HOJA DE DATOS

# Protección de One Identity

Almacene, administre, grabe y analice de forma segura el acceso con privilegios

## Beneficios

- Mitigue el posible daño de las infracciones de seguridad.
- Satisfaga los requisitos de cumplimiento de normas.
- ROI rápido con implementación y administración simplificadas.
- Creación eficiente de informes de auditorías.
- Identifique usuarios con privilegios de alto riesgo, comportamientos riesgosos y eventos inusuales.
- Simplifica la administración de cuentas con privilegio.

## Introducción

Los métodos que los hackers usan para obtener acceso a sus sistemas y datos evolucionan constantemente. Básicamente, quieren llegar hasta las cuentas con privilegios. En casi todas las infracciones recientes de alto perfil, las cuentas con privilegios se han visto afectadas para ganar acceso a los sistemas y datos críticos. Puede limitar el daño de una infracción al implementar soluciones que ofrezcan una manera segura, eficiente y conforme a las normas de acceder a las cuentas con privilegios.

Para los administradores del área de TI, estas cuentas con acceso ilimitado son un desafío para administrar por diversos motivos, entre ellos, la gran cantidad de cuentas con privilegios y la cantidad de personas que necesitan tener acceso a ellas. Además de estos problemas, las soluciones tradicionales de administración de acceso con privilegios (PAM) incluyen arquitecturas complejas, tiempos de implementación prolongados y requisitos de administración onerosos.

Sí, la PAM puede ser un gran problema, pero no tiene por qué serlo. La Protección de One Identity es una solución integrada que combina una contraseña segura reforzada y una solución de monitoreo y administración de sesiones con análisis y detección de amenazas. Almacena, administra, graba y analiza de forma segura el acceso con privilegios.


## Asegure el acceso con privilegios sin comprometerse

Elimine el estrés de proteger sus cuentas con privilegios al almacenar, administrar, grabar y analizar de forma segura el acceso con privilegios a la vez que satisface a sus administradores y auditores con la Protección de One Identity.

## Protección para contraseñas con privilegios

La solución de Protección de One Identity para contraseñas con privilegios controla y protege el proceso de otorgar credenciales con privilegios con administración de acceso basada en roles y flujos de trabajo automatizados. El diseño centrado en el usuario de la Protección para contraseñas con privilegios implica una menor curva de aprendizaje. Además, la solución le permite administrar contraseñas desde cualquier parte y a través de casi cualquier dispositivo. El resultado es una solución que protege su empresa y les otorga a los usuarios con privilegios un nuevo nivel de libertad y funcionalidad.

## Protección para sesiones con privilegios

Con la Protección de One Identity para sesiones con privilegios, puede controlar, monitorear y grabar sesiones con privilegios de administradores, proveedores remotos y otros usuarios de alto riesgo. El contenido de las sesiones grabadas se indexa, lo que facilita encontrar los eventos de las sesiones más tarde y ayuda a simplificar y automatizar la generación de informes; ambas funciones facilitan los requisitos de cumplimiento y auditoría. Además, la Protección para sesiones con privilegios cumple la función de proxy, inspecciona el tráfico del protocolo a nivel de la aplicación y puede rechazar cualquier tráfico que infrinja el protocolo, lo que la convierte en un escudo eficaz contra ataques.

## Protección para análisis con privilegios

Con la Protección de One Identity para análisis con privilegios, puede hacer que los análisis de comportamiento del usuario trabajen para usted y saber qué usuarios con privilegios presentan el mayor riesgo, descubrir amenazas internas y externas previamente desconocidas, y encontrar y detener actividades sospechosas. La Protección para análisis con privilegios clasifica el nivel de riesgo potencial de las amenazas para que pueda priorizar su respuesta (tomar medidas inmediatas sobre las amenazas más inminentes) y, por último, evitar las filtraciones de datos.

# Características

## Control de versión basado en políticas

Al usar un navegador web seguro con soporte para dispositivos móviles, usted puede solicitar acceso y proporcionar aprobaciones para las contraseñas y sesiones con privilegios. Las solicitudes se pueden aprobar de manera automática o requerir dos o múltiples aprobaciones según la política de la empresa. Ya sea que sus políticas tengan en cuenta el nivel de acceso y la identidad del solicitante, el horario y el día del intento de solicitud y los recursos específicos requeridos, o todos estos elementos, puede configurar Protección de One Identity para que cubra sus necesidades personalizadas. Además, usted puede ingresar códigos de razón o integrarse directamente en los sistemas de tickets.

## Auditoría de sesión completa, grabación y reproducción

Toda la actividad de la sesión (las pulsaciones de teclas, el movimiento del mouse y las ventanas vistas) se captura, se indexa y se almacena en seguimientos seguros de las auditorías que se pueden ver como un video y realizar búsquedas como en una base de datos. Los equipos de seguridad pueden buscar eventos específicos en las sesiones y reproducir la grabación a partir de la ubicación exacta en que ocurrieron los criterios de búsqueda. Los seguimientos de las auditorías se cifran y se firman criptográficamente, además de registrarse la fecha y hora para fines de análisis forense y cumplimiento.

## Control de cambios

Soporta el control de cambios configurable y granular de las credenciales compartidas, incluido el cambio basado en el tiempo, en el último uso y el manual o forzado.

## Biometría del comportamiento del usuario

Cada usuario tiene un patrón idiosincrásico de comportamiento, incluso cuando realiza acciones idénticas, como escribir o mover un mouse. Los algoritmos integrados en la Protección para análisis con privilegios inspeccionan estas características del comportamiento (capturadas por la Protección para sesiones con privilegios). Los análisis del movimiento del mouse y la dinámica de las pulsaciones de teclas ayudan a identificar filtraciones y también sirven como autenticación biométrica continua.

## Aprobación en cualquier parte

Al aprovechar la autenticación de dos factores de One Identity Starling, puede aprobar o denegar las solicitudes en cualquier parte, y con casi cualquier dispositivo, sin estar conectado a la VPN.

## Favoritos

Acceda rápidamente a las contraseñas que usa más a menudo desde la pantalla de inicio de sesión. Puede agrupar varias solicitudes de contraseña en una única favorita, así puede obtener acceso a todas las cuentas que necesita con un solo clic.

## Detección

Detecte rápidamente las cuentas o los sistemas con privilegios en su red con opciones de detección de red, host y directorio.

## Alertas en tiempo real y bloqueos

La Protección para sesiones con privilegios monitorea el tráfico en tiempo real y ejecuta varias acciones, si aparece un determinado patrón en la línea de comandos o en la pantalla. Los patrones predefinidos pueden ser un comando riesgoso o un texto en un protocolo orientado a texto, o un título de ventana sospechoso en una conexión gráfica. En caso de detectar una acción de usuario sospechosa, Safeguard puede registrar el evento, enviar un alerta o finalizar de inmediato la sesión.

## Identifique los usuarios riesgosos

Safeguard evalúa las concesiones de derechos frente a las reglas de clasificación de riesgos para identificar las cuentas de alto riesgo. Las notificaciones proactivas se envían cuando los cambios en las concesiones de derechos pasan el perfil del usuario al estado de alto riesgo. Esto elimina el riesgo de derechos innecesarios o inactivos, antes de que alguien pueda hacer un uso indebido de ellos o explotarlos.

## Control de aplicaciones y comandos

La Protección para sesiones con privilegios soporta listas blancas y negras de títulos de ventanas y comandos.

## Encendido instantáneo

La Protección para sesiones con privilegios se puede implementar en modo transparente sin necesidad de cambios en los flujos de trabajo del usuario. Al actuar como gateway de un proxy, Safeguard puede operar como enrutador en la red, invisible para el usuario y el servidor. Los administradores pueden seguir usando las aplicaciones del cliente con las que están familiarizados y pueden acceder a sistemas y servidores de destino sin ninguna interrupción a su rutina diaria.

## Amplio soporte para protocolos

Soporte completo para protocolos SSH, Telnet, RDP, HTTP(s), ICA y VNC. Además, los equipos de seguridad pueden decidir qué servicios de red (por ejemplo, transferencia de archivos, acceso a shell, etc.) dentro de los protocolos desean habilitar/deshabilitar para los administradores.

## Búsqueda de texto completo

Con su motor de reconocimiento óptico de caracteres (OCR), los auditores pueden hacer búsquedas de texto completo para los comandos y cualquier texto visto por el usuario en el contenido de las sesiones. Incluso puede hacer listas de operaciones de archivos y extraer los archivos transferidos para revisarlos. La capacidad de buscar metadatos y contenido de las sesiones acelera y simplifica los análisis forenses y la solución de problemas del área de TI.

## Disminución de la implementación

Con una implementación rápida basada en dispositivos y un nuevo enrutamiento de tráfico simplificado, la Protección de One Identity puede permitirle grabar sesiones en cuestión de días sin perjudicar a sus usuarios.

## API RESTful

Safeguard utiliza una API modernizada basada en REST para conectarse con otras aplicaciones y sistemas. Cada función se expone mediante la API para permitir la integración rápida y sencilla, independientemente de qué quiera hacer o en qué lenguaje están escritas sus aplicaciones.

## Suscripción híbrida a One Identity

Expanda las capacidades de Safeguard con la suscripción híbrida a One Identity, que ofrece acceso inmediato a servicios y características en la nube. Estos incluyen la Autenticación de dos factores de Starling ilimitada para proteger el acceso de Safeguard y el Análisis de identidades e inteligencia de riesgo de Starling para Safeguard, a fin de que pueda detectar de forma preventiva derechos y usuarios riesgosos. Una única suscripción permite todas las implementaciones de la solución de One Identity.

## El enfoque de One Identity hacia la administración del acceso con privilegios

El portafolio de One Identity incluye el conjunto más completo de soluciones de administración de acceso con privilegios. Puede tomar como base las capacidades de la Protección de One Identity con soluciones para la delegación granular de la cuenta raíz de UNIX y la cuenta de administrador de Active Directory, funciones adicionales para sudo de código abierto preparado para uso empresarial y registro de pulsaciones de tecla para las actividades raíz de UNIX, todo perfectamente integrado en la solución de puente de Active Directory, líder del sector.

## Acerca de One Identity

One Identity permite que las empresas se ocupen de la administración de identidades y acceso (IAM). Con nuestra exclusiva combinación de ofertas, incluido un portafolio de gestión de identidades, administración de accesos, administración e identidades con privilegios como soluciones de servicio, las empresas pueden alcanzar su máximo potencial sin impedimentos de seguridad, ya que estarán protegidas contra las amenazas. Más información en OneIdentity.com.