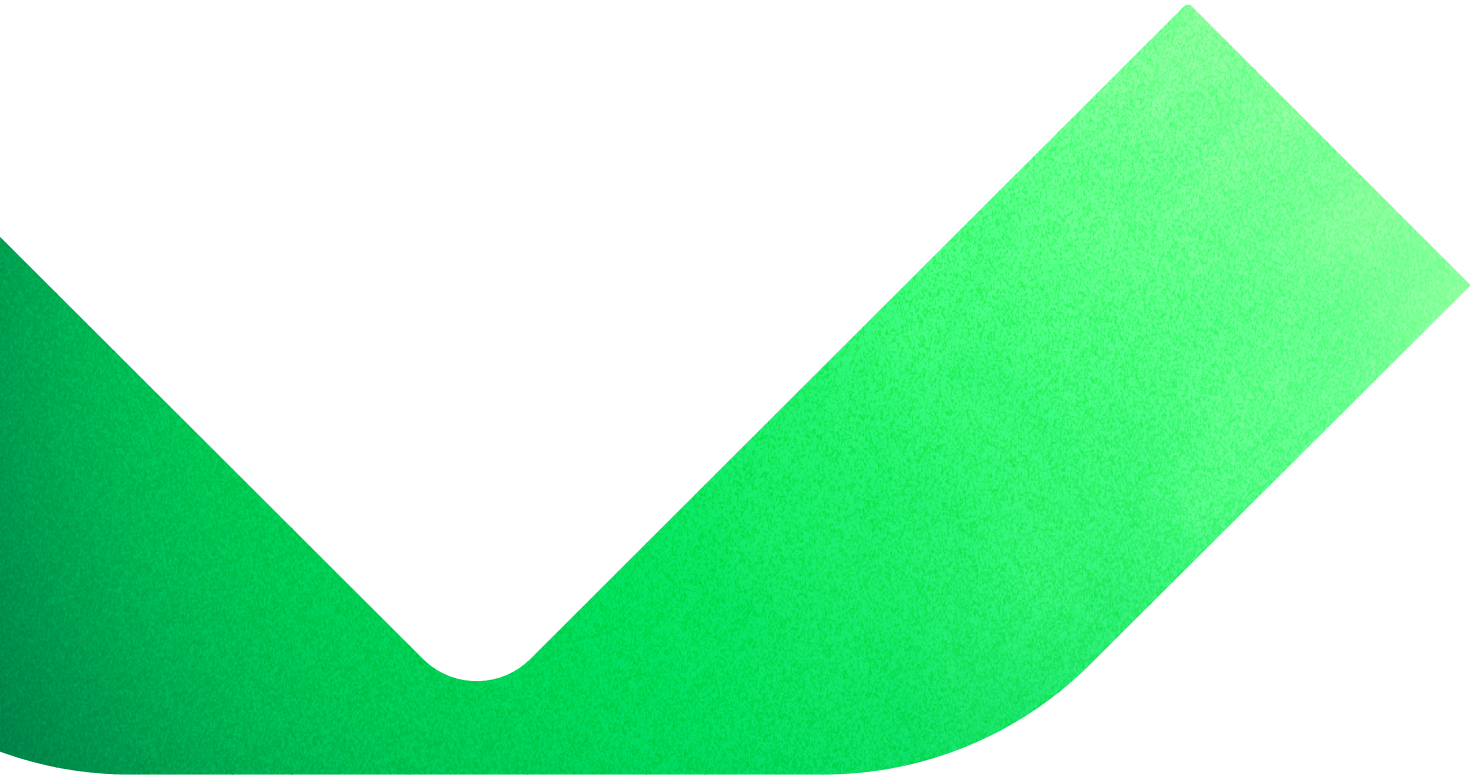
Resiliência de Dados Zero Trust

Um modelo seguro de backup e recuperação de dados



Conteúdo

Sumário executivo

Atualmente, as empresas enfrentam desafios contínuos significativos para proteger seus dados e redes contra agentes maliciosos, em particular contra ataques de ransomware e exfiltração de dados. Para enfrentar esses desafios, a estratégia Zero Trust tem ganhado destaque no setor de segurança da informação e está sendo amplamente adotada por empresas do mundo todo.

No entanto, mesmo os modelos de Zero Trust mais amplamente utilizados carecem de diretrizes abrangentes em certas áreas importantes, especialmente em relação ao backup e recuperação de dados. Reconhecendo a importância de preencher essa lacuna e aplicar os princípios de Zero Trust a essa área, apresentamos o conceito de Resiliência de Dados de Zero Trust. Isso inclui um conjunto de requisitos, uma arquitetura e uma extensão dos Modelos de Maturidade de Zero Trust existentes.

Especificamente, as empresas devem implementar um sistema de backup e recuperação de dados que ofereça storage e configurações imutáveis, ao mesmo tempo em que assegura acesso contextual e fortemente autenticado tanto aos dados de origem no ambiente de produção quanto aos dados de backup. Esse sistema também deve suportar de forma ininterrupta as arquiteturas híbridas, comuns nas empresas atuais, e lidar com a recuperação de forma flexível para ambientes diferentes.

Ao adotar uma arquitetura de Zero Trust que atenda a esses requisitos, as empresas conseguirão proteger de maneira mais eficaz seus dados, redes e aplicativos contra ameaças de agentes mal-intencionados. O modelo Zero Trust tem demonstrado oferecer uma segurança superior em relação às abordagens tradicionais, e as organizações têm a responsabilidade de adotá-lo. Os novos requisitos de resiliência de dados apresentados neste white paper reforçam e expandem o modelo Zero Trust, devendo ser considerados essenciais e obrigatórios dentro da estratégia de segurança de qualquer empresa.

Introdução

Zero Trust é uma abordagem de segurança que, por sua natureza, envolve um escopo abrangente. No entanto, os modelos e estruturas de Zero Trust amplamente adotados não abrangem tudo[1]. Isso pode resultar em lacunas ou falhas nas arquiteturas de segurança corporativa. Especificamente, os sistemas de backup e recuperação de dados não são contemplados nas estruturas de Zero Trust comumente adotadas. Essa é uma lacuna preocupante, pois os dados corporativos frequentemente se tornam o alvo principal de agentes maliciosos, seja em ataques de ransomware ou em tentativas de exfiltração de dados.

Os sistemas de backup e recuperação de dados são componentes essenciais da infraestrutura de TI corporativa e devem ser tratados com a devida importância. Eles possuem acesso de leitura a todos os dados essenciais para o processo de backup. Eles também precisam da capacidade de gravar dados em ambientes de produção para desempenhar sua função de restauração de dados. Além disso, eles armazenam uma cópia completa dos dados mais críticos da empresa. Juntos, todos esses atributos ressaltam a importância dos sistemas de backup e recuperação de dados e destacam seu valor como alvo de agentes maliciosos.

É claro que os sistemas de backup e recuperação de dados fazem parte da responsabilidade da TI há décadas, mas muitas vezes não são incluídos no escopo ou na responsabilidade das equipes de segurança. No entanto, dado o nível e a sofisticação das ameaças de segurança que as empresas enfrentam atualmente, adotar somente uma perspectiva de infraestrutura de rede e TI para o backup e a recuperação de dados não é mais suficiente. Na prática, muitas organizações apresentam sistemas mal configurados e sem monitoramento adequado, o que resulta em riscos significativos para a segurança.

Uma segurança moderna e eficaz se baseia em princípios de Zero Trust, então é hora de dar uma nova olhada nos sistemas de backup e recuperação de dados sob esse prisma. Este whitepaper aborda essa questão ao introduzir o conceito de Resiliência de Dados Zero Trust. Ao adotar essa abordagem, as empresas terão um caminho claro e sólido para fortalecer suas defesas, otimizar operações e garantir uma recuperação mais ágil.

[1] O documento CISA ZTMM afirma "Embora o ZTMM cubra muitos aspectos da segurança cibernética críticos para as empresas federais, ele não aborda outros aspectos da segurança cibernética, tais como... recuperação".

Abordagem

Os elementos fundamentais clássicos da segurança da informação — a tríade de Confidencialidade, Integridade e Disponibilidade da CIA — são todos aplicáveis ao backup e à recuperação de dados. As empresas precisam evitar a exfiltração de dados (Confidencialidade), impedir que o ransomware criptografe os dados (Integridade) e garantir que os sistemas estejam protegidos contra ataques e possam ser restaurados rapidamente após um ataque (Disponibilidade).

Os princípios fundamentais do Zero Trust são claramente relevantes para essa área e devem ser aplicados tanto ao acesso aos sistemas de TI da empresa e dos usuários quanto aos sistemas de backup e recuperação de dados. Esses princípios envolvem a remoção da confiança implícita e de redes não segmentadas, o controle de todo o acesso por meio de políticas dinâmicas e contextuais aplicadas por Pontos de Aplicação de Políticas (PEPs), a exigência de autenticação robusta para todos os usuários, a suposição de que violações possam ocorrer e a garantia e validação contínua da integridade do sistema e dos dados. Ao longo deste whitepaper, veremos como esses princípios fluem para o novo conjunto de requisitos proposto para uma arquitetura de resiliência de dados de confiança zero.

A estrutura padrão para avaliar a maturidade do modelo Zero Trust é o Modelo de Maturidade Zero Trust da CISA[2], conforme ilustrado na Figura 1, que define cinco pilares principais: Identidade, Dispositivos, Redes, Aplicações e Cargas de Trabalho, e Dados. Ele também define três capacidades transversais: Visibilidade e Análise, Automação e Orquestração, e Governança.

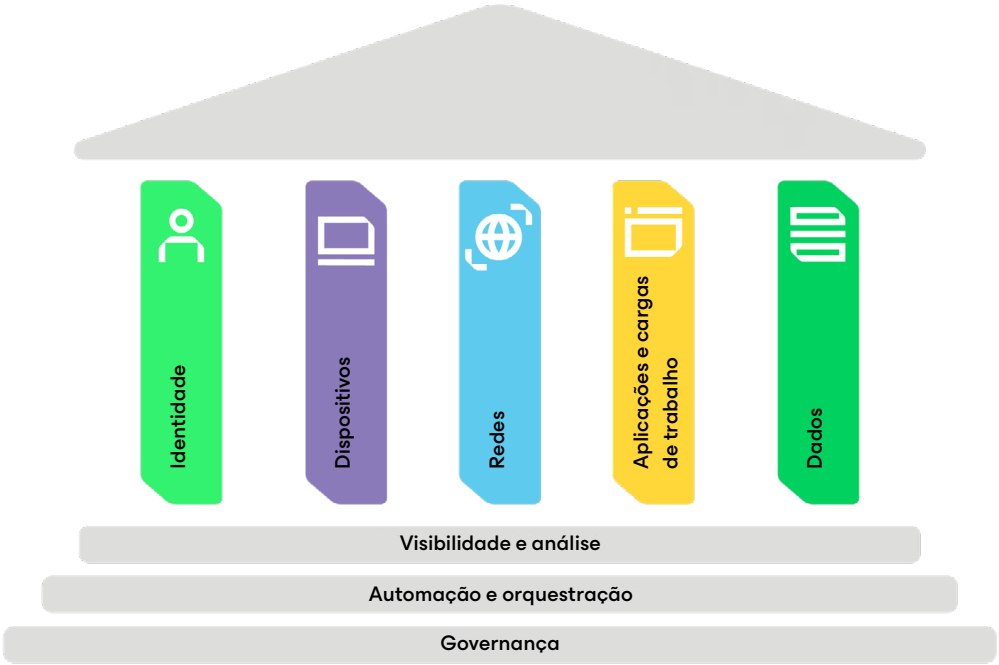


Figura 1: Modelo de Maturidade de Zero Trust da CISA

[2] https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model

Dentro do pilar Dados, o modelo CISA identifica cinco funções detalhadas, com capacidades e atributos esperados para cada nível de maturidade.

No entanto, dentro dessas funções, o tema de integridade e recuperação de backup de dados é abordado de maneira mínima, e a CISA direciona os leitores para um documento do NIST de 2020, que não está diretamente relacionado ao modelo Zero Trust. Em resumo, o modelo Zero Trust da CISA não aborda de maneira adequada os requisitos e níveis de maturidade para sistemas de backup e recuperação de dados. Dado que essa área é crucial para a confidencialidade, integridade e disponibilidade dos dados da empresa, acreditamos que essa lacuna precisa ser corrigida.

Para preencher essa lacuna, estamos introduzindo o conceito de Resiliência de Dados Zero Trust, que abrange princípios, uma arquitetura de referência e um novo conjunto de capacidades para o Modelo de Maturidade Zero Trust. Juntos, esses elementos representam uma extensão e aprimoramento do modelo Zero Trust, levando a uma postura de segurança mais robusta para a empresa.

As funções são:

- Gerenciamento de inventário de dados
- Categorização de dados
- Disponibilidade de dados
- Acesso a dados
- Criptografia de dados

Resiliência de Dados Zero Trust: Princípios

Os princípios básicos da Resiliência de Dados Zero Trust (ZTDR) são:

Acesso de menor privilégio

Imutabilidade

Resiliência do sistema

Validação proativa

Simplicidade operacional

Vamos discutir cada um deles sucessivamente.

Acesso de menor privilégio

Esse princípio é fundamental para o Zero Trust e é uma parte necessária de qualquer arquitetura Zero Trust. No entanto, vale a pena examinar sua aplicabilidade às especificidades do ZTDR, uma vez que ele se aplica em vários níveis. Do ponto de vista da rede, o próprio sistema de geranciamento de backup deve ser isolado na rede para que nenhum usuário ou dispositivo não autenticado ou não autorizado possa acessá-lo. Da mesma forma, o sistema de storage de backup deve ser isolado. Isso impede que agentes mal-intencionados descubram qualquer sistema por meio de reconhecimento de rede ou explorando uma vulnerabilidade.

O acesso legítimo e autorizado ao sistema de backup só deve ocorrer por meio de um Ponto de Aplicação de Política de Zero Trust (PEP), com autenticação forte apropriada e verificações de postura do dispositivo. O PEP de Zero Trust também deve controlar o acesso aos dados de origem (ou seja, os dados que estão sendo copiados), com autenticação apropriada e algum nível de validação de dispositivo ou sistema para garantir que o sistema de geranciamento de backup seja quem está lendo os dados de produção, e não um sistema ou processo malicioso.

O acesso do sistema de geranciamento de backup ao armazenamento de backup também deve ser controlado por um PEP e segmentado do resto da rede com autenticação apropriadamente forte. Observe que vamos revisitar esse requisito no diagrama de arquitetura abaixo, pois é importante — o sistema de storage de backup deve ser segmentado do sistema de geranciamento de backup.

Imutabilidade

O conceito e requisito de dados de backup imutáveis se tornaram amplamente adotados nos últimos anos, em conjunto com o aumento da prevalência e sofisticação do ransomware. Um backup imutável é aquele em que os dados são armazenados em um mecanismo de storage que, uma vez gravado, não pode ser modificado. A premissa é que, mesmo que um agente malicioso consiga acessar a rede, assumir o controle do sistema de backup e ter acesso ao storage de backup, ele não seria capaz de excluir ou modificar os dados de backup. A imutabilidade é parcialmente garantida pelas propriedades físicas da mídia de storage, como os discos ópticos Write-Once-Read-Many (WORM). Já as tecnologias mais recentes aplicam a imutabilidade por meio de camadas de hardware, firmware ou software. Recentemente, os principais provedores de serviços de nuvem passaram a oferecer recursos de storage imutável para atender às necessidades corporativas de conformidade e arquivamento.

NOTA

Os requisitos de inalterabilidade não se limitam apenas aos dados armazenados, mas também devem abranger os períodos de retenção desses dados. Alguns dados imutáveis podem ser configurados para storage ilimitado, enquanto outros podem ter um período de retenção específico, como um ou cinco anos. Os dados que excedem o período de retenção podem ser excluídos, por isso, o sistema de storage também deve garantir que o período de retenção dos dados seja imutável. Isso impede a redução maliciosa dos períodos de retenção.

Resiliência do sistema

Nós temos uma visão bastante ampla da resiliência do sistema e acreditamos que ela deve ser aplicada não apenas à infraestrutura de backup em si, mas a todo o ecossistema de ferramentas, tecnologias e processos relacionados ao backup e à recuperação de dados. Especificamente, a infraestrutura de backup deve ser resiliente a falhas e ataques, como indisponibilidade de componentes ou de rede, ou manipulação de servidor de tempo de rede (NTP) para expirar maliciosamente os dados de backup. Também é importante que seja fácil configurar o uso de storage de dados de backup distribuído e heterogêneo, como em diferentes regiões geográficas ou tipos de infraestrutura. A resiliência também é aprimorada ao separar os dados de backup do sistema de gerenciamento de backup, garantindo que, mesmo que o sistema de backup seja comprometido, o storage de dados permaneça protegido. Na verdade, é crucial procurar um sistema de gerenciamento de backup que, em caso de comprometimento ou falha, possa ser restaurado sem impactar a capacidade de acessar e restaurar os dados de backup.

O sistema também deve ser resiliente a mudanças, tanto esperadas quanto inesperadas, no ambiente corporativo. As mudanças esperadas incluem adição ou remoção planejada de componentes de infraestrutura, incluindo a adoção de aplicações e dados híbridos ou baseados em nuvem. Ou seja, o sistema de backup deve ser capaz de capturar e armazenar dados corporativos de maneira eficiente, independentemente de sua origem ou da tecnologia utilizada. Mudanças inesperadas geralmente acontecem durante a resposta a incidentes ou processos de recuperação de desastres (DR), sendo, na maioria das vezes, classificadas como suporte para recuperação em ambientes não semelhantes. Quando uma organização está recuperando dados, é perfeitamente possível que o ambiente de recuperação esteja sendo executado em um local ou tipo de infraestrutura diferente. Por exemplo, um data center localmente afetado por uma inundação pode exigir a recuperação para um ambiente baseado na nuvem, permitindo operações contínuas por um período prolongado. Portanto, o sistema de backup deve suportar tanto a recuperação nesse ambiente diferente quanto novos backups desse ambiente de produção a partir de agora.

O próprio sistema de storage de dados de backup, além de oferecer storage imutável, deve ser facilmente reforçado para garantir maior segurança. Isso pode se manifestar como um appliance pré-seguro ou como um sistema configurável administrativamente, com recomendações claras de proteção, sendo esta última opção mais adequada para empresas sofisticadas.

Validação proativa

Garantir a operação adequada do sistema requer que o sistema seja monitorado e todos os aspectos funcionais e processos sejam validados. Isso tem dois aspectos. Primeiramente, o sistema de backup deve ser monitorado em relação à rede, ao desempenho e à segurança. Ou seja, esse sistema deve ser tratado como qualquer outro sistema de produção de alto valor.

Em segundo lugar, e mais importante, a validade dos dados de backup — e a confiabilidade e eficácia dos processos de recuperação — devem ser validadas regularmente. Por definição, a recuperação de dados de backup vai ocorrer em momentos inesperados e, provavelmente, em um ambiente de alto estresse. É fundamental que a organização tenha um processo claro, bem documentado e amplamente praticado. Também é preciso que haja várias pessoas capazes de realizar isso para dar conta das férias dos funcionários, indisponibilidade e rotatividade.

Tenha em mente que, embora isso exija um investimento de tempo e energia, isso demonstra maturidade operacional, e é uma "apólice de seguro" em caso de desastre. Vale ressaltar que "desastre" não precisa se referir a um evento de grande escala, como a inundação de um data center. Por exemplo, uma empresa com a qual trabalhamos enfrentou um fluxo de trabalho automatizado descontrolado devido a um erro de programação, o que levou à exclusão de grandes volumes de dados de produção em seu sistema de gerenciamento financeiro. Embora isso não tenha sido um desastre real, foi evitado de se transformar em um desastre potencial graças aos processos de recuperação de dados da empresa, que já estavam validados.

Além disso, o sistema de geranciamento de backup deve ter a capacidade, direta ou indireta, de organizar backups em uma linha do tempo de infecção por malware. Ou seja, ele deve ser capaz de detectar (ou ser informado sobre) infecções por malware e categorizar os backups como limpos, questionáveis ou comprometidos, dependendo de quando foram capturados.

NOTA

Os processos de validação e recuperação de dados também devem atender aos requisitos de privacidade e de localização dos dados. Isso pode adicionar complexidade e risco, por isso deve ser feito com cuidado, com conhecimento do conteúdo dos dados e das obrigações legais e de conformidade da organização.

Simplicidade operacional

Nosso princípio final é a simplicidade operacional, que definimos como um sistema suficientemente fácil de operar para que a organização tenha confiança, mas que também ofereça capacidade, escalabilidade e sofisticação adequadas para atender plenamente às necessidades da empresa. Ou seja, um sistema adequado para a sua organização.

Isso é fundamental — temos observado empresas enfrentando dificuldades para utilizar e operacionalizar sistemas que são excessivamente complexos para o porte, a equipe, as habilidades e as necessidades específicas de suas organizações. Isso resulta em benefícios limitados, frustração e incapacidade de fornecer maturidade de segurança ou valor comercial. Um conjunto de atributos a serem observados em um fornecedor de backup é sua força relativa em orquestração e automação. Fornecedores com recursos sólidos em suas plataformas serão mais rápidos e fáceis de operacionalizar.

Para concluir esta seção, cada um desses princípios está incorporado nas novas extensões do Modelo de Maturidade, que serão detalhadas mais adiante neste documento, e também será refletido na arquitetura de referência que abordaremos em seguida.

Resiliência de Dados Zero Trust: Arquitetura de referência

As arquiteturas de backup de dados necessariamente variam de acordo com as empresas, considerando-se, entre outros fatores, a enorme variabilidade das infraestruturas de rede, aplicação e dados. Ainda assim, existem elementos arquitetônicos comuns, derivados dos princípios do Zero Trust, que devem estar presentes em qualquer arquitetura de Resiliência de Dados Zero Trust.

Nossa arquitetura de referência é mostrada na Figura 2 e ilustra os principais requisitos nesse tipo de sistema. Observe que isso retrata o ambiente da perspectiva do sistema de geranciamento de backup. O acesso diário de usuários e sistemas aos sistemas de produção também seria controlado pelos PEPs do Zero Trust, embora isso tenha sido omitido no diagrama para simplificar a visualização.

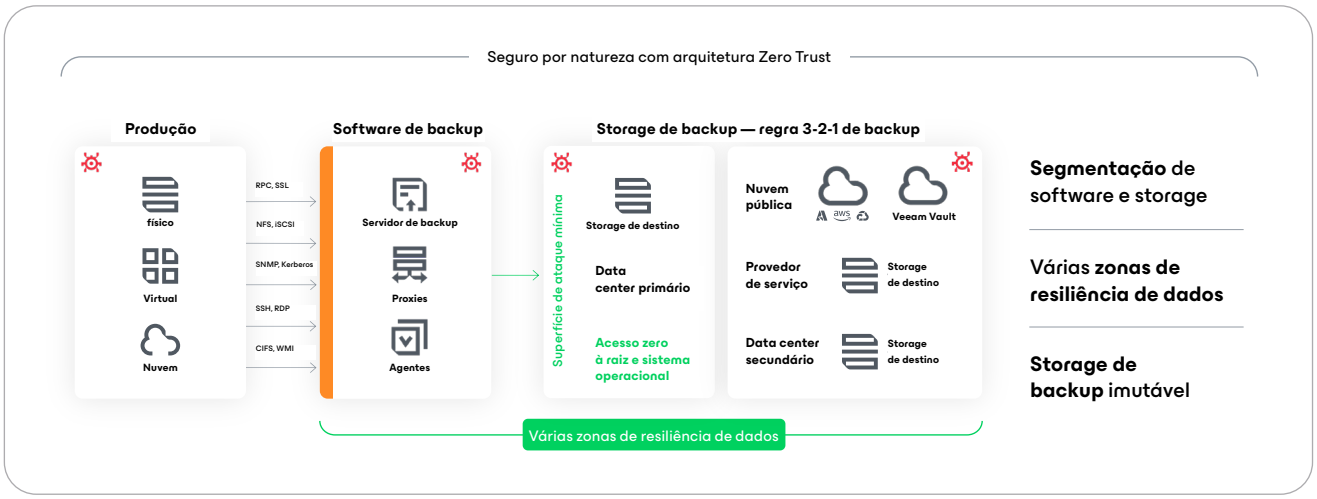


Figura 2: Resiliência de Dados Zero Trust: Arquitetura de referência

Primeiramente, observe os componentes principais de qualquer arquitetura Zero Trust — o PDP (Policy Decision Point, ponto de decisão de política) centralizado, que delega a autenticação de identidade ao sistema corporativo de Identity and Access Management (IAM). O PDP depende de seu armazenamento de políticas para tomar decisões de acesso para identidades autenticadas, incluindo identidades humanas e não pessoais (sistema). Nessa arquitetura, o PDP toma decisões de acesso para o sistema de geranciamento de backup. Essas decisões são transmitidas por meio do plano de controle (representado por linhas pontilhadas) para os Pontos de Aplicação de Políticas (PEPs), que se posicionam logicamente entre o sistema de gerenciamento de backup, as fontes de dados a serem copiadas e os locais de backup de destino.

A arquitetura também inclui uma estrutura recomendada para dados de backup. Além do requisito de imutabilidade dos dados, a empresa deve garantir que pelo menos uma cópia seja mantida em um local primário, com uma conexão de rede de baixa latência para o site de restauração pretendido. Isso permite snapshots de backup rápidos, que incentivam pontos de recuperação mais frequentes e tempos de recuperação mais rápidos. É importante notar que o local primário geralmente está colocalizado com os sistemas de produção. Portanto, nossa arquitetura de referência também enfatiza a necessidade de ter pelo menos duas cópias dos dados em locais secundários[3]. Esses locais secundários devem ser geograficamente isolados do local principal para garantir resiliência contra desastres regionais. A provável compensação é uma conexão de rede mais lenta, o que pode resultar em pontos de recuperação de frequência mais baixos e tempos de recuperação mais longos.

NOTA

O sistema de gerenciamento de backup é intencionalmente separado dos seus níveis de storage. Isso permite que o sistema de backup distribua facilmente os dados de backup por múltiplos repositórios imutáveis e geograficamente distribuídos. Ele também permite que as corporações selecionem repositórios de storage de backup que ofereçam a melhor combinação de desempenho, preço e simplicidade operacional para seus requisitos únicos. Ele também fornece uma camada adicional de segurança, controlando a comunicação através de um PEP.

[3] Existem diversas abordagens sobre a quantidade de backups em locais distintos, frequentemente representadas por mnemônicos como 3-2-1 ou 3-2-1-1-0.

Resiliência de Dados Zero Trust: Modelo de Maturidade Estendida

Embora os princípios e a arquitetura de referência que propomos para a Resiliência de Dados Zero Trust sejam universalmente aplicáveis, sua implementação total e imediata não é viável na maioria das empresas. Como ocorre com a maioria dos aspectos do Zero Trust, esses elementos devem ser planejados e adotados de maneira gradual. A maneira padrão de modelar e comunicar isso é por meio de um modelo de maturidade. Como mencionamos na introdução, estamos seguindo a estrutura padrão do Modelo de Maturidade de Zero Trust da CISA e ampliando-a com quatro novas funções que incorporam nossos princípios e requisitos.

Estas novas funções são:

Acesso a dados e sistemas corporativos

Acesso ao storage de backup e aos dados

Resiliência do sistema

Monitoramento e validação do sistema

Essas extensões ZTDR para o modelo de maturidade estão representadas nas Figuras 3 a 6, que mostram como cada uma das quatro novas funções deve ser avançada nos níveis de maturidade padrão: Tradicional, Inicial, Avançado e Otimizado.

Para cada uma das funções, identificamos os atributos esperados para cada nível de maturidade. Assim, o modelo retrata as melhorias e mudanças que uma organização precisa fazer para avançar na maturidade de cada função. Em seguida, analisamos cada uma das funções individualmente, à medida que elas avançam pelos diferentes níveis de maturidade.

Acesso a dados e sistemas corporativos

Essa função é definida como os meios e mecanismos pelos quais o sistema de gerenciamento de backup (BMS) obtém acesso aos dados de origem que ele é responsável por proteger por meio de backup.

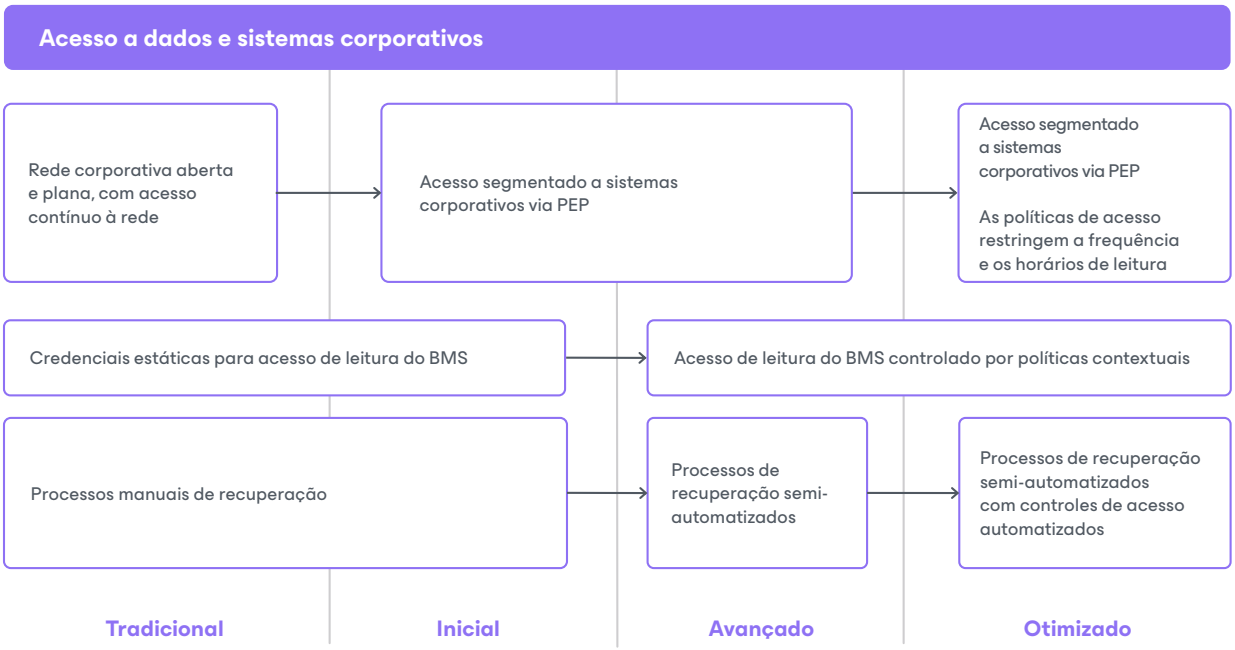


Figura 3 — Acesso a dados e sistemas corporativos: Modelo de Maturidade

No nível **Tradicional** de maturidade, a empresa conta com uma rede plana e aberta, e o sistema de gerenciamento de backup tem acesso contínuo e irrestrito aos sistemas de origem. O BMS utiliza credenciais estáticas, como uma chave de API, nome de usuário e senha armazenados ou um certificado, para autenticar e acessar os dados de origem. Quando a empresa usa o BMS para recuperar um sistema, ela depende de processos manuais.

Para avançar para o nível **Inicial**, a empresa deve começar a implementar uma segmentação de rede mais robusta e restringir o acesso do BMS aos sistemas corporativos por meio de um Ponto de Aplicação de Políticas de Zero Trust, adotando o princípio do menor privilégio.

Quando a empresa estiver no nível **Avançado**, ela terá implementado políticas de acesso contextual para o acesso do BMS aos dados e sistemas empresariais, aproveitando de maneira mais eficaz as capacidades dinâmicas de imposição de políticas do Zero Trust. Eles também terão começado a usar processos de recuperação automatizados com algumas etapas manuais para iniciar e validar o processo.

No nível **Otimizado**, a organização terá aprimorado o uso de políticas de acesso, restringindo o acesso do BMS a períodos de tempo específicos ou a eventos de recuperação ativos. Isso reforça ainda mais o princípio do menor privilégio.

Acesso ao storage de backup e aos dados

Esta função é definida como sendo o meio e o mecanismo pelos quais o sistema de geranciamento de backup tem acesso de gravação e leitura ao armazenamento de backup e aos dados armazenados nele.

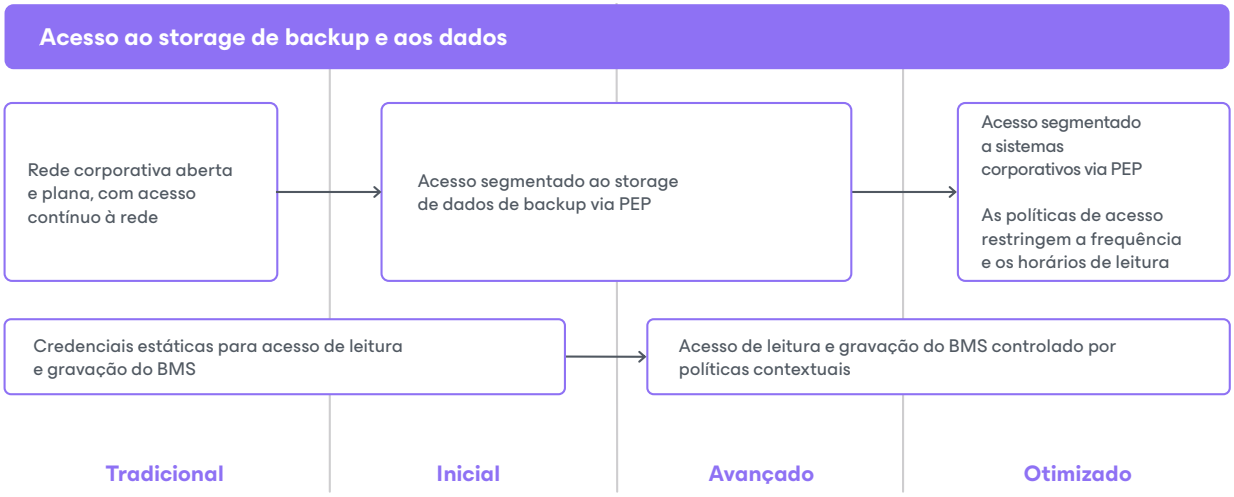


Figura 4 — Acesso ao storage de backup e aos dados: Modelo de Maturidade

No nível de maturidade **Tradicional**, a empresa possui uma rede plana e aberta, e o sistema de gerenciamento de backup tem acesso contínuo e irrestrito ao sistema de storage de backup e aos dados ali armazenados. O BMS utiliza credenciais estáticas, como uma chave de API, nome de usuário e senha armazenados ou um certificado, para autenticar, gravar no storage e ler os dados ali armazenados.

Para avançar ao nível **Inicial**, a empresa deve começar a aplicar uma melhor segmentação de rede e a restringir o acesso do BMS ao armazenamento de backup e aos dados armazenados por meio de um Ponto de Aplicação de Política de Zero Trust, aplicando o princípio do menor privilégio.

Quando a empresa estiver no nível **Avançado**, terá implementado políticas de acesso contextual para controlar o acesso do BMS ao sistema de storage de backup e aos dados nele armazenados. Isso aproveita de maneira mais eficaz as capacidades dinâmicas de imposição de políticas dentro da organização.

No nível **Otimizado**, a organização terá aprimorado o uso de políticas de acesso, restringindo o acesso do BMS a storage a períodos de tempo específicos ou durante eventos de recuperação ativos. Isso reforça ainda mais o princípio do menor privilégio.

Resiliência do sistema

Esta função é definida como sendo as características do sistema de backup com relação à sua resistência a falhas de sistema, falha de componentes ou atividade maliciosa.

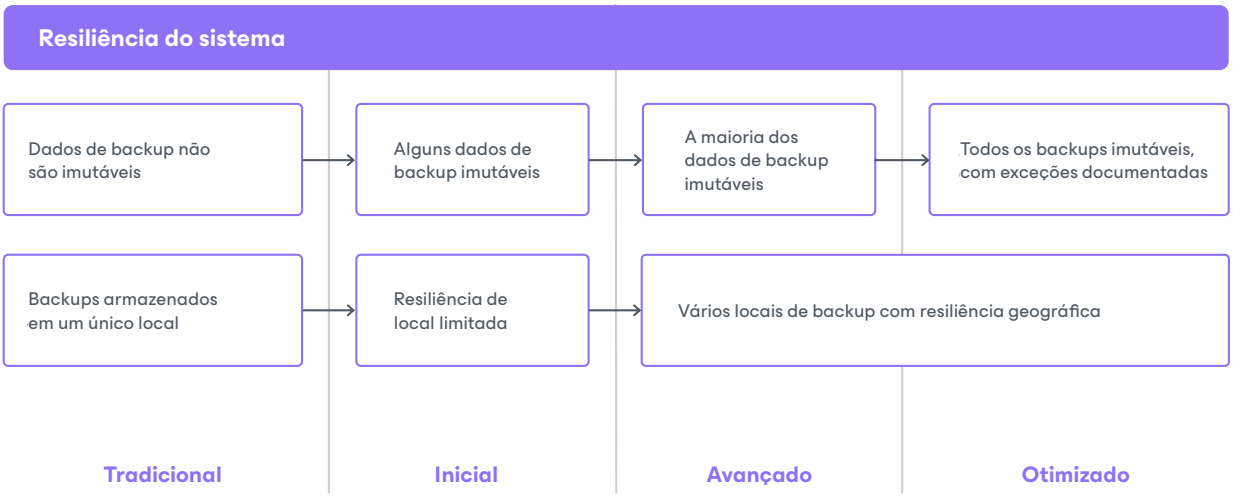


Figura 5 — Resiliência do sistema: Modelo de Maturidade

No nível **Tradicional** de maturidade, a organização usa storage mutável para dados de backup, colocando em risco sua integridade e disponibilidade. Ela também normalmente armazena backups em apenas um local, sujeitando a organização a perda total no caso de um desastre regional.

Conforme a empresa avança para o **nível Inicial**, ela deve começar a utilizar o storage imutável para alguns dos seus backups de dados e introduzir alguma resiliência de local limitada para esses backups.

No nível **Avançado**, a empresa usará principalmente storage de backup imutável, idealmente priorizado pela sensibilidade e criticidade dos dados. Ela também terá introduzido e operacionalizado o uso de vários locais de storage de backup, em diferentes localizações geográficas distribuídas.

Quando a empresa estiver no nível **Otimizado**, ela terá adotado o uso total de storage de backup imutável, com quaisquer exceções devidamente documentadas e aprovadas. Por padrão, as novas fontes de dados e aplicações usarão backup imutável. Esse nível proporciona à organização a resiliência máxima contra desastres regionais e ameaças de agentes maliciosos.

Monitoramento e validação do sistema

Essa função abrange as ferramentas e os processos que asseguram o funcionamento adequado do sistema de gerenciamento de backup e storage de backup da empresa, além de garantir que seja possível realizar a recuperação de dados quando necessário.

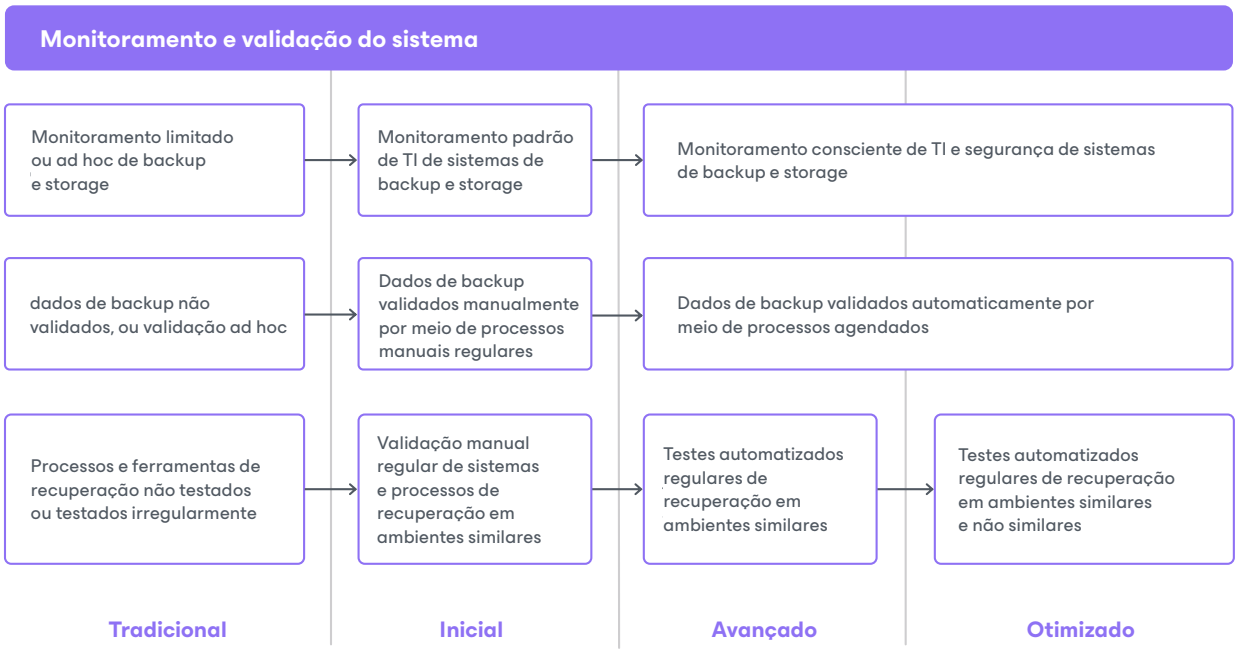


Figura 6 — Monitoramento e validação do sistema: Modelo de Maturidade

No nível de maturidade **Tradicional**, a empresa realizará apenas o monitoramento básico da infraestrutura de backup e storage, o que geralmente reflete uma maturidade mais baixa nas áreas de TI e operações. A organização pode não validar os dados de backup ou realizar apenas verificações esporádicas, geralmente manuais e com pouca frequência. Além disso, a empresa não realizará testes regulares das ferramentas e processos de recuperação, o que comprometerá sua compreensão, documentação e capacidade de execução consistente.

No nível **Inicial**, ela terá adotado um nível padronizado de monitoramento de TI e operacional do sistema de backup e storage. Eles também instituirão a validação regular dos dados de backup por meio de processos manuais. Ela também terá implementado a validação regular (manual) dos processos de recuperação, a fim de assegurar o conhecimento institucional e a familiaridade com esses procedimentos.

No nível **Avançado**, as organizações terão implantado ferramentas e processos de monitoramento de TI e segurança para sistemas de backup e storage. Além disso, eles validarão automaticamente os dados de backup com verificações agendadas que relatam e encaminham quaisquer resultados anômalos. Isso incluirá testes automatizados de ferramentas e processos de recuperação em ambientes semelhantes aos de produção.

No nível **Otimizado**, a empresa terá refinado a sofisticação de seus testes de recuperação para testá-los para recuperação em ambientes diferentes.

Resumo do Modelo de Maturidade

Tomadas como um todo, essas novas funções definem um conjunto de recursos e um conjunto esperado de competências mapeadas nos quatro níveis de maturidade de Zero Trust. Eles fornecem um roteiro prático e um guia para corporações que buscam trazer seus sistemas de backup e recuperação de dados para sua iniciativa Zero Trust.

Conclusão

O Zero Trust é uma maneira comprovadamente melhor de abordar a segurança da informação e, como líderes em segurança, temos a obrigação de trazer essa estratégia para dentro de nossas empresas. As arquiteturas atuais de Zero Trust e os modelos de maturidade são pontos de partida sólidos, mas estão incompletos. Particularmente, os requisitos e abordagens de backup e recuperação de dados estão ausentes deles.

Tradicionalmente, as empresas tratavam o backup e a recuperação como estando dentro do domínio da TI, mas a prevalência do ransomware e a digitalização quase completa dos negócios exige que os líderes de segurança ampliem seu escopo para incluir isso.

Neste whitepaper, apresentamos o conceito de Resiliência de Dados de Zero Trust, com um conjunto de princípios fundamentais, uma arquitetura de referência e extensões para o Modelo de Maturidade de Zero Trust. Acreditamos que, ao adotar essa abordagem de Resiliência de Dados Zero Trust, as empresas terão um caminho claro e sólido para fortalecer suas defesas, otimizar operações e acelerar a recuperação. Os dados da empresa são valiosos demais para que não adotemos as melhores práticas de segurança, e a abordagem Zero Trust é a maneira mais eficaz de garantir essa proteção.

Sobre a Veeam Software

Veeam®, a líder nº 1 do mercado global em resiliência de dados, acredita que toda empresa deve ser capaz de retornar à frente após uma interrupção com a confiança e o controle de todos os seus dados, quando e onde forem necessários. A Veeam chama isso de resiliência radical, e estamos determinados a criar formas inovadoras de ajudar nossos clientes a alcançá-lo. As soluções da Veeam são desenvolvidas especificamente para potencializar a resiliência de dados, fornecendo backup, recuperação, liberdade de dados, segurança e inteligência de dados. Com a Veeam, os líderes de TI e segurança ficam tranquilos sabendo que seus aplicativos e dados estão protegidos e sempre disponíveis em seus ambientes físicos, virtuais, na nuvem, SaaS e Kubernetes. Com sede em Seattle e escritórios em mais de 30 países, a Veeam protege mais de 550.000 clientes no mundo inteiro, incluindo 74% dos participantes da Global 2000, que confiam na Veeam para manter seus negócios em operação. Resiliência radical começa com a Veeam. Saiba mais em www.veeam.com ou siga a Veeam no LinkedIn @veeam-software e no X @veeam.

Saiba mais: veeam.com