One Identity Safeguard

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

Introducción

Los piratas informáticos desarrollan constantemente los métodos que usan para obtener acceso al sistema y los datos. Lo que buscan es acceder a sus cuentas con privilegios. En casi todas las infracciones de gran resonancia que se han producido recientemente, las cuentas con privilegios se vieron comprometidas en un intento de acceder a los datos y sistemas más importantes. Con las soluciones adecuadas, puede limitar el daño que causa una infracción mediante la implementación de soluciones que proporcionan un método de acceso a las cuentas con privilegios seguro, eficaz y que satisface el cumplimiento normativo.

Para los administradores de sistemas informáticos, estas cuentas con acceso a todo constituyen un reto a la hora de gestionarlas por varias razones, entre ellas, el número de cuentas con privilegios y la cantidad de personas que necesitan acceder a ellas. Además de estos retos, las soluciones de gestión de accesos con privilegios (PAM) tradicionales implican arquitecturas complejas, tiempos de implementación prolongados y requisitos de gestión engorrosos.

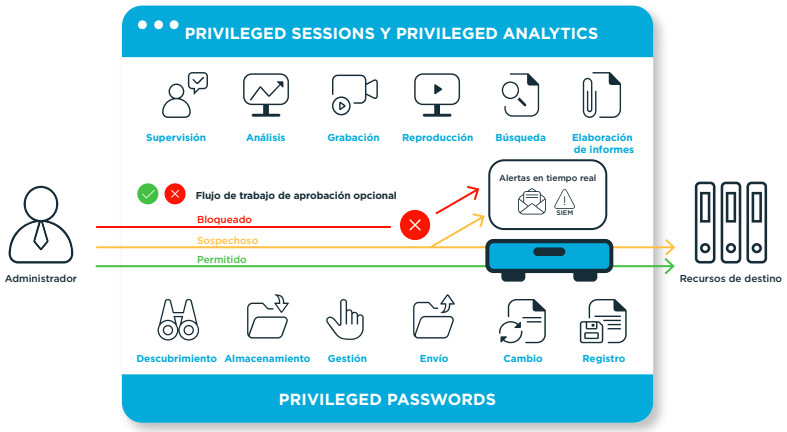
Es cierto que la PAM puede suponer un gran reto, pero esto no tiene por qué ser así. One Identity Safeguard es una solución integrada que combina una solución de caja fuerte de contraseñas altamente segura y una solución de supervisión y gestión de sesiones con análisis y detección de amenazas. Se encarga de almacenar, gestionar, grabar y analizar el acceso con privilegios de forma segura.

Ventajas

- **Mitigue el daño potencial de** las infracciones de seguridad
- **Satisfaga los requisitos de cumplimiento normativo**
- **Agilice la obtención de un ROI** con procesos simplificados de gestión e implementación
- **Disfrute de una creación eficaz de informes de auditoría**
- **Identifique y detenga comportamientos peligrosos** y eventos inusuales
- **Simplifique la gestión de cuentas con privilegios**

Proteja el acceso con privilegios sin sacrificios

No se preocupe en exceso por la protección de las cuentas con privilegios: almacene, gestione, grabe y analice de forma segura el acceso con privilegios y mantenga a sus administradores y auditores satisfechos con One Identity Safeguard.



Safeguard for Privileged Passwords

One Identity Safeguard for Privileged Passwords automatiza, controla y protege el proceso de concesión de credenciales con privilegios mediante la gestión de acceso basada en funciones y los flujos de trabajo automatizados.

El diseño centrado en el usuario de Safeguard for Privileged Passwords reduce la curva de aprendizaje. Además, la solución le permite gestionar las contraseñas desde cualquier parte, así como usar prácticamente cualquier dispositivo. Como consecuencia, se obtiene una solución que protege su empresa y que les proporciona un nuevo nivel de libertad y funcionalidad a los usuarios con privilegios.

Safeguard for Privileged Sessions

Con One Identity Safeguard for Privileged Sessions, puede controlar, supervisar y grabar las sesiones con privilegios de los administradores, los proveedores remotos y otros usuarios de riesgo elevado. Las acciones realizadas por los usuarios en las sesiones se graban e indexan, por lo que resulta sencillo encontrar eventos de sesiones, ayuda a simplificar y automatizar la elaboración de informes y simplifica los requisitos de cumplimiento normativo y auditoría. Además, Safeguard for Privileged Sessions desempeña la función de proxy e inspecciona los protocolos de tráfico en las aplicaciones, de forma que pueda rechazar cualquier tipo de tráfico que infrinja dichos protocolos; por ello, constituye un escudo protector eficaz ante ataques.

Safeguard for Privileged Analytics

Con One Identity Safeguard for Privileged Analytics, puede aprovechar los análisis de comportamiento de los usuarios para descubrir amenazas internas y externas que desconocía y, además, detectar y detener actividades sospechosas.

Safeguard for Privileged Analytics clasifica los niveles de riesgo potencial de las amenazas para que pueda dar prioridad a sus respuestas, es decir, intervenir de inmediato en el caso de las amenazas inminentes y, en última instancia, prevenir las infracciones de datos.

Características

Controles de versiones basados en políticas

Mediante un explorador web seguro compatible con dispositivos móviles, puede solicitar acceso y aprobar sesiones y contraseñas con privilegios. Se pueden aprobar las solicitudes de forma automática o establecer un proceso de aprobación doble o múltiple en función de la política de su organización. Así, tanto si sus políticas tienen en cuenta la identidad del solicitante y el nivel de acceso, la fecha y la hora del intento de solicitud o el recurso específico solicitado (como todos estos factores), puede configurar One Identity Safeguard para que satisfaga sus necesidades concretas. Además, puede introducir códigos de incidencias o realizar una integración directa con sistemas de tickets.

Auditoría, grabación y reproducción de sesiones completas

Toda la actividad de una sesión (incluso las pulsaciones de teclas, los movimientos del ratón y las ventanas visualizadas) se captura, se indexa y se almacena en trazas de auditoría que se pueden visualizar como un vídeo y en las que se pueden realizar búsquedas como si se tratara de una base de datos. Los equipos de seguridad buscan eventos específicos en las sesiones y reproducen las grabaciones desde la ubicación exacta en la que se han hallado los criterios de búsqueda. Las trazas de auditoría se cifran, se les añade una marca de tiempo y se les aplica una firma criptográfica con fines de cumplimiento normativo y análisis forense.

ONE IDENTITY by Quest

Activación instantánea

Safeguard for Privileged Sessions se puede implementar en modo transparente sin necesidad de realizar modificaciones en los flujos de trabajo de los usuarios. Al actuar como un gateway del proxy, Safeguard funciona como un router en la red y es invisible para el usuario y para el servidor. Los administradores pueden seguir usando aplicaciones cliente conocidas y pueden acceder a los sistemas y servidores de destino sin que su rutina diaria sufra interrupciones.

Datos biométricos del comportamiento del usuario

Cada usuario cuenta con un patrón de comportamiento idiosincrático, incluso cuando realiza acciones idénticas como escribir con el teclado o mover el ratón. Los algoritmos integrados en Safeguard for Privileged Analytics analizan estas características del comportamiento registradas por Safeguard for Privileged Sessions. El análisis de las dinámicas de pulsación de teclas y movimiento del ratón ayuda a identificar infracciones y sirven como método de autenticación biométrica continua.

Compatibilidad con la autenticación en varias fases

No basta con proteger el acceso a las contraseñas con otra contraseña. Mejore la seguridad exigiendo la autenticación en dos fases en Safeguard. Safeguard admite cualquier solución de autenticación en dos fases basada en RADIUS.

Safeguard for Privileged Passwords es compatible con el perfil de inicio de sesión único para navegadores web de SAML 2.0, lo que le permite configurar la autenticación federada con muchos servidores y servicios diferentes de STS de proveedores de identidades, y utilizar su autenticación en varias fases.

Las cuentas con privilegios pueden requerir un código generado por un autenticador TOTP como fase de autenticación. Safeguard for Privileged Passwords puede actuar como un autenticador y proporcionar el código asociado junto con la comprobación de credenciales/sesión.

Almacén personal de contraseñas

Todos los empleados pueden almacenar y generar contraseñas aleatorias para cuentas empresariales no federadas en un almacén de contraseñas personales. Esto permite que su organización use una herramienta autorizada con capacidad para compartir y recuperar con seguridad contraseñas, con lo que así se proporciona mucha seguridad y visibilidad, necesarias para las cuentas empresariales.

Favoritos

Acceda rápidamente a las contraseñas que usa más a menudo desde la pantalla de inicio de sesión. Puede agrupar varias solicitudes de contraseñas en una única entrada favorita para que pueda acceder a todas las cuentas que necesita con un solo clic.

Descubrimiento

Descubra rápidamente sistemas o cuentas con privilegios de su red mediante las opciones de descubrimiento de hosts, directorios y redes.

Bloqueo y alertas en tiempo real

Con Safeguard for Privileged Sessions se supervisa el tráfico en tiempo real y se ejecutan varios tipos de acciones si aparece un tipo de patrón determinado en la línea de comandos o en la pantalla. Los patrones predefinidos pueden ser un extracto de texto o un comando peligroso en un protocolo de texto o un título de ventana sospechoso en una conexión gráfica. Si se detecta una acción sospechosa del usuario, Safeguard sirve para registrar el evento y enviar una alerta o cerrar inmediatamente la sesión.

Control de comandos y aplicaciones

Safeguard for Privileged Sessions es compatible con la creación de listas blancas y negras en las que se incluyan comandos y títulos de ventanas.

Amplia compatibilidad con protocolos

Safeguard for Privileged Sessions ofrece compatibilidad total con los protocolos SSH, Telnet, RDP, HTTP, HTTPS, ICA y VNC. Además, los equipos de seguridad pueden tomar decisiones acerca de los servicios de red (por ejemplo, transferencia de archivos, acceso a shells, etc.) de los protocolos que quieren habilitar o deshabilitar para los administradores.

Búsqueda en texto completo

Gracias al motor de reconocimiento óptico de caracteres (OCR), los auditores pueden realizar búsquedas en texto completo tanto de comandos como de cualquier texto que haya consultado el usuario en el contenido de las sesiones.

También se pueden realizar listas de operaciones con archivos y extraer archivos transferidos para revisarlos. La función de búsqueda en los metadatos y el contenido de la sesión agiliza y simplifica los análisis forenses y la solución de problemas de tecnología informática.

Menos implementación

Gracias a la implementación rápida basada en dispositivos y a los cambios de enrutamiento del tráfico simplificados, puede grabar sesiones con One Identity Safeguard en cuestión de días sin que los usuarios sufran interrupciones.

API RESTful

Safeguard utiliza una API modernizada basada en REST para conectar otras aplicaciones y sistemas. Todas las funciones quedan expuestas mediante la API, que habilita una integración rápida y sencilla sin importar lo que quiera hacer o en qué lenguaje estén escritas sus aplicaciones.

Control de cambios

Es compatible con un control de cambios configurable y detallado de credenciales compartidas, entre los que se incluyen el cambio en función del tiempo y el último uso, y el cambio manual o forzado.

Enfoque de One Identity con respecto a la gestión de acceso con privilegios

En el catálogo de One Identity se incluye el conjunto de soluciones de gestión de acceso con privilegios más completo del sector. Puede partir de la potente funcionalidad de One Identity Safeguard, que presenta soluciones que facilitan la delegación pormenorizada de la cuenta raíz de UNIX y la cuenta de administrador de Active Directory, complementos para adaptar el sudo de código abierto a la empresa y el registro de pulsaciones de teclas para las actividades raíz de UNIX; todo, en estrecha integración con la solución de bridge de Active Directory líder en el sector.

Acerca de One Identity

One Identity ofrece soluciones de seguridad de identidad unificada que ayudan a los clientes a fortalecer su postura general de ciberseguridad, así como a proteger a la gente, las aplicaciones y los datos esenciales para la empresa. Nuestra plataforma de seguridad de identidad unificada reúne las mejores funciones de administración y gobernanza de identidades (IGA), gestión de acceso (AM), gestión de acceso con privilegios (PAM) y gestión de Active Directory (ADMgmt) para permitir que las organizaciones pasen de un enfoque fragmentado a uno holístico de la seguridad de la identidad.One Identity es fiable y está probada a escala global: gestiona más de 500 millones de identidades de más de 11 000 organizaciones en todo el mundo.
Para obtener más información, visite www.oneidentity.com.

ONE IDENTITY by Quest