REPORTE OFICIAL • SEPTIEMBRE DE 2017

ca technologies

Reduzca el riesgo de violación de datos en sus servidores más cruciales: Cómo puede ayudar CA

Tabla de contenidos

Resumen ejecutivo

Reto

Las empresas de hoy deben reducir el riesgo de violaciones de seguridad para proteger los datos valiosos en sus organizaciones. Al mismo tiempo, los auditores de TI imponen, progresivamente, requisitos cada vez más estrictos a las empresas. El resultado final es que las cuentas y accesos con privilegios son el nuevo objetivo como nueva superficie de ataque de los piratas informáticos, y son el foco de los auditores que insisten en mayores controles para las cuentas con privilegios.

Oportunidad

La solución de administración de acceso con privilegios indicada brinda protección integral para sus servidores fundamentales para la misión, con controles potentes y específicos del acceso operativo a nivel del sistema y de las acciones de los usuarios con privilegios. Esta solución basada en alojamiento a nivel del sistema, que es capaz de implementar controles de acceso en potentes cuentas de Superusuarios nativas, como la raíz UNIX® y Linux®, y el administrador Microsoft® Windows®, controla, monitorea y realiza auditorías de la actividad de los usuarios con privilegios; lo que mejora la seguridad, y simplifica la auditoría y el cumplimiento.

Beneficios

CA Technologies brinda soluciones de administración de acceso con privilegios integrales y fáciles de implementar, con administración de credenciales integrada, autenticación sólida, control de acceso de confianza cero, filtración de comandos proactiva, monitoreo y registro de sesiones, y controles específicos sobre servidores de alto valor. CA Privileged Access Management brinda capacidades y controles que impiden activamente que los atacantes utilicen componentes clave de sus ataques, además de reducir riesgos y mejorar la eficacia operativa. Los beneficios incluyen la reducción de riesgos, el aumento de la responsabilidad, la mejora de auditorías y cumplimiento, y la reducción de complejidad.

Introducción

Las empresas de hoy deben reducir el riesgo de violaciones de seguridad para proteger los datos valiosos en sus organizaciones. Al mismo tiempo, los auditores de TI imponen, progresivamente, requisitos cada vez más estrictos a las empresas. El resultado final es que las cuentas y accesos con privilegios son el nuevo objetivo como nueva superficie de ataque de los piratas informáticos, y son el foco de los auditores que insisten en mayores controles para las cuentas con privilegios.

El hecho lamentable es que robar y vulnerar cuentas con privilegios es un factor de éxito fundamental para los piratas informáticos en el 100 % de todos los ataques avanzados, independientemente del origen. Estas cuentas incluyen usuarios, cuentas y credenciales con privilegios: empleados, contratistas de terceros e innumerables aplicaciones y scripts que contienen credenciales con privilegios (a menudo, no modificables y visibles para cualquier cantidad de individuos) que se encuentran en su infraestructura de TI.

Además, los sistemas operativos como UNIX, Linux y Windows están creados a partir del concepto de un "superusuario" que puede eludir la mayoría o todos los controles de seguridad en sus sistemas. Los administradores utilizan estas cuentas con altos privilegios con propósitos legítimos, pero también los usuarios internos malintencionados o atacantes externos pueden darles un uso indebido.

Proteger a estos usuarios y sus credenciales es un elemento crucial para ayudar a prevenir ataques, y la administración del acceso con privilegios se convirtió en un componente nuevo y necesario para la estrategia de defensa en profundidad, tan esencial como los firewalls y antivirus para proteger la empresa. La solución de administración de acceso con privilegios indicada brinda protección integral para sus servidores fundamentales para la misión, con controles potentes y específicos del acceso operativo a nivel del sistema y de las acciones de los usuarios con privilegios. Esta solución basada en alojamiento a nivel del sistema, que es capaz de implementar controles de acceso en potentes cuentas de superusuarios nativas, como la raíz UNIX y Linux, y el administrador Windows, controla, monitorea y realiza auditorías de la actividad de los usuarios con privilegios; lo que mejora la seguridad, y simplifica la auditoría y el cumplimiento.

Este reporte oficial examina los retos en seguridad para los servidores fundamentales para la misión y algunas de las estrategias disponibles actualmente. También presenta CA Privileged Access Manager Server Control, que proporciona la solución más consolidada, comprobada y potente para proteger a los servidores fundamentales para la misión. CA Privileged Access Manager Server Control se basa en un modelo de seguridad de mainframe comprobado para permitirle aplicar controles de acceso proactivos y auditoría superior que sean singularmente efectivos, incluso contra los superusuarios.

Los retos de hoy en seguridad para los servidores fundamentales para la misión

Los usuarios internos malintencionados y los atacantes externos están determinados a tomar el control y vulnerar las cuentas de usuarios con privilegios en sus servidores fundamentales para la misión. Una única violación puede causar importante daño de reputación y financiero a cualquier organización. Los departamentos de TI se encuentran bajo una enorme presión para frenar los ataques dirigidos y mitigar las amenazas internas mientras cumplen con los requisitos y estándares de seguridad del sector a fin de lograr y mantener el cumplimiento. TI también tiene la tarea de administrar y proteger una infraestructura híbrida cada vez más compleja mientras intenta alcanzar la eficiencia operativa a través de la automatización y la escalabilidad. El alcance de las responsabilidades parece enorme.

Normalmente, el riesgo se reduce a un nivel aceptable según lo fundamental para la misión de lo que se encuentra almacenado en el servidor. Algunos servidores son simplemente más valiosos que otros debido a la información que contienen, tal como información sobre tarjetas de crédito, números de seguro social, información de identificación personal, registros médicos, direcciones de correo electrónico o propiedad intelectual como planos, resultados financieros e información interna. Si bien la administración de acceso con privilegios reduce el riesgo, debe tomar medidas adicionales para proteger los servidores más cruciales. Analicemos algunas de estas estrategias.

Estrategias clave: La protección de los sistemas clave exige algo más que el "refuerzo" básico

Es evidente que uno de los retos más apremiantes para TI es garantizar la seguridad de los servidores que alojan los activos electrónicos confidenciales de la organización, como datos de clientes, registros financieros y propiedad intelectual. Estos activos son el alma de muchas organizaciones y una violación podría generar un daño irreparable.

Mediante el "refuerzo del servidor" típico, se puede lograr lo siguiente:

- Instalar todos los parches antes de conectarse a una red.
- Quitar los servicios innecesarios.
- Borrar los archivos de software y muestra no utilizados.
- Instalar software antivirus, antispyware o antiphishing.
- Cifrar las unidades confidenciales.
- Usar contraseñas potentes.
- Compartir la contraseña del superusuario con una cantidad reducida de administradores clave únicamente.

Si bien la mayoría de estos pasos son un buen consejo y siguen principios de seguridad generalmente aceptados, el último se basa en la suposición en esencia incorrecta de que es imposible controlar de manera eficiente las cuentas de los sistemas administrativos. Esto deja una brecha en la seguridad de un servidor que tanto un usuario interno malintencionado como un atacante externo pueden vulnerar. Sin importar la fuente, los ataques más dañinos incluyen el uso de identidades con privilegios. Por su naturaleza, estas cuentas tienen permisos para realizar grandes cambios en un sistema, una aplicación o una base de datos. Las acciones que se realizan con estas cuentas tienen el potencial de ser excepcionalmente destructivas y deben monitorearse de cerca.

Seguridad del sistema operativo nativo

En el núcleo del reto de seguridad de los controles de los sistemas operativos nativos se encuentra el hecho de que se basan fundamentalmente en el concepto del superusuario, un nivel de privilegio que, esencialmente, elude, y por lo tanto niega, cada control de seguridad en el servidor. Esto suele verse en casos como el de la cuenta "raíz" Linux o UNIX, así como el de la cuenta "administrador" Windows.

El diseño del sistema operativo en sí mismo asume la naturaleza sin restricciones de estas cuentas. Por tal motivo, los atacantes codician las cuentas de superusuario y las toman como objetivos. Una vez que el pirata informático tiene el control de la cuenta, tiene, virtualmente, acceso sin restricciones a cualquier cosa en el servidor, además de anonimidad, dado que la cuenta no se asocia con un individuo nombrado. Por este motivo, la mayoría de las soluciones comerciales basadas en servidores intenta controlar y limitar la capacidad y necesidad del usuario de usar la cuenta de superusuario. ***La deficiencia enorme de ese tipo de estrategias es que no pueden defender el servidor contra un usuario que ya está explotando los privilegios de superusuario***. Incluso los atacantes habilidosos y motivados pueden vencer los mismos controles de seguridad. Además, los administradores de sistemas, generalmente, administran y mantienen los controles de seguridad y representan, de hecho, uno de los grupos que la solución debería intentar controlar. Es el caso del zorro cuidando el gallinero.

Por los motivos anteriormente mencionados, resulta difícil proteger los activos electrónicos más confidenciales de una organización (como bases de datos de clientes, registros de pacientes de un hospital o información de propiedad) porque las capacidades del sistema operativo nativo no ofrecen la protección adecuada contra ataques accidentales o intencionales ni auditoría confiable de todo el entorno del servidor. Este problema se intensifica cuando los sistemas host de clientes externos contienen datos confidenciales y aplicaciones esenciales, o cuando los sistemas o la información clave se exponen a contratistas o son alojados por proveedores de servicios.

Los controles de acceso del sistema operativo también están en riesgo de ser analizados y evitados porque son **controles conocidos**. Cuando un atacante malintencionado obtiene acceso a una cuenta con privilegios, ya sea alguien externo con acceso no autorizado o un usuario interno, un primer paso usual es investigar la configuración de seguridad. Esto incluye ver los permisos del sistema operativo y buscar vulnerabilidades en los controles que se puedan aprovechar. Los usuarios malintencionados también buscarán modificar los registros del sistema operativo para ocultar sus huellas. Incluso en sistemas donde los controles de acceso están aplicados rigurosamente, los atacantes bien capacitados solo evitarán tomar acciones que generen alertas y ocasionen una detección. Solo un sistema de seguridad completamente externalizado, ***en el que se regulen incluso los superusuarios***, puede aportar **elementos inesperados** y **desconocidos** a un sistema de seguridad y proporcionar los controles de acceso y los registros de actividad de los usuarios necesarios para proteger realmente un sistema.

Además, los sistemas operativos son inherentemente incapaces de garantizar la integridad de sus propios controles. Todos los sistemas tienen cuentas con privilegios que pueden cambiar o eludir los controles de seguridad de ese sistema. Un usuario con el acceso correspondiente puede deshabilitar los controles necesarios para realizar una acción no autorizada y modificar los archivos de registro del sistema con el fin de borrar los registros de esa actividad.

Otro problema que surge de confiar en los controles de seguridad de los sistemas operativos es la **falta de uniformidad**.

Puede haber una gran variación en las capacidades y la disponibilidad de los controles de seguridad en las plataformas (los controles de los archivos y los directorios de UNIX son considerablemente diferentes de los de Windows). Esto puede generar problemas concretos de seguridad:

- Las políticas de seguridad se crean para adaptarse a las limitaciones de los sistemas y no para satisfacer las necesidades empresariales.
- La complejidad adicional de la administración de seguridad genera errores y omisiones.

Contenedores de shell

Un método común para controlar el uso de los controles de sistemas operativos de los usuarios con privilegios consiste en usar un contenedor de shell que se pueda configurar para permitir o denegar a usuarios específicos el acceso a ciertos comandos. Un contenedor de shell se ejecuta en modo usuario en el sistema operativo, donde el kernel (componente de un nivel inferior de un sistema operativo) procesa los comandos.

Los contenedores de shell tienen muchas debilidades:

- No pueden ofrecer protección contra la cuenta de superusuario. Los usuarios que tienen acceso a la cuenta raíz, al igual que aquellos que son expertos técnicos, siempre pueden eludir un contenedor de shell con estas técnicas:
  - El usuario raíz cancela el proceso del shell actual y el kernel crea un shell nuevo sin restricciones del contenedor.
  - Un usuario carga un script en el sistema de destino y ejecuta el archivo. Todos los comandos evitarán el contenedor de shell que debe ejecutar el kernel del sistema operativo. Este script podría modificar, eliminar o enviar fuera del sistema información confidencial y ser completamente invisible para el contenedor de shell, el cual no lo controlaría.
- Los contenedores de shell solo pueden proteger contra los comandos ingresados en un shell. Otras aplicaciones de un sistema (como Oracle) podrían tener brechas en la seguridad que se podrían aprovechar para ejecutar comandos malintencionados. Un contenedor de shell no detectará, controlará ni registrará estos comandos.
- Los registradores de pulsaciones de teclas también pueden ser ineficaces si son parte de un contenedor de shell, ya que solo capturan las teclas que se presionan, en vez de los comandos que se ejecutan. Un usuario malintencionado (administrador u otro) podría cargar un script que realiza diversas acciones. Un registrador de pulsaciones de teclas únicamente puede registrar que se ejecutó un script, no lo que este hizo en realidad. Esto genera falta de responsabilidad, lo que frustra el propósito de un registrador de pulsaciones de teclas.
- Los proveedores que apoyan el empleo de contenedores de shell suelen recomendar que no se utilice ni se comparta la contraseña raíz, lo cual no suele ser viable operativamente. Con frecuencia, las aplicaciones requieren la contraseña raíz para la instalación o el funcionamiento.

Sudo

Sudo (el superusuario hace) es un programa informático gratuito que permite a un administrador del sistema brindar a ciertos usuarios (o grupos de usuarios) la capacidad de ejecutar algunos comandos (o todos ellos) como raíz, a la vez que se registran todos los comandos utilizados. Sudo se usa en la mayoría de los entornos de UNIX y Linux, donde el personal de operaciones no necesita acceso a un shell de raíz, pero aún debe ejecutar algunos comandos como raíz (p. ej., iniciar o detener procesos, actualizar archivos de configuración específicos y reiniciar el servidor). Proporciona una capacidad importante (delegación de tareas con privilegios), sin embargo, por sí solo es un control inadecuado.

Sudo tiene muchas debilidades:

- Depende del uso de uno o más archivos sudoers, cuya administración puede ser prolongada, requerir muchos recursos y ser propensa a errores. Además, los archivos sudoers, y su administración, pueden presentar riesgos de seguridad debido a que los administran identidades con privilegios, las cuales, a su vez, pueden estar comprometidas.
- Sudo no proporciona capacidades de registro de clase empresarial. Este programa se basa en el registro del sistema de UNIX, que el usuario raíz puede alterar. No proporciona una rendición de cuentas por cada acción de sudo ya que no se registran todos los comandos que se ejecutan mediante sudo para rastrear al usuario original. Esto no facilita el cumplimiento de los requisitos de la PCI (industria de tarjetas de pago) y la SOX (Ley Sarbanes-Oxley).
- Sudo no audita ni rastrea las acciones basadas en el id. de usuario original que invoca el editor "vi", aunque el usuario ingrese a un shell. Cuando un usuario usa sudo para invocar este editor como raíz, existe la posibilidad de salir de él y ejecutar comandos shell con privilegios raíz. Con sudo de CA Privileged Identity Suite, todos estos comandos shell que se ejecutan se atribuyen al usuario original que efectúa la invocación de sudo.
- Sudo tiene graves restricciones de funcionalidad. No puede asignar ni restringir un archivo o una carpeta específicos del usuario o el acceso a un comando.
- Sudo falla si un usuario escala privilegios. Un usuario regular que explota una vulnerabilidad del sistema operativo para obtener acceso "raíz" evita todas las restricciones de sudo.
- El uso de controles del sistema operativo nativo también suele generar un cumplimiento incoherente de las políticas de seguridad entre servidores y plataformas. Se necesita un único conjunto de controles de acceso sólidos que se pueda hacer cumplir en plataformas dispares para neutralizar las diferencias de las plataformas.

Controles del proxy

Otro método para implementar controles del acceso es el proxy. En este método, todos los comandos atraviesan un "punto de cuello de botella" que puede filtrar (denegar) todos los comandos especificados por un conjunto de reglas. Este método puede prevenir que un usuario con privilegios elimine el shell reconociendo y bloqueando los comandos necesarios para hacerlo.

El proxy tiene muchas debilidades:

- Se lo puede evadir con aplicaciones. Un usuario puede crear y ejecutar un archivo que contenga comandos restringidos con un editor de texto (como vi). Un proxy no comprende qué acciones realiza el usuario en la aplicación. Tampoco puede detectar los comandos que se han "autocompletado" o ensamblado.
- El proxy se puede evadir con descargas externas. De modo similar a lo que ocurre con los contenedores de shell, un usuario también puede evitar el proxy por completo si descarga en el sistema de destino un archivo que contenga comandos restringidos mediante el empleo de diversos métodos, que van desde el FTP o SSH a una unidad USB física. No siempre es posible denegar el acceso a estas utilidades de transferencia de archivos, porque suelen ser necesarias para la administración y las tareas del sistema habituales.
- Un único comando que no está protegido se puede usar como un acceso indirecto para evitar los controles del proxy.
- El proxy puede ser ineficiente contra las vulnerabilidades del software. Los controles basados en el proxy son ineficientes contra los ataques que afectan el software vulnerable, como los ataques de día cero.

Controles de acceso y seguridad del host

Como mencionamos anteriormente, el uso de cuentas Superusuario compartidas normalmente resulta en usuarios con privilegios que tienen acceso innecesario a sistemas y datos fundamentales. Esto viola los principios básicos de seguridad de "privilegios mínimos" y "separación de funciones". Los sistemas operativos no tienen la capacidad de restringir acciones y acceso para múltiples personas con una cuenta compartida. Los controles de acceso específicos superan la seguridad del sistema operativo y ***examinan la identidad original del usuario para determinar si una acción se debe permitir o denegar***. Esto permite el verdadero acceso de privilegios mínimos.

Las capacidades que se describen a continuación son necesarias para garantizar que los administradores solo tengan los privilegios que necesitan para realizar su trabajo y nada más.

Cómo puede ayudar CA

CA Technologies brinda soluciones de administración de acceso con privilegios integrales y fáciles de implementar, con administración de credenciales integrada, autenticación sólida, control de acceso de confianza cero, filtración de comandos proactiva, monitoreo y registro de sesiones, y controles específicos sobre servidores de alto valor. La solución cuenta con dos opciones de implementación que brindan el nivel apropiado de defensa para distintas necesidades de seguridad y habilitan la defensa a fondo de cuentas con privilegios, para minimizar los riesgos de cumplimiento y seguridad.

- **CA Privileged Access Manager** proporciona la funcionalidad integral necesaria para prevenir violaciones, demostrar el cumplimiento e impulsar la eficiencia operativa y, así, proporcionar protección a la más amplia y profunda gama de infraestructura, incluido el centro de datos, centros de datos virtuales y redes definidos por software, además de nubes públicas o privadas.
- **CA Privileged Access Manager Server Control** mejora la seguridad y simplifica la auditoría y el cumplimiento mediante el control, monitoreo y auditoría de las actividades de usuarios con privilegios en servidores clave, con potentes controles específicos del acceso operativo a nivel del sistema y de las acciones de los usuarios con privilegios.
- **CA Threat Analytics for PAM** ofrece un conjunto potente de análisis del comportamiento de los usuarios y algoritmos de aprendizaje automático que lo ayudan a detectar y combatir los intentos de violaciones antes de que afecten su empresa.

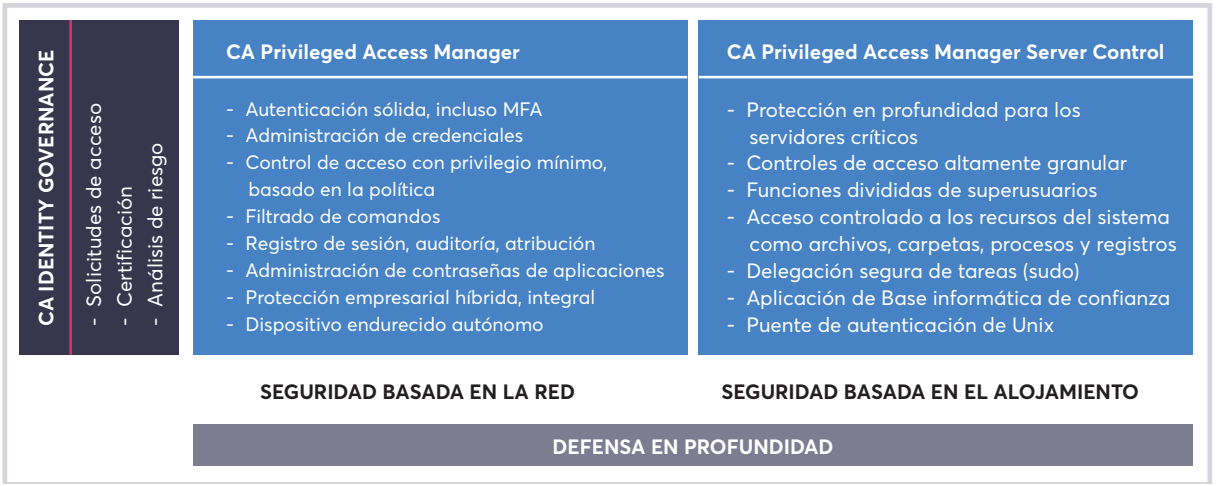


FIGURA A.
Los elementos clave de una estrategia de seguridad de defensa en profundidad de CA.

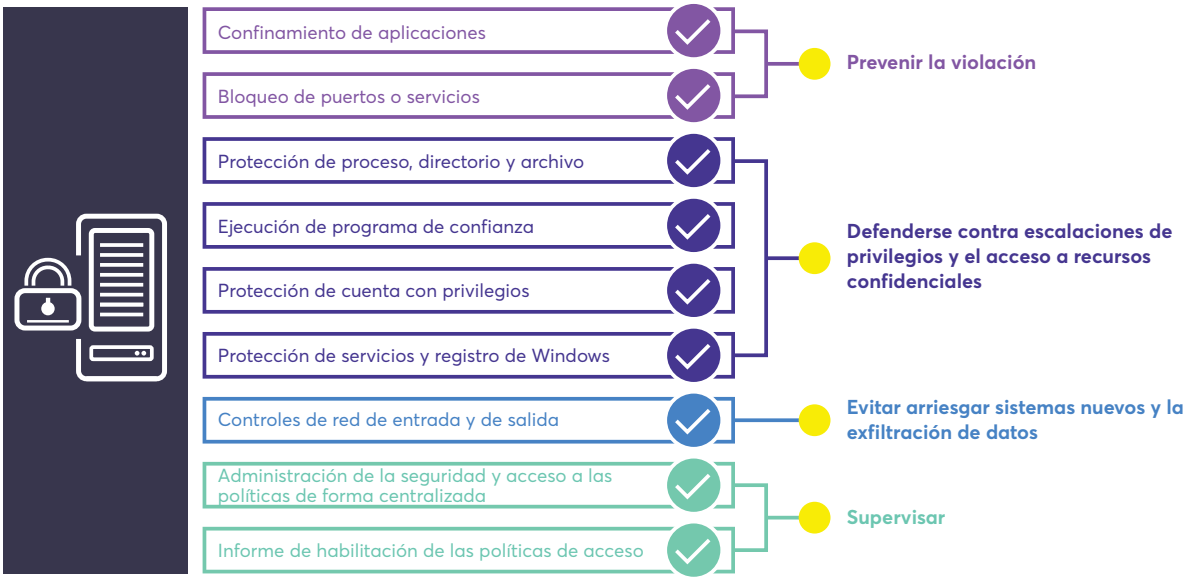
Una mirada de cerca a CA Privileged Access Manager Server Control

Para aquellas organizaciones que poseen requisitos de seguridad adicionales para servidores de alto valor que alojan activos esenciales empresariales, CA Privileged Access Manager Server Control ofrece control y protección de acceso detallado localizado a nivel de acceso al sistema operativo y a nivel de aplicación. Cuenta con protección a nivel de kernel basada en agentes disponible para archivos individuales, carpetas y comandos específicos basados en políticas o controles detallados de host específicos.

CA Privileged Access Manager Server Control maneja de manera única y elegante las brechas de seguridad inherentes a los modelos defectuosos de seguridad basados en Superusuarios de los servidores fundamentales para la misión. CA Privileged Access Manager Server Control brinda los siguiente:

- Uso del seguimiento de identificación de usuario original para la segregación de funciones (SoD) y responsabilidades, incluso cuando la cuenta de superusuario está siendo utilizada. Esto cambia fundamentalmente el modelo de seguridad basado en superusuarios. Por ejemplo, el usuario A que utiliza la cuenta raíz Linux tendrá privilegios diferentes a los del usuario B que usa la cuenta raíz Linux. Además, los registros de auditoría inviolables identificarán la identidad real del usuario detrás de todas las operaciones de superusuarios.
- Control de acceso específico a los recursos de archivo, directorio y procesos del sistema.
- Protección de la identificación del usuario y del cumplimiento del inicio de sesión.
- Carga y descarga del módulo de kernel en UNIX o Linux.
- Protección del registro de Windows.
- Protección entrante y saliente TCP/IP.
- Delegación de tareas (reemplazo seguro de Sudo) para UNIX/Linux y Windows.
- Capacidad de ocultar la contraseña raíz.
- Monitoreo integral de archivos y programas.
- Autoprotección contra la desviación o finalización.

FIGURA B.
Una mirada de cerca a CA Privileged Access Manager Server Control.



Beneficios de la solución

CA Privileged Access Manager brinda capacidades y controles que impiden activamente que los atacantes utilicen componentes clave de sus ataques, además de reducir riesgos y mejorar la eficacia operativa. Más concretamente, CA Privileged Access Manager les permite a las organizaciones realizar lo siguiente:

- **Reducir el riesgo.** Evitar el acceso no autorizado y limitar el acceso a los recursos previamente aprobados una vez que se concede la entrada a la red. Proteger las contraseñas y otras credenciales contra la utilización no autorizada y la vulneración. Limitar las acciones que los usuarios pueden realizar en los sistemas. Prevenir la ejecución de comandos no autorizados y movimiento lateral dentro de la red.
- **Aumentar la responsabilidad.** Observar la atribución completa de la actividad del usuario, incluso cuando se utilizan cuentas compartidas. Mediante el registro, la grabación de la sesión y las advertencias de usuario integrales, capturar la actividad y proporcionar un elemento disuasorio de la conducta no autorizada.
- **Mejorar la auditoría y facilitar el cumplimiento.** Simplificar el cumplimiento mediante el respaldo de nuevos requisitos emergentes de autenticación y control de acceso, y limitar el alcance de los requisitos de cumplimiento a través de la segmentación lógica de la red.
- **Reducir la complejidad y aumentar la productividad del operador.** El inicio de sesión único con privilegios no solo limita el riesgo, sino que también aumenta la productividad de los administradores individuales al hacer que sea más fácil y rápido el acceso a los sistemas y recursos que necesitan administrar. La definición y ejecución centralizada de políticas simplifican la creación y aplicación de controles de seguridad. Esta solución puede proteger la extensa infraestructura de TI híbrida, ya que cubre los centros de datos físicos tradicionales (servidores, dispositivos en red, bases de datos, interruptores y recursos relacionados) y crea plataformas virtuales y en la nube. Esto ayuda a proteger la infraestructura de administración subyacente y los recursos implementados en centros de datos y redes definidos por software, entornos de infraestructura como servicio (IaaS) y ofertas de software como servicio (SaaS).

Los clientes se dan cuenta de que las soluciones de CA son fáciles de adoptar y evitan los costos ocultos del hardware. La facilidad de administración o de uso ayuda a entregar tiempo de posicionamiento en el mercado así como la habilidad de escalar, por lo que no solo puede preparar su infraestructura de TI híbrida para el futuro, sino también reducir el riesgo, así como lograr y mantener el cumplimiento. Recomendamos que los clientes que actualmente tienen CA Privileged Access Manager instalado y desean proteger sus servidores fundamentales para la misión, realicen una actualización a CA Privileged Access Manager Server Control. Si recién comienza a mejorar la postura de seguridad de su organización con un programa de defensa en profundidad, considere CA Privileged Access Manager para mitigar el riesgo de amenazas internas y abusos de cuentas con privilegio.

Conclusiones

Para defenderse contra violaciones de datos costosas, las empresas inteligentes protegen y automatizan el acceso a cuentas con privilegios en sus servidores más cruciales. Emplear un modelo de confianza cero con una estrategia de defensa en profundidad para la seguridad que incluya la administración del acceso con privilegios le ofrece a su organización la mejor oportunidad de protección contra las amenazas en continua evolución. CA Privileged Access Manager brinda capacidades y controles que impiden activamente que los atacantes utilicen componentes clave de sus ataques, además de reducir riesgos y mejorar la eficacia operativa.

Próximos pasos

Lea la **Guía para compradores de CA Technologies Privileged Access Management** para obtener más información sobre la protección del acceso y lo que las empresas pueden hacer para prevenir las violaciones de datos.

Para obtener más información sobre Privileged Access Management de CA, visite: **ca.com/ar/pam**

Comuníquese con CA Technologies

CA Technologies (NASDAQ: CA) ofrece soluciones de administración de TI que ayudan a los clientes a administrar y proteger los entornos de TI complejos para permitir la provisión de servicios de negocios ágiles. Las organizaciones aprovechan el software de CA Technologies y las soluciones SaaS para acelerar la innovación, transformar la infraestructura y proteger los datos y las identidades, desde el centro de datos hasta la nube. CA Technologies asume el compromiso de garantizar que los clientes obtengan los resultados deseados y el valor empresarial previsto, gracias a la utilización de nuestra tecnología. Para obtener más información sobre los programas para el éxito del cliente, visite www.ca.com/ar/company/customer-success.html. Para obtener más información sobre CA Technologies, visite ca.com/ar.

CS200-305094_0917