

COHESITY

A CAMADA DE IDENTIDADE

É O PONTO ZERO DOS ATAQUES CIBERNÉTICOS



*Por que os líderes de segurança e TI
precisam **provar** que são capazes de recuperar a
infraestrutura de identidade*

INTRODUÇÃO

A identidade corporativa deveria facilitar a sua vida. As organizações centralizaram o acesso digital pela primeira vez no final da década de 1960 e início da década de 1970, o que lhes proporcionou um único ponto de controle para decidir quem tinha acesso e o que essas pessoas podiam acessar. O LDAP e plataformas como o Active Directory transformaram posteriormente essa ideia em uma única fonte de verdade para toda a rede. Funcionou muito bem.

Esse é exatamente o problema.

Essa fonte única de verdade é, agora, a maneira mais fácil de entrar. Os invasores não invadem mais. Eles fazem login, usando credenciais roubadas e acesso legítimo, e vão direto para os seus sistemas mais críticos. Nada dispara. Nenhum alarme soa. Eles estão usando a mesma porta que seus funcionários usam todas as manhãs, o que torna esse problema fundamentalmente diferente daquele que a maioria dos programas de segurança foi criada para solucionar.

Durante anos, você construiu suas defesas em torno de um perímetro: um muro destinado a impedir a entrada de invasores. O muro ainda está de pé, mas os invasores pararam de escalá-lo. **Comprometer sua infraestrutura de identidade é mais fácil, mais discreto e mais confiável; é por isso que a identidade substituiu o perímetro da rede como o principal campo de batalha.** A maioria das pilhas de segurança nunca foram projetadas para atuar nesse campo.

Os números não são sutis. Em 2024, 79% dos ataques não envolveram malware: nenhum vírus para ser detectado, apenas engenharia social, credenciais roubadas e ferramentas remotas confiáveis que passaram despercebidas. Em 2025, esse número subiu para 82%, à medida que os invasores passaram a recorrer cada vez mais a credenciais válidas, fluxos de identidade confiáveis e integrações SaaS aprovadas para se deslocarem entre domínios sem serem detectados (Relatório global de ameaças da CrowdStrike). A linha de tendência aponta exatamente para uma direção.

Esse é o ponto delicado do qual qualquer programa de segurança sério precisa partir atualmente. O sistema que você criou para controlar o acesso a tudo acabou se tornando, sem que ninguém percebesse, a maneira mais fácil de acessar tudo. Isso não é motivo para pânico. É por isso que, antes de mais nada, devemos proteger a identidade e ser capazes de comprovar que podemos recuperá-la.

Por que a identidade corporativa está **sob ataque**

Para um invasor, a identidade é o alvo de maior valor e menor esforço em sua empresa, pois uma única credencial comprometida pode dar acesso a tudo o que está por trás dela. A identidade não é apenas mais um vetor. É o único vetor que um invasor moderno está buscando ativamente.

Mas eis o problema: quase nada na sua pilha foi desenvolvido para impedir isso. O EDR, os firewalls e a segmentação de rede foram todos projetados para detectar invasões, e não para questionar alguém que tenha feito login com credenciais válidas. Para suas defesas, o invasor parece exatamente com o seu funcionário.

E o ponto cego só aumenta. A maioria dos ambientes do Active Directory já existem há décadas. Anos de soluções provisórias, contas esquecidas e erros de configuração que passaram despercebidos se acumularam nos bastidores, onde ninguém está prestando atenção. Essa pilha não é apenas dívida técnica. É uma janela aberta, e é exatamente isso que os invasores procuram em primeiro lugar.

A identidade híbrida agrava ainda mais a situação. Atualmente, a maioria das organizações utiliza uma combinação do Active Directory local e de provedores de identidade na nuvem, como o Entra ID e o Okta, e cada conexão entre eles amplia a superfície de ataque. Pior ainda, uma vulnerabilidade no Entra ID ou no Okta geralmente remonta diretamente ao Active Directory, pois o Active Directory costuma ser a única fonte de informação confiável na qual todos os demais sistemas se baseiam. Se a fundação se romper, toda a estrutura se abala.

O ACTIVE DIRECTORY É O NÚCLEO DA IDENTIDADE CORPORATIVA

O Active Directory vem gerenciando a identidade corporativa há mais de 25 anos e continua em uso em 90% das organizações em todo o mundo. A maioria dos provedores de identidade na nuvem estão federados ou sincronizados com ele, o que significa que, mesmo à medida que você adota plataformas mais recentes, o Active Directory continua sendo a base que sustenta todas elas.

Na verdade:

- Os invasores comprometem um controlador de domínio em mais de 78% das invasões operadas por humanos.
- Em 35% desses casos, o controlador de domínio se torna o ponto a partir do qual o ransomware se espalha por todo o ambiente.

Quando ocorre um ataque, o Active Directory costuma ser o único obstáculo entre você e a recuperação. Pense no que isso significa: se você não conseguir acessar sua própria solução de backup, não poderá iniciar a recuperação de nada. Os invasores entendem isso perfeitamente, e é por isso que, cada vez mais, atacam seus sistemas de backup e seu Active Directory ao mesmo tempo. Tire os dois, e você não terá mais um dia ruim. Há uma situação com reféns.

E o tempo não tem piedade. A recuperação completa de uma floresta do Active Directory pode levar dias ou até semanas, e cada hora de inatividade pode custar às organizações até US\$ 730.000 por hora (*Forrester, The Total Economic Impact™ of Quest Recovery Manager for Active Directory Disaster Recovery Edition*).

As ferramentas tradicionais de backup não vão salvar você aqui. Ele pode copiar controladores de domínio e arquivos individualmente, mas não consegue coordenar as etapas precisas e ordenadas necessárias para reconstruir uma floresta inteira do Active Directory. Fazer o backup das peças não é o mesmo que conseguir montá-las novamente.

DADOS COMPLEMENTARES

32%

do aumento nos ataques baseados em identidade, primeiro semestre de 2025. 97% foram do tipo “password spray” ou força bruta

(Relatório de defesa digital da Microsoft 2025)

22%

No total, 22% das violações envolveram credenciais roubadas; especificamente, 88% dos ataques a aplicativos web básicos envolveram credenciais roubadas

(Relatório de investigações sobre violações de dados da Verizon de 2025)

35%

dos incidentes na nuvem foram causados pelo uso indevido de contas válidas

(Relatório global de ameaças da CrowdStrike 2025)

A identidade é a **base da MVC** e da confiança, agora e no futuro

Uma Empresa mínima viável (Minimum Viable Company, MVC) é a versão menor e mais enxuta de uma organização necessária para sobreviver e manter as operações essenciais. Quando as organizações são atingidas por um incidente cibernético, elas não deixam de se recuperar porque seus backups falham. Muitas vezes, elas falham porque tentam recuperar tudo de uma vez ou na ordem errada.

A dimensão que a maioria das organizações deixa de considerar gira em torno da confiança e do controle, e a identidade se situa exatamente na interseção entre ambas. É a chave-mestra da empresa. Se você não conseguir estabelecer uma identidade confiável, não será possível restaurar nada com segurança.

A gestão de identidade e acesso (Identity and access management, IAM) é responsável por três funções principais:

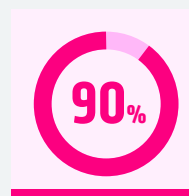
- **Gerenciamento do ciclo de vida da identidade:** Automatiza a integração, as atualizações de funções e o cancelamento de acesso, para que os direitos de acesso permaneçam precisos à medida que as pessoas entram, mudam de função e saem da empresa.
- **Autenticação:** Verifica se uma pessoa é quem afirma ser, geralmente por meio da autenticação multifatorial (multifactor authentication, MFA) e do login único (single sign-on, SSO).
- **Autorização:** Concede a cada usuário autenticado o acesso específico de que precisa para realizar seu trabalho, ao mesmo tempo em que restringe todo o restante.

Junte essas três funções e o Active Directory, o Entra ID e o Okta deixam de ser apenas infraestrutura e passam a ser a espinha dorsal operacional da sua empresa. Eles autenticam cada funcionário, cada aplicativo e cada transação. Isso nos leva a uma verdade simples, porém incômoda: se a infraestrutura de identidade ficar fora do ar, a empresa cai junto com ela.

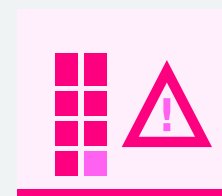
E essa espinha dorsal operacional está prestes a ficar muito mais exposta. À medida que as organizações se apressam em adotar a IA e fluxos de trabalho baseados em agentes, esses agentes dependem da infraestrutura de identidade para operar com segurança, e essa mudança já é visível nos dados: 93% das organizações já utilizam ou planejam utilizar agentes de IA para tarefas sensíveis de segurança, como redefinição de senhas e acesso à VPN (Semperis, maio de 2026).

Eis o que deve chamar sua atenção: esses agentes costumam se passar pelos funcionários que os instruem a realizar tarefas e acessar dados confidenciais. Cada um deles é um novo conjunto de chaves. Os desafios relacionados à garantia, proteção e recuperação da identidade nunca foram tão grandes.

DADOS COMPLEMENTARES



O Active Directory e o Entra ID são utilizados por mais de **90% das empresas** em todo o mundo (Semperis).



O Active Directory está envolvido em **9 em cada 10 ataques cibernéticos**, não porque seja mal projetado, mas porque está presente em todos os lugares (Cohesity CERT).

A interseção entre identidade, continuidade dos negócios e resiliência cibernética

O planejamento tradicional de continuidade de negócios trata a identidade como a eletricidade: uma infraestrutura que você presume que estará funcionando assim que ligar o interruptor. É exatamente essa suposição que leva as organizações à ruína. A identidade não pode mais ser dada como certa. Ela precisa do seu próprio plano de recuperação.

A resiliência cibernética inverte essa suposição. Ela considera a identidade como o primeiro elemento a ser atacado e o primeiro que você deve ser capaz de restabelecer (de forma independente, testada, isolada e confiável), mesmo quando tudo ao seu redor estiver comprometido. A diferença entre “presumimos que vai funcionar” e “já provamos que vai funcionar” é exatamente o que faz com que as organizações percam dias ou semanas após um ataque. Elas conseguem restaurar seus arquivos sem problemas. Elas simplesmente não conseguem fazer login nem mesmo de uma única pessoa para usá-los.

Para os líderes das áreas de segurança, TI e executivos, a conclusão é clara: a continuidade dos negócios e a resiliência cibernética só são bem-sucedidas quando a segurança proativa de identidades e a recuperação de identidades são planejadas, testadas e dotadas de recursos como disciplinas próprias. Nunca presuma que isso vai acontecer automaticamente enquanto você restaura todo o resto. A esperança não é um plano de recuperação.

DADOS COMPLEMENTARES

Active Directory 66%

Okta 57%

Entra ID 43%

Os planos de recuperação de desastres incluem o Active Directory em apenas 66% das organizações, o Entra ID em 43% e o Okta em 57%, o que deixa uma grande parcela dos planos de continuidade com um ponto cego justamente na camada de identidade

(Semperis, novembro de 2025).

51% 57% 90%

90% das organizações realizam varreduras em busca de vulnerabilidades de identidade, mas apenas 51% possuem procedimentos de correção e apenas 57% automatizam a recuperação de identidade (Semperis, novembro de 2025).

O custo da inércia

Vamos falar sobre o custo da espera, porque esperar também é uma decisão, e é a mais cara de todas as opções em jogo. Não apenas financeiramente, mas também em termos operacionais e de reputação.

Esse custo não se resume a uma única conta. São três, e elas se acumulam:

- **A conta da violação de segurança:** resposta a incidentes, multas regulatórias e riscos legais
- **A conta do tempo de inatividade:** perda de produtividade, receitas perdidas e ataques repetidos enquanto a camada de identidade permanece exposta
- **A conta da confiança:** aumento dos prêmios de seguro cibernético, responsabilidade civil de executivos e risco de transações

E ficar esperando não congela o medidor. A superfície de ataque relacionada à identidade está entre as mais visadas nas empresas, e é uma área com a qual as defesas tradicionais não conseguem acompanhar o ritmo; por isso, o custo da inércia não permanece estático. Ela aumenta a cada trimestre que você deixa sem solução. Atraso não é cautela. São juros compostos sobre uma dívida que você nunca escolheu contrair.

DADOS COMPLEMENTARES



Ao longo de três anos, as organizações podem enfrentar um ataque bem-sucedido à identidade que custe **US\$ 1,2 milhão**, o monitoramento manual da identidade híbrida que custe **US\$ 109.000** e a perda de produtividade e o tempo de inatividade decorrentes da recuperação manual do Active Directory que custem **US\$ 3,9 milhões**. *(Estudo de impacto econômico total da Forrester).*



O custo médio global de uma violação de dados é de **US\$ 4,44 milhões**, mas as violações baseadas em credenciais custam cerca de **US\$ 4,67 milhões** e levam aproximadamente **292 dias** para serem identificadas e contidas, sendo o vetor de ataque mais demorado *(Custo de uma violação de dados, IBM 2025).*



A dinâmica econômica do ransomware está mudando, mas não sem dificuldades: o valor mediano do resgate caiu para **US\$ 115.000**, e **64%** das vítimas se recusaram a pagar, o que significa que mais organizações estão arcando com os custos operacionais da recuperação, em vez de pagar o resgate propriamente dito, aumentando a pressão sobre a velocidade da recuperação de identidades *(Verizon DBIR 2025).*



Atualmente, **8 das 8** principais seguradoras cibernéticas exigem e validam medidas de segurança e resiliência específicas para identidades ao subscrever apólices cibernéticas, e demonstrar um forte fortalecimento das identidades está diretamente relacionado a prêmios mais baixos e cobertura mais ampla *(Cohesity, "A resiliência das identidades é fundamental para o seguro cibernético").*

Esses dados não são independentes uns dos outros. São a cobrança detalhada por violação de dados e a cobrança por tempo de inatividade, com a cobrança por confiança logo atrás delas, já que as seguradoras vinculam os prêmios diretamente ao seu nível de segurança de identidade. Cada um deles fica mais caro quanto mais tempo a questão da identidade permanecer sem solução. Você vai pagar essa conta de qualquer jeito. A única questão é se você paga um pouco agora, nos seus termos, ou tudo mais tarde, nos termos do invasor..

CONCLUSÃO

Atualmente, as violações relacionadas à identidade estão presentes em praticamente todas as grandes brechas de segurança, e o padrão nunca muda. Os invasores não invadem. Eles fazem login com credenciais válidas e fluxos de identidade confiáveis e se movimentam sem serem detectados por ambientes que nunca foram projetados para identificá-los. Em seguida, eles roubam seus dados, tomam o controle de seus sistemas e instalam o ransomware deles.

Nada disso é inevitável.

O que diferencia as organizações que se recuperam em questão de horas daquelas que levam semanas para restabelecer a confiança em seus serviços de identidade não tem nada a ver com sorte, nem com quanto gastaram. Tudo se resume a uma única decisão: se eles desenvolveram a resiliência de identidade como uma disciplina própria, abrangendo todo o ciclo de vida do ataque, antes mesmo de precisarem dela.

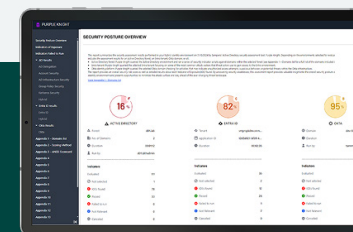
Portanto, encare a resiliência de identidade como o que ela se tornou: não algo opcional, mas um requisito essencial para a segurança corporativa. A identidade é, ao mesmo tempo, a sua porta de entrada, o seu alicerce e o seu gargalo na recuperação. Um conjunto heterogêneo de ferramentas específicas sempre será insuficiente. O mesmo vale para qualquer plano de continuidade que simplesmente presuma que a identidade estará lá quando chegar a hora. A única estratégia que resiste a um ataque real é aquela que você testou e comprovou antes de precisar dela.

A boa notícia é que você pode se antecipar a isso. Você pode aumentar a resiliência cibernética dos seus sistemas de identidade mais críticos.

E podemos ajudar.

Saiba mais sobre como a Cohesity pode ajudar a construir e fortalecer a resiliência de identidade

Faça uma avaliação gratuita de segurança de identidade para identificar vulnerabilidades e lacunas no Active Directory, no Entra ID e no Okta





© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

6100036-001 ptBR 8-2026