

HOJA DE DATOS

One Identity Safeguard On Demand

Almacene, gestione, grabe y analice el acceso con privilegios de forma segura con la entrega mediante SaaS

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

La nube sin compromiso

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. Sin embargo, usted puede limitar el daño con una solución bajo demanda que proporciona un método seguro, eficaz y acorde con las normativas para gestionar las cuentas con privilegios.

Para los administradores de sistemas, estas cuentas de administrador 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 complejos. Es cierto que la PAM puede suponer un gran reto, pero esto no tiene por qué ser así. One Identity Safeguard On Demand es una solución mediante SaaS que combina una solución de caja fuerte de contraseñas con un alto grado de seguridad y una solución de supervisión con análisis y detección de amenazas que se gestiona y entrega plenamente desde la nube.

Safeguard on Demand automatiza, controla y protege el proceso de concesión de credenciales con privilegios mediante la gestión de acceso basada en roles y los flujos de trabajo automatizados. El diseño centrado en el usuario de Safeguard on Demand supone reducir la curva de aprendizaje. Además, se trata de una solución flexible y cómoda, ya que 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.

Con Safeguard On Demand también puede controlar, supervisar y grabar las sesiones con privilegios de los administradores, los proveedores remotos y otros usuarios de riesgo elevado. El contenido de las sesiones se indexa, por lo que resulta sencillo encontrar eventos de sesiones más adelante, además de que se simplifica y automatiza la elaboración de informes. Estas funciones le ayudan a satisfacer los requisitos de cumplimiento normativo y auditoría. Además, Safeguard on Demand 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 On Demand también incluye el análisis con privilegios, lo que le permite analizar el comportamiento de los usuarios y descubrir amenazas internas y externas que desconocía anteriormente y, además, detectar y detener actividades sospechosas. Safeguard On Demand 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 más 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, 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 (o todos estos factores), puede configurar One Identity Safeguard on Demand 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.

Activación instantánea

Safeguard on Demand funciona en modo transparente sin necesidad de realizar modificaciones en los flujos de trabajo de los usuarios. Al actuar como un gateway del proxy, Safeguard On Demand 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 incorporados en Safeguard On Demand inspeccionan estas características de comportamiento. 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.

Aprobación en cualquier parte

Mediante One Identity Cloud Assistant, puede aprobar o rechazar solicitudes desde cualquier parte, y prácticamente con cualquier dispositivo.

Almacén personal de contraseñas

Todos los empleados de su organización 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

Safeguard On Demand supervisa el tráfico en tiempo real y ejecuta 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 On Demand sirve para registrar el evento y enviar una alerta o cerrar inmediatamente la sesión.

Control de comandos y aplicaciones

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

Amplia compatibilidad con protocolos

Se dispone de 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.

API RESTful

Safeguard On Demand utiliza una API modernizada basada en REST para conectarse con 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 esté escrito su aplicación.

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 On Demand, 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, una empresa de Quest, permite a las organizaciones implementar una estrategia de seguridad centrada en la identidad, ya sea en el sitio, en la nube o en un entorno híbrido. Gracias a nuestra cartera particularmente amplia e integrada de ofertas de gestión de identidades, en las que se engloban la gestión de cuentas, la gobernanza de identidades y la gestión de accesos con privilegios y administración, las organizaciones disponen de las herramientas necesarias para alcanzar, por ellas mismas, el máximo potencial en lo que a seguridad se refiere. Todo ello es posible cuando las identidades ocupan el centro del programa y se permite el acceso adecuado a todos los tipos de usuarios, sistemas y datos. Más información en [OneIdentity.com](https://www.oneidentity.com).

© 2021 One Identity LLC. Todos los derechos reservados. One Identity y el logotipo de One Identity son marcas y registradas de One Identity LLC en los Estados Unidos y otros países. Para consultar la lista completa de las marcas de One Identity, visite el sitio web www.oneidentity.com/legal. El resto de las marcas, marcas de servicio, marcas registradas y marcas de servicio registradas son propiedad de sus respectivos titulares.

Datasheet-Safeguard-OnDemand-RS-ES-WL-64557