Resiliência de dados Zero Trust (ZTDR)

Arquitetura segura de backup e recuperação de dados

Uma abordagem pragmática para implementar Zero Trust

Visão geral

Empresas de todos os tamanhos, em todos os setores, entendem a importância da Zero Trust para garantir a segurança dos seus dados e negócios. No entanto, o modelo Zero Trust atual ainda não foi aplicado ao backup e recuperação de dados de forma substantiva. O conceito de estender os princípios de Zero Trust para o backup e a recuperação de dados está alinhado com a natureza holística da cibersegurança, e proteger informações confidenciais envolve mais do que apenas a segurança de perímetro.

Para enfrentar esse desafio, a Veeam colaborou com Jason Garbis, especialista em Zero Trust, da Numberline Security, na Estrutura de Resiliência de Dados de Zero Trust, criada para diminuir riscos, fortalecer a proteção de dados e revolucionar a postura de segurança de uma empresa. Essa estrutura se baseia no Modelo de Maturidade de Confiança Zero (ZTMM) da Cybersecurity and Infrastructure Security Agency (CISA) e estende os princípios principais da ZTMM para um cenário de backup e recuperação. A Estrutura de Resiliência de Dados Zero Trust estabelece que a confiança nunca deve ser presumida e que as medidas de segurança devem ser aplicadas de maneira consistente ao longo de todo o ciclo de vida dos dados, incluindo os processos de backup e recuperação. Trata-se de um modelo prático que auxilia as equipes de TI e segurança a reduzir significativamente os riscos, fortalecer a proteção de dados e aprimorar a postura de segurança de qualquer organização.

Quer saber mais sobre a Resiliência de Dados Zero Trust? Faça o download do white paper

A abordagem da Veeam referente a Zero Trust: Resiliência de Dados Zero Trust (ZTDR)

Zero Trust é fundamental para a estratégia de segurança de uma organização e seus principais locatários, incorporando princípios fundamentais como a segmentação dos ativos de dados mais essenciais, o acesso de menor privilégio e a autenticação e autorização contínuas. Essas práticas são especialmente importantes para a proteção de ambientes de backup, alinhando-se às melhores práticas do Identity and Access Management (IAM). Ao incorporar uma função de Resiliência de Dados com Zero Trust, as organizações podem enfrentar os desafios únicos colocados pelas soluções de proteção de dados e garantir uma estratégia de segurança abrangente para as organizações, independentemente de estarem no local, na nuvem ou em ambientes híbridos.

Um conceito crítico de Zero Trust é sempre assumir uma violação, independentemente da segurança de um determinado ambiente. Na metodologia ZTDR, uma técnica crítica para combater esse risco é separar o software de geranciamento de backup e o storage de backup em zonas de resiliência ou domínios de segurança separados, isolando os dados de backup de quaisquer ameaças ao software de geranciamento de backup, sejam essas ameaças internas ou externas. A Veeam suporta múltiplas tecnologias para criar zonas de resiliência com storage altamente seguro e imutável (veja a Figura 1).

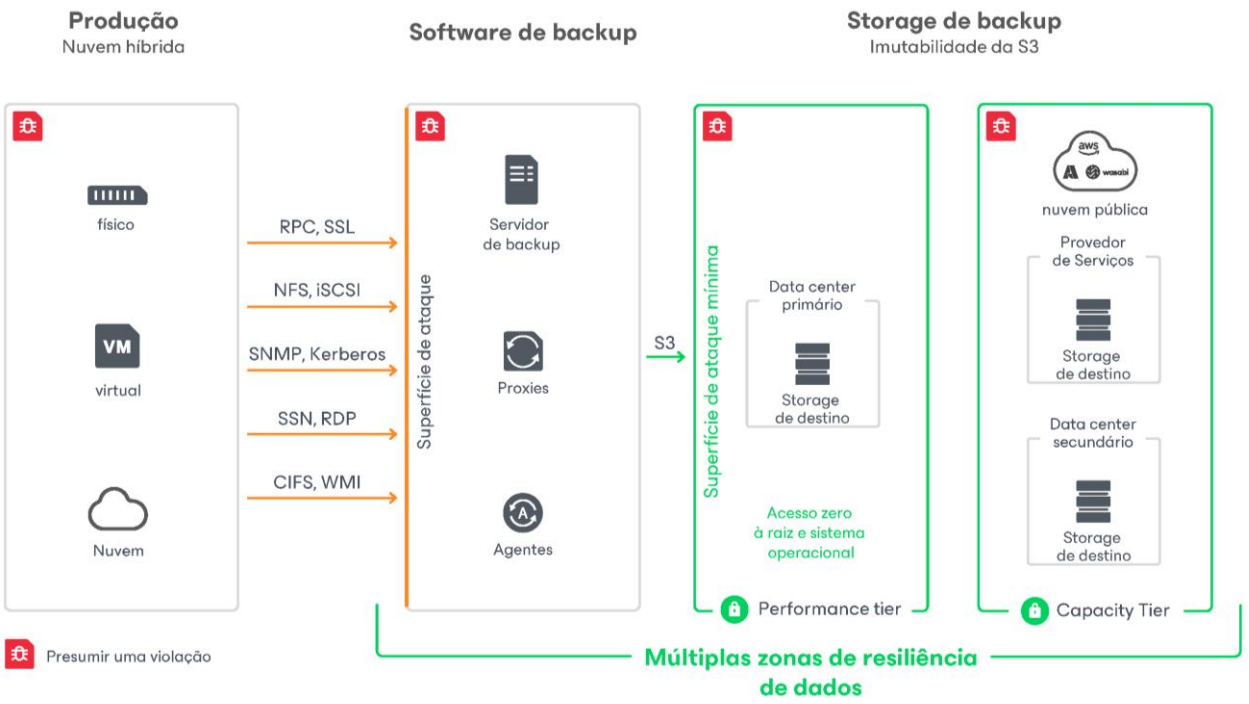

Figura 1

Como as soluções de proteção de dados têm alguns dos mais altos níveis de acesso de leitura e gravação aos dados de produção em toda a organização e, muitas vezes, aos dados mais essenciais, é imperativo que o ambiente de backup de uma organização esteja seguro e protegido por meio das melhores práticas de Zero Trust.

Princípios de Resiliência de Dados Zero Trust

De acordo com o Modelo de Maturidade de Zero Trust da CISA (veja a Figura 2), existem considerações adicionais que uma organização deve implementar especificamente no pilar Dados.

Modelo de Maturidade de Zero Trust da CISA

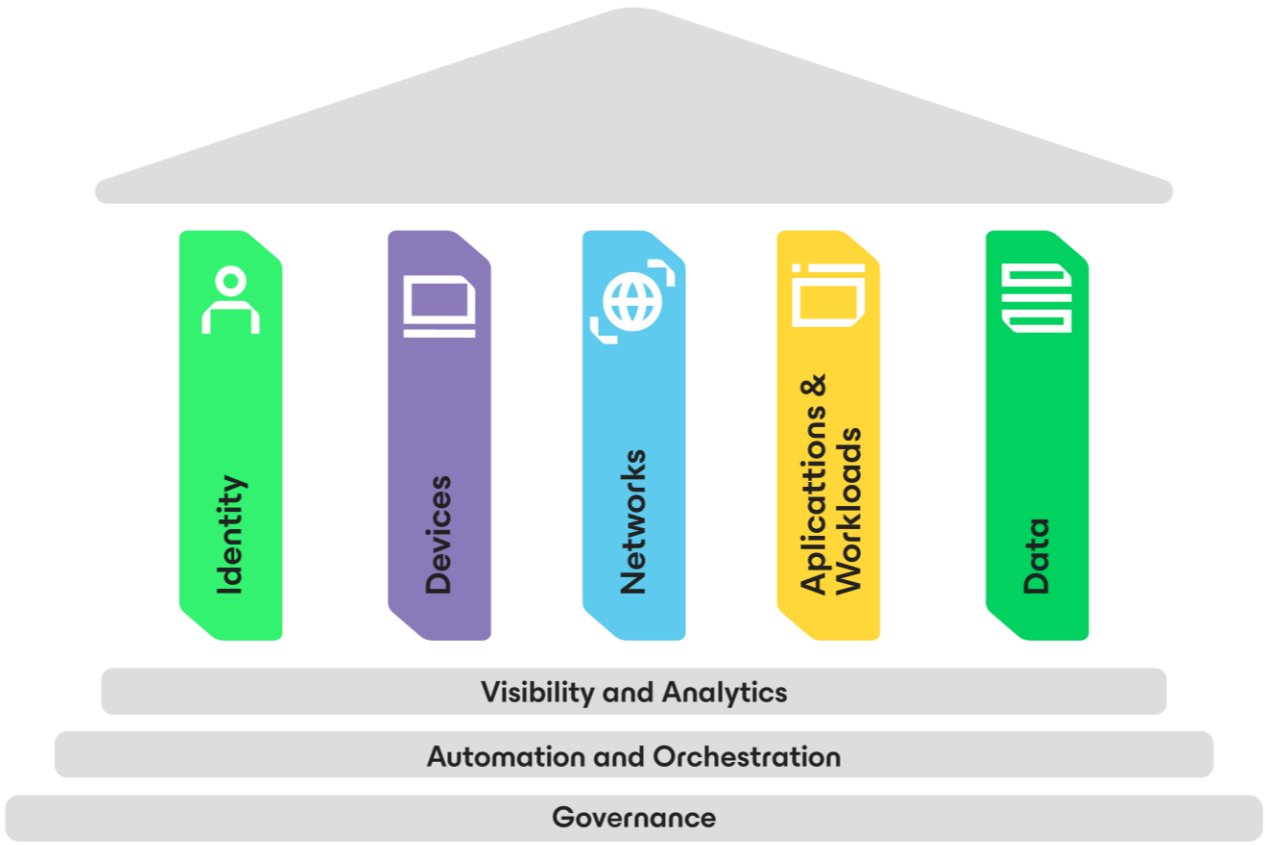

Figura 2

O documento de pesquisa Resiliência de Dados Zero Trust destaca 5 princípios fundamentais da Resiliência de Dados Zero Trust (ZTDR) para ajudar a estratégia geral de resiliência cibernética da organização, garantindo a proteção de ativos de dados essenciais diante das ameaças cibernéticas em constante evolução.

Acesso de menor privilégio

Esse princípio destaca a importância de conceder acesso apenas a pessoas, processos, dispositivos ou cargas de trabalho que sejam essenciais para o desempenho de suas funções designadas.

Acesso controlado para infraestrutura de backup:

- A implementação de políticas de Zero Trust para controlar o acesso à infraestrutura de backup garante que somente usuários validados possam estabelecer conexões com a solução de backup. Essa é uma etapa crucial para evitar o acesso não autorizado e possíveis violações de dados.

Funções granulares de autosserviço e funções restritas de administrador de backup:

- Fornecer funções granulares de autosserviço e funções restritas de administrador de backup dentro da Veeam demonstra um compromisso com o princípio do menor privilégio. Isso garante que os usuários tenham acesso apenas às funções específicas necessárias para suas tarefas, reduzindo a probabilidade de uso indevido inadvertido ou intencional.

Melhores práticas do Identity and Access Management (IAM)

- Aplicar as melhores práticas do IAM, como o uso da autenticação multifator (MFA), adiciona uma camada extra de segurança ao ambiente de backup. Essa é uma medida crítica para impedir o acesso não autorizado, especialmente devido aos altos níveis de privilégio associados às soluções de backup.

Princípio de "quatro olhos" para decisões operacionais críticas:

- A incorporação do princípio de "quatro olhos" para decisões operacionais críticas garante que as ações-chave exijam a aprovação ou verificação de pelo menos duas pessoas autorizadas. Isso adiciona uma camada adicional de supervisão e reduz o risco de atividades maliciosas ou errôneas.

Imutabilidade

Mesmo com um perímetro de rede seguro, um conceito crítico de Zero Trust é assumir a invasão. A imutabilidade dos backups é uma poderosa medida de defesa, pois assegura que agentes maliciosos, internos ou externos, não consigam modificar ou excluir dados essenciais de backup.

Segmentação para minimizar a superfície de ataque e o raio de explosão:

- Segmentar o software de backup e o armazenamento de backup em zonas de resiliência separadas é o conceito-chave da ZTDR. Isso minimiza o impacto potencial de ameaças internas ou externas, isolando componentes críticos. Assegurar que o software de backup não possua permissões de nível de sistema operacional ou de gerenciamento no storage de backup oferece uma camada adicional de proteção.

Múltiplas zonas de resiliência e regra de backup 3-2-1-1:

- Várias zonas de resiliência de dados ou domínios de segurança fornecem segurança em várias camadas. Além disso, a regra de backup 3-2-1-1 é uma das melhores práticas para estratégia de backup e está bem alinhada aos princípios de resiliência de dados. Manter pelo menos três cópias dos dados, utilizando dois tipos de mídia e garantindo que ao menos uma cópia esteja externa e outra isolada ou imutável, proporciona uma segurança em múltiplas camadas, diminuindo o risco de perda de dados.

Zonas de resiliência

Um conceito central de Zero Trust para rede é a microssegmentação para dividir os perímetros de segurança em zonas menores, reduzindo assim a superfície de ataque, o raio de explosão de qualquer zona comprometida e o movimento lateral de um invasor. Para ZTDR, esse conceito pode ser aplicado usando zonas de resiliência de dados. As zonas de resiliência separam o storage de backup e isolam o painel de controle do storage do software de backup e seu painel de controle. Isso fornece uma linha de demarcação crítica que garante a sobrevivência dos dados de backup mesmo no caso de software de backup comprometido. Isso pode acontecer por uma infinidade de razões, incluindo atores de ameaças internas. Um sistema de backup deve garantir que os dados de backup possam ser recuperados de forma simples e rápida a partir de uma instalação limpa do software de backup.

Infraestrutura de produção

Infraestrutura da Veeam

Dados de backup autônomos

Imutável | Criptografada | 3-2-1-1-0

Integridade de dados e segurança aprimorada:

- Configurar um repositório de backup compatível e definir um período de retenção para backups imutáveis é uma medida proativa para garantir a integridade dos dados e a segurança aprimorada. Backups imutáveis funcionam como uma proteção contra ataques de ransomware e outras formas de manipulação de dados.

Resiliência do Sistema

Uma abordagem holística para a segurança de TI abrange a resiliência em todo o ecossistema, incluindo plataformas, ferramentas, tecnologia e processos. As diversas opções de resiliência da Veeam demonstram o compromisso de fornecer às organizações ferramentas para suportar vários tipos de interrupções, incluindo a perda total do sistema.

Detecção de desvio de tempo para backups imutáveis:

- A implementação da Detecção de Desvio de Tempo é uma medida proativa para prevenir a exclusão de backups imutáveis, mesmo que haja comprometimento do NTP (Network Time Protocol). Esse recurso aumenta a segurança e a confiabilidade dos repositórios de backup, garantindo a integridade dos dados essenciais de backup.

Opções flexíveis de recuperação:

- A Veeam possibilita opções de recuperação flexíveis, até mesmo para ambientes diferentes, e suporta implantações físicas e virtuais, além de ambientes híbridos, para se alinhar com as diversas infraestruturas de TI que as organizações podem operar. Essa flexibilidade permite às organizações uma recuperação rápida: por exemplo, VMware no local para AWS ou Azure, ou AWS para Azure caso o ambiente original não esteja disponível.

Opções granulares de restauração de dados:

- A flexibilidade em restaurar dados para ambientes diferentes e em granularidades diferentes aumenta a resiliência geral dos dados. Essa adaptabilidade permite que as organizações adaptem seus processos de recuperação com base nas necessidades específicas de diferentes cenários.

Validação proativa

A validação constante de aspectos funcionais e processos é fundamental para garantir que os dados permaneçam protegidos e que quaisquer anomalias sejam detectadas e tratadas prontamente.

Monitoramento e validação contínuos:

- A prioridade dada a sistemas de monitoramento contínuo, 24 horas por dia e 7 dias por semana, demonstra a consciência de que as ameaças à segurança cibernética podem aparecer a qualquer instante. Com insights em tempo real sobre o estado do ambiente, os administradores podem identificar anomalias precocemente, permitindo que as organizações investiguem e respondam antes que um ataque cibernético ou perda de dados aconteça.

- Aproveitar ferramentas como o Veeam ONE é uma abordagem proativa para manter a integridade e a segurança dos ambientes de backup e recuperação. A capacidade do Veeam ONE de monitorar vários parâmetros, incluindo utilização da CPU, taxa de gravação do datastore, taxa de transmissão da rede e tamanho do backup incremental, fornece às organizações insights valiosos sobre possíveis problemas.

Visibilidade de ponta a ponta:

- O conceito de visibilidade de ponta a ponta em toda a infraestrutura de proteção de dados é essencial. Ele garante que as organizações tenham uma compreensão abrangente da integridade e do status de seus sistemas de backup e recuperação, permitindo que tomem decisões informadas e tomem ações rápidas quando necessário.
- Na recente versão 12.1 da Veeam, o novo Centro de Ameaças agrega informações de toda a plataforma e infraestrutura, reunindo tudo em um painel único. Ele destaca ameaças, identifica riscos e oferece às empresas um scorecard de segurança acessível e eficaz para todo o seu ambiente de proteção de dados.

Simplicidade Operacional

A importância da simplicidade operacional durante desastres ou eventos de cibersegurança é um reconhecimento do papel crítico que a simplicidade desempenha na recuperação eficaz. Quanto maior o tempo de inatividade, maior o impacto sobre as operações e os resultados da empresa.

Tempo de inatividade médio em ataques de ransomware:

- Conforme relatado no Relatório da Veeam sobre Tendências de Ransomware em 2023, o tempo de inatividade médio de um ataque de ransomware é de três semanas. Isso destaca a necessidade de uma recuperação ágil, que se torna especialmente crucial em momentos de alta pressão, onde cada segundo é valioso.

Equilibrando ferramentas, pessoas e processos:

- Encontrar o equilíbrio ideal entre ferramentas, pessoas e processos é um desafio crucial, especialmente quando as empresas enfrentam um desastre ou um ciberataque. A simplicidade operacional abrange a desburocratização dos fluxos de trabalho, a otimização dos processos e a garantia de que as ferramentas adequadas estejam disponíveis para uma recuperação eficaz.

Investimento na simplificação dos recursos de restauração:

- Líderes do setor, como a Veeam, investem proativamente no fornecimento de recursos de restauração ao lidar com as complexidades da recuperação. A capacidade de restaurar dados de uma plataforma para outra e aproveitar ferramentas como o Veeam Recovery Orchestrator demonstra uma dedicação à simplificação de cenários complexos de restauração e mantém os planos de failover atualizados, automatizados e totalmente testados, garantindo a prontidão durante cenários de alta pressão.

Saiba mais sobre os recursos de segurança mais recentes na Versão 12.1

Conclusão

À medida que nosso cenário digital evolui e se expande, o mesmo acontece com os ataques virtuais e as capacidades dos agentes ameaçadores. Como resultado, temos uma necessidade premente de unificar e fortalecer a colaboração e a eficácia de TI e segurança para melhor proteger e defender os dados, dispositivos e pessoas de nossas organizações. Essa jornada rumo à maturidade não ocorrerá de maneira instantânea, mas é essencial que comece o quanto antes. O primeiro passo é o Zero Trust. O Modelo de Maturidade de Confiança Zero (ZTMM) da CISA fornece princípios fundamentais que são críticos para proteger uma organização, mas não cobre tudo. A introdução do Zero Trust Data Resilience (ZTDR) como uma extensão do Zero Trust Maturity Model (ZTMM) da CISA é uma abordagem estratégica e com visão de futuro para lidar com o cenário em evolução das ameaças cibernéticas.

A incorporação dos princípios ZTDR, incluindo acesso de menor privilégio, imutabilidade, resiliência do sistema, validação proativa e simplicidade operacional, demonstra uma estratégia abrangente para proteger os dados organizacionais. Ao adotar a ZTDR, as organizações terão um caminho claro e concreto para fortalecer sua postura de segurança. Isso significa operações mais eficientes e alinhamento entre as equipes de TI e segurança, o que acabará levando a uma recuperação mais rápida e segura.

Sobre a Veeam Software

A Veeam, líder global Nº 1 do mercado em proteção de dados e recuperação de ataque de ransomware, tem a missão de ajudar cada empresa não só a se recuperar de uma perda ou paralisação de dados, mas também de avançar. Com a Veeam, as organizações alcançam a resiliência radical por meio da segurança, recuperação e liberdade de dados para a sua nuvem híbrida. A Veeam Data Platform fornece uma solução única para ambientes físicos, virtuais, na nuvem, SaaS e Kubernetes que oferece tranquilidade aos líderes de TI e segurança, mantendo suas aplicações e dados protegidos e sempre disponíveis. Com sede em Columbus, Ohio, e escritórios em mais de 30 países, a Veeam protege mais de 450.000 clientes no mundo inteiro, incluindo 73% das empresas da lista Global 2.000, que confiam na Veeam para manter seus negócios em operação. A resiliência radical começa com a Veeam. Saiba mais em www.veeam.com/pt ou siga a Veeam no LinkedIn @veeam-software e no X @veeam.