Netdata®

CYBERSECURITY

Caso de éxito

Cómo fortalecer la seguridad de accesos privilegiados en infraestructura crítica

+10 plataformas
críticas integradas

Cumplimiento de normativa
ISO 27001

Proyecto entregado 1,5 meses
antes de lo previsto

Desafío

Una compañía líder del sector energético, responsable de operar infraestructura crítica de alta sensibilidad, enfrentaba el desafío de fortalecer su estrategia de protección sobre cuentas privilegiadas utilizadas por administradores, operadores y equipos de tecnología dentro de su ecosistema tecnológico.

Antes del proyecto, la organización no contaba con una plataforma centralizada para la gestión de accesos privilegiados, lo que generaba limitaciones en materia de visibilidad, auditoría, control de credenciales y trazabilidad de acciones administrativas sobre recursos críticos.

El riesgo asociado era significativo: la eventual exposición o compromiso de una cuenta privilegiada podía permitir acceso a servidores, dispositivos de red, plataformas cloud, herramientas de seguridad y sistemas fundamentales para la continuidad operacional del negocio.

Adicionalmente, la organización requería robustecer sus capacidades de control de acceso para responder a exigencias asociadas al cumplimiento de ISO 27001, particularmente en materias relacionadas con gestión de contraseñas, control de privilegios, auditoría y seguridad operacional.

La ausencia de un modelo centralizado incrementaba la probabilidad de incidentes de seguridad, riesgos reputacionales, impactos económicos y posibles incumplimientos regulatorios.

Netdata®

Proceso

El proyecto inició con un levantamiento detallado del entorno tecnológico y de las plataformas críticas utilizadas por la organización.

La implementación siguió una metodología estructurada basada en fases de entendimiento, diseño de arquitectura, definición de requerimientos, configuración, validación y puesta en marcha.

Durante la ejecución se establecieron sesiones ejecutivas de seguimiento y espacios técnicos dedicados a configuraciones, integraciones y validaciones operativas.

Como parte del cierre, el equipo consolidó documentación técnica AS BUILT, realizó transferencia de conocimiento al administrador del cliente y ejecutó onboarding al servicio de soporte para garantizar continuidad operativa posterior a la implementación.

Netdata®

Solución

Se implementó una arquitectura de **gestión de accesos privilegiados basada en Privilege Cloud**, diseñada para centralizar credenciales administrativas, fortalecer los controles de seguridad y reducir los riesgos asociados al uso de privilegios elevados.

La solución permitió incorporar capacidades de:

Custodia centralizada de credenciales privilegiadas.	Auditoría completa sobre acciones administrativas.	Rotación automática y continua de contraseñas.	Visibilidad y monitoreo de accesos críticos.	Registro y grabación de sesiones administrativas.

Como parte del proyecto se realizaron integraciones con distintos componentes del ecosistema tecnológico del cliente, incluyendo:

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

A través del módulo **Secure Cloud Access**, la organización implementó esquemas de **acceso justo a tiempo (Just-In-Time)** y accesos efímeros, evitando permisos administrativos permanentes y fortaleciendo la seguridad sobre entornos cloud.

La solución también integró plataformas clave del entorno operativo y de seguridad, incluyendo:

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

Frente a limitaciones propias de conectores estándar del mercado, el equipo desarrolló **integraciones personalizadas** para plataformas específicas como **VMware, NetApp y Veeam Cloud**, entregando estas capacidades como valor agregado dentro del proyecto.

Resultados Tangibles

+10 plataformas críticas integradas bajo un modelo unificado de acceso privilegiado

La solución permitió centralizar el control, auditoría y monitoreo sobre un ecosistema tecnológico diverso que integró más de 10 plataformas críticas de infraestructura, cloud, networking, seguridad, virtualización y respaldo, incluyendo entornos Microsoft, Google Cloud, IBM QRadar, Cisco, Fortinet, Aruba, VMware, NetApp y Veeam.

Cumplimiento de objetivos regulatorios

La implementación permitió fortalecer los controles de seguridad asociados a gestión de privilegios y apoyar los requerimientos vinculados al cumplimiento de ISO 27001.

Mayor control y visibilidad sobre accesos críticos

La organización obtuvo trazabilidad centralizada sobre cuentas administrativas, accesos, sesiones y actividades ejecutadas sobre infraestructura crítica.

Reducción de riesgos asociados a credenciales privilegiadas

La adopción de rotación automática, almacenamiento centralizado y accesos controlados disminuyó la exposición frente a escenarios de robo, reutilización o mal uso de credenciales.

Proyecto entregado anticipadamente

La implementación fue finalizada exitosamente un mes y medio antes del cronograma proyectado, acelerando la adopción de capacidades de seguridad para el cliente.

Testimonio del Cliente

"La implementación permitió fortalecer significativamente nuestra gestión de accesos privilegiados, aumentando la visibilidad, control y trazabilidad sobre infraestructura crítica. Destacamos especialmente el compromiso, flexibilidad y capacidad técnica del equipo durante todo el proyecto."

Área de Tecnología y Seguridad.

Conclusión

La protección de accesos privilegiados no se resuelve únicamente con almacenamiento de credenciales. Este caso demuestra que la combinación de PAM, accesos Just-In-Time, integraciones avanzadas y desarrollos personalizados transforma la gestión de privilegios en una capacidad estratégica de seguridad y cumplimiento.

Netdata conoce los desafíos asociados a infraestructuras críticas, entornos híbridos y arquitecturas multicloud. La experiencia integrando plataformas complejas y desarrollando conectores adaptados a requerimientos específicos reduce tiempos de implementación, acelera la adopción tecnológica y fortalece la resiliencia operacional de las organizaciones.

Netdata®

www.netdatanetworks.com