Netdata®

CYBERSECURITY

How to Strengthen Privileged Access Security in Critical Infrastructures

+10 critical platforms integrated

ISO 27001 compliance

Project delivered 1.5 months ahead of schedule

Netdata®

Challenge

A leading company in the energy sector, responsible for operating highly sensitive critical infrastructure, faced the challenge of strengthening its protection strategy for privileged accounts used by administrators, operators, and technology teams within its technology ecosystem.

Before the project, the organization did not have a centralized platform for privileged access management, which created limitations in terms of visibility, auditing, credential control, and traceability of administrative actions over critical resources.

The associated risk was significant: the potential exposure or compromise of a privileged account could allow access to servers, network devices, cloud platforms, security tools, and systems that are fundamental to the operational continuity of the business.

Additionally, the organization needed to strengthen its access control capabilities to respond to requirements associated with ISO 27001 compliance, particularly in areas related to password management, privilege control, auditing, and operational security.

The absence of a centralized model increased the likelihood of security incidents, reputational risks, economic impact, and potential regulatory non-compliance.

Netdata®

Process

The project began with a detailed assessment of the organization's technology environment and critical platforms.

The implementation followed a structured methodology based on phases of discovery, architecture design, requirements definition, configuration, validation, and go-live.

During execution, executive follow-up sessions and dedicated technical meetings were established for configurations, integrations, and operational validations.

As part of the project closure, the team consolidated AS BUILT technical documentation, transferred knowledge to the client's administrator, and completed onboarding to the support service to ensure operational continuity after implementation.

Netdata®

Solution

A privileged access management architecture based on Privilege Cloud was implemented, designed to centralize administrative credentials, strengthen security controls, and reduce the risks associated with the use of elevated privileges.

The solution enabled capabilities such as:

Centralized custody of privileged credentials.	Complete auditing of administrative actions.	Automatic and continuous password rotation.	Visibility and monitoring of critical access.	Recording and logging of administrative sessions.

As part of the project, integrations were carried out with different components of the client's technology ecosystem, including:

Microsoft Entra ID | Plataformas SIEM
Google Cloud Platform | Microsoft Azure

Through the Secure Cloud Access module, the organization implemented Just-In-Time access and ephemeral access models, avoiding permanent administrative permissions and strengthening security across cloud environments.

The solution also integrated key platforms within the operational and security environment, including:

- IBM QRadar
- Cisco
- Fortinet / FortiAnalyzer
- Aruba
- VMware
- NetApp
- Veeam Cloud

In response to limitations in standard market connectors, the team developed custom integrations for specific platforms such as VMware, NetApp, and Veeam Cloud, delivering these capabilities as added value within the project.

Netdata®

Tangible Results

+10 critical platforms integrated under a unified privileged access model

The solution enabled centralized control, auditing, and monitoring across a diverse technology ecosystem that integrated more than 10 critical infrastructure, cloud, networking, security, virtualization, and backup platforms, including Microsoft environments, Google Cloud, IBM QRadar, Cisco, Fortinet, Aruba, VMware, NetApp, and Veeam.

Regulatory objectives achieved

The implementation strengthened security controls associated with privilege management and supported requirements linked to ISO 27001 compliance.

Greater control and visibility over critical access

The organization gained centralized traceability over administrative accounts, access, sessions, and activities executed across critical infrastructure.

Reduced risks associated with privileged credentials

The adoption of automatic rotation, centralized storage, and controlled access reduced exposure to scenarios involving credential theft, reuse, or misuse.

Project delivered ahead of schedule

The implementation was successfully completed one and a half months ahead of the projected timeline, accelerating the adoption of security capabilities for the client.

Client Testimonial

"The implementation significantly strengthened our privileged access management, increasing visibility, control, and traceability across critical infrastructure. We especially value the team's commitment, flexibility, and technical capabilities throughout the entire project."

Technology and Security Area

Conclusion

Protecting privileged access is not solved solely through credential storage. This case demonstrates that the combination of PAM, just-in-time access, advanced integrations, and custom developments transforms privilege management into a strategic capability for security and compliance.

Netdata understands the challenges associated with critical infrastructure, hybrid environments, and multicloud architectures. Its experience integrating complex platforms and developing connectors adapted to specific requirements reduces implementation times, accelerates technology adoption, and strengthens the operational resilience of organizations.

Netdata®

www.netdatanetworks.com