LIBRO BLANCO | DICIEMBRE DE 2015

Conformidad con la PCI

mediante la gestión del acceso con privilegios

ca technologies

Resumen ejecutivo

Reto

Las organizaciones que asumen transacciones con tarjetas de crédito o de débito se ven sometidas a una presión cada vez mayor para satisfacer los requisitos de diversas normativas. En concreto, deben cumplir la versión 3 de la normativa Payment Card Industry Data Security Standard (PCI DSS), que entró en vigor en enero de 2015.[1] Este estándar estableció diversos requisitos para proteger las redes y los sistemas relevantes de las organizaciones, que albergan el entorno de datos de los titulares de las tarjetas (CDE). Ante unos requisitos que exigen reforzar la autenticación y el control del acceso en el CDE, las organizaciones se enfrentan al difícil reto de implementar la autenticación de varios factores, el control del acceso, y las prácticas o herramientas de generación de informes de actividades, sobre todo en el acceso administrativo o con privilegios a estos sistemas.

Oportunidad

Los requisitos de la PCI DSS relacionados con la gestión del acceso con privilegios señalan los riesgos asociados al uso indebido de las cuentas con privilegios y al acceso que proporcionan a los activos esenciales del negocio. Prácticamente, todos los incidentes de seguridad recientes apuntan a que las credenciales o los usuarios con privilegios constituyen un importante vector de ataque en la culminación de una infracción. Si se adopta un enfoque eficaz de gestión del acceso con privilegios, las organizaciones podrán restringir, registrar y monitorizar todas las actividades que realicen las cuentas con privilegios, por ejemplo, los administradores de bases de datos, sistemas y redes. En consecuencia, obtienen un control y una visibilidad más eficaz de los usuarios con privilegios y del acceso de los superusuarios a los activos más importantes del negocio. Sin esta capacidad, muchas organizaciones no solo tienen problemas para cumplir los requisitos de control del acceso, autenticación e identificación de la versión 3 de la PCI DSS, sino que también se quedan cortas a la hora de minimizar el nivel de exposición a posibles infracciones y ataques.

Ventajas

Un enfoque de defensa en profundidad de la gestión del acceso con privilegios proporcionada en una solución fácil de implementar, como CA Privileged Access Manager, puede ayudar a las organizaciones a abordar los requisitos de la versión 3 de la PCI DSS y a proteger mejor no solo sus CDE, sino también toda su infraestructura de TI híbrida, que abarca sus entornos virtuales, en la nube, de redes y de servidores. Como resultado, las organizaciones obtendrán una mejor seguridad frente a las infracciones, así como menos riesgos de incumplimientos de la PCI DSS.

Sección 1:

La necesidad de gestionar el acceso con privilegios

La necesidad de gestionar el acceso con privilegios es mayor que nunca. Todos los estudios revelan que las defensas de seguridad tradicionales fallan de forma sistemática. Algunos de ellos señalan incluso que prácticamente todas las organizaciones tienen, como mínimo, un activo en riesgo en cualquier momento.[2] Los medios de comunicación suelen informar de importantes fugas de datos, como las que sufrieron Target a finales del 2013, Home Depot en el 2014 y la Oficina de Gestión de personal (Office of Personel Management u OPM) de EE. UU. en el 2015, donde algunos terceros llegaron a usar credenciales robadas. De hecho, en el informe de investigaciones de fugas de datos de Verizon del 2014 se citó el uso de las credenciales robadas como la principal amenaza para las organizaciones.[3]

Estas no suelen ser conscientes de los peligros que implican la enorme cantidad de cuentas con privilegios que gestionan y el uso de este tipo de cuentas. Las cuentas con privilegios no solo las usan los empleados de una organización, sino también terceros, como proveedores, contratistas y otras personas que prestan servicios técnicos a sistemas, redes, dispositivos y aplicaciones. Una sola empresa podría tener miles o incluso cientos de miles de cuentas con privilegios, y cada una de ellas presenta un riesgo de seguridad diferente a la organización.

Lo que se pretende con la gestión del acceso con privilegios es que los administradores realicen acciones con mayor responsabilidad y visibilidad. Los administradores han confiado plenamente en el modelo tradicional, pero ofrece un ingenuo punto de vista que obvia dos problemas importantes: la posibilidad de que un administrador descontento se convierta en una amenaza interna y las consecuencias de que un atacante externo comprometa la seguridad de una cuenta administrativa, sobre todo cuando dicho administrador es un distribuidor u otro tercero.

Una forma de evitar esto es adoptando un modelo llamado “de confianza cero”, es decir, un enfoque que aborda CA Privileged Access Manager (anteriormente, Xceedium Xsuite, un componente clave de las soluciones de gestión del acceso con privilegios de CA Technologies) cuando se considera que los administradores no son totalmente fiables. Con este modelo, se reduce el número de infracciones y el nivel de gravedad de aquellas que se seguirán produciendo. Los requisitos de la PCI DSS reflejan en parte este modelo de cero confianza, por ejemplo, el requisito 7.1.2, que trata sobre restringir el acceso para que los identificadores de usuarios con privilegios obtengan los privilegios mínimos necesarios para llevar a cabo las responsabilidades del cargo correspondiente.

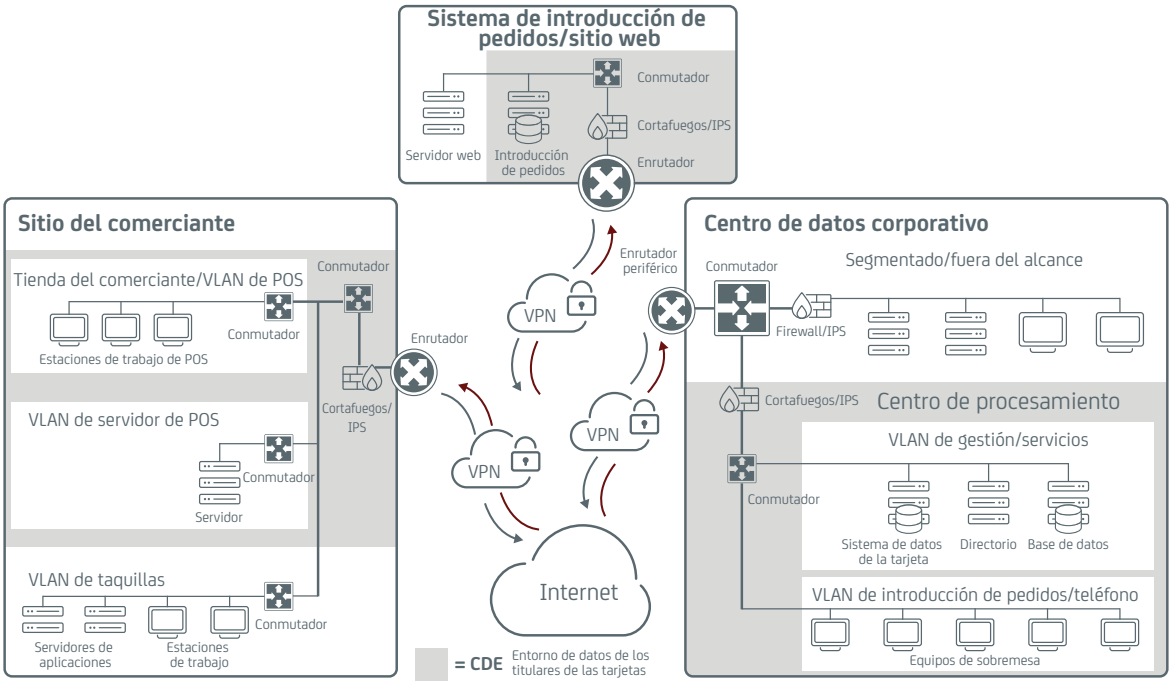
No obstante, si bien la conformidad con la PCI garantiza una base sólida para proteger los CDE, para aplicar un sistema de defensa eficaz contra las amenazas de hoy en día no basta con realizar una serie de comprobaciones rutinarias y cumplir solo los requisitos mínimos. Con la gestión del acceso con privilegios se cumplen con creces los requisitos de la PCI para proteger de una forma más eficaz el CDE de una organización.

Además de conseguir cumplir la PCI, otros motivos importantes por los que se precisa gestionar el acceso con privilegios son la interrupción de la cadena de ciberataques, la mitigación de las amenazas internas, los comandos de registro y monitorización, y la eliminación de las contraseñas no modificables.

Ilustración A:

El alcance los requisitos de la PCI DSS

La versión 3 de la PCI DSS exige la implantación de medidas para proteger el CDE.



Interrupción de la cadena de ciberataques

El concepto básico de una cadena de ciberataques consiste en que los atacantes siguen un patrón repetitivo para obtener acceso a un sistema (o extender dicho acceso). Cuando lo consiguen, pasan a aumentar los privilegios. Estos privilegios se suelen usar para obtener acceso a otro sistema o para extender el acceso actual. A continuación, vuelven a aumentar los privilegios y continúan esta cadena de aprovechamiento hasta que alcanzan el objetivo final. Si esta cadena de aprovechamiento puede romperse en cualquier punto del ciclo, podremos detener el ataque antes de que llegue al auténtico objetivo del ataque.

CA Privileged Access Manager proporciona todas las capacidades que nos ayudarán a interrumpir la cadena de ciberataques. Por ejemplo, CA Privileged Access Manager admite la autenticación de varios factores para cuentas con privilegios, con lo que serán mucho más difíciles de atacar, ya que el delincuente necesita comprometer varias credenciales de una misma cuenta. Asimismo, gracias al uso de privilegios mínimos en lo que respecta a qué comandos podrán ejecutar las cuenta con privilegios en cada componente del CDE, se reduce el acceso a la información confidencial, lo que dificulta más que un atacante obtenga acceso no autorizado a datos de interés.

Otra forma con la que CA Privileged Access Manager ayuda a interrumpir la cadena de ciberataques es posibilitando la segmentación de la red. De este modo, se restringe las subredes a las que podrá acceder una cuenta con privilegios concreta y los sistemas de dichas subredes que podrán administrarse. Por otro lado, la segmentación de la red ayuda a limitar la propagación lateral de los ataques de un sistema a otro; además, restringe la visibilidad del atacante de la red de una organización. Del mismo modo, CA Privileged Access Manager ofrece un agente de filtro de sockets (SFA), que evita que un administrador abra una conexión de red no autorizada a otro sistema, por ejemplo, para intentar conectarse mediante SSH o Telnet a un host autorizado a través de una política de CA Privileged Access Manager.

Fuentes como Mandiant recomiendan específicamente todas estas capacidades de CA Privileged Access Manager para reducir el fraude de las tarjetas de crédito.[4]

Mitigación de las amenazas internas

Aunque los requisitos de la PCI se centran en los atacantes externos, también reconocen la importancia de las amenazas internas, que suponen un problema acuciante para las organizaciones de hoy en día. En un estudio, se señaló que más de un 10 % de empleados robaron información de sus empleadores con fines lucrativos o conocían a personas que lo habían hecho.[5]

CA Privileged Access Manager ayuda a mitigar las amenazas internas de diversas formas. En primer lugar, la implementación de los principios de privilegios mínimos restringe qué comandos podrá ejecutar un empleado interno y en qué componentes del CDE. De esta forma, se minimiza el daño que puede provocar el personal interno. En segundo lugar, el registro y la monitorización de todas las actividades de las cuenta con privilegios proporcionan un registro detallado de todos los comandos ejecutados, con un seguimiento por identificadores que pertenecen a personas concretas, no genéricos (compartidos).

Comandos de registro y monitorización

Por muy sólidos que sean los controles de seguridad, siempre encontraremos puntos débiles, así que, con independencia del entorno, será inevitable que se produzcan infracciones. Como CA Privileged Access Manager registra y monitoriza todas las actividades que se producen en las cuentas con privilegios, simplifica en gran medida los procesos forenses para determinar las acciones que los atacantes llevaron a cabo con éxito usando credenciales administrativas no autorizadas.

Eliminación de contraseñas no modificables

Muchos desarrolladores de software, administradores y otros usuarios siguieron la práctica de incluir contraseñas no modificables en scripts, códigos fuente y otras partes. Estamos ante una vulnerabilidad importante, dado que los desarrolladores de software, los comprobadores y otros usuarios pueden acceder a estas contraseñas, y los atacantes también saben cómo encontrarlas cuando se infiltran en un sistema, así que pueden obtener acceso a otros sistemas, como las bases de datos de titulares de tarjetas. CA Privileged Access Manager proporciona unas capacidades de autenticación de aplicación a aplicación que acaban con la necesidad de tener que incluir contraseñas no modificables.

Sección 2:

Cómo la gestión del acceso con privilegios puede ayudar a cumplir la PCI

Tal y como hemos comentado anteriormente, la gestión del acceso con privilegios constituye una parte esencial de la conformidad con la PCI. En los entornos empresariales habituales no se pueden cumplir una multitud de requisitos de la PCI sin emplear una solución de gestión del acceso con privilegios. Por ejemplo, un importante minorista tuvo que hacer frente a una multa de 100 000 dólares mensuales debido a que no cumplió los requisitos de la PCI en materia de identificación, autenticación y control del acceso. Al incorporar CA Privileged Access Manager a su cartera de soluciones de seguridad, este minorista pudo cumplir los requisitos anteriores y evitar evitar futuras multas.

Esta solución aborda los siguientes requisitos de la PCI.[6]

Requisito 2: No utilizar los valores predeterminados tal como los proporciona el distribuidor como contraseñas del sistema ni otros parámetros de seguridad

CA Privileged Access Manager aborda este requisito de dos formas diferentes. En primer lugar, cuando se utiliza durante la implementación de sistemas, puede controlar las cuentas con privilegios predeterminadas y restablecer las contraseñas predeterminadas de dichas cuentas. En segundo lugar, restringe los protocolos que pueden emplearse para el acceso administrativo remoto, como SSH o SSL/TLS. De esta forma, se evita tener que realizar labores de administración de sistemas en redes que emplean protocolos no seguros.

Requisito 6: Desarrollar y mantener sistemas y aplicaciones de seguridad

Una parte importante de este requisito consiste en la gestión adecuada de las credenciales y la separación de funciones en los entornos de desarrollo, prueba y producción. CA Privileged Access Manager aplica en todos estos entornos un control del acceso basado en roles para cuentas con privilegios, con lo que permite separar las funciones y, al mismo tiempo, facilitar también la eliminación sencilla de las cuentas de desarrollo y de prueba, así como otras que ya no se requieran cuando se implemente un sistema o una aplicación.

Requisito 7: Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber del negocio

CA Privileged Access Manager permite a las organizaciones implementar el principio de privilegios mínimos para los accesos con privilegios, un área que suele pasarse por alto. En concreto, el modelo de cero confianza de CA Privileged Access Manager aplica un control del acceso exhaustivo para usuarios individuales con privilegios o grupos de este tipo de usuarios (por ejemplo, administradores de bases de datos). De este modo, se se restringen los componentes del sistema a los que cada usuario o grupo puede acceder (por ejemplo, servidores, dispositivos de red y aplicaciones) y los comandos que pueden ejecutar en cada uno de estos componentes. CA Privileged Access Manager puede integrarse con Active Directory, LDAP y otros directorios empresariales con el fin de volver a utilizar sus definiciones de roles y grupos.

Requisito 8: Identificar y autenticar el acceso a componentes del sistema

CA Privileged Access Manager respalda prácticamente todas las secciones del requisito 8. Esta solución precisa un identificador único para cada usuario con privilegios, proporciona todas las funciones de gestión de contraseñas estándares, y respalda una amplia variedad de tecnologías de autenticación de varios factores y de un solo factor. En concreto, CA Privileged Access Manager respalda el requisito 8 de la siguiente forma:

- **8.1.** CA Privileged Access Manager puede identificar de forma única cada usuario con privilegios, incluso cuando las organizaciones utilizan cuentas compartidas para determinados componentes de la infraestructura, como los routers. Asimismo, posibilita la separación de funciones entre los usuarios con privilegios. Proporciona funciones estándares para finalizar de forma inmediata los privilegios de acceso revocados, con lo que se desactivan las cuentas con privilegios y se aplican políticas de bloqueo para los intentos de autenticación fallidos, así como políticas de reautenticación para las sesiones inactivas.
- **8.2.** Se integra con numerosos métodos de autenticación, con lo que se requiere la autenticación de todos los usuarios con privilegios. Almacena las contraseñas y otras credenciales (por ejemplo, claves criptográficas privadas) en un almacén con un cifrado seguro y las transmite exclusivamente por canales cifrados. Asimismo, aplica políticas estándares de reutilización, antigüedad, seguridad y longitud de contraseñas.
- **8.3.** Admite numerosos métodos de autenticación de varios factores, certificados RADIUS y X.509, y tarjetas inteligentes.
- **8.5 y 8.6.** Permite a las organizaciones utilizar cuentas compartidas en segundo plano al mismo tiempo que requiere que cada usuario con privilegios, incluidos los terceros, se identifiquen y autentiquen de forma única. Entre estos procesos de identificación única se encuentra el uso de tarjetas inteligentes, certificados digitales, tokens criptográficos y otros tipos de credenciales que no son contraseñas.
- **8.7.** Restringe el acceso a la base de datos de titulares de tarjetas solo a los administradores autorizados. Asimismo, ofrece capacidades de autenticación de aplicación a aplicación con el fin de garantizar que los usuarios no puedan acceder a las credenciales de las aplicaciones ni reutilizarlas.

Requisito 10: Rastrear y monitorizar todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas

Al igual que en el requisito 8, CA Privileged Access Manager respalda prácticamente todas las secciones del requisito 10. CA Privileged Access Manager registra todas las actividades que se llevan a cabo usando las cuentas con privilegios.

Se incluyen los registros de auditoría en formato Syslog y las grabaciones DVR de sesiones de administradores, con etiquetas en dichas grabaciones que señalan posibles infracciones de políticas con el fin de agilizar el proceso de revisión. CA Privileged Access Manager respalda el requisito 10 de la siguiente forma:

- **10.1.** CA Privileged Access Manager vincula cada instancia de acceso con privilegios a una persona concreta. Asimismo, proporciona pistas de auditoría para el acceso con privilegios con todos los componentes del sistema.
- **10.2.** Utiliza capacidades nativas de Syslog y registro con el fin de generar pistas de auditoría automatizadas que registren todas las acciones que lleven a cabo los usuarios con privilegios en servidores, dispositivos de red y otras aplicaciones. Se incluyen todas las actividades de autenticación e identificación de cuentas con privilegios. Asimismo, restringe el acceso a las pistas de auditoría, de modo que solo los usuarios autorizados puedan consultarlas, además de registrar dichas actividades.
- **10.3.** Registra todos los campos que exige la PCI en cada evento registrado, incluidos la identificación de usuarios, el tipo de evento, la fecha y hora, el éxito o el fracaso, el origen de los eventos, y la identidad de los recursos afectados (nombre de host, etc.).
- **10.4.** Utiliza la tecnología de sincronización horaria (es decir, Network Time Protocol [NTP]) con el fin de realizar la sincronización de relojes.
- **10.5.** Utiliza técnicas hashing para identificar alteraciones con grabaciones y registros de auditoría. Asimismo, proporciona capacidades de reenvío de Syslog con el fin de realizar copias de seguridad de registros de auditoría en almacenamientos de registros centralizados.
- **10.7.** Utiliza Syslog y sus capacidades de reenvío, de modo que pueden mantenerse los registros de auditoría durante el tiempo que se desee.

Requisito 12: Mantener una política que aborde la seguridad de la información

CA Privileged Access Manager permite capturar y aplicar políticas de usuarios con privilegios. Asimismo, CA Privileged Access Manager registra todos los intentos de infracciones de políticas, que forman parte de todo proceso de evaluación de riesgos.

Protección del CDE desde una perspectiva de control de servidores

Las capacidades de gestión del acceso con privilegios de CA Technologies también abordan otros requisitos para realizar un control del acceso localizado y muy exhaustivo en el host con el objetivo de proteger más aún los recursos de alto valor, incluido el CDE. CA Privileged Access Manager Server Control proporciona una capa adicional esencial de protección en todas las plataformas de servidores, con lo que permite obtener un control del acceso exhaustivo, una gestión basada en políticas y las auditorías seguras que resultan esenciales para proteger los activos electrónicos. Pueden designarse políticas de acceso para regular el acceso a procesos, archivos, programas y recursos de servidores empleando diversos criterios.

Sección 3:

Cambios de la versión 2 a la 3 de la PCI DSS

Cuando se actualizó la PCI DSS de la versión 2 a la 3, se incorporaron protecciones significativas para el CDE, incluidas las siguientes:

- Implementar la segmentación de la red para el CDE con el fin de aislar sus sesiones entre sí de forma más eficaz. Esto implica garantizar que todos los datos que fluyen entre los componentes del sistema estén documentados y auditar todas las actividades que lleven a cabo los usuarios con privilegios.
- Realizar pruebas de penetración en el perímetro de CDE.
- Gestionar las credenciales e implementar capacidades de control del acceso con privilegios, así como auditar todo el acceso al CDE.
- Aplicar controles de seguridad más estrictos para los proveedores de servicios.[7]

Estas protecciones subrayan la necesidad de contar con una solución de gestión del acceso con privilegios, como CA Privileged Access Manager, para proteger el CDE y abordar los requisitos de la PCI. En la mayoría de los entornos, la única forma de implementar de forma eficaz el principio de privilegios mínimos en el control del acceso para administradores y el registro exhaustivo de las actividades que realice este tipo de usuario consiste en utilizar una solución de gestión del acceso con privilegios. Además, la gestión del acceso con privilegios puede resultar inestimable para implementar la segmentación de la red y monitorizar todas las actividades con datos que fluyen entre los segmentos de la red.

En la actualización de la PCI DSS se incorporaron otros cambios relacionados con la gestión del acceso con privilegios. En primer lugar, se reestructuró en profundidad el requisito 8 sobre identificación y autenticación, por lo que, a primera vista, da la impresión de que se ha modificado considerablemente. Sin embargo, el objetivo principal consistió simplemente en reestructurar este requisito.

El cambio más significativo fue la incorporación del requisito 8.6, que dice así: "Cuando se emplean mecanismos de autenticación distintos a las contraseñas, como tokens criptográficos o tarjetas inteligentes, solo deben estar a disposición de un único usuario; no se permiten utilizar mecanismos de autenticación compartidos". Tal y como explicamos en la sección anterior, CA Privileged Access Manager aborda este nuevo requisito.

Sección 4:

Ventajas

Las organizaciones que implementan soluciones de gestión del acceso con privilegios obtienen mayor seguridad, reducen los riesgos de amenazas externas e internas, y mejoran la conformidad con las normativas, incluida la PCI DSS.

CA Privileged Access Manager no solo aborda la conformidad con la PCI DSS, sino que también mejora seguridad global de la empresa de la forma más rentable. En concreto, puede aportar las siguientes ventajas a las organizaciones:

- **Reducción de costes.** CA Privileged Access Manager puede ayudar a reducir significativamente el coste de las auditorías de PCI DSS, sobre todo porque proporciona una manera sencilla y muy rentable de segmentar de forma lógica la red de una organización. Se trata de un dispositivo similar a un proxy que trabaja en la capa de las aplicaciones de la red y controla los usuarios con privilegios que pueden acceder a los sistemas. La segmentación lógica del plano de gestión permite a las organizaciones mantener las topologías de red físicas actuales al mismo tiempo que separan los sistemas con datos de titulares de tarjetas en islas donde el acceso se controla de forma estricta. Con este enfoque, gracias a CA Privileged Access Manager, las organizaciones pueden aislar de forma lógica los sistemas con datos de titulares de tarjetas, lo que limita el alcance de las auditorías de PCI sin tener que realizar un gran desembolso en segmentar las redes de manera física.
- **Mayor seguridad.** El enfoque de defensa en profundidad de seguridad de CA Privileged Access Manager ayuda a las empresas a implementar una serie de controles exhaustivos. El objetivo radica en reducir los riesgos asociados a los usuarios con privilegios y proporcionar una mayor protección contra las amenazas externas, lo que evita que se produzcan infracciones o que se minimice su impacto.
- **Menos tiempo de protección y gestión.** Como la solución se implementa y gestiona fácilmente desde una única plataforma, se mejora y agiliza el control del acceso con privilegios y la protección de las credenciales en sistemas de toda la infraestructura híbrida de la empresa (centros datos tradicionales, entornos virtualizados, nubes públicas o cualquier combinación de estas tecnologías). Todo ello sin los gastos generales que, normalmente, van asociados a otros enfoques.

Sección 5:

Conclusiones

La gestión del acceso con privilegios resulta fundamental para abordar la conformidad con la PCI. No obstante, su importancia va más allá de cumplir meramente los requisitos de la PCI, ya que permite que una organización mejore su seguridad global contra las amenazas externas e internas que existen en la actualidad. CA Privileged Access Manager proporciona una manera eficaz de implementar capacidades de gestión del acceso con privilegios que cumplan la PCI y satisfagan las exigencias en seguridad.

Al utilizar CA Privileged Access Manager, las organizaciones pueden:

- reducir los costes de cumplimiento de la PCI abordando muchos de sus requisitos con una única solución lista para usar que se integra a la perfección con las soluciones actuales de la organización.
- ahorrar en gastos relacionados con infracciones y mantener la reputación de la organización evitando muchas fugas de datos y minimizando el impacto que las infracciones que sigan produciéndose.

1. PCI DSS v3.0, https://www.pcisecuritystandards.org/document_library?agreements=pcidss&association=pcids
2. Cisco 2014 Annual Security Report, http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
3. Verizon 2014 Data Breach Investigations Report, http://www.verizonenterprise.com/DBIR/2014/?utm_source=earlyaccess&utm_medium=redirect&utm_campaign=DBIR
4. M-Trends 2014: Beyond the Breach, https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf
5. Data Leakage Worldwide: The High Cost of Insider Threats, http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-506224.pdf
6. PCI DSS v3.0, https://www.pcisecuritystandards.org/document_library?agreements=pcidss&association=pcids
7. PCI DSS Summary of Changes v2.0 to v3.0, https://www.pcisecuritystandards.org/document_library?agreements=pcidss&association=pcids

CS200-163851_1215