked closely with us and responded quickly whenever we needed help. It felt like a partnership built around understanding our environment and priorities.

ELISABETTA VIERO, CHIEF INFORMATION OFFICER, SANMARCO INFORMATICA

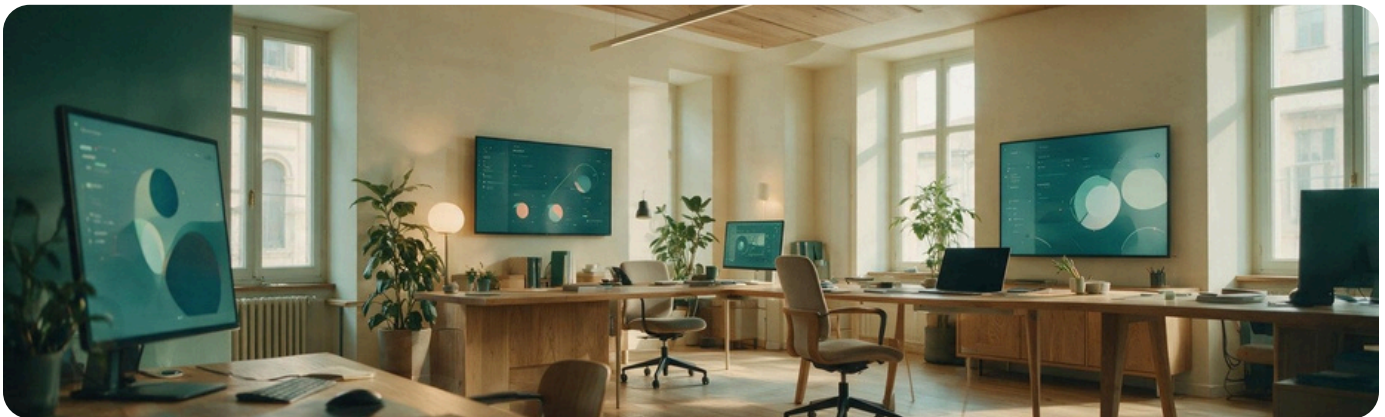
About Securden

Securden is a leading provider of privileged access governance solutions that holistically combines the principle of least privilege with other critical security principles such as zero-trust and provide visibility into privileged activities to continuously monitor cyber risk to effectively prevent cyberattacks, malware & ransomware propagation, and insider exploitation.

With simplicity and robustness in its core design, Securden offers a refreshing and intuitive panel of controls to govern privileged access across cloud, physical, and virtual environments. Here is a quick list of Securden's offerings:

- Password Vault for Enterprises
- Endpoint Privilege Manager
- Unified PAM
- Vendor PAM
- UnifiedPAM forMSPs
- Password Self-Service
- Secure Remote Access

The products have been built to be extremely scalable and secure. Securden is trusted by small businesses and large enterprises such as large banking and financial services, manufacturing companies, government agencies, healthcare organizations, managed IT service providers, educational institutions, and security service provider. To learn more, visit www.securden.com



Enforce tight password security without slowing down operations

[REQUEST A DEMO](#)

Try Securden Password Vault for Enterprises.