Netdata®

CYBERSECURITY

Caso de éxito

Cómo una empresa industrial obtuvo visibilidad sobre cada acción ejecutada dentro de sus plataformas cloud

Desafío

Tener MFA no significa saber qué ocurre dentro de cloud.

La transformación digital ha cambiado profundamente la forma en que las organizaciones administran su infraestructura tecnológica.

En entornos industriales modernos, las plataformas cloud ya no son únicamente servicios complementarios: sostienen componentes críticos de administración, seguridad, operación e integración tecnológica.

Para una importante organización industrial latinoamericana, esto planteaba un desafío creciente.

La compañía contaba con controles maduros de autenticación, incluyendo Single Sign-On y Multi-Factor Authentication. Sin embargo, su equipo identificó una brecha importante dentro de su postura de seguridad:

los accesos estaban protegidos, pero las actividades realizadas dentro de las consolas cloud permanecían con visibilidad limitada.

Administradores internos, equipos especializados y proveedores externos podían ingresar a plataformas críticas y ejecutar acciones sensibles sin un mecanismo robusto de registro detallado, evidencia operacional o trazabilidad completa.

Netdata®

Preguntas simples se volvían difíciles de responder:

¿Quién cambió esta configuración?
¿Qué acciones ejecutó un proveedor externo?
¿Qué ocurrió exactamente dentro de una sesión administrativa?
¿Existe evidencia verificable sobre las operaciones realizadas?

En un entorno donde múltiples plataformas cloud forman parte del ecosistema tecnológico, esa falta de visibilidad representa mucho más que una necesidad técnica: implica riesgos de gobernanza, control operacional y capacidad de investigación frente a incidentes potenciales.

El desafío no terminaba allí.

La arquitectura tecnológica existente dependía de un proveedor de identidad específico, generando restricciones adicionales para integrar correctamente las capacidades de auditoría requeridas.

El proyecto necesitaba resolver simultáneamente visibilidad, auditoría, identidad e integración arquitectónica.

Solución

Construyendo una capa de observabilidad sobre accesos privilegiados cloud.

Para responder al desafío, se diseñó una arquitectura especializada orientada a identidad, auditoría y control de actividad administrativa cloud.

La solución combinó:

Secure Cloud Access:

para fortalecer el control y supervisión de accesos hacia plataformas cloud críticas.

Cyber Identity:

para soportar el modelo de identidad requerido por el entorno tecnológico.

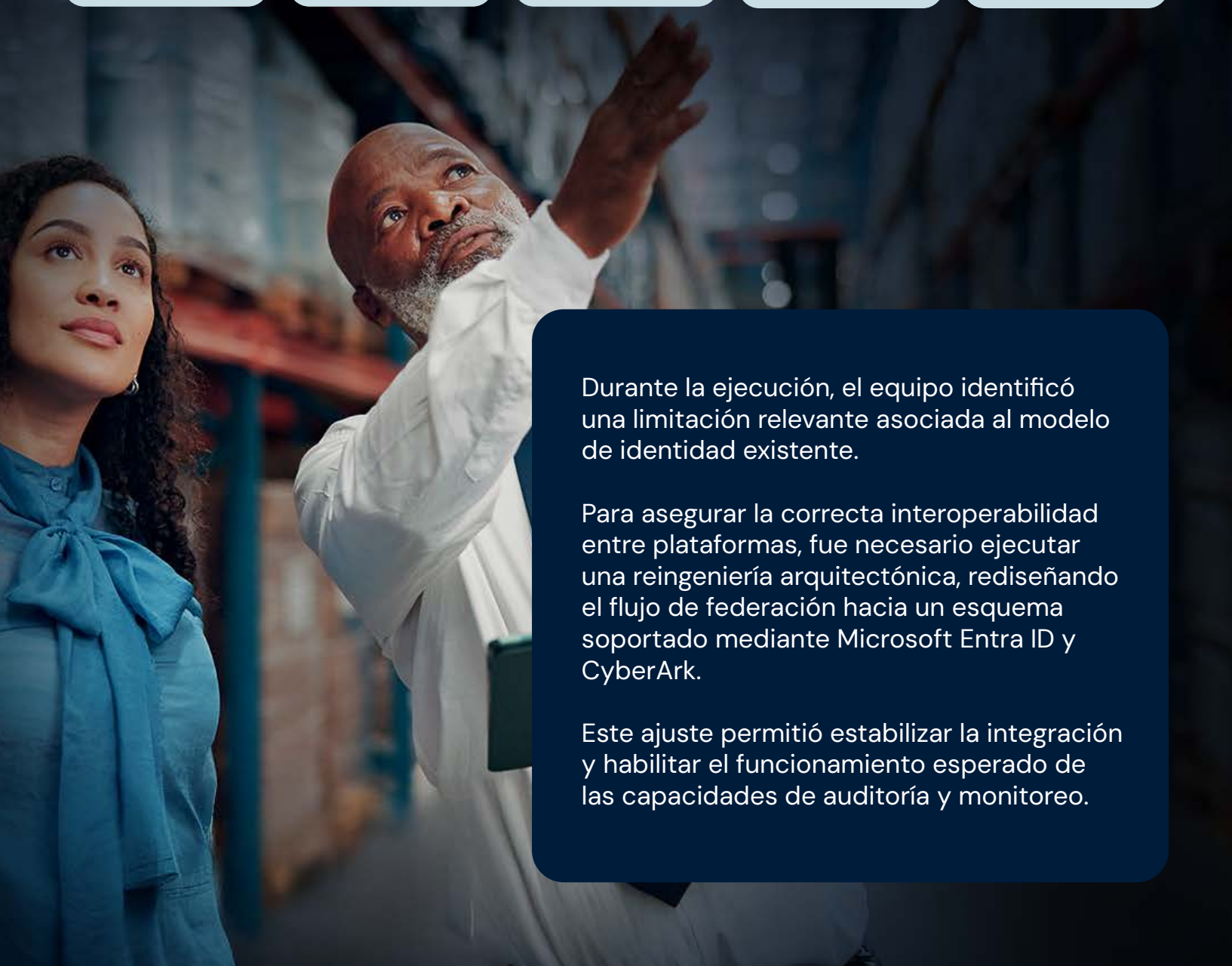
Secure Web Session:

para capturar, grabar y auditar las actividades ejecutadas dentro de sesiones administrativas

Netdata®

La implementación se desarrolló durante aproximadamente tres meses, siguiendo una metodología estructurada basada en:

- Levantamiento técnico y entendimiento del entorno
- Diseño arquitectónico
- Configuración e integraciones
- Pruebas funcionales
- Transición a producción



Durante la ejecución, el equipo identificó una limitación relevante asociada al modelo de identidad existente.

Para asegurar la correcta interoperabilidad entre plataformas, fue necesario ejecutar una reingeniería arquitectónica, rediseñando el flujo de federación hacia un esquema soportado mediante Microsoft Entra ID y CyberArk.

Este ajuste permitió estabilizar la integración y habilitar el funcionamiento esperado de las capacidades de auditoría y monitoreo.

Resultados Tangibles

De acceso autenticado a evidencia completa sobre actividad administrativa.

+10 plataformas críticas integradas bajo auditoría centralizada

La organización integró inicialmente 10 plataformas cloud dentro del nuevo modelo de custodia y monitoreo.

Posteriormente, el servicio continuo permitió expandir el alcance incorporando seis plataformas adicionales, aumentando progresivamente la cobertura del entorno protegido.

Visibilidad detallada sobre sesiones administrativas.

La implementación entregó capacidades que anteriormente no estaban disponibles para el cliente:

- Grabación de sesiones administrativas web.
- Auditoría de actividades ejecutadas dentro de consolas cloud.
- Evidencia sobre acciones realizadas por administradores y terceros.
- Trazabilidad operacional sobre cambios y operaciones sensibles.

El resultado fue un cambio de paradigma: pasar de saber quién accede, a comprender qué sucede realmente después del acceso.

Arquitectura optimizada para integración segura

La reingeniería basada en Entra ID + CyberArk permitió superar restricciones de diseño preexistentes y establecer un modelo de integración alineado con la complejidad tecnológica del cliente.

Customer Success como capacidad operativa continua

El proyecto evolucionó más allá de una implementación puntual.

Posteriormente, el cliente adoptó un modelo de acompañamiento técnico continuo, donde un ingeniero dedicado trabaja semanalmente en:

- Nuevas integraciones
- Recomendaciones técnicas
- Optimización de configuraciones
- Evolución del entorno protegido

Este modelo permitió mantener estabilidad operativa con un enfoque preventivo, registrando únicamente dos tickets de soporte durante la etapa posterior a implementación.

Netdata®

Testimonio del Cliente

"La implementación nos permitió incorporar un nivel de visibilidad que antes no teníamos sobre nuestros entornos cloud. Hoy contamos con mayor capacidad para auditar accesos administrativos, registrar actividades ejecutadas dentro de nuestras plataformas y fortalecer el control sobre operaciones realizadas por distintos actores del ecosistema tecnológico.

Más allá de la tecnología, destacamos el acompañamiento técnico del equipo, su capacidad para adaptarse a los desafíos de arquitectura y el enfoque continuo de mejora posterior a la implementación."

Área de Tecnología y Seguridad.

Conclusión

La seguridad cloud moderna ya no se limita a autenticar usuarios.

Las organizaciones necesitan responder una pregunta mucho más compleja: qué sucede realmente dentro de sus plataformas una vez que el acceso ha sido autorizado.

Este caso demuestra cómo una estrategia basada en auditoría de sesiones, gobierno de accesos privilegiados, identidad federada y acompañamiento técnico continuo puede transformar un entorno con visibilidad parcial en un modelo operativo basado en trazabilidad, evidencia y control administrativo sobre plataformas cloud críticas.

La combinación de Secure Cloud Access, Cyber Identity y Secure Web Session permitió fortalecer no solo el acceso, sino también la capacidad de observar, registrar y comprender las actividades ejecutadas dentro del entorno tecnológico.

Netdata conoce los desafíos asociados a arquitecturas híbridas, modelos complejos de identidad y operaciones cloud en evolución constante. La experiencia integrando plataformas, resolviendo restricciones arquitectónicas y acompañando la madurez operacional de sus clientes permite acelerar implementaciones complejas y convertir la seguridad cloud en una capacidad continua de gobernanza y control.

Netdata®

www.netdatanetworks.com