Ransomware em 2022:

7 recursos de que você precisa para uma recuperação rápida e confiável

Dave Russell,

Vice-Presidente
de Estratégia Corporativa,
Veeam Software

Jeff Reichard,

Diretor Sênior
de Estratégia Corporativa,
Veeam Software

Chris Hoff,

Gerente de Marketing
de Proteção de Dados
e Ransomware,
Veeam Software

Índice

As empresas não podem impedir ataques virtuais

O crescimento e a evolução do ransomware são algumas das tendências mais destrutivas da última década. Essa explosão transformou o ransomware de um crime econômico em um crime com imensas implicações globais de segurança. A OTAN, o governo federal, as forças armadas dos EUA e o G7 reconheceram recentemente a gravidade da ameaça do ransomware e a necessidade de uma resposta coordenada em grande escala dos governos e do setor.

Uma resposta coordenada dos governos e do setor leva tempo. Enquanto isso, organizações de todos os tamanhos precisam proteger a si e a seus clientes e usuários hoje. Felizmente, há passos concretos que podem ajudar, usando ferramentas e estruturas de segurança já disponíveis.

A sofisticação e adaptabilidade do ransomware e outras ameaças virtuais requerem uma defesa ágil e em camadas. Apesar disso, muitas empresas ainda mantêm produtos de segurança autônomos que são focados em um único vetor de ataque, o que pode ser facilmente comprometido. Agravando o problema da tecnologia, há uma grande falta de conhecimento entre as equipes de segurança. Uma estimativa recente aponta que o número de vagas não preenchidas, no setor de segurança virtual, em mais de três milhões no mundo todo. Os problemas com as equipes vão além das habilidades técnicas para saber como aplicar políticas que criam consistência e fornecem uma forma de medir a eficácia geral da sua organização.[i] Essas falhas de pessoal, processos e tecnologia tornam mais fácil do que nunca o ataque aos seus dados por criminosos virtuais sofisticados.

As organizações não podem impedir ataques virtuais, mas precisam tomar as medidas necessárias para proteger seus dados de forma eficaz quando um ataque ocorre.

Crescimento do ransomware de 2016 a 2021

Custo global: US$ 325M a US$ 20B

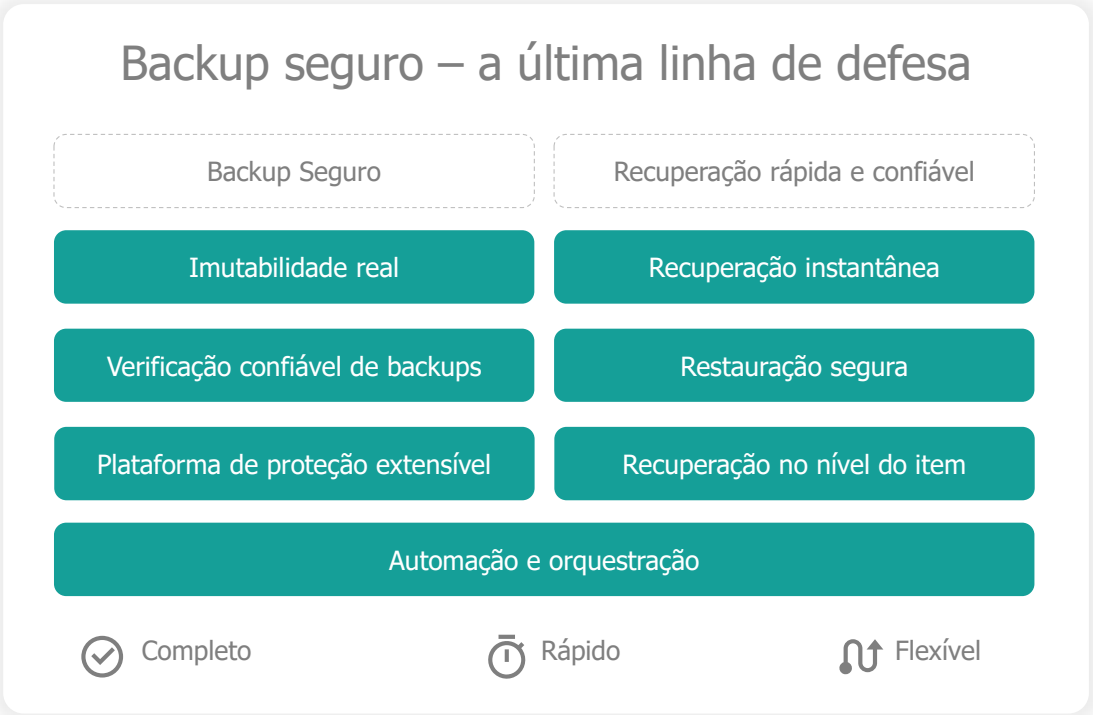
Frequência: A cada 2 minutos — a cada 11 segundos

Inovação: Bitcoin, ransomware como serviço, extorsão dupla/tripla

Criando uma estrutura de recuperação resiliente

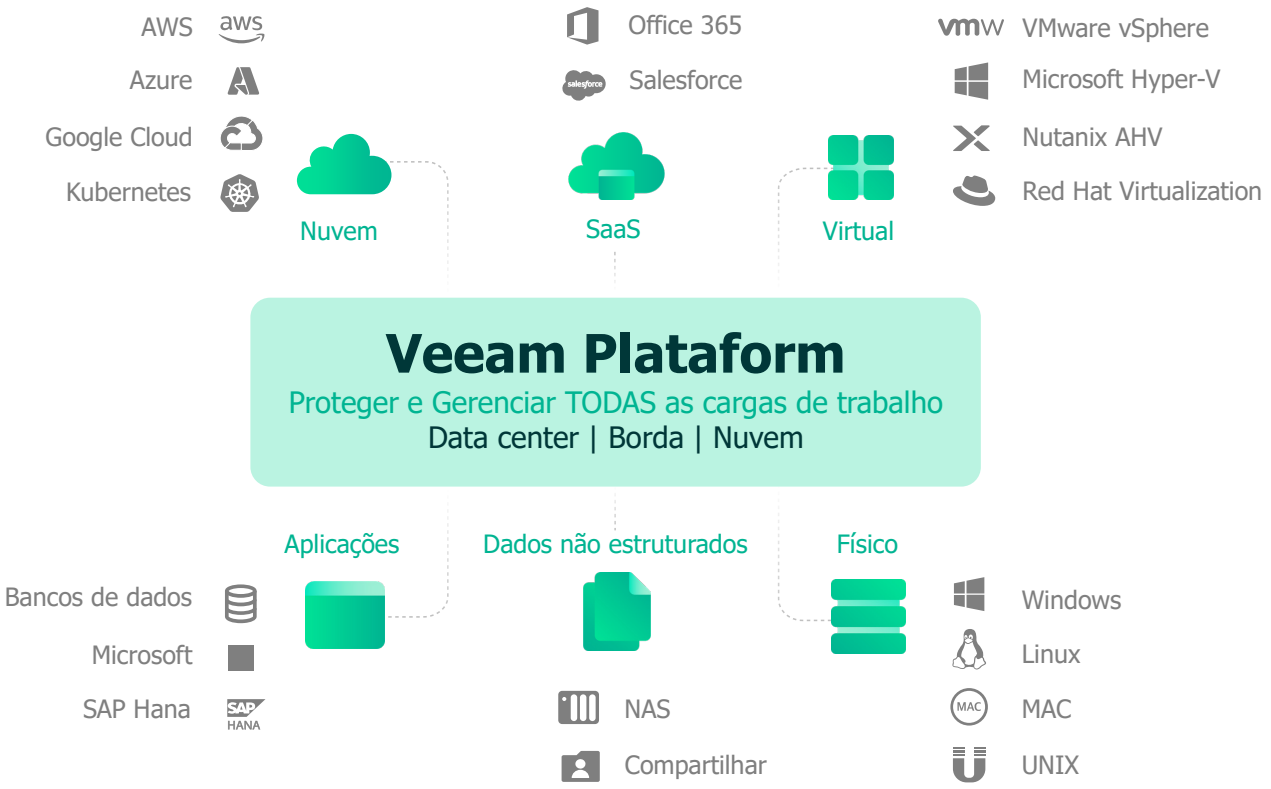
Programas de segurança eficazes requerem uma estrutura para compreender o que deve ser protegido e o valor dos ativos para a organização, a fim de determinar como a proteção deve ser implementada. Não importa a metodologia que as empresas escolham, a estrutura precisa definir resultados mensuráveis que permitam que as equipes de TI se defendam contra ataques e se recuperem rapidamente, se um ataque for bem-sucedido. Por exemplo, a NIST Cybersecurity Framework (CSF) é amplamente adotada, constantemente atualizada e foi projetada para criar uma linguagem comum entre as diferentes partes interessadas. O NIST CSF se tornou a base sobre a qual os profissionais de segurança virtual criaram seus programas para definir melhores práticas e criar um léxico unificado para a compreensão e gerenciamento dos riscos associados às infraestruturas modernas. Essa abordagem organizada também pode ajudar a justificar investimentos em segurança virtual, ilustrando claramente o resultado desses investimentos. E o processo é iterativo, permitindo uma implementação em fases e o aprendizado com os ciclos anteriores de implementação.

Sem uma forma estruturada de gerenciar o risco de segurança virtual, seria fácil focar todos os seus esforços em defesas baseadas em detecção, como firewalls e antivírus, negligenciando os processos e ferramentas que são obrigatórios para reagir com eficácia e se recuperar de um ataque bem-sucedido. Em outras palavras, o melhor ataque é uma defesa sólida, incluindo uma estratégia robusta de backup e proteção para seus dados e cargas de trabalho. Backups bem-sucedidos são a última linha de defesa contra ataques virtuais e podem ser o fator decisivo para impedir um tempo de inatividade considerável, perda de dados e o pagamento de um resgate caro. Para essa finalidade, reunimos esse guia de melhores práticas a fim de fornecer conselhos do mundo real para proteger seus dados.



Melhores práticas contra ransomware e recursos selecionados da Veeam

Desde 2019, cada lançamento da plataforma de proteção de dados moderna da Veeam® forneceu uma grande resiliência virtual e recursos seguros de proteção contra ransomware, ajudando as organizações a se recuperar com confiança de qualquer ataque virtual em minutos. Nossa abordagem focada em software dá a você a flexibilidade para manter um storage resiliente e imutável no local e na nuvem, sem ficar preso a hardware proprietário. Essas melhores práticas permitem que você tenha as salvaguardas apropriadas para garantir o fornecimento de backup e recuperação confiáveis para os seus serviços críticos de infraestrutura e garantir que os seus dados estarão lá quando você precisar deles.



1. Plataforma de proteção ampla e extensível

A solução de disponibilidade implantada deve ser capaz de proteger todas as cargas de trabalho de missão crítica, sejam físicas, virtuais ou baseadas em contêineres. Independentemente das cargas de trabalho serem implantadas no local, na nuvem com IaaS ou como SaaS, os dados de missão crítica agora residem em vários locais e precisam ter portabilidade para atender a requisitos futuros. A plataforma de proteção deve ter escalabilidade para aumentar ou diminuir, dependendo dos requisitos e das cargas de trabalho a serem protegidas. A solução de backup deve ser capaz de capturar dados por uma variedade de métodos, incluindo backup, replicação, proteção contínua de dados (CDP) e integrações com storage arrays.

A Veeam oferece uma arquitetura de storage definido por software (SDS) horizontalmente escalável. A Veeam pode ser estendida facilmente no front-end, para receber mais dados, conforme o seu backup fica mais volumoso ou seu desempenho precisa de mudança. No back-end, o Scale-out Backup Repository™ (SoBR) é uma construção definida por software que agrupa diferentes tipos de dispositivos de storage para dados de backup. Por meio do mecanismo de política da Veeam, os dados podem ser colocados em dispositivos mais apropriados – incluindo storage anexado diretamente (DAS) no local, appliances de deduplicação, storage conectado à rede (NAS), storage de objetos e na nuvem – gerenciados automaticamente ao longo do tempo ou por um provedor de serviços.

A Veeam Platform fornece todos esses recursos, possibilitando uma solução que escala e amplia conforme o seu negócio e seus requisitos evoluem com o tempo. A abordagem da Veeam é modular e extensível, sem exigir soluções pontuais, sem dependências de hardware e sem a preocupação de crescer demasiadamente.

Os recursos de remediação contra ransomware definidos por software da Veeam funcionam com qualquer infraestrutura, hoje e no futuro. Não é necessário possuir infraestrutura proprietária, permitindo que a empresa implemente no hardware e na nuvem que escolher. A flexibilidade de infraestrutura não permite apenas que a organização determine o hardware em que sua solução de backup será executada, mas também protege seus backups contra ransomware, não importa onde os dados vitais residam.

2. Sucesso no backup com verificação automática

Uma estratégia de defesa virtual robusta e abrangente sempre começa com backups válidos. Backups confiáveis, verificados e testados são o primeiro passo em qualquer recuperação bem-sucedida. Equipes de TI ocupadas precisam de uma forma de verificar automaticamente a integridade dos dados conforme os backups são feitos. Se houver algum problema, outro backup pode ser feito enquanto os dados de produção ainda estão disponíveis, garantindo que não haverá problemas com a disponibilidade dos dados descobertos depois que os dados de produção não estiverem mais disponíveis, tenham sido comprometidos ou definidos como não confiáveis e sem integridade.

O Veeam SureBackup® foi pioneiro na verificação automatizada de backups, e é um recurso principal em nossas melhores práticas de resiliência contra ransomware. O SureBackup aciona automaticamente servidores e aplicações em um ambiente isolado da rede e executa avaliações de integridade que incluem muitas formas conjuntas de verificação de aplicações, como executar comandos específicos do Active Directory ou do SQL para verificar a integridade da aplicação. Essa capacidade de testes automatizados pode ser estendida e personalizada para atender aos seus requisitos e pode ser agendada para execução quando você julgar mais apropriado, enviando um relatório de status para a sua caixa de entrada quando o teste for concluído.

A Veeam recomenda seguir a regra de backup 3-2-1-1-0, que é o nosso aprimoramento da conhecida regra 3-2-1 do setor.

Há muitos anos, a Veeam defende a Regra 3-2-1 como uma estratégia geral de gerenciamento de dados. A Regra 3-2-1 recomenda que haja pelo menos três cópias dos dados importantes, em pelo menos dois tipos de mídia, com pelo menos uma cópia off-site. A Regra 3-2-1 não exige qualquer hardware específico e é versátil o suficiente para tratar de praticamente qualquer cenário de falha.

Com o avanço da ameaça do ransomware, a Veeam enfatiza que pelo menos "uma" cópia dos dados deve ser resiliente (ou seja, isolada, off-line ou imutável). Essa recomendação é imperativa para tornar-se resiliente contra ransomware.

A aplicação moderna da regra 3-2-1-1-0 trata da necessidade do requisito de uma cópia resiliente e é um dos conceitos mais importantes que uma organização pode implementar, a fim de se preparar melhor para combater e se recuperar de ameaças virtuais.

3. Backups resilientes: isolados e imutáveis

Os criminosos virtuais agora tentam com frequência criptografar ou excluir os backups da organização como parte de um ataque de ransomware. Para o adversário, o sucesso aqui é crucial, porque sem os backups a vítima precisa pagar caro para recuperar seus dados.

Backups resilientes são apenas backups que não podem ser destruídos por um adversário, mesmo se ele tiver adquirido credenciais administrativas.

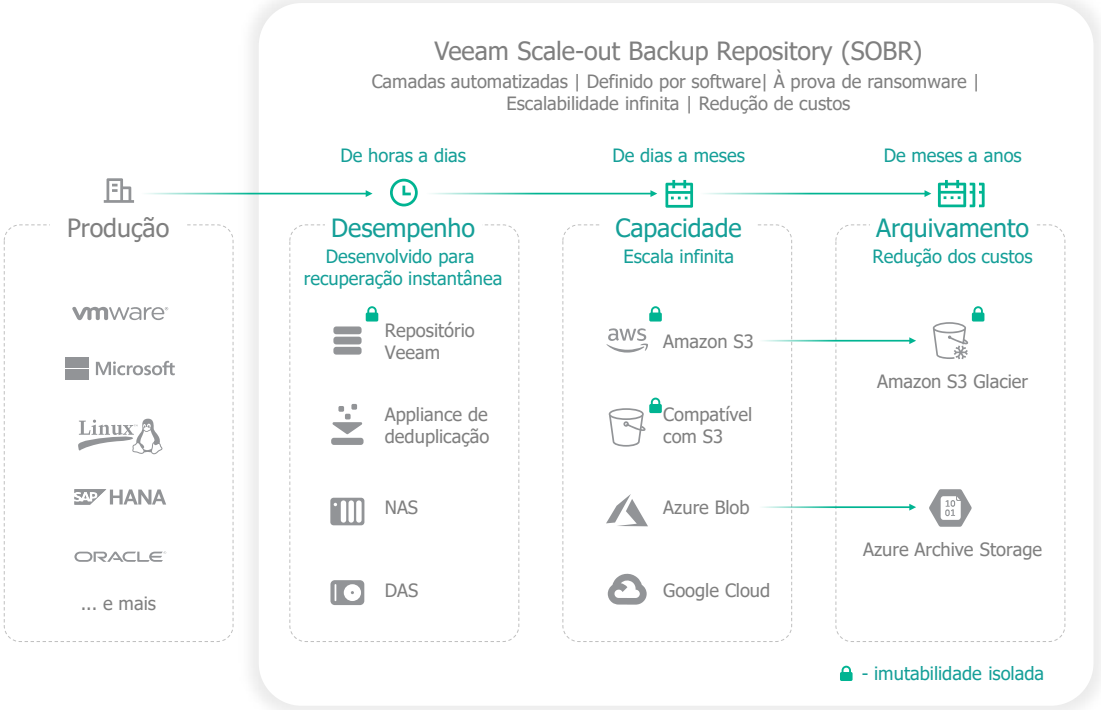
No nível mais simples, uma resiliência robusta pode ser alcançada com o backup para unidades removíveis ou fitas que então são retiradas da biblioteca de fitas. Ter backups off-line e isolados é o primeiro passo.

A Veeam oferece uma abordagem à prova de falhas e orientada por políticas para o gerenciamento de dados entre várias opções de storage resiliente. Aumentando a resiliência geral, soluções certificadas de storage[ii] da Veeam[iii] e nosso amplo ecossistema de parceiros garantem a*imutabilidade* (a incapacidade de excluir ou alterar dados por um tempo definido). **Essas opções incluem o Repositório Seguro da Veeam, que oferece uma opção imutável robusta para os seus backups locais.** Se você prefere manter seus dados na nuvem, a Veeam fornece imutabilidade usando a AWS Amazon S3 e outros provedores de storage de objetos compatíveis com S3, usando seu recurso de bloqueio de objeto.

Backups gravados em um storage resiliente serão uma das defesas mais essenciais para garantir a resiliência contra ransomware. Um storage de backup resiliente significa que você tem uma ou mais cópias de dados de backup em qualquer combinação das seguintes mídias:

- Backups em fita (removidos da biblioteca ou marcados como WORM)
- Backups imutáveis em storage de objeto S3 ou compatível com S3
- Mídia isolada e off-line (por exemplo, unidades removíveis, unidades rotativas)
- Backups no Veeam Cloud Connect com proteção interna (um recurso disponivel nos parceiros de serviço)
- Backups imutáveis em um repositório seguro

A Veeam Platform inclui um conjunto completo de recursos de remediação contra ransomware em seu produto principal, que são facilmente configuráveis pelos próprios clientes e flexíveis o bastante para funcionar com qualquer infraestrutura, no local ou na nuvem.



Gerenciamento do ciclo de vida de dados de backup orientado por políticas

4. A imutabilidade é só o início

Alguns clientes da Veeam buscam implementar a imutabilidade por meio de uma abordagem de imutabilidade dupla ou tripla. Isso pode incluir a utilização do Repositório Seguro da Veeam para backups locais de primeiro nível, e então a utilização do recurso de imutabilidade no Capacity Tier da Veeam, gerenciada automaticamente, com o S3 Object Lock para storage de objetos na nuvem ou no local, e/ou gravar automaticamente os backups para fitas físicas WORM (write one, read many) – observe que a Veeam suporta nativamente as fitas sem a necessidade de integrações de terceiros.

Embora a imutabilidade, implementada com uma abordagem única, dupla ou tripla, seja muito útil para remediação de ameaças virtuais, ela é só o início de uma prática abrangente de proteção contra ransomware.

A criptografia de ponta a ponta é necessária para evitar o vazamento de dados. Hoje, uma das ameaças virtuais com crescimento mais rápido é o vazamento e o roubo de dados, em que um resgate deve ser pago para evitar que dados confidenciais sejam compartilhados na dark web.

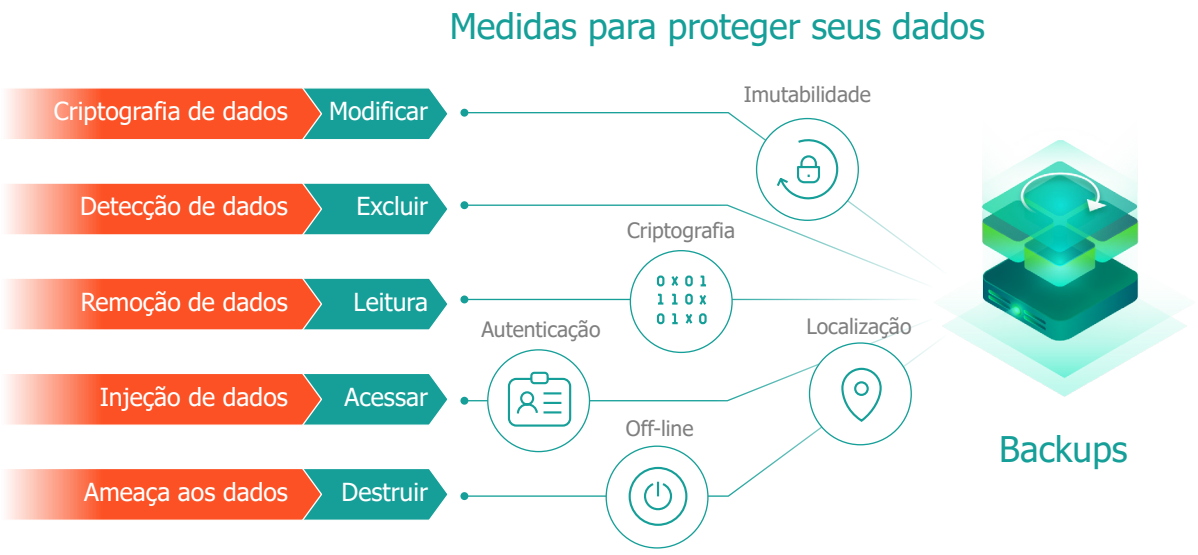
Uma autenticação adequada e a "higiene digital" em relação ao acesso com o menor privilégio são necessárias para corrigir a injeção de dados. Os dados também precisam ser protegidos contra alterações, de forma que os registros e entradas que pareçam válidos não tenham sido maliciosamente alterados para se tornarem inválidos.

Outras melhores práticas de higiene digital incluem:

- Senhas únicas para cada origem de login. Assim, você pode garantir que, se uma senha ou máquina for violada, a senha roubada não dará aos hackers acesso a outras contas.
- Um gerenciador de senhas. Um gerenciador de senhas robusto pode ajudar a gerenciar todas as suas informações de login, facilitando a criação e o uso de senhas únicas e fortes.
- Autenticação Multifator (MFA) Você pode configurar a autenticação multifator para segurança adicional das suas contas, que exigirão uma validação secundária contínua a cada login.
- Remova dispositivos não utilizados, aplicações, programas e utilitários não essenciais de todos os servidores.
- Gerenciamento de patch – certifique-se de que todo software, hardware e firmware em uso estejam executando níveis de software atualizados, que corrijam quaisquer vulnerabilidades conhecidas.

Cópias off-line dos dados são necessárias para combater ameaças internas, incluindo a destruição dos dados. As ameaças internas são uma preocupação crescente, com algumas empresas de análises afirmando que a maioria das ameaças virtuais nos próximos três anos poderão vir dos funcionários da empresa.

Correção abrangente contra ransomware: implemente uma estratégia completa de correção contra ransomware. O amplo conjunto de recursos de correção contra ransomware, da Veeam, ajudam você a realizar todas as funções de correção contra ransomware: identificar, proteger, detectar, responder e recuperar.



5. Recuperação instantânea de dados

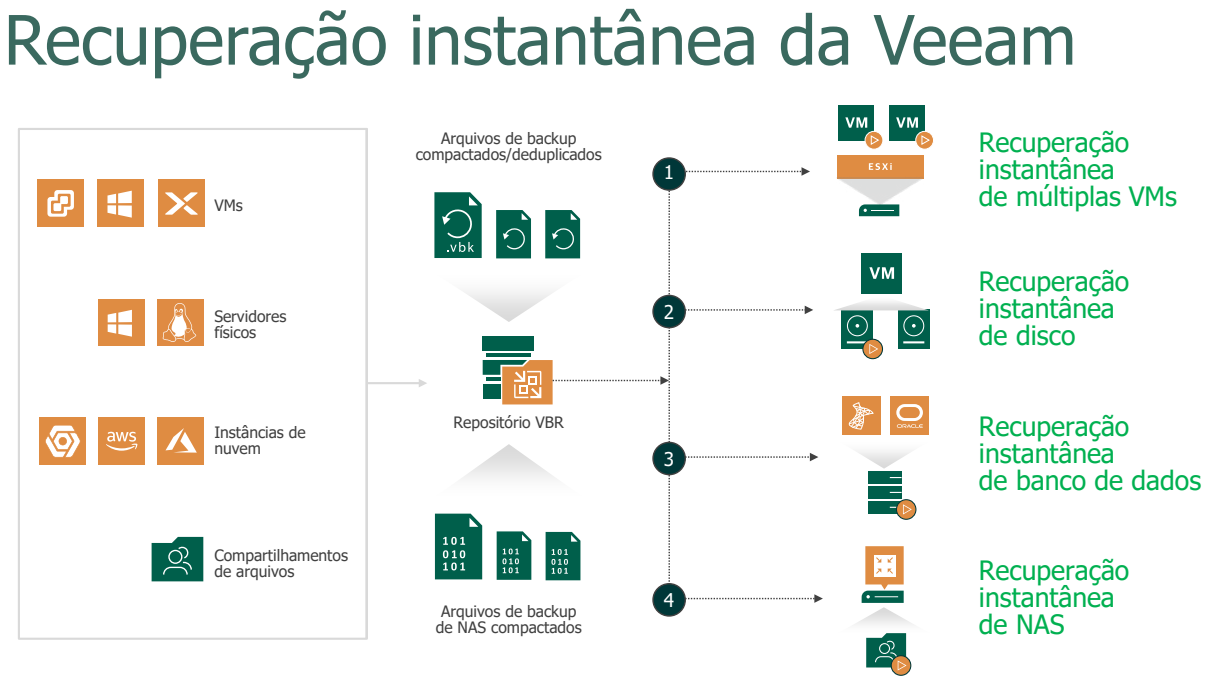
Antes do ransomware, as organizações normalmente só restauravam de 3% a 5% de seus dados de backup em um período de um ano. Mas em um ataque de ransomware, 100% dos seus dados de produção podem ser criptografados ou contaminados com malware, e você precisa recuperar tudo, rapidamente. O acesso rápido aos dados é crucial, com o objetivo sendo mais a continuação do que a restauração de todas as operações vitais.

A Veeam foi pioneira na recuperação instantânea de dados em 2010, refinando e ampliando essa capacidade desde então. Hoje, a Veeam está otimizada para restaurar rapidamente várias máquinas ao mesmo tempo a fim de atender às necessidades de recuperação até das maiores corporações.

A Veeam oferece recuperação instantânea de dados:

- Sem exigir appliances proprietários caros ou unidades de estado sólido
- Sem limitação aos dados de backup mais recentes
- Fornecendo a capacidade de recuperar arquivos físicos e virtuais e cargas de trabalho para um ambiente virtualizado (como VMware vSphere, Microsoft Hyper-V e Nutanix AHV), e até migrar de um hipervisor para outro automaticamente, com apenas dois cliques do mouse
- Fornecendo a capacidade de recuperar arquivos e servidores físicos e virtuais para um ambiente de nuvem (como AWS, Azure e Google Cloud Platform) com apenas dois cliques do mouse
- Fornecendo a capacidade de recuperar instantaneamente aplicações corporativas essenciais, como bancos de dados Oracle e SQL Server para uso imediato
- Fornecendo a capacidade de reverter todo o Network-Attached Storage (NAS) e compartilhamentos de arquivos para um estado conhecido íntegro, prévio à infecção, para que sua empresa volte rapidamente às operações normais

A recuperação instantânea de dados, que pode utilizar um formato de dados portátil para fornecer acesso entre plataformas para os dados, garante uma recuperação rápida, quando e onde você precisar dela. Do AHV, Hyper-V ou vSphere para Windows ou Linux físico para Azure, AWS ou GCP, a Veeam Platform pode ajudar você.



6. Recuperação segura de dados

O período de latência do ransomware (o tempo em que o adversário está na rede da vítima antes de ativar um ataque) pode ser de vários meses. Por causa disso, você precisa de automação para garantir que nunca irá restaurar o malware para o seu ambiente limpo ou novo.

Um dos aspectos versáteis de uma tarefa do SureBackup (descrita acima no item 2) é a capacidade de deixar a tarefa em execução para que análises forenses e verificações adicionais sejam executadas no sistema, a partir do ponto de restauração do backup. Isso pode incluir uma inspeção manual para ver se a ameaça de ransomware ainda existe ou investigar arquivos específicos.

Expandindo a capacidade de recuperação instantânea já mencionada, a Veeam tem integração com as principais soluções anti-malware para verificar e limpar dados de backup infectados, garantindo que os dados de backup recuperados para a produção estejam livres de ameaças virtuais e eliminando as reinfecções.

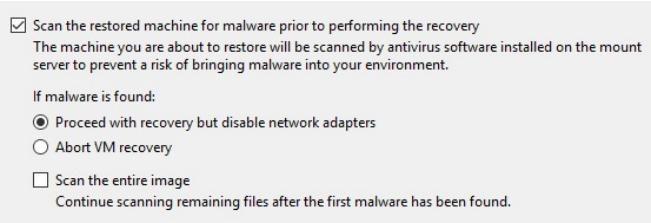
A restauração segura da Veeam fornece uma etapa de verificação antivírus opcional e totalmente integrada como parte de qualquer processo de recuperação escolhido. Esse recurso soluciona os problemas associados ao gerenciamento do malware, fornecendo a capacidade de garantir que todos os dados de cópia que você precisa recuperar para a produção estejam em bom estado e livres de malware. **A restauração segura foi outra inovação no setor, um método de patente requerida para remediar um ataque realizado por malware escondido em seus dados de backup.** A restauração segura fornece confiança adicional de que uma ameaça foi corretamente neutralizada e não existe mais em seu ambiente.

A restauração segura é totalmente configurável pelo PowerShell, o que significa que se você automatizar processos de recuperação por meio de uma integração ou portal, também poderá aproveitar esse recurso para garantir que as ameaças não sejam reintroduzidas no seu ambiente de produção.

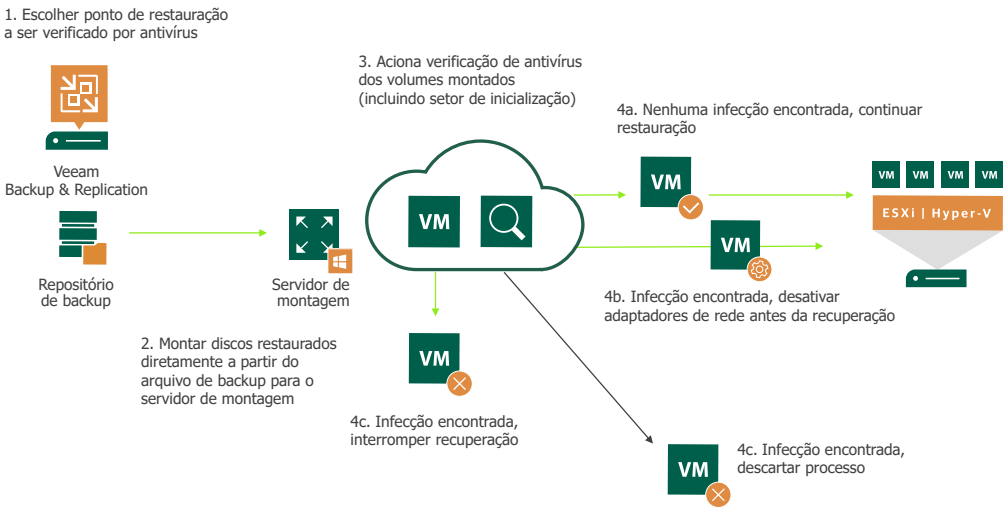
Esse recurso avançado é útil para:

- Detectar ransomware "adormecido" em dados de backup e ativar a correção antivírus para limpar os dados antes que eles sejam devolvidos ao ambiente de produção
- Verificar backups de locais com menos controle da TI como escritórios remotos e filiais (ROBO), antes de restaurá-los aos dados primários
- Verificar dados de backup com soluções antivírus adicionais para detectar melhor o malware raro ou zero-day

Assim como todos os recursos da Veeam Platform, implementar a restauração segura é rápido e fácil de configurar, com apenas alguns cliques do mouse:



Veeam DataLabs: Restauração segura



7. Automação da recuperação

Não se iluda, os ataques virtuais são desastrosos. Em uma emergência, a sua equipe precisa de resultados automatizados e reproduzíveis. Seu conjunto de ferramentas deve permitir testes e auditorias regulares da velocidade com que você pode se recuperar de um desastre, incluindo testes automatizados de acessibilidade e usabilidade de servidores e aplicações após a restauração. E o processo de testes e os resultados devem ser autodocumentáveis para satisfazer o gerenciamento e as auditorias externas de segurança.

O **Veeam Disaster Recover Orchestrator** (VDRO), líder de mercado, **permite que você automatize totalmente e documente fluxos de trabalho complexos, incluindo testes de recuperação em grande escala sem interrupções e com documentação dinâmica.** A documentação de resposta a incidentes e recuperação também pode ser atualizada com informações que não sejam da Veeam, como listas de contato e outras informações de resposta de missão crítica.

Recuperação confiável

- Orquestração confiável e escalável
- Centrado em aplicações

Testes automatizados

- Não disruptiva
- Programada e sob demanda
- Verificação de prontidão

Documentação dinâmica

- Trilhas de auditoria
- Geração de relatórios de conformidade
- Controle de alterações integrado
- Remediação proativa

A maioria das organizações têm muitos tipos de planos de continuidade dos negócios (BC) e recuperação de desastres (DR). Aqui estão alguns exemplos:

- Falha no nível de aplicação
- Falha no nível do site
- Falha em componente de infraestrutura
- Aplicações de missão crítica
- Aplicações de desenvolvimento e teste

Assim como a verificação de backup automatizada, como o SureBackup da Veeam, é importante nas operações diárias de backup, também é importante testar regularmente o seu plano geral de resiliência virtual de recuperação. Após criar um plano de recuperação, a coisa mais importante que você pode fazer é testá-lo. Você precisa saber se o plano que montou funciona. Existe uma tendência de não testar completamente os planos de recuperação de desastres, ou de simplesmente não testá-los. Na melhor das hipóteses, a maioria das organizações testam parcialmente seus planos de DR uma ou duas vezes ao ano.

Testes contínuos são importantes, especialmente porque as aplicações mudam constantemente. Para responder a alterações de configuração, os planos de recuperação devem ser atualizados sempre que uma mudança for feita em uma aplicação, como adicionar mais servidores para aumentar a capacidade ou remover servidores antigos. Ao testar, lembre-se de prestar atenção especial ao que não correu conforme o desejado. Essa é a única forma de melhorar o seu plano de recuperação de desastres. O verdadeiro propósito de um teste é descobrir se o seu plano funciona ou não.

A resiliência virtual e a remediação contra ransomware precisam ser parte do seu plano geral de recuperação de desastres. Uma das formas mais claras de se preparar para incidentes de segurança virtual é criar um plano de resposta a incidentes. Criar um plano de resposta a incidentes bem definido permitirá que você especifique procedimentos para detectar, comunicar, controlar e corrigir incidentes de segurança para que os funcionários saibam como reagir a eventos de segurança virtual, caso ocorram.

Além disso, esse plano deve ser capaz de ser automaticamente testado, atualizar dinamicamente a documentação essencial, e permitir a integração com outras ferramentas e fluxos de trabalho necessários, que garantirão a continuidade das operações de negócio cruciais.

Conclusão

Os dados da empresa são seu ativo mais valioso, porém, o ransomware é uma ameaça crescente para organizações de todos os tamanhos, setores e locais geográficos, colocando dados essenciais em risco. É imperativo que as empresas continuem melhorando seus programas de segurança para garantir que os dados sejam protegidos de forma adequada e que recursos robustos estejam à disposição de todas as organizações para se recuperar de um incidente com rapidez e segurança. A construção de um programa de segurança abrangente requer a combinação de pessoas, processos e tecnologia de modo concentrado na melhoria contínua, fornecendo a melhor defesa possível. Não importa a metodologia que as empresas escolham, a estrutura precisa definir resultados mensuráveis que permitam que as equipes de TI se defendam contra ataques e se recuperem rapidamente, se um ataque for bem-sucedido.

A resposta a ameaças como o ransomware exige a implementação de uma estratégia abrangente de remediação. O amplo conjunto de recursos de remediação contra ransomware da Veeam fornece a solução mais completa do mercado e a maior experiência em garantir que os dados estejam disponíveis durante uma crise. Fazemos isso adotando uma abordagem focada em software, que dá a você a flexibilidade para manter um storage resiliente e imutável no local e na nuvem, sem ficar preso a hardware proprietário. Seguindo as melhores práticas e implantando nossa plataforma de proteção de dados moderna, a Veeam pode ajudar sua empresa a alcançar a resiliência digital, minimizando o tempo de inatividade após um ataque de ransomware com o uso de processos totalmente automatizados para fornecer restaurações livres de ransomware e orquestração de DR, não importa onde os seus dados residam.

Não importa se os seus dados estejam no local ou na nuvem, é essencial ter um conjunto completo de recursos de remediação contra ransomware. Adotar essas melhores práticas em seu programa de segurança simplifica a resposta a ataques virtuais e evita a perda de dados e o pagamento de resgates caros.

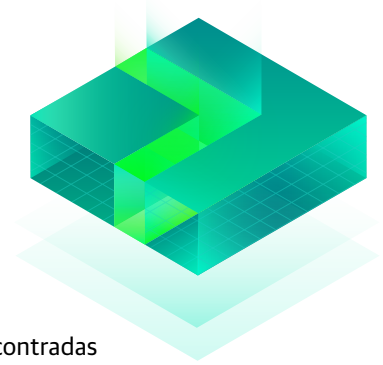
Sobre a Veeam Software

A Veeam® é a líder em soluções de backup, recuperação e gerenciamento de dados que oferecem proteção de dados moderna. Nós entregamos uma única plataforma para ambientes virtuais, na nuvem, SaaS, Kubernetes e físicos. Nossos clientes têm a confiança de que suas aplicações e dados estão protegidos e sempre disponíveis com a plataforma mais simples, flexível e avançada do setor. A Veeam protege mais de 400.000 clientes no mundo inteiro, incluindo mais de 82% das empresas da lista Fortune 500 e mais 60% da Global 2.000. O ecossistema global da Veeam inclui mais de 35.000 parceiros de tecnologia, revendedores, provedores de serviços e parceiros de aliança, e tem escritórios em mais de 30 países. Para saber mais, acesse www.veeam.com/br ou siga a Veeam no LinkedIn @veeamsoftware e no Twitter @veeam.

Produtos da Veeam para sua prática de remediação contra ransomware

Produtos da Veeam para sua prática de remediação contra ransomware

- Veeam Backup & Replication
- Veeam ONE
- Veeam Disaster Recovery Orchestrator
- Veeam Backup *for AWS*, *Azure* e *Google Cloud Platform*
- Veeam Backup *for Microsoft Office 365*
- Kasten K10 by Veeam



Mais informações sobre os recursos contra ransomware da Veeam podem ser encontradas nesse site dedicado: https://www.veeam.com/ransomware-protection.html.

Um longo e detalhado white paper sobre as melhores práticas contra ransomware e uma cobertura aprofundada dos recursos de segurança virtual da Veeam está disponível em: https://www.veeam.com/wp-protection-yourself-from-ransomware.html?wpty.

Sobre os autores

Dave Russell é um veterano de 32 anos no setor de storage, atuando como Vice-Presidente de Estratégia Corporativa da Veeam, responsável pela condução de programas estratégicos de produtos e inserção no mercado, liderando o engajamento da indústria e difundindo a visão da Veeam sobre a proteção de dados moderna. Antes da Veeam, ele foi Vice-Presidente e Analista na Gartner por 13 anos e passou 15 anos na IBM, no desenvolvimento de produtos para mainframe e backup e recuperação de sistemas abertos.

Jeff Reichard é Diretor Sênior de Estratégia Corporativa na Veeam, com foco em risco, conformidade e parcerias. Jeff tem 25 anos de experiência em soluções de proteção/disponibilidade de dados, continuidade dos negócios e conformidade normativa. Suas funções anteriores incluem desde o design de soluções de backup de dados e de SAN até a engenharia de sistemas e a liderança de engenharia, atendendo ao setor público e clientes corporativos. Antes da Veeam, Jeff liderou a equipe federal civil SE da Commvault. Na Veeam, Jeff trabalha com parceiros, clientes e analistas do setor para difundir a visão da Veeam sobre gerenciamento de dados na nuvem

e transformação digital.

A carreira de Chris tem raízes profundas na segurança virtual, com mais de 15 anos de experiência técnica diversa. No momento, ele lidera a iniciativa de Marketing de Segurança e Proteção de Dados na Veeam. Antes de entrar para a equipe, Chris desempenhou várias funções nas áreas de engenharia, vendas e gerenciamento de produtos. Durante sua carreira, ele ajudou várias organizações a gerenciar os riscos virtuais, projetando soluções alinhadas às estruturas do setor, aos programas e às normas de conformidade.

i https://www.infosecurity-magazine.com/news/cybersecurity-skills-shortage-1/

ii Certificações técnicas para storage imutável chegaram em resposta à regulamentação do setor financeiro. Várias normas governamentais foram projetadas para garantir que as organizações reguladas mantenham cópias inalteradas de registros financeiros por um período determinado (por exemplo, nos EUA, veja SEC Rule 17a-4(f), FINRA Rule 4511 e CFTC Rule 1.31 (c)-(d)). Felizmente, as mesmas certificações de controle que garantem a probidade financeira também podem garantir dados de backup que não podem ser excluídos ou alterados.

iii Consulte https://www.veeam.com/blog/hardened-repository-passes-compliance.html para ver as certificações de conformidade recentes do Repositório Linux Seguro da Veeam

