HOJA DE DATOS

Protección para sesiones con privilegios

Reduzca el riesgo al controlar, monitorear y grabar el acceso con privilegios

Beneficios

- Mitiga el riesgo de una infracción de seguridad al controlar el acceso a activos sensibles del área de TI.
- Cumpla fácilmente con los requisitos para el monitoreo del acceso con privilegios.
- Obtenga valor con mayor rapidez mediante una implementación y administración simples.
- Mantenga a los administradores contentos al permitir el uso de herramientas conocidas para administrar sistemas.
- Maximice la productividad con una pequeña curva de aprendizaje y un elegante diseño de interfaz de usuario.
- Reduzca los esfuerzos relacionados con los informes de auditoría con el rápido acceso a toda la información que necesita.
- Realice el seguimiento del acceso a cualquier tipo de sistemas debido a un diseño sin agentes e independiente de los hosts.
- Acelere la respuesta ante incidentes a través de búsquedas rápidas de texto completo en sesiones grabadas.

Introducción

Otorgar acceso con privilegios no controlado a los administradores internos, los proveedores externos, los contratistas y los proveedores de servicio puede generar un riesgo importante. Esto le abre la puerta a los atacantes que se apropian de cuentas con privilegios y a los administradores no autorizados. El impacto desafortunado y costoso de este tipo de riesgo se demostró una y otra vez a través de incidentes recientes muy publicitados. Para lograr una verdadera seguridad y cumplimiento, usted debe hacer algo más que simplemente controlar las cuentas de usuarios con privilegios. Debe monitorear y grabar lo que hacen con el acceso 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 para que la búsqueda de eventos sea simple y también ayuda a automatizar la generación de informes, a fin de que pueda cumplir fácilmente con los requisitos de auditoría y cumplimiento.

La Protección para sesiones con privilegios también cumple la función de proxy, al inspeccionar el tráfico del protocolo a nivel de la aplicación. Esto la convierte en un escudo eficaz contra los ataques al rechazar todo el tráfico que infringe el protocolo. En modo transparente, se requieren mínimos cambios en la red y los usuarios no tienen que cambiar su flujo de trabajo actual ni las aplicaciones del cliente, lo que hace que la implementación sea rápida. Sin embargo, las reglas del flujo de trabajo se pueden configurar para que sean más estrictas, lo que incluye requerirles autorización previa a los usuarios, limitar el acceso a recursos específicos y recibir alertas si las conexiones superan los límites de tiempo preestablecidos. Safeguard también puede monitorear sesiones en tiempo real y ejecutar varias acciones: si aparece una aplicación o un comando riesgoso, la Protección de One Identity puede enviarle un alerta o finalizar de inmediato la sesión.

Grabe y monitoree todos los accesos con privilegios

Con búsqueda de texto completo, bloqueo y alertas en tiempo real, Safeguard reduce el riesgo a la vez que facilita el cumplimiento de los requisitos.

Características

Auditoría de sesión completa, grabación y reproducción

Toda la actividad de la sesión (las pulsaciones de teclas individuales, 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 se identificaron 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.

Alertas en tiempo real y bloqueo

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.

Dos modos de operaciones

Elija el modo que se adapte a sus necesidades.

- **Motor de flujos de trabajo**: Un motor de flujos de trabajo que soporta restricciones de tiempo, aprobadores múltiples, revisores, acceso de emergencia y expiración de política. También incluye la capacidad para ingresar códigos de razón o integrarse directamente en los sistemas de tickets. Una solicitud de contraseña puede aprobarse automáticamente o requerir cualquier nivel de aprobaciones.
- **Encendido instantáneo**: Impleméntelo en modo transparente para que no haya necesidad de cambios en los flujos de trabajo del usuario. Puede actuar como gateway de un proxy, que funciona como enrutador en la red, invisible para el usuario y el servidor. Los administradores pueden seguir usando aplicaciones del cliente familiares y pueden acceder a sistemas y servidores de destino sin ninguna interrupción a su rutina diaria.

Acceso a través de proxy

Dado que los usuarios no tienen acceso directo a los recursos, la empresa está protegida contra acceso no autorizado y sin restricciones a sistemas y datos confidenciales. La Protección para sesiones con privilegios puede transmitir y grabar en muchos recursos de destino, incluidos UNIX/Linux, Windows, dispositivos de red, firewalls, enrutadores y más.

Control de aplicaciones y comandos

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

Trabaje de la manera que quiera

Incluso cuando el flujo de trabajo está habilitado, los administradores pueden elegir a sus clientes, herramientas y preferencias cuando acceden a las sesiones con privilegios. Esto crea una solución sin problemas que ofrece a los administradores el acceso que necesitan al tiempo que satisface los requisitos de cumplimiento y las normas de seguridad.

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.

Inicio de sesión automático

Con la función de inyección de la contraseña, el acceso se puede configurar para el inicio de sesión automático, lo que mejora la seguridad y el cumplimiento, ya que nunca se expone la contraseña al usuario.

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.

Apagado instantáneo

Al actuar como un firewall virtual, la Protección de One Identity aumenta la protección de sus servidores mediante la finalización de accesos maliciosos o cuestionables de forma casi instantánea. Además de evitar la desconfiguración accidental y otros errores humanos, la solución soporta el principio de autorización de cuatro ojos, según el cual el administrador de monitoreo puede finalizar la sesión en cualquier momento.

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.

Listo para el análisis

Recopile toda la información que necesita para analizar el comportamiento y a los usuarios con privilegios, y detecte amenazas internas y externas.

Acceso seguro a los sistemas heredados

Use SmartCard, 2FA u otros métodos de autenticación poderosos para obtener acceso seguro a los sistemas. Dado que Safeguard actúa como un gateway del proxy para el sistema, permite la autenticación sólida en destinos que no pueden soportar, o no soportan, estos métodos de manera nativa.

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 la poderosa función de administración de sesiones de la Protección para sesiones con privilegios, con nuestras soluciones de contraseña segura con privilegios y análisis con privilegios. Nuestra oferta de productos incluye 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.