COHESITY

GUÍA DEL COMPRADOR

GUÍA EJECUTIVA PARA EVALUAR SOLUCIONES DE RESILIENCIA DE IDENTIDAD

Todo lo que necesita saber para encontrar la solución adecuada que le permita reforzar el control de acceso, proteger sus activos más valiosos y recuperarse rápidamente de ciberataques destructivos.

Sus sistemas de gestión de identidades y accesos (IAM) son uno de los principales objetivos de los ciberatacantes.

¿Por qué?

9 de cada 10 ciberataques involucran sistemas de gestión de identidades y accesos (IAM). Es la parte más atacada de la infraestructura de cualquier organización.

Un sistema de identidad considerado fuente de referencia es un objetivo de alto valor porque, al comprometerlo, los atacantes obtienen acceso a prácticamente cualquier recurso de la organización. Por eso, la resiliencia de identidad es un pilar fundamental de una estrategia integral de ciberresiliencia. Para restaurar rápidamente una organización operativa mínima, los servicios de identidad deben estar entre las primeras cargas de trabajo que regresen a un estado confiable, ya que muchos sistemas críticos y procesos empresariales dependen de ellos.

Para la mayoría de las organizaciones, la principal plataforma de IAM y fuente de referencia para otros proveedores de identidad es Microsoft Active Directory (AD) local. La recuperación cibernética de AD, especialmente en entornos complejos con múltiples bosques, es un proceso difícil que requiere conocimientos especializados; no se trata simplemente de "otra carga de trabajo". Además de AD, probablemente también utilice alguna combinación de Entra ID y Okta.

A medida que refuerza sus defensas frente a los ciberataques, debe asegurarse de contar con una estrategia integral de resiliencia de identidad que abarque todos sus servicios de identidad críticos.

> ***"Ninguna organización puede estar 100 % protegida frente a los ciberataques. Por eso necesita invertir en resiliencia, la capacidad de recuperarse rápidamente tras una brecha de seguridad."***

La resiliencia de identidad permite a su organización:

- **Detectar y remediar amenazas de identidad**: Detectar ataques basados en identidades en curso y revertir automáticamente cambios riesgosos que no pueden esperar la intervención humana mediante capacidades de detección y respuesta ante amenazas de identidad.
- **Recuperar los servicios de identidad de forma limpia y restaurar la confianza**: Restaurar los servicios de identidad sin reintroducir atacantes ni puertas traseras que puedan provocar reinfecciones persistentes.
- **Reducir el tiempo de inactividad: La identidad es fundamental para el acceso y la autenticación. Cuando falla, la operación empresarial se detiene**. Garantice una recuperación segura y fluida de las operaciones tras un ataque de identidad para minimizar el tiempo de inactividad.

Ninguna organización puede estar protegida al 100 % frente a los ciberataques, por lo que es necesario invertir en resiliencia: la capacidad de recuperarse tras una brecha de seguridad. Su organización debe fortalecer y ampliar continuamente la resiliencia de identidad mediante la detección y remediación continua de ataques basados en identidades y la implementación de una estrategia de recuperación probada que permita restaurar AD, Entra ID y Okta de forma limpia y rápida en cualquier situación. Esta guía le ayudará a evaluar soluciones, formular las preguntas adecuadas y realizar una inversión con confianza para proteger su infraestructura de identidad frente a las amenazas actuales.

Qué debe buscar en una solución de resiliencia de identidad

Al evaluar opciones, puede resultar tentador considerar la identidad simplemente como otra carga de trabajo que se respalda y recupera cuando es necesario. Se trata de una forma de pensar peligrosamente obsoleta. Un enfoque moderno que extiende la ciberresiliencia a los sistemas de identidad y acceso combina seguridad proactiva avanzada y recuperación limpia durante todas las etapas del ciclo de vida del ataque. Estos son los aspectos que diferencian una verdadera solución de resiliencia de identidad preparada para la empresa:

ITDR (Detección y Respuesta Avanzada de Amenazas de Identidad) avanzado: La resiliencia de identidad comienza antes de la brecha. Los sistemas IAM (Gestión de Identidad y Acceso) como AD suelen ser los primeros objetivos de los atacantes porque les proporcionan acceso privilegiado al entorno. Realizar copias de seguridad no es suficiente. La solución debe ofrecer supervisión continua de la postura de seguridad del entorno de identidad mediante capacidades de Detección y Respuesta ante Amenazas de Identidad (ITDR). Esto ayuda a identificar vulnerabilidades, reforzar la infraestructura de identidad y automatizar la remediación. La reversión automática y la corrección de cambios maliciosos que no pueden esperar intervención humana reducen la probabilidad de ataques exitosos. Gracias a la detección continua de amenazas, la remediación automatizada y el fortalecimiento proactivo, puede dificultar considerablemente el avance de los atacantes.

Protección capaz de resistir ataques: Si se produce una intrusión, es fundamental poder recuperar la infraestructura de identidad mediante datos de respaldo limpios. Los atacantes saben que las copias de seguridad son la última línea de defensa, por lo que intentan cifrarlas, modificarlas o eliminarlas mediante tácticas de doble extorsión. La solución de resiliencia de identidad debe proporcionar inmutabilidad por diseño, garantizando que las copias de seguridad de AD no puedan manipularse, incluso si los atacantes obtienen credenciales de administrador de dominio. El almacenamiento WORM, las aprobaciones basadas en quórum y la verificación criptográfica son capacidades esenciales para unas copias de seguridad resilientes. Si su capa de protección no puede resistir cuando los adversarios ya se encuentran dentro de su red, entonces realmente no cuenta con protección.

Recuperación rápida y libre de malware: Cuando la identidad se ve comprometida, el impacto se extiende a toda la organización. La velocidad de recuperación es importante, pero también lo es su integridad. Restaurar la identidad sin verificar que sea confiable puede volver a introducir malware o puertas traseras, provocando reinfecciones repetidas. Una solución eficaz debe combinar recuperación rápida, automatizada y orquestada de AD, Entra ID y Okta. En el caso específico de AD, las recuperaciones deben desacoplarse del sistema operativo (OS) para garantizar que no se restauren credenciales comprometidas ni malware. Esto puede reducir el tiempo de inactividad durante el proceso de recuperación al evitar infecciones persistentes y ofrecer una recuperación en la que pueda confiar.

Opciones de recuperaciones granulares: No todos los incidentes de identidad requieren una restauración completa. La recuperación granular ahorra tiempo y reduce el impacto operativo al ofrecer recuperación a nivel de objeto, atributo y bosque. Contar con capacidades tanto de recuperación granular como de bosque completo permite responder eficazmente tanto a solicitudes rutinarias del soporte técnico como a incidentes cibernéticos de gran escala.

Protección en entornos de identidad híbrida: La identidad ya no se limita al AD local. Entra ID y Okta se han convertido en componentes esenciales de la arquitectura de identidad empresarial, especialmente para el acceso a aplicaciones en la nube. Necesita una solución preparada para el futuro que proteja de forma integrada AD, Entra ID y Okta en entornos híbridos. Dado que muchas organizaciones sincronizan Entra ID y Okta con AD, la recuperación segura de estos entornos depende primero de la protección y recuperación de AD. Entra ID y Okta son aplicaciones independientes de AD que utilizan sincronizaciones unidireccionales desde entornos locales hacia la nube. Sin la protección del entorno local, solo dispone de la mitad de la solución. Su solución de resiliencia de identidad también debe incluir capacidades de protección y recuperación que garanticen que Entra ID y Okta permanezcan seguros y puedan recuperarse de forma limpia, asegurando así la continuidad de la identidad en la nube.

Análisis forense posterior a una brecha para validar la confianza y prevenir futuros ataques: Una recuperación sin visibilidad deja a la organización expuesta a incidentes repetidos Una solución moderna debe integrar capacidades forenses que permitan validar si la recuperación se ha realizado correctamente. Además de apoyar las investigaciones posteriores al incidente, estas capacidades ayudan a fortalecer las defensas y cumplir requisitos regulatorios en reportes y de cumplimiento. Sin la debida diligencia posterior a la recuperación, su organización queda expuesta al riesgo de sufrir un ataque posterior. Los análisis forenses no deben ser una función secundaria; son una parte integral de la resiliencia de identidad.

Capacidad de recuperación sin acceso a Internet: Durante una interrupción masiva o un ciberataque, no puede asumir que dispondrá de una conexión a Internet estable o segura. La solución de resiliencia de identidad debe permitir restaurar los sistemas de identidad críticos sin depender de la disponibilidad de Internet para garantizar una recuperación limpia en cualquier escenario.

Soporte de respuesta a incidentes 24/7: La identidad es una carga de trabajo única y compleja, especialmente cuando se trata de recuperarla. Es esencial que el proveedor cuente con experiencia demostrada en protección, seguridad y recuperación de identidades, así como con especialistas capaces de ofrecer orientación durante situaciones críticas. Las situaciones varían y por esolLa asistencia adecuada y la experiencia forense de profesionales especializados son fundamentales para recuperarse con rapidez y confianza de los ataques o interrupciones más graves.

Preguntas clave para formular a los proveedores

1. ¿Cómo evita que los atacantes manipulen o eliminen copias de seguridad de AD, Entra ID u Okta?
2. ¿Puede demostrar la recuperación completa de toda la infraestructura de identidad en menos de un día?
3. ¿Cómo verifica que AD, Entra ID u Okta recuperados estén libres de malware, puertas traseras o credenciales comprometidas?
4. ¿Puede recuperar la identidad con la misma experiencia de uso y la misma interfaz sin acceso a Internet?
5. ¿Es compatible con entornos de identidad híbrida (AD local + Entra ID + Okta)?
6. ¿Puede su solución ejecutar recuperaciones completas de bosques de AD de forma automatizada y siguiendo el Microsoft Recovery Runbook?
7. ¿Su solución busca amenazas específicas de identidad para detectar y expulsar a los actores maliciosos antes de que ocurra una vulneración?

Señales de alerta que debe tener en cuenta

- No ofrece capacidades de seguridad de identidad. La resiliencia incluye la reducción del riesgo antes de que se produzca un impacto y la mitigación de amenazas para evitar un compromiso de seguridad.
- Las soluciones dependen exclusivamente de herramientas nativas de Microsoft. Estas son manuales, lentas e inestables cuando más lo necesite.
- Almacena las copias de seguridad dentro del entorno de producción. Los atacantes pueden borrarlos y dejarlo sin nada con qué recuperarse.
- Carece de orquestación o automatización para recuperar múltiples controladores de dominio (DC) en paralelo. Sin esto, los administradores se ven forzados a seguir pasos largos y manuales durante un momento estresante y caótico.
- La solución depende de una conexión a Internet segura y estable. No puede asumir ni depender de disponer de una conexión a Internet durante un ciberataque o un proceso de recuperación.
- No permite realizar pruebas de recuperación. Si no puede ensayar una recuperación, no puede confiar en ella.
- No permite desacoplar el sistema operativo durante la recuperación. Restaurar el sistema operativo (OS) junto con los datos de identidad puede reintroducir malware y ataques de puertas traseras.
- No permite restaurar hacia cualquier destino físico o virtual. Exigir un nivel de parcheo exacto puede provocar períodos prolongados de inactividad.
- No dispone de servicios forenses de identidad ni de experiencia en respuesta a incidentes (IFIR) con soporte 24/7.

Lista de verificación para evaluar proveedores

Use esta lista de verificación para evaluar proveedores:

Requisito	Proveedor 1	Proveedor 2	Proveedor 3	Notes
Copias de seguridad de AD inmutables y aisladas				
Recuperación desde objetos hasta bosques completos				
Flujos de trabajo automatizados para recuperación de bosques				
Fortalecimiento proactivo para identificar y cerrar rutas de ataque				
Detección de malware o corrupción en las copias de seguridad				
Seguimiento y reversión de cambios de múltiples orígenes con protección contra manipulaciones				
Inventario y supervisión de cuentas de servicio altamente atacadas				
Compatibilidad con AD híbrido (AD local + Entra ID)				
Análisis forense posterior a una brecha				
Escalabilidad (múltiples bosques / global)				
Soporte especializado de respuesta a incidentes de identidad 24/7				
Recuperación paralela de múltiples DC (para AD)				
Recuperación hacia cualquier destino físico o virtual				
Recupera varios controladores de dominio en paralelo (para AD)				

Conclusión

Las intrusiones basadas en identidades están detrás de prácticamente todas las brechas de seguridad importantes. Por ello, acelerar la ciber resiliencia en sus sistemas de identidad críticos ya no es opcional: es un componente fundamental de la seguridad empresarial.

Una solución probada de resiliencia de identidad va mucho más allá de las copias de seguridad. Refuerza la identidad frente a compromisos, protege contra amenazas y ataques basados en identidades, proporciona una recuperación confiable y extremadamente rápida, y ayuda a eliminar puertas traseras para garantizar restauraciones limpias y libres de malware.

Para obtener más información sobre la resiliencia de identidad y descubrir cómo puede ayudarle a proteger sus servicios de identidad más críticos, contacte hoy mismo con su equipo de cuenta de Cohesity.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

4500064-001-ES 8-2026