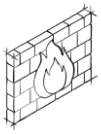
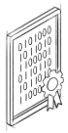
ARDEXA

POR QUÉ ARDEXA ES LIDER EN CIBERSEGURIDAD

NUESTROS PRINCIPIOS CLAVE PARA TODOS LOS SECTORES INDUSTRIALES



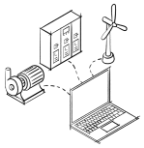
NO ABRA LAS REDES DE LA PLANTA O DE LA MÁQUINA A INTERNET



UTILIZAR CERTIFICADOS DIGITALES PARA IDENTIFICAR, AUTENTICAR Y CIFRAR

BLINDAR LOS SISTEMAS ANTICUADOS "MÁS DÉBILES" DETRÁS DE LAS PASARELAS "MÁS FUERTES"

AUTENTICAR EL ACCESO DE LOS USUARIOS DE FORMA RIGUROSA Y CON LÍMITES BIEN DEFINIDOS



INTEGRAR SIN PROBLEMAS LOS MÉTODOS DE TRABAJO A DISTANCIA SEGUROS

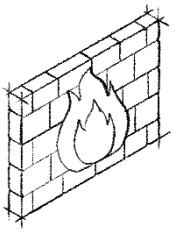
MANTENER EL SOFTWARE A DISTANCIA A MEDIDA QUE SE IDENTIFICAN LAS VULNERABILIDADES

INSPECCIONAR CADA COMANDO PARA DETECTAR ACCIONES NO DESEADAS

AUDITAR TODAS LAS ACCIONES PARA GARANTIZAR EL CUMPLIMIENTO

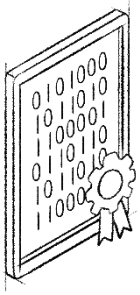
ARDEXA

Ardexa ha diseñado con la ciberseguridad como base, lo que permite la ventaja de una protección amplia y de varios niveles contra los ciberataques. Las organizaciones deben considerar seriamente las implicaciones de la ciberseguridad, especialmente cuando se trata de infraestructuras críticas y/o la seguridad de los sistemas operados por una organización cliente.



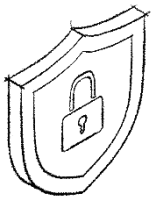
NO ABRA LAS REDES DE LA PLANTA O DE LA MÁQUINA A INTERNET

Las conexiones de Ardexa no requieren que se abran puertos o cortafuegos de red externos a las conexiones entrantes. No hay servicios abiertos a Internet o a la red local. Ardexa logra esto mediante el uso de un dispositivo local en una planta, gestionado por un agente de Ardexa que puede conectar y proteger máquinas y redes anticuadas que pueden no tener capacidades avanzadas de ciberseguridad. No hay necesidad de direcciones IP públicas, puertos abiertos u otros métodos anticuados.



UTILIZAR CERTIFICADOS DIGITALES PARA IDENTIFICAR, AUTENTICAR Y CIFRAR

La identificación y la autenticación son muy complejas cuando se trata de muchas máquinas dispersas y remotas. Mediante el uso de certificados digitales, Ardexa puede identificar, cifrar y autenticar simultáneamente máquinas individuales sin los problemas que afectan a los sistemas con contraseñas. Estos certificados digitales son únicos para cada dispositivo local, se renuevan para una mayor protección, y pueden ser revocados o aislados, si se requiere mitigar los riesgos. Nuestra API y aplicación web utilizan estándares TLS modernos y de confianza.

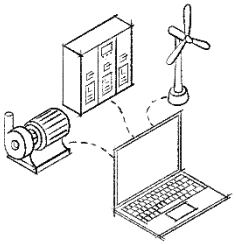


BLINDAR LOS SISTEMAS ANTICUADOS "MÁS DÉBILES" DETRÁS DE LAS PASARELAS "MÁS FUERTES"

La mayoría de las organizaciones necesitan conectar máquinas y redes, muchas de las cuales tienen protocolos de comunicación industrial con poca o ninguna capacidad de seguridad. Es importante proteger estos "enlaces más débiles" con dispositivos robustos. Ardexa puede proporcionar esa protección con dispositivos de alta seguridad en cada planta, estrechamente controlados por agentes de software avanzados.

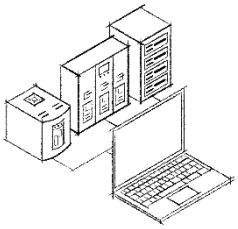
AUTENTICAR EL ACCESO DE LOS USUARIOS DE FORMA RIGUROSA Y CON LÍMITES BIEN DEFINIDOS

Cuando se trata de carteras de activos dispersas, el acceso debe concederse únicamente al personal autorizado. Ardexa dispone de un amplio conjunto de permisos, desde el control de toda la cartera hasta la supervisión de sólo lectura en un único dispositivo. Como complemento al control de acceso, está disponible la autenticación multifactor y se recomienda encarecidamente.



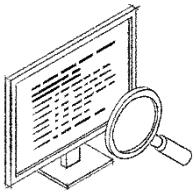
INTEGRAR SIN PROBLEMAS LOS MÉTODOS DE TRABAJO A DISTANCIA INTELIGENTES

Los métodos de acceso remoto obsoletos para el mantenimiento, las reparaciones y los diagnósticos utilizados por el personal autorizado o los proveedores de terceros pueden crear vulnerabilidades de ciberseguridad involuntarias en sus plantas. Ardexa utiliza túneles y VPNs (pasarelas de acceso altamente seguras) que permiten el acceso a una sola máquina o a una red, reduciendo en gran medida el riesgo de malware. Todo el acceso a los túneles y VPN se realiza a través de los productos de Ardexa, que están auditados y controlados por permisos basados en la nube.



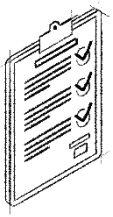
MANTENER EL SOFTWARE A DISTANCIA A MEDIDA QUE SE IDENTIFICAN LAS VULNERABILIDADES

El software que no puede ser parcheado regularmente puede conducir a graves riesgos de ciberseguridad. Ardexa garantiza que todos los sistemas de nube y software puedan actualizarse de forma remota, automática o manualmente, en cualquier momento. Nuestros dispositivos se actualizan periódicamente con nuevas funciones de rendimiento y seguridad, lo que permite mantener la seguridad de los activos y minimizar el tiempo de inactividad.



INSPECCIONAR CADA COMANDO PARA DETECTAR ACCIONES NO DESEADAS

Gracias a la infraestructura basada en mensajes de Ardexa, se puede auditar y supervisar el sistema con mucha más facilidad. No hay intercambios ocultos que puedan albergar acciones no autorizadas o no deseadas. Los mensajes individuales pueden ser autentificados a niveles muy finos, una característica que requieren muchos intercambios de datos con múltiples actores. Además, Ardexa permite un escaneo rápido y vital de carteras de activos enteras para identificar cualquier amenaza activa o latente que pueda estar presente, pero ser desconocida.



AUDITAR TODAS LAS ACCIONES PARA GARANTIZAR EL CUMPLIMIENTO

Ardexa registra todos los comandos y acciones para supervisar el uso del sistema y proporcionar una base sólida para el cumplimiento de la seguridad. Los datos de auditoría se almacenan en la nube como un almacén de datos inmutable, que no puede ser eliminado. Todas las acciones relacionadas con el uso de la nube, los comandos o las transferencias de archivos al dispositivo local y el uso de herramientas de trabajo remoto se registran en la nube.

ARDEXA

ARDEXA, INC
201 N Union St, Suite 110
Alexandria, Virginia, 22314,
Estados Unidos

ARDEXA GMBH
Mariahilfer Straße 32/6
Viena, 1070,
Austria

ARDEXA PTY LTD
Unit 244, 102 Northbourne Avenue
Braddon, ACT, 2612,
Australia

correo electrónico: business.development@ardexa.com
sitio web: https://ardexa.com