Resiliencia de la ciberseguridad en una era de expansión de identidades

Cómo la seguridad de identidad unificada puede ayudar a cerrar las brechas de exposición críticas y apoyar las iniciativas de Zero Trust

ONE IDENTITY by Quest

Como CISO, sus preocupaciones expresadas a la junta directiva acerca de la ciberseguridad se han visto acalladas en gran medida por los desafíos macroeconómicos, la complejidad de los procesos y la necesidad de permitir un aumento drástico en el acceso remoto.

Ahora es sábado por la mañana y su teléfono de trabajo suena en su casa.

¿Por qué su director de seguridad de tecnología informática le envía mensajes de texto y le llama al mismo tiempo?

"No son buenas noticias", piensa.

No lo son.

Ha habido un ciberataque. Se desconoce su alcance, pero su director de seguridad de tecnología informática le dice que el equipo está evaluando la situación.

Se le vienen varias preguntas a la cabeza:

- ¿Cómo han entrado?
- ¿Ha sido un usuario interno parte del ataque?
- ¿A cuánta información privilegiada han accedido?
- ¿Cómo le voy a contar esto a la junta directiva?
- ¿Ayudará o perjudicará esto mi presupuesto de ciberseguridad propuesto para el próximo año fiscal?
- ¿Debo actualizar mi currículum?

Ha habido un ciberataque. Se desconoce su alcance, pero su director de seguridad de tecnología informática le dice que el equipo está evaluando la situación.

El riesgo de expansión de la identidad

Su organización ha sido víctima de su propia expansión de identidad. Se trata de un riesgo de seguridad de creación insidiosa que va tomando forma progresivamente bajo el pretexto de la productividad y la innovación destinadas a ayudar a la organización a funcionar de forma más rápida y eficaz.

Parecía lo correcto para apoyar a la empresa con recursos que mejoraran la ejecución de sus tareas diarias. El problema es que cada nuevo sistema, aplicación o base de datos a la que se conectan sus usuarios tiene un proceso y requisitos únicos de gestión de credenciales. Algunos menos estrictos que otros. Algunos menos seguros que otros. Algunos mejores. Algunos peores. A menudo, no hay visibilidad sobre quién tiene acceso y qué hacen con ello.

Además de esos problemas, se encuentra la necesidad constante de ofrecer acceso remoto con privilegios a sus administradores; gestionar un número cada vez mayor de usuarios externos que se conectan con una cantidad aún mayor de dispositivos, sistemas operativos y exploradores; y los intentos de controlar un gran volumen de cuentas, ID y contraseñas.

Tiene una expansión de identidad.

¿Qué va a hacer para controlarla, gestionarla y equilibrar la productividad con la seguridad?

Lo siguiente es un resumen general de alto nivel de ocho pasos sobre la expansión de la identidad. En este libro electrónico, se analiza la desaparición del perímetro de seguridad tradicional, el logro de la resiliencia de la ciberseguridad y el modelo Zero Trust. Descubrirá cómo adoptar un enfoque holístico y cómo una plataforma de seguridad de identidad unificada puede proteger su organización y su reputación.

Tendencias que impulsan la expansión de la identidad

Como se ha descrito anteriormente, el panorama de tecnología informática está evolucionando ante nuestros ojos, lo que repercute considerablemente en cómo las organizaciones deben protegerse para garantizar la resiliencia de la ciberseguridad. Es difícil mantenerse al día. Entre algunos de los ejemplos de cambios a los que los profesionales de la seguridad deben adaptarse rápidamente se incluyen los siguientes:

- La rápida desaparición de la oficina y la infraestructura tradicionales
- Las organizaciones dispersas han llegado para quedarse: los empleados trabajan cada vez más desde casa y desde ubicaciones remotas
- La dependencia de contratistas y socios externos para ampliar y aumentar el valor
- El impulso para adoptar nuevas plataformas y tecnologías que permitan el acceso remoto y entornos de trabajo no tradicionales
- El auge de la informática principalmente en la nube y la distribución de servicios en la nube a diferentes ubicaciones físicas
- El deseo constante de optimizar la eficiencia, la accesibilidad y el ahorro de costes
- Una mayor complejidad de la tecnologia informática debido a la adaptación a las normativas de privacidad, como GDPR, HIPAA y CCPA, y a los procesos de intercambio de datos que ayudan a mantener la privacidad o la seguridad
- La automatización robótica de procesos (RPA) se está empleando de forma gradual para optimizar los procesos que antes eran manuales y consumían mucho tiempo.

Cada una de estas tendencias crea nuevas oportunidades para lograr eficiencia y una mayor resiliencia de la ciberseguridad, pero cada una puede dar lugar a nuevos problemas también. ¿Por qué? Un hilo común entre cada uno es la explosión de identidades. En pocas palabras, más personas (internas y externas), robots, máquinas y dispositivos necesitan acceder a los activos de la empresa. Además de eso, las cuentas de usuario se multiplican a medida que las organizaciones admiten un panorama de tecnología informática multigeneracional. Todo esto contribuye al que quizás sea el mayor reto de ciberseguridad hasta el momento: la expansión de la identidad.

ONE IDENTITY by Quest

Por qué es importante controlar la expansión

Todos sabemos que los infractores aprovechan las brechas de ciberseguridad dondequiera que existan y, a menudo, a gran escala. Esto se está produciendo en tiempo real con la expansión de la identidad, ya que hemos visto un aumento masivo de ataques de robo de identidad y credenciales recientemente.

Por ejemplo, el informe de investigaciones de infracción de datos (DBIR, por sus siglas en inglés) de 2021 de Verizon descubrió que el 63 % de todas las infracciones involucraban credenciales, mientras que CensusWide reveló que casi la mitad de las organizaciones encuestadas se vieron afectadas por el robo de credenciales con privilegios el año anterior.

Verá el impacto devastador de estas brechas relacionadas con la identidad que aparecen en la página principal de los portales de noticias prácticamente todos los días. El hackeo de SolarWinds, el ciberataque de Colonial Pipeline y una vulnerabilidad de Exchange Server son solo algunos ejemplos de incidentes de gran repercusión. Estas infracciones no solo afectaron a la seguridad, el sustento y la protección de una persona normal, sino que también tuvieron repercusiones negativas para las organizaciones.

Es más, el éxito de algunos ataques podría haberse impedido fácilmente. En un informe reciente, Cybersecurity Insiders señaló que casi la mitad de todos los usuarios tienen más privilegios de los que necesitan para hacer su trabajo. Por eso, no solo ve empresas que dan prioridad a la identidad y los privilegios, sino que incluso hay gobiernos que destacan su importancia relativa. En un borrador de memorándum de septiembre de 2021, la Oficina de Administración y Presupuesto (OMB, por sus siglas en inglés) de EE. UU. destacó una serie de resultados que debían lograrse antes del cierre del año fiscal 2024, entre ellos, que los organismos públicos adoptaran la autenticación en varias fases y establecieran procesos de gestión de identidades en toda la empresa.

Para que las organizaciones cierren esta brecha de exposición a la ciberseguridad, deberán controlar la expansión de la identidad o, de lo contrario, se enfrentarán a multas, demandas y pérdida de confianza e ingresos de los clientes.

La aparición de la identidad como nuevo perímetro

Dado que los problemas relacionados con la identidad son cada vez más frecuentes y tienen un mayor impacto, es lógico que la seguridad de la identidad sea cada vez más importante.

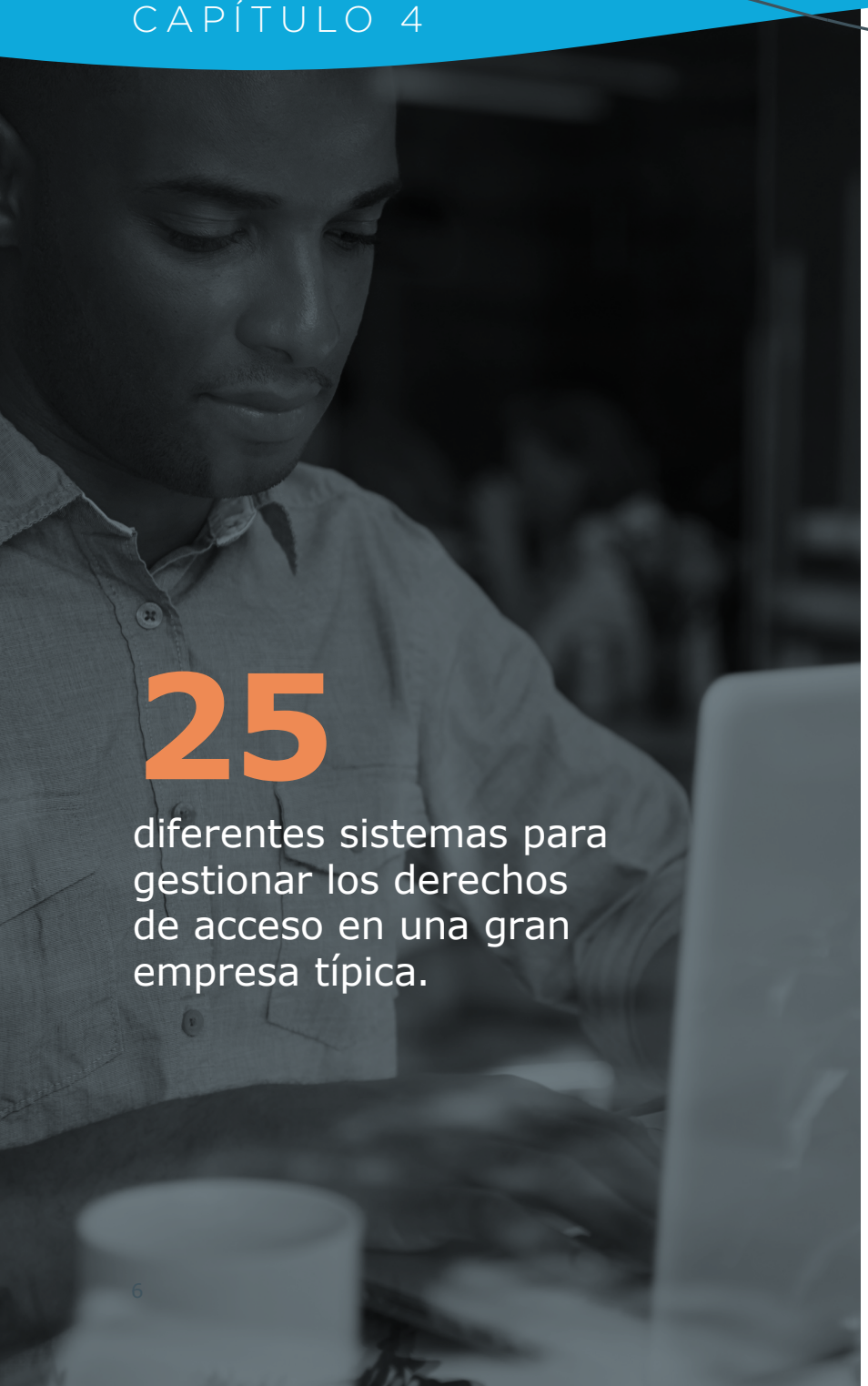
El perímetro tradicional sigue siendo una defensa importante para un ciberataque, pero en muchos sentidos, nació para otra era. Este enfoque centrado en la infraestructura, que ha sido una piedra angular de las estrategias de ciberseguridad durante muchos años, se basa en la creencia de que es posible proteger todo dentro de la empresa. Lógicamente, la única forma de lograr este ambicioso objetivo es optimizar su defensa en los puntos más externos donde se podría evitar el compromiso en todos los puntos.

Puesto que el perímetro de seguridad se está convirtiendo rápidamente en una tradición de tecnología informática, confiar en este enfoque simplemente no es práctico ni anticuado. Los altos ejecutivos de seguridad de tecnología informática ahora reconocen que el compromiso es inevitable. Y, como tal, una estrategia más pragmática es tomar medidas para mantener alejados a los infractores, pero también para evitar la explotación una vez que entran en la red. Gracias a este enfoque centrado en la identidad, las organizaciones con visión de futuro dan prioridad a lo más importante y toman medidas para comprobar todo antes de conceder acceso desde un principio; por ejemplo, ¿quién es este usuario? ¿A qué deberían tener acceso? ¿Qué van a hacer con esa autorización? Y ¿cuándo deberían cambiar sus derechos?

En resumen, el perímetro tradicional se está deteriorando, y la identidad está emergiendo como la nueva ventaja.

El enfoque **centrado en la infraestructura** PROTEGE todo

El enfoque **centrado en la identidad** COMPRUEBA todo



25

diferentes sistemas para gestionar los derechos de acceso en una gran empresa típica.

Obstáculos clave para la resiliencia de la ciberseguridad

Aunque la seguridad de la identidad es una tendencia emergente clave, el éxito de esta tarea no siempre resulta sencillo. Esto se debe en gran parte a cómo evolucionan las identidades. Antes, las organizaciones se preocupaban principalmente por los empleados internos que se contrataban para hacer un solo trabajo, que trabajaban en la oficina y que accedían a los recursos desde un único punto. La mayoría de las identidades eran usuarios.

Al contrastar eso con la actualidad, nos encontramos con una dinámica completamente diferente. Los profesionales de la seguridad no solo deben preocuparse por los empleados internos, sino que también deben tener en cuenta las identidades de los contratistas, proveedores y socios. En lugar de realizar un trabajo, los empleados tienden a cambiar de rol con frecuencia, no están atados a la oficina y suelen acceder a lo que necesitan desde varios puntos. Los profesionales de la seguridad deben tener en cuenta no solo a los usuarios, sino también a las aplicaciones y las máquinas. Ahora los usuarios humanos pueden tener varias identidades en más cuentas, pueden ser máquinas y robots, pueden tener varios dispositivos que se conectan con diferentes versiones o generaciones de aplicaciones y todos pueden moverse sobre recursos desde distintos sistemas y puntos de acceso físicos.

Además, la mayoría de las organizaciones gestionan actualmente los derechos de acceso en silos. Según el tercer informe anual global de seguridad de contraseñas, la media de identidades de grandes empresas es de 25 sistemas diferentes. Este amplio y variado entorno puede evitar que el equipo de seguridad de tecnología informática obtenga una visibilidad completa de las actividades de los usuarios. Asimismo, evita que el equipo aplique los análisis de manera integral. Estos retos generan, en última instancia, brechas e incoherencias, y pueden convertirse en una barrera a la hora de comprobar todo antes de conceder acceso al usuario, que constituye una parte fundamental para implementar un enfoque de seguridad moderno.

Si no se superan estas brechas, su organización no podrá adaptarse a los cambios en los roles/responsabilidades de los usuarios, a los cambios en la infraestructura informática y a las amenazas nuevas y en desarrollo. Abordar adecuadamente la brecha contribuirá a la resiliencia de la ciberseguridad de su organización.

El caso de un enfoque holístico de la seguridad de la identidad

La seguridad de la identidad es flexible y puede adoptar formas muy diferentes en función de las poblaciones y necesidades de los usuarios, así como de los recursos a los que están conectados y los que constituyen una empresa. La clave del éxito es pasar de un estado de seguridad de identidad fragmentado a uno unificado.

Muchas organizaciones abordan las formas clave de seguridad de la identidad — administración y gobernanza de identidades (IGA), gestión identidad y acceso (IAM), gestión de acceso con privilegios (PAM) y gestión y seguridad de Active Directory (ADMS)— por separado. Dentro de cada una, suele haber varios silos para considerar y las personas, las aplicaciones y los datos se administran de manera distinta. Este estado fragmentado genera mucha fricción, impide la automatización y obliga a las organizaciones a hacer las mejores conjeturas sobre cuándo y cómo gestionar los derechos de acceso.

El modelo emergente es mucho más holístico y las formas clave de seguridad de la identidad se abordan de forma conjunta. Esto significa que las aplicaciones se solapan, los silos de datos se emancipan y las personas, las aplicaciones y los datos se alinean como uno solo. Gracias a este enfoque de seguridad de identidad unificada, puede correlacionar todas las identidades, eliminar la fricción con una mejor integración, reducir su superficie de ataque y fortalecer su resiliencia de ciberseguridad.

ONE IDENTITY by Quest

Seguridad de identidad unificada como componente básico de Zero Trust

A estas alturas, se entiende ampliamente que Zero Trust es un modelo probado para implementar una seguridad sólida y selectiva. Elimina los permisos vulnerables, el acceso innecesario y excesivo a favor de la delegación de derechos específicos y el aprovisionamiento con granularidad. El paso de un estado fragmentado a uno unificado de la seguridad de la identidad permite a las organizaciones dar un gran salto hacia adelante en el cumplimiento de esta promesa.

El éxito de Zero Trust empieza con ampliar la red de forma suficiente. Esto implica centrarse no solo en las personas, sino también en las identidades de las máquinas y las cuentas en constante expansión a medida que las organizaciones se adentran en un panorama de tecnología informática multigeneracional, híbrido y periférico. Si dibuja el círculo demasiado pequeño, dejará el camino abierto a los infractores. Unificar su estrategia de seguridad de identidad le ayudará a evitar este problema.

Un segundo elemento clave de Zero Trust es ofrecer una serie de derechos en toda la organización. Con una mayor visibilidad e información disponible, los profesionales de seguridad podrán añadir, eliminar y ajustar privilegios a tiempo con mayor rapidez y eficiencia. Al hacerlo, podrán controlar a los usuarios para que accedan únicamente a lo que necesitan para su trabajo, y solo en el momento adecuado, al tiempo que eliminan los procesos manuales propensos a errores y la gran implicación de la tecnología informática.

Finalmente, un elemento clave de Zero Trust es la adaptabilidad, que se permite con una estrategia unificada de seguridad de identidad. Al aprovechar un enfoque holístico que incluye conocimiento contextual y análisis de comportamiento, las organizaciones podrán anticipar, detectar y tomar medidas correctivas con mayor rapidez y eficiencia para hacer frente a amenazas emergentes.

Prácticas recomendadas para unificar su enfoque de seguridad de identidad

La tecnología puede mejorar drásticamente las posibilidades de éxito de una organización a la hora de unificar la seguridad de la identidad, pero ¿qué deben buscar los profesionales de la seguridad en un proveedor de soluciones para optimizar sus resultados? A continuación, se presentan cinco elementos imprescindibles como alternativas:

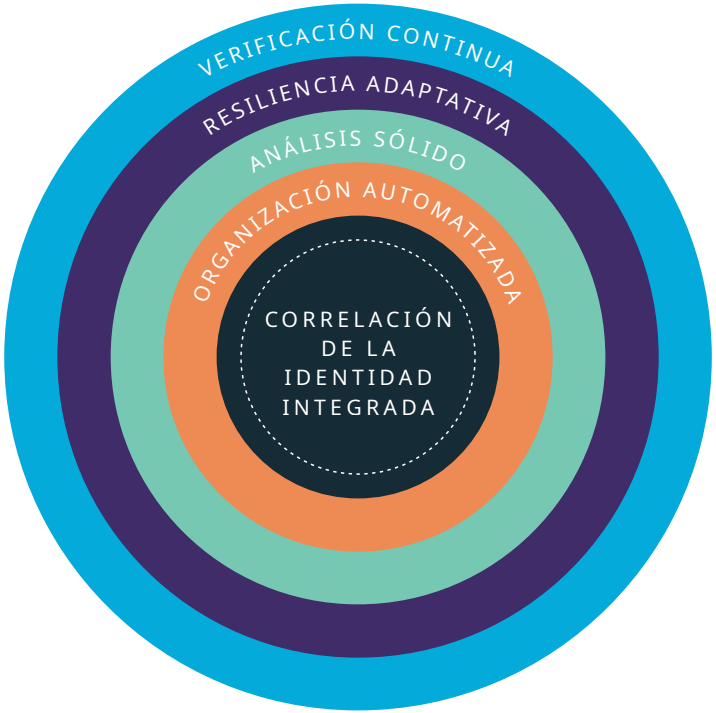
1. **Correlación holística:** en primer lugar y por encima de todo, las organizaciones necesitarán la unificación integral de todas las identidades y cuentas para optimizar la visibilidad y tomar decisiones fundamentadas correctamente.

2. **Organización automatizada:** un segundo elemento básico de una estrategia de seguridad de identidad unificada es la gobernanza fluida, a través de la identidad y los privilegios. Esto le permite impulsar la eficiencia a gran escala.

3. **Análisis sólido:** dada la amplitud y la naturaleza cambiante de la seguridad de la identidad, las organizaciones necesitan soluciones que ofrezcan el nivel de conocimientos necesario para anticipar, detectar y tomar medidas correctivas ante amenazas emergentes a gran escala.

4. **Resiliencia adaptativa de la ciberseguridad:** con el reconocimiento de que el panorama de amenazas y la empresa ya no son estáticos, los profesionales de la ciberseguridad deben tener la capacidad de cambiar rápidamente según sea necesario y preparar sus inversiones para el futuro.

5. **Verificación continua:** la seguridad de identidad unificada tiene más éxito cuando se puede comprobar todo antes de conceder acceso. La tecnología enriquecida con conocimiento de la situación, supervisión de sesiones y análisis de comportamiento ayudará a lograr resultados.



Problemas clave resueltos mediante la seguridad de identidad unificada

Por ahora, hemos descrito los retos y ventajas de carácter general que supone adoptar un enfoque unificado de la seguridad de la identidad. Pero ¿cuáles son los estudios de empleo específicos que los líderes de ciberseguridad pueden esperar con dicha estrategia? A continuación, se ofrece una muestra de los resultados comunes:

Problemas clave	Estudios de empleo	Resultados
Proteja la organización: **proteja a su gente, aplicaciones y datos**	• Zero Trust: proteja a gran escala y reduzca el riesgo de infracciones mediante la creación de un marco adaptable de Zero Trust • Acceso remoto con privilegios: garantice que los trabajadores y contratistas remotos puedan acceder de forma segura a información importante, sin fricciones con la VPN • Gestión de privilegios de punto final: unifique la seguridad de puntos finales de equipos de sobremesa AD/Azure AD, Unix/Linux y Windows y macOS • Análisis con privilegios y finalización de sesiones: detecte riesgos en sus usuarios con privilegios y evite daños a su organización • Gestión y seguridad de AD híbrido: reduzca la implicación de la tecnología informática en tareas de aprovisionamiento y elimine errores manuales • Seguridad privilegiada para AD/Azure AD: proteja su entorno interno tan firmemente como el perímetro con el fin de proteger sus activos críticos y dirigidos con frecuencia • Almacenamiento de contraseñas: simplifique la gestión de contraseñas y proteja las credenciales con privilegios	• Elimine vulnerabilidades y riesgos • Implemente Zero Trust • Evite infracciones • Unifique identidades en entornos locales y en la nube • Acceso seguro con privilegios
Impulse eficiencias operativas: **centralice los procesos de seguridad**	• Control de acceso con privilegios: cierre las brechas políticas y de seguridad entre el acceso con privilegios y las identidades de usuario estándar • Gestión y seguridad de Active Directory: proteja y gestione usuarios y grupos, y controle el acceso del administrador a través de la delegación • Puente de Active Directory: unifique la gestión basada en políticas en todos sus sistemas operativos y plataformas • Fusiones y adquisiciones: adáptese sin problemas a los cambios, como las acciones de los trabajadores y las pandemias, que normalmente requieren una intervención manual importante	• Unifique las políticas y los procesos de gestión de identidades • Mejore drásticamente la eficiencia • Controle el acceso a todos los recursos, sistemas y plataformas • Automatice las tareas comunes para optimizar el enfoque de trabajo del personal informático • Disfrute sin complicaciones de procesos de incorporación/traslado/bajas

Problemas clave	Estudios de empleo	Resultados
Aborde los requisitos de cumplimiento normativo y auditoría: **gestione su expansión de identidad y demuestre el cumplimiento de las políticas**	• Gobernanza de identidades: asegúrese de que las políticas se aplique, el acceso de los usuarios se gestione según los requisitos y pueda mostrar pruebas • Auditoría de sesiones sin agentes: proteja sus recursos y usuarios más importantes mediante registros y análisis automatizados. Asimismo, respalde las investigaciones forenses y cumpla los requisitos de cumplimiento normativo para el acceso con privilegios • Generación de informes de cumplimiento normativo inmediatos: obtenga capacidades de generación de informes en tiempo real sobre medidas de cumplimiento normativo para todos los usuarios y recursos de su empresa con el fin de cumplir los requisitos de cumplimiento normativo y auditorías	• Satisfaga las demandas de los auditores de información relacionada con permisos • Minimice y elimine el riesgo de violaciones de políticas centradas en la identidad • Cree trazas de auditoría fiables para todas las actividades de sesión con privilegios • Permita que los equipos de seguridad busquen eventos específicos y reproduzcan sesiones con privilegios • Satisfaga las necesidades de cumplimiento normativo para supervisar el acceso con privilegios
Asegure su transformación digital: **proteja las identidades mientras aumenta la funcionalidad y el acceso**	• Organización de seguridad de DevOps: proteja los procesos de DevOps con la seguridad centrada en la identidad • Gobernanza de aplicaciones: simplifique las decisiones de acceso a las aplicaciones y permita a los gestores de negocios tomar decisiones fundamentadas • Optimización de la seguridad de RPA: gestione los riesgos asociados con las identidades de RPA en expansión • Gestión de entornos complejos: reduzca la sobrecarga de administración de entornos heterogéneos para impulsar la seguridad, la velocidad y la toma de decisiones	• Gestione sin complicaciones su entorno híbrido • Adopte de forma segura las prácticas de RPA • Haga que los secretos de DevOps sean fáciles de usar • Aumente la responsabilidad de los empleados y los contratistas • Reduzca errores, aumente la seguridad, optimice la eficiencia y minimice la complejidad

Conclusión

Hay fuerzas potentes en acción, y un panorama empresarial y de tecnología informática en rápida evolución contribuyendo a una proliferación de identidades. Esta expansión de identidades se agrava a diario. Crea un serie de riesgos muy reales que los profesionales de la ciberseguridad deben tomar en serio. Es hora de dejar de gestionar la ciberseguridad de forma fragmentada.

Al adoptar un enfoque holístico para gestionar los derechos de acceso, los CISO pueden cerrar una brecha crítica de exposición a la ciberseguridad, fomentar una mayor resiliencia de la ciberseguridad para su organización y dar un paso importante para cumplir la promesa de Zero Trust, que se está convirtiendo rápidamente en un imperativo empresarial.

La identidad es la nueva ventaja. Una estrategia de seguridad de identidad unificada es la forma de combatir los métodos de ataque modernos e impulsar a su organización hacia el futuro.

Ahora, cuando su director de seguridad de tecnología informática llame, estará seguro de que tiene la información para evaluar de inmediato el estado de su seguridad de identidad y las medidas que se han llevado a cabo en su red.

Acerca de One Identity

One Identity ofrece soluciones de seguridad de identidad unificada que ayudan a los clientes a fortalecer su postura general de ciberseguridad, así como a proteger a la gente, las aplicaciones y los datos esenciales para la empresa. Nuestra plataforma de seguridad de identidad unificada reúne las mejores capacidades de administración y gobernanza de identidades (IGA), gestión identidades y acceso (IAM), gestión de acceso con privilegios (PAM) y gestión y seguridad de Active Directory (ADMS) para permitir que las organizaciones pasen de un enfoque fragmentado a uno holístico de la seguridad de la identidad. One Identity es fiable y está probada a escala global: gestiona más de 250 millones de identidades de más de 5000 organizaciones en todo el mundo. Para obtener más información, visite www.oneidentity.com.

Si tiene alguna duda sobre el uso que puede hacer de este material, póngase en contacto con nosotros:
www.quest.com

eBook-UnifiedIdentitySecurity-KA-ES-WL-69156

ONE IDENTITY by Quest