KYOCERA | semperis

kyoceradocumentsolutions.es

La plataforma de detección y de respuesta a las amenazas contra los entornos de Active Directory más completa del sector.

Directory Services Protector (DSP) automatiza la seguridad de tu Active Directory híbrido con una supervisión continua y una visibilidad sin parangón de los entornos de AD locales y de Azure AD, un seguimiento a prueba de manipulaciones y la reversión automática de los cambios malintencionados.

Bussiness Solutions

Si tu AD híbrido no está seguro, nada lo está.

Las aplicaciones empresariales on-premise y en la nube confían en Active Directory y en Azure Active Directory, por lo que son un elemento crucial de tu infraestructura de TI. Sin embargo, Active Directory es difícil de proteger, debido a su flujo constante, a la enorme cantidad de ajustes y a la creciente sofisticación del panorama de amenazas. Por otro lado, la protección de un sistema híbrido plantea desafíos adicionales, ya que muchos ataques comienzan de forma local y luego pasan a la nube. Directory Services Protector (DSP) supervisa de manera constante Active Directory y Azure Active Directory en busca de indicadores de exposición al riesgo y proporciona una vista única de las actividades locales y en la nube.

+ Impide que los atacantes accedan a tu AD local y a Azure AD.
+ Automatiza la protección y la respuesta a las amenazas.
+ Valida de manera continua la posición de seguridad de tu AD.

Protege de manera proactiva AD y Azure AD de los ciberataques.

Los atacantes mejoran constantemente su capacidad de dirigir los ataques a los puntos débiles del sistema de AD híbrido, aprovechando las vulnerabilidades del AD local para introducirse en su entorno y trasladarse luego a la red para llegar a Azure AD.

Detecta las vulnerabilidades de AD y Azure AD antes de que lo hagan los atacantes.

DSP supervisa de manera continua los indicadores de exposición al riesgo y las vulneraciones de la seguridad que suponen un peligro para AD y Azure AD.

Acaba con los puntos críticos para la seguridad de los entornos híbridos de Active Directory.

Los atacantes utilizan potentes herramientas de detección e intrusión para crear puertas traseras y accesos permanentes en su entorno híbrido de Active Directory — impidiendo su detección por parte de las soluciones SIEM tradicionales —.

DSP utiliza múltiples fuentes de datos — incluido el flujo de replicación de AD — para captar los cambios que burlan la detección basada en agentes o en registros. Los intrusos y los administradores malintencionados pueden causar estragos rápidamente en tus sistemas a una escala que es difícil de controlar y de solucionar de manera efectiva con una intervención humana.

Permite una recuperación rápida.

DSP revierte automáticamente los cambios malintencionados en el AD local, ofrece una reversión manual de los cambios en Azure AD y proporciona un panel de control unificado para que pueda correlacionar los cambios en tu entorno de AD local.

Los sistemas de identidad híbrida son objeto de ataques.

Los sistemas de identidad híbrida —que abarcan a Active Directory y a Azure Active Directory— son cada vez más habituales, ya que las organizaciones implementan una combinación óptima de recursos locales y servicios en la nube. Sin embargo, esta flexibilidad conlleva una mayor complejidad, sobre todo a la hora de gestionar la seguridad de la identidad híbrida en un entorno de Microsoft.

Para proteger Active Directory se necesita un enfoque distinto que para proteger Azure Active Directory: las herramientas, los procesos y las amenazas son diferentes.

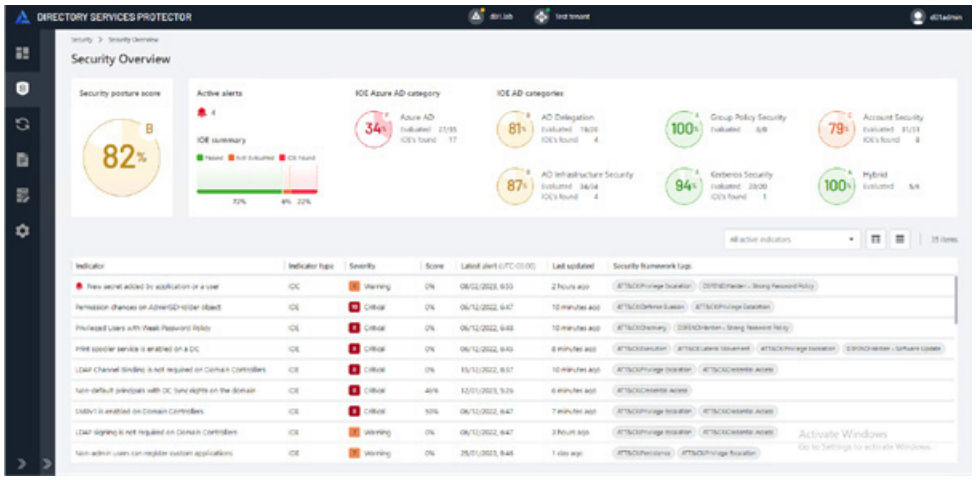
Con un escenario híbrido, los atacantes tienen a su disposición una mayor superficie potencialmente vulnerable.

Ahora es habitual que los ataques empiecen localmente y pasen luego a la nube —como en el ataque a SolarWinds— o que se extiendan de la nube a los sistemas locales. La gestión de la seguridad de un sistema de identidad híbrida es complicada. Y como Azure AD es una pieza fundamental del rompecabezas de la seguridad, las organizaciones que han adoptado un modelo de identidad híbrida tienen que protegerse de un número interminable de posibles puntos de entrada. Directory Services Protector protege los entornos de AD híbridos frente a los ciberataques con el seguimiento de los cambios en Azure AD, la reversión manual de los cambios malintencionados en Azure AD y una vista híbrida del entorno que ayuda a correlacionar los cambios en el AD local y en Azure AD.

Realiza de forma sencilla un seguimiento de la posición de seguridad de AD y Azure AD con Directory Services Protector.

Comunica claramente la posición general en materia de seguridad de tu AD híbrido y gestiona la detección y la respuesta a las amenazas en AD y Azure AD:

+ Visualiza la puntuación general y los resultados por categorías de seguridad concretas, como la seguridad de la cuenta de AD, la seguridad de la directiva de grupo, la seguridad de Kerberos, la delegación de AD, la infraestructura de AD, Azure AD y la seguridad híbrida.
+ Explora en profundidad los indicadores de exposición al riesgo (IOE) y los indicadores de vulneraciones (IOC).
+ Utiliza las instrucciones de corrección clasificadas por prioridades para reducir inmediatamente la superficie expuesta a ataques de AD.
+ Haz un seguimiento y revierte manualmente los cambios malintencionados en Azure AD.
+ Visualiza y correlaciona los cambios en Azure AD y el AD local en una sola vista híbrida.
+ Detecta los ataques avanzados a AD que logran eludir la supervisión tradicional basada en registros y eventos, como SIEM.



Evaluación de la vulnerabilidad, seguimiento de los cambios y corrección en una solución única para el Active Directory local y para Azure Active Directory

Evaluación de la vulnerabilidad
Supervisa constantemente los "indicadores de exposición al riesgo" que podrían poner en peligro la seguridad de tu entorno de AD híbrido. Utiliza la inteligencia sobre amenazas integrada, creada por una comunidad de investigadores del campo de la seguridad.

Remediación automática
Crea notificaciones de auditoría sobre los cambios en los objetos y los atributos confidenciales de AD, con la opción de deshacer automáticamente los cambios seleccionados.

Seguimiento a prueba de manipulaciones
Detecta los cambios, aunque el registro de seguridad esté desactivado, los registros estén borrados, los agentes estén deshabilitados o hayan dejado de funcionar o los cambios se hayan insertado directamente en AD o Azure AD.

Búsqueda y reparación al instante
Utiliza la base de datos en línea de DSP para encontrar y reparar los cambios no deseados en los objetos y los atributos de tu AD híbrido en dos minutos o menos.

Reversión granular
Revierte los cambios en los atributos individuales, los miembros de grupos, los objetos y los contenedores en el AD local y en Azure AD — y hazlo en cualquier momento específico y no solo a una copia de seguridad anterior —.

Análisis forenses
Identifica los cambios sospechosos, aísla las modificaciones realizadas por las cuentas vulneradas, etc. Usa los datos de DSP para respaldar las operaciones de análisis forense digital y respuesta a incidentes (DFIR), para rastrear el origen y los detalles de los incidentes.

Enriquecimiento del sistema SIEM
Acaba con los puntos débiles de tu sistema de gestión de eventos e incidentes de seguridad (SIEM) con una integración inmediata.

Delegación
Aprovecha el sólido control de acceso basado en roles (RBAC) y una rica interfaz de usuario web para ofrecer a los administradores unas funciones de visualización y restauración pensadas para su ámbito de control específico.

Informes potentes
Obtén información sobre los aspectos operativos, de buenas prácticas, de cumplimiento normativo y de seguridad de tu entorno de AD híbrido gracias a los informes integrados creados por expertos en AD — lo que incluye un informe gráfico de tu posición general en materia de seguridad —. Crea informes personalizados basados en consultas sofisticadas de bases de datos LDAP y DSP.

Notificaciones en tiempo real
Mantente informado mediante las notificaciones por correo electrónico que se envían en cuanto se producen cambios en el funcionamiento y la seguridad de tu entorno de AD híbrido.

Compatible con PowerShell
Utiliza el módulo PowerShell de DSP para automatizar los procesos e integrar las operaciones y la gestión de DSP en el conjunto de herramientas existente.

Adáptate a los marcos de seguridad
Vincula los indicadores de seguridad con los marcos de seguridad estándar del sector, como MITRE ATT&CK y MITRE D3FEND.

Validación continua de la seguridad
Supervisión automatizada para combatir el deterioro de la posición de seguridad debido a los desfases en la configuración, es decir, los ajustes de la configuración que suponen un peligro y se van acumulando con el tiempo hasta hacer que acabe siendo vulnerable a los ataques.

Rastrea los cambios en Azure AD
Utiliza el seguimiento de cambios casi en tiempo real del módulo de DSP para Azure AD, para supervisar los cambios en la asignación de roles, la pertenencia a grupos y los atributos de los usuarios.

Visualiza la seguridad de tu AD híbrido
Con el módulo DSP para Azure AD, verás fácilmente los cambios que se originaron en Azure AD y podrás usar la vista híbrida para establecer la correlación entre los cambios de tu AD local y Azure AD.

¿Tu entorno de AD híbrido es seguro?

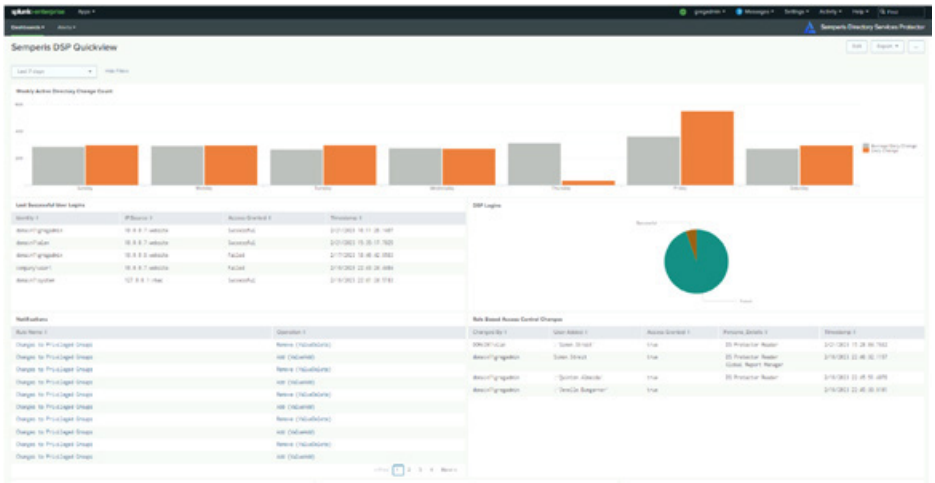
Solo el 27% de las organizaciones empresariales "confían mucho" en ser capaces de impedir un ataque a Azure AD.
La falta de visibilidad de los ataques que empiezan en el AD local y luego pasan a Azure AD hace que la prevención de los ataques cada vez preocupe más.

Recupera la visión de tu sistema SIEM.

Cada vez son más los ataques que logran sortear los controles de seguridad
A diferencia de las herramientas de seguimiento que se basan únicamente en los registros y los agentes de seguridad de cada controlador de dominio, DSP supervisa múltiples fuentes de datos, incluido el flujo de replicación de Active Directory. El flujo de replicación de AD es el único método fiable para detectar todos los cambios, por mucho que los atacantes intenten ocultar su rastro. DSP envía los cambios sospechosos de AD a su sistema SIEM, junto con un contexto significativo, lo que reduce drásticamente la carga de los analistas de seguridad. Puedes usar las alertas predefinidas para Microsoft Sentinel, Splunk y otras herramientas SIEM y SOAR y crear alertas personalizadas para las herramientas de SecOps y los sistemas de control de vales como ServiceNow.

Integraciones SIEM listas para usar.

DSP simplifica la detección y la respuesta a las amenazas con una integración inmediata y trae a primer plano unos datos de seguridad de AD que anteriormente estaban ocultos, con unas vistas que los usuarios de Sentinel y Splunk conocen y pueden utilizar.



splunk> Microsoft Sentinel

DSP proporciona los datos de seguridad de Active Directory con unas vistas conocidas por los usuarios de Splunk.

"Es fundamental contar con un partner con experiencia en el campo de la preparación para las vulneraciones y la respuesta a los incidentes en Active Directory y a otros ciberataques basados en la identidad. El enfoque basado en la solución de DSP no solo se centra en su tecnología excelente para dar respuesta a los problemas de los clientes, sino también en las mejores prácticas y las instrucciones para las personas y los procesos, lo que los diferencia de sus competidores". **SARAH PAVLAK, Frost & SullivanW.**

Kyocera es un partner global de soluciones que generan conocimiento para acelerar y maximizar la eficiencia en los negocios. Nuestras soluciones abarcan los procesos end to end de la gestión de datos de nuestros clientes, que facilitan estilos de trabajo híbridos apoyados en la tecnología y conectados a través de entornos seguros, optimizados y sostenibles.

Kyocera Document Solutions ha liderado la innovación tecnológica desde 1934. Gracias a ello, hacemos posible que nuestros clientes conviertan su información en conocimiento, alcancen la excelencia y creen una sólida ventaja competitiva. Con una dilatada experiencia profesional y un gran sentido de la empatía, ayudamos a las organizaciones a poner el conocimiento en práctica para impulsar su transformación.

KYOCERA Document Solutions S.A.
Edificio KYOCERA — C/Manacor, 2 — 28290 Las Rozas — Madrid
Tel + (34) 91 631 8392 — Fax + (34) 91 631 82 19

Delegación de Cataluña
Gran Via de les Corts Catalanes 641,
Oficina 3. Planta Ático 08010 Barcelona
Tel + (34) 93 595 12 50

KYOCERA | semperis

kyoceradocumentsolutions.es