COHESITY

GUIA DO COMPRADOR

GUIA EXECUTIVO SOBRE COMO AVALIAR SOLUÇÕES DE RESILIÊNCIA DE IDENTIDADE

Tudo o que você precisa saber para restringir o acesso, proteger dados valiosos e se recuperar rapidamente de ataques cibernéticos destrutivos

Seus sistemas de gerenciamento de identidade e acesso são um alvo privilegiado para agentes mal-intencionados.

Por quê?

9 em cada 10 ataques cibernéticos envolvem sistemas de gerenciamento de identidade e acesso (identity and access management, IAM). É a parte mais atacada da infraestrutura de qualquer organização.

Um sistema de identidade de referência é um alvo de alto valor, pois sua violação proporciona aos invasores acesso a praticamente qualquer recurso da organização. É por isso que a resiliência de identidade é um pilar fundamental de uma estratégia abrangente de resiliência cibernética. Para restaurar rapidamente uma empresa minimamente viável, os serviços de identidade devem estar entre as primeiras cargas de trabalho a serem restauradas a um estado confiável, uma vez que muitos sistemas e processos de negócios críticos dependem deles.

Para a maioria das organizações, o principal sistema de IAM e a fonte de referência para outros provedores de identidade é o Microsoft Active Directory (AD) local. A recuperação cibernética do AD, especialmente em ambientes complexos que incluem várias florestas, é um processo desafiador que exige conhecimento especializado; não se trata de "apenas mais uma carga de trabalho". Além do AD, é bem provável que você tenha uma combinação do Entra ID com o Okta.

Ao buscar reforçar suas defesas contra ataques cibernéticos, é fundamental garantir que você tenha uma estratégia de resiliência de identidade de ponta a ponta em todos os seus serviços críticos de identidade.

> ***"Nenhuma organização está 100% protegida contra ataques cibernéticos. Por isso, é necessário investir em resiliência, a capacidade de se recuperar rapidamente após uma violação.."***

A resiliência de identidade garante que sua empresa possa:

- **Detectar e corrigir ameaças à identidade:** Detecte ataques baseados em identidade em andamento e reverta automaticamente alterações de risco que não podem esperar por intervenção humana com a detecção e resposta a ameaças de identidade (identity threat detection and response, ITDR).
- **Recuperar os serviços de identidade de forma segura e restabelecer a confiança:** Restaure seus serviços de identidade sem trazer de volta os invasores e/ou backdoors que levam à reinfecção persistente.
- **Reduzir o tempo de inatividade:** A identidade é a chave para acesso e autenticação. Quando ela cai, os negócios param. Garanta que as operações comerciais possam ser recuperadas de forma segura e contínua após um ataque à identidade, a fim de reduzir o tempo de inatividade.

Nenhuma organização está 100% a salvo de ataques cibernéticos, por isso, é preciso investir em resiliência, ou seja, na capacidade de se recuperar após uma violação. Sua organização deve aprimorar e ampliar a resiliência de identidade por meio da detecção e correção contínuas de ataques baseados em identidade e da implementação de uma estratégia de recuperação comprovada que restabeleça o AD, o Entra ID e o Okta de forma segura e rápida em qualquer circunstância. Este guia irá ajudá-lo a avaliar soluções, fazer as perguntas certas e realizar um investimento com confiança para proteger sua infraestrutura de identidade contra as ameaças atuais.

O que procurar em uma solução de resiliência de identidade

Ao avaliar as opções, é tentador pensar na identidade simplesmente como mais uma carga de trabalho a ser copiada e recuperada quando necessário. Essa é uma mentalidade perigosamente ultrapassada. Uma abordagem moderna que amplia a resiliência cibernética aos sistemas de identidade e acesso combina segurança proativa avançada e recuperação completa em todas as etapas do ciclo de vida do ataque. Veja o que diferencia uma solução de resiliência de identidade verdadeiramente pronta para o ambiente corporativo das demais:

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.

Perguntas críticas a fazer aos fornecedores

1. Como evitar que invasores alterem ou excluam os backups do AD, do Entra ID ou do Okta?
2. Você consegue comprovar a recuperação total de toda a sua infraestrutura de identidade em menos de um dia?
3. Como você verifica se o AD, o Entra ID ou o Okta recuperados estão livres de malware, backdoors, ou se não trouxeram de volta credenciais comprometidas?
4. É possível recuperar a identidade com a mesma experiência e interface de usuário sem acesso à internet?
5. Vocês oferecem suporte a ambientes híbridos de identidade (AD local + Entra ID + Okta)?
6. A sua solução é capaz de executar recuperações completas da floresta do AD de forma automatizada e seguir o Runbook de Recuperação da Microsoft?
7. Sua solução busca ativamente por ameaças específicas de identidade para detectar e expulsar agentes maliciosos antes que ocorra um comprometimento?

Sinais de alerta a serem observados

- Não há recursos de segurança de identidade. A resiliência inclui a redução de riscos antes do impacto e a mitigação de ameaças para evitar comprometimentos.
- Soluções que dependem apenas de ferramentas nativas da Microsoft. Elas são manuais, lentas e não confiáveis quando você mais precisa.
- Backups armazenados em produção. Os atacantes podem apagá-los e deixar você sem nada para recuperar.
- Não há orquestração nem automação para recuperações paralelas de vários controladores de domínio (domain controllers, DCs). Sem isso, os administradores são obrigados a seguir etapas manuais e demoradas em um momento de grande estresse e em um ambiente caótico.
- A solução depende de um acesso à internet seguro e estável. Não se pode presumir nem contar com uma conexão à Internet durante um ataque cibernético ou um processo de recuperação.
- Não é possível testar a recuperação. Se você não puder ensaiar, não pode confiar nisso.
- Não é possível desacoplar o sistema operacional durante a recuperação. Restaurar o sistema operacional com seus dados de identidade pode fazer com que malware e backdoors sejam restaurados também.
- Não é possível selecionar nenhuma fonte física ou virtual para recuperação. Exigir um nível exato de patch pode resultar em tempo de inatividade prolongado.
- Falta de especialização em análise forense de identidade e resposta a incidentes (identity forensics and incident response expertise, IFIR) para oferecer suporte 24 horas por dia, 7 dias por semana, na resposta a incidentes. Lista de verificação para avaliação de fornecedores

Lista de verificación para evaluar proveedores

Use esta lista de verificación para evaluar proveedores:

Requisitos	Fornecedor 1	Fornecedor 2	Fornecedor 3	Observações
Backups imutáveis e isolados do AD				
Granularidade de recuperação do nível de objeto ao nível de floresta				
Fluxos de trabalho automatizados para recuperação florestal				
Fortalecimento proativo para identificar e bloquear vias de ataque				
Detecção de malware/corrupção em backups				
Rastreamento de alterações de múltiplas fontes à prova de adulteração e reversão				
Inventário e monitoramento de contas de serviço altamente direcionadas				
Suporte ao AD híbrido (local + Entra ID)				
Análise forense pós-violação				
Escalabilidade (múltiplas florestas/globais)				
Suporte especializado 24 horas por dia, 7 dias por semana, para resposta a incidentes de identidade				
Recupera vários DCs em paralelo (para o AD)				
Selecione qualquer fonte física ou virtual para recuperação				
Recupera vários DCs em paralelo (para AD)				

O resultado

A violação baseada em identidade está no cerne de praticamente todas as grandes violações de segurança. É por isso que acelerar a resiliência cibernética no que diz respeito aos seus sistemas críticos de identidade não é mais uma opção, é fundamental para a segurança da empresa.

Uma solução de resiliência de identidade comprovada vai além dos backups. Ela fortalece a identidade contra violações, protege contra ataques e ameaças à identidade, oferece uma recuperação confiável e ultrarrápida e ajuda a eliminar brechas de segurança para restaurações confiáveis e livres de malware. Para saber mais sobre resiliência de identidade e como ela pode ajudar a proteger seus serviços de identidade mais críticos, entre em contato com a equipe de atendimento da Cohesity hoje mesmo.

COHESITY

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

4500064-001-PT 8-2026