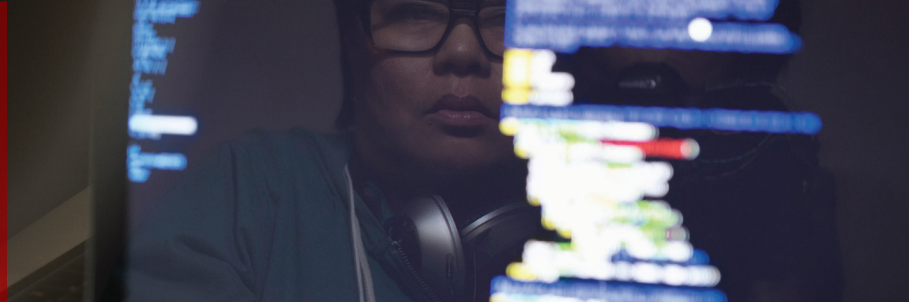

Servicio de control y auditoría de Centrify

Reforzar el entorno con total garantía

En las sesiones con privilegios, la práctica recomendada es auditarlo todo, por supuesto. Gracias a la grabación documentada de todas las acciones realizadas, los registros de auditoría se pueden utilizar no solo para buscar el problema exacto en un análisis forense, sino también para atribuir acciones a un usuario concreto. Dada la transcendencia de estas sesiones, otra buena práctica consiste en guardar una grabación en vídeo que se pueda revisar o utilizar como evidencia en relación con los activos más importantes o en las industrias altamente reguladas. Existen múltiples normativas, por ejemplo, PCI-DSS para los datos de tarjetas de pago, que requieren específicamente este nivel de auditoría. Si hay un departamento de seguridad en la empresa, la práctica recomendada consiste en integrar estos datos de auditoría en el Sistema de gestión de eventos e información de seguridad (SIEM) para minería automatizada, en el que es posible identificar actividades de riesgo y generar alertas.

Auditarlo todo

Los analistas de la industria y los organismos públicos reguladores reconocen que, actualmente, la principal causa de las brechas de seguridad está relacionada con el uso indebido del acceso con privilegios. Las credenciales con privilegios son las «llaves del reino» y permiten moverse libremente por toda la infraestructura. La revelación de una sola credencial con privilegios puede afectar a millones de credenciales. A su vez, los auditores internos y los ordenamientos normativos establecen controles específicos y requisitos de informes para la utilización de estas credenciales.

Incluso las organizaciones de pequeña y mediana envergadura tienen que cumplir con diversos reglamentos de la industria y de las administraciones públicas y enfrentarse a sus propios desafíos a la hora de recopilar, agregar y atestiguar los datos de acceso con privilegios.

A menudo, las organizaciones carecen de transparencia respecto a su posición sobre el cumplimiento, y las auditorías y certificaciones se convierten en una carrera contra reloj durante la que se dispara la carga de trabajo de los auditores internos y del personal de cumplimiento.

Esto da lugar a que se utilice un método de «muestreo» en el que se evalúa solo un subconjunto de controles específicos y se dejan muchos cabos sueltos desde la perspectiva del cumplimiento y la seguridad. En general, conseguir respuestas de una gran variedad de partes interesadas y evaluar conjuntos de datos diversos menoscaba la eficiencia y la precisión.

Desde la perspectiva de la seguridad, es importante obtener información específica y detallada acerca de cualquier actividad sospechosa de un acceso con privilegios. Los administradores de seguridad pueden adoptar medidas correctoras de inmediato para proteger la infraestructura contra un riesgo potencial o una amenaza que esté en curso. Pueden hacerlo directamente desde la pantalla de alerta o terminar una sesión de forma manual o automática en función del riesgo.

En la historia reciente, las brechas de seguridad de datos más relevantes han sido posibles porque, dentro de la organización, una o varias personas crearon cuentas de puerta trasera que eludían los métodos tradicionales de bóveda de contraseñas. Además, los usuarios con privilegios suelen encontrar el modo de eludir la bóveda de contraseñas de su entorno para simplificar su rutina diaria. En este tipo de acceso malicioso, a menudo se aprovechan las claves SSH almacenadas localmente en los servidores, y el riesgo de sufrir una brecha de seguridad aumenta porque se amplía la superficie de una organización expuesta a ataques.

Reforzar el entorno con total garantía

El Servicio de control y auditoría de Centrify permite a los clientes satisfacer sus obligaciones de cumplimiento mediante informes y auditorías, así como poner fin a los atajos peligrosos aplicando la supervisión basada en host. El servicio ayuda a grabar todos los metadatos y las sesiones con privilegios y atribuye la actividad a una persona para ofrecer una imagen completa de las intenciones y de los resultados.

GRABACIÓN Y AUDITORÍA DE SESIÓN

Grabe y gestione una visión global de las actividades con privilegios en sus servidores Windows y Linux, en IaaS y en las bases de datos para establecer un solo origen de información fidedigno sobre cuentas individuales y compartidas. Demuestre el cumplimiento con informes sobre los privilegios de cada usuario y la actividad asociada.

SUPERVISIÓN Y CONTROL DE SESIONES DE PUERTA DE ENLACE

Alcance nuevos niveles de supervisión de las sesiones con privilegios en su infraestructura crítica. Los usuarios administrativos observan la actividad de las sesiones remotas en tiempo real y pueden terminar al instante las sesiones sospechosas a través del portal de administración de Centrify.

AUDITORÍA, GRABACIÓN Y GENERACIÓN DE INFORMES BASADAS EN HOST

Asegúrese, mediante la auditoría basada en host, de que no se pueda eludir la grabación de la sesión. Descubra cualquier actividad maliciosa, por ejemplo, la creación e instalación de pares de claves SSH, que permitirían eludir fácilmente los controles de seguridad, y atribuya cualquier actividad a un usuario individual. Audite toda la actividad de las sesiones con privilegios en el nivel de proceso con detalles minuciosos para poder revisar la seguridad, tomar medidas correctoras para los informes de cumplimiento y evitar la suplantación de identidad.

> **«No existe ninguna normativa que Centrify no nos haya ayudado a cumplir. Ahora, cada vez que un administrador toca un servidor, queda registrado. Puedo extraer un informe, imprimirlo y entregárselo al auditor».**
>
> — Peter Manina, especialista en TI y arquitecto de sistemas de UNIX, Departamento de tecnología, gestión y presupuestos del Estado de Michigan

Grabación de sesión y auditoría para el acceso con privilegios

Cree informes y audite sesiones con privilegios utilizadas por las cuentas compartidas y por las cuentas individuales mediante una captura completa de vídeo y metadatos. El Servicio de control y auditoría de Centrify permite a los clientes realizar un análisis forense y utilizar grabaciones de alta fidelidad para fines de auditoría y cumplimiento.

- Capture y recopile datos de cada sesión con privilegios en una grabación de alta fidelidad en el nivel de la puerta de enlace. El Servicio de control y auditoría de Centrify almacena las sesiones en una base de datos de SQL Server fácil de consultar para ofrecer una visión global de lo que ha ocurrido exactamente. La función de búsqueda de reproducción del servicio proporciona a los administradores y auditores de seguridad de TI la capacidad de ver exactamente lo que han hecho los usuarios y los resultados de sus acciones, y de identificar el uso indebido de los privilegios o el origen de un incidente de seguridad.
- Grabe todos los metadatos y sesiones con privilegios y atribuya la actividad a una persona para obtener una imagen completa de las intenciones y de los resultados.
- Compruebe que los controles de seguridad están activos, funcionan tal como se diseñaron y facilitan pruebas del cumplimiento. Encuentre las grabaciones de sesión por servidor o usuario, además de realizar búsquedas personalizadas. Puede encontrar todas las sesiones de un usuario o servidor concretos o según un conjunto de criterios personalizados que simplifican las investigaciones forenses y permiten identificar proactivamente las amenazas internas o las actividades sospechosas.
- Obtenga visibilidad completa con acceso unificado e informes de actividad en una sola plataforma común. Las consultas integradas y personalizables, así como los informes ya preparados para el cumplimiento de los reglamentos SOX y PCI, proporcionan información sobre los controles de acceso a cuentas con privilegios, la descarga de contraseñas y las sesiones con privilegios en Windows, Linux y UNIX.

Supervisar y controlar las sesiones con privilegios en IaaS y en sus instalaciones

Utilice una infraestructura de auditoría común para capturar y grabar las actividades con privilegios realizadas en su infraestructura, ya sea de forma local o en la nube. Detecte cualquier actividad sospechosa de los usuarios para obtener alertas en tiempo real de los ataques que puedan estar en curso. El Servicio de control y auditoría de Centrify permite supervisar y controlar las sesiones con acceso privilegiado que utilicen cuentas compartidas o cuentas individuales.

- Alcance nuevos niveles de supervisión de las sesiones con privilegios en su infraestructura crítica. Los usuarios administrativos observan la actividad de las sesiones remotas en tiempo real y pueden terminar al instante las sesiones sospechosas a través del portal de administración de Centrify. Este modo de «cuatro ojos» permite a los administradores supervisar a un empleado remoto o las actividades de TI externalizadas tras conectarse a una sesión activa. Pueden observar todas las acciones que realiza el usuario con privilegios o terminar la sesión si la actividad es sospechosa.
- Los datos de acceso con privilegios se capturan y almacenan para facilitar las consultas potentes mediante herramientas de gestión de registros y mediante la integración con herramientas externas de generación de informes. La integración simplificada con SIEM y las herramientas de generación de alertas como Micro Focus® ArcSight™, IBM® QRadar™ y Splunk® identifican los riesgos o las actividades sospechosas rápidamente.

Evitar la suplantación de identidad o la elusión del acceso con privilegios mediante auditorías, grabaciones e informes de sesión basados en host

Adoptar un método aplicable al host para la auditoría, grabación y generación de informes de sesión facilita en definitiva un mejor control sobre el acceso con privilegios a su entorno. El Servicio de control y auditoría de Centrify extiende sus prestaciones de puerta de enlace con un método basado en host que garantiza que no se eludan los controles de acceso con privilegios, lo que puede suceder cuando se utiliza únicamente una bóveda de contraseñas/claves secretas.

- Capture y recopile los datos en una grabación de alta fidelidad para cada sesión con privilegios en cualquier servidor de su infraestructura local y en la nube. Almacene las sesiones en una base de datos de SQL Server fácil de consultar para obtener una visión global de lo que ha ocurrido exactamente en un sistema, si la acción ha sido realizada por un usuario o por todos, y el momento concreto.
- La auditoría, grabación y creación de informes de sesión basadas en host de Centrify incluyen prestaciones de supervisión avanzada en el nivel de proceso que, combinadas con la auditoría basada en shell, permiten identificar los cambios de aplicación sospechosos.
- La Supervisión de la integridad de los archivos de Centrify cambia a configuraciones y archivos críticos en tiempo real y habilita la activación de alertas de seguridad dentro del sistema SIEM de una organización para avisar de la creación de una puerta trasera para eludir la bóveda de contraseñas.
- Una función de búsqueda de reproducción ofrece a los auditores y gestores de seguridad de TI la posibilidad de ver qué hicieron los usuarios exactamente e identificar el uso indebido de privilegios o el origen de un incidente de seguridad.
- Genere informes sobre accesos, descargas, sesiones y uso de privilegios en Windows, Linux, UNIX y en su infraestructura de red.
- Integración simplificada con SIEM y con herramientas de generación de alertas e informes.

Nuestra misión es impedir la principal causa de las brechas de seguridad: el uso indebido del acceso con privilegios. Centrify facilita a sus clientes un método Cloud Ready Zero Trust Privilege para proteger el acceso a la infraestructura, a DevOps, a la nube, a los contenedores, al Big Data y a otras superficies de la empresa actual expuestas a ataques. Para obtener más información, visite www.centrify.com.

Sede central en EE. UU. +1 (669) 444 5200
EMEA +44 (0) 1344 317950
Asia-Pacífico +61 1300 795 789
Brasil +55 11 3958 4876
Latinoamérica +1 305 900 5354
sales@centrify.com

www.centrify.com