Estendendo a Zero Trust para Backup e Recuperação de Dados

Um Guia Prático para Profissionais de TI e Segurança

Sumário

Sumário Executivo

Zero Trust é uma estratégia moderna e altamente eficaz para proteger melhor nossa infraestrutura de TI corporativa contra o ransomware e outras ameaças. Os sistemas de backup e recuperação de dados são essenciais para nossas corporações e devem ser incluídos em qualquer iniciativa Zero Trust.

No entanto, pode ser complicado arquitetar e implementar a Zero Trust e, até agora, não havia consenso sobre a melhor forma de aplicá-la aos sistemas de backup e recuperação de dados.

Resiliência de Dados Zero Trust (ZTDR) — um novo modelo introduzido pela Veeam e pela Numberline Security — baseia-se no Modelo de Maturidade de Zero Trust da Cybersecurity and Infrastructure Security Agency (CISA). A ZTDR estende os princípios de Zero Trust para backup e recuperação, garantindo que as corporações possam reduzir riscos e atingir suas metas de segurança e resiliência.

Seguindo a abordagem Resiliência de Dados Zero Trust explicada neste guia, você aprenderá o que procurar em uma arquitetura e plataforma de backup e recuperação de dados e poderá começar de forma rápida e eficaz em seu ambiente.

Zero Trust: Uma Breve Introdução

Zero Trust é uma moderna estratégia de segurança baseada na ideia de que nenhum usuário, dispositivo ou pacote de rede deve ser implicitamente confiável. Para garantir a segurança dos dados, o acesso a ativos de dados críticos deve ser segmentado e todas as comunicações devem ser autenticadas, avaliadas e autorizadas antes que qualquer acesso seja concedido. Isso deve ser aplicado a cada segmento e seus dados, aplicativos, ativos ou serviços.

Essa é uma mudança significativa em relação às arquiteturas tradicionais de segurança da informação, que eram baseadas em perímetros estáticos e baseados em rede, e que claramente falharam em manter nossas corporações seguras contra ransomware e agentes maliciosos.

Introdução à Resiliência de Dados Zero Trust (ZTDR)

Os sistemas de backup e recuperação de dados são elementos críticos da TI corporativa, assim como alvos frequentes de ataques. Eles devem ser protegidos de forma adequada e holística.

Seguindo os princípios da ZTDR e escolhendo fornecedores de backup e storage com base nas orientações da ZTDR, sua empresa obterá defesas mais fortes, operações mais eficientes e recuperação mais rápida e confiável.

ZTDR Estende os Princípios Básicos de Zero Trust

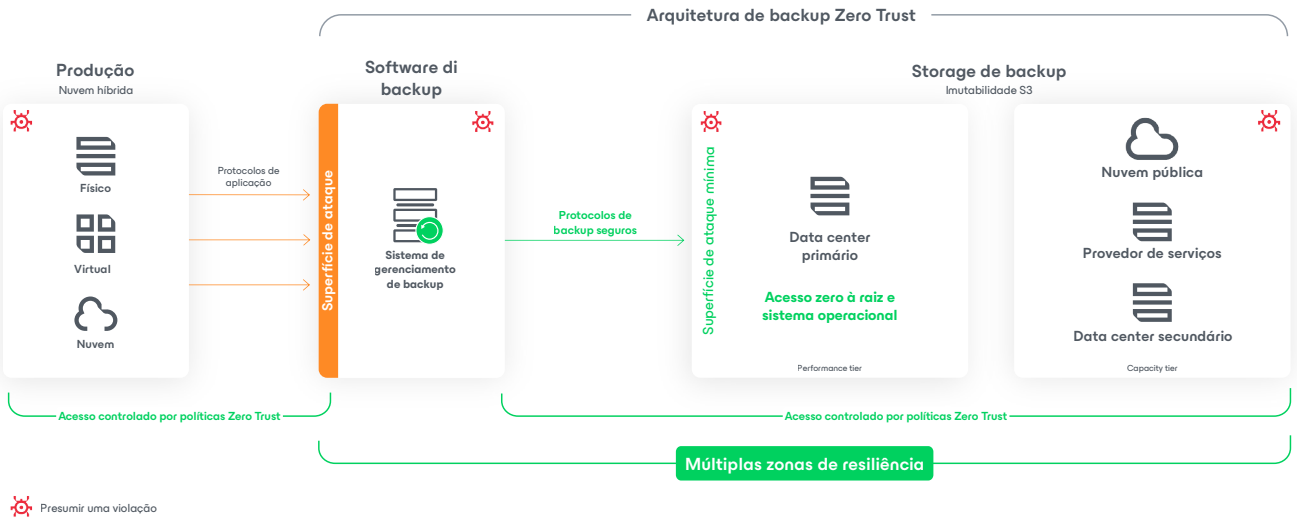
	Separação entre software de backup e armazenamento de backup	Múltiplas zonas de resiliência	Storage de backup imutável
Minimize a superfície de ataque e o raio de explosão	Regra de backup 3-2-1	Proteger os dados de backup contra modificação ou exclusão
REQUISITOS DA SOLUÇÃO	Procure soluções de backup e recuperação de dados que sejam arquitetadas com separação entre o software de backup e o storage e que, idealmente, impeçam o acesso principal ou root ou do SO ao storage de backup. Esses recursos permitirão que você imponha estritamente os controles de acesso por meio de políticas de Zero Trust.	Procure soluções de backup e recuperação de dados que ofereçam suporte a múltiplas zonas de resiliência, o que significa que sua empresa pode sobreviver à perda ou comprometimento de qualquer sistema de backup ou ambiente de storage. Isso permitirá que você cumpra facilmente as diretrizes de backup 3-2-1.	Procure soluções de backup e recuperação de dados que suportem de forma fácil e eficiente um storage de backup imutável robusto e confiável. Isso lhe dará total confiança de que seus dados de backup estão protegidos contra exclusão ou modificação, mesmo na presença de um agente malicioso.

A regra 3-2-1 para melhores práticas de backup:

3	2	1
3 cópias de dados, incluindo dados de produção.	2 cópias de dados de backup em storage imutável em zonas de resiliência separadas.	1 cópia fora do local.

Arquitetura de referência ZTDR

Esta arquitetura de Referência ZTDR mostra como uma plataforma de Zero Trust deve ser implantada em conjunto com seus sistemas de geranciamento de backup e storage.



Introdução ao ZTDR

Embora a Zero Trust seja uma jornada, há medidas imediatas e impactantes que você pode tomar para aprimorar a resiliência de segurança da sua infraestrutura de backup e recuperação de dados.

Esta semana:

Explore como os seus sistemas de backup e recuperação atendem aos requisitos da ZTDR.

Tarefa	Perguntas a fazer
Fale com as equipes de rede e infraestrutura de TI sobre a segmentação de sua rede	• Como nossa rede é segmentada? • O software de backup e o storage de backup são segmentados em zonas de segurança separadas? • Como é controlado o acesso de e para cada segmento da infraestrutura de backup?
Avalie se o seu storage de dados de backup está organizado em múltiplas zonas de resiliência	• Estamos seguindo as orientações do setor em relação ao 3-2-1? • O que acontece aos nossos processos de backup e recuperação se uma das nossas zonas de backup não estiver disponível? • O que acontece aos nossos processos de backup e recuperação se duas das nossas zonas de backup não estiverem disponíveis?
Determine se os seus sistemas de storage de backup são corretamente imutáveis	• Como o seu fornecedor de armazenamento documenta e garante a imutabilidade? • Um administrador malicioso pode alterar as configurações de imutabilidade ou retenção usando o acesso principal ou do SO ao storage? • O que acontece se o tempo do sistema for maliciosamente avançado?
Valide seus processos de recuperação	• Qual é o nosso Plano de Resposta de DR? Quando o testamos pela última vez? • Quantas pessoas da equipe de TI ou de armazenamento podem recuperar um sistema com sucesso seguindo as etapas documentadas? • O que acontece se a (pessoa importante X) não estiver disponível durante um incidente?

Na próxima semana:

Valide seus processos e ferramentas, depois planeje e construa consensos para mudanças de curto e médio prazo na sua infraestrutura e processos de backup e recuperação.

Tarefa	Perguntas a fazer
Avalie a sua confiança e a repetibilidade dos seus processos de recuperação executando testes regulares (semanais/mensais)	• Com que frequência fazemos nossos testes de recuperação? • O que aprendemos sobre documentação ou lacunas no processo? • Quando podemos remediá-los?

Tarefa	Perguntas a fazer
Comece a planejar alterações na regra de configuração, segmentação ou firewall de rede	• Com quem na equipe de TI ou Segurança posso colaborar para definir o escopo de possíveis mudanças? • Quem na equipe de Segurança está liderando nossa iniciativa Zero Trust e como posso apoiá-la? • Quais mudanças de segmentação de rede ou infraestrutura temos em andamento?
Planeje qualquer mudança na configuração de storage ou avaliações de novos fornecedores, a fim de fechar quaisquer lacunas de imutabilidade	• Qual é o nosso processo de avaliação e aquisição de storage de backup adicional? • Que tipo de justificativa financeira, de eficiência ou de risco precisaríamos fazer? • Como devo obter aprovação para iniciar um processo de avaliação de fornecedores?
Designe proprietários responsáveis por quaisquer melhorias de processo e documentação	• Quem estaria envolvido na aprovação e implementação de mudanças no (processo X)? • Como podemos estabelecer um prazo mutuamente acordado para a implementação?

Próximo mês:

Comece a implementar mudanças de curto prazo e a identificar quaisquer mudanças necessárias de longo prazo.

Tarefa	Perguntas a fazer
Implante seus processos aprimorados de recuperação de desastres e teste novamente	• O quanto nossos processos de DR melhoraram? • Nós solucionamos todas as lacunas de processo e documentação?
Valide e itere na segmentação de rede	• Quais áreas da rede ainda concedem amplo acesso à rede para e de nossos sistemas de backup? • Como podemos reforçar isso para melhorar nossa resiliência contra ransomware?
Execute melhorias na capacidade, nos locais e na imutabilidade do storage	• Quão confortáveis estamos com nossa capacidade de storage de backup? • Estamos confiantes de que nossos sistemas de storage de backup são imutáveis? • Quão bem estamos seguindo as orientações das melhores práticas 3-2-1? • Como estamos utilizando múltiplas zonas de resiliência?

O que Mais Você Deve Procurar?

Validação Proativa de Recuperação de Desastres

Incidentes que requerem a recuperação de dados de backup ocorrerão em momentos inesperados e, provavelmente, em circunstâncias de grande estresse. É importante que sua organização tenha planos e processos de recuperação de desastres bem compreendidos, bem documentados e bem preparados. Certifique-se também de que tem um alto grau de confiança na integridade e validade dos dados de backup.

Simplicidade Operacional

Certifique-se de selecionar um sistema que seja simples o suficiente para que sua organização opere com facilidade e confiança, ao mesmo tempo que fornece recursos, escalabilidade e sofisticação suficientes para atender totalmente às necessidades da sua corporação. Trabalhe para entender claramente a capacidade e as habilidades de sua equipe, para que as operações não dependam de um único indivíduo ou "super-herói".

Perguntas Frequentes

Zero Trust é algo que você pode comprar de um fornecedor?

Não, Zero Trust é algo que você **faz**, é uma estratégia de segurança que muda e melhora a TI, a segurança e os resultados dos negócios.

Zero Trust é apenas sobre restringir o acesso e reduzir a produtividade do usuário?

Não — Zero trust diz respeito à eliminação de todo acesso **desnecessário**, mantendo a produtividade dos usuários. Muitas corporações realmente **melhoram** a produtividade e a experiência do usuário com a Zero Trust.

Por que a Zero Trust é importante?

A Zero Trust é a forma mais eficaz de defender nossas corporações contra riscos, como ransomware, agentes maliciosos e outros riscos. Considerando o panorama atual de ameaças, temos a responsabilidade de utilizar essa iniciativa.

Você pode usar sua infraestrutura de segurança atual para Zero Trust?

Muito provavelmente, sim! Quando usados corretamente, os sistemas modernos de firewall, identidade e infraestrutura podem oferecer suporte a você ao iniciar sua jornada de Zero Trust. Atingir níveis ótimos de maturidade Zero Trust pode exigir investimentos adicionais, que podem ser guiados por ferramentas como a arquitetura de referência ZTDR.

Recursos adicionais

Quer saber mais sobre Zero Trust e ZTDR?

- Visite o site da Veeam para ler a pesquisa completa sobre ZTDR e ver a abordagem da Veeam à segurança de dados e resiliência cibernética.

- Para ler o whitepaper completo da pesquisa ZTDR e obter a perspectiva da segurança da Numberline sobre isso, visite o site da Numberline.

Sobre a Veeam Software

A Veeam, líder de mercado global nº 1 em resiliência de dados, acredita que as empresas devem controlar todos os seus dados quando e onde eles precisarem. A Veeam oferece resiliência de dados por meio de backup, recuperação, liberdade, segurança e inteligência de dados. Com sede em Seattle, a Veeam protege mais de 550.000 clientes em todo o mundo que confiam na Veeam para manter seus negócios em operação. Saiba mais em www.veeam.com/pt ou siga a Veeam no LinkedIn @veeam-software e no X @veeam.

Saiba mais: veeam.com