VERITAS

Melhore a recuperação de dados com air gap e isolamento

Mantenha cópias seguras de seus dados para neutralizar o impacto de ataques cibernéticos.

Informe oficial | Maio de 2023

Por que criar um cofre de dados?

A segurança cibernética ocupa um lugar de destaque nas mentes dos líderes empresariais. As ameaças cibernéticas estão cada vez mais sofisticadas, refinando constantemente suas técnicas para obter o máximo de dano. De acordo com o Gartner, até 2025, 40% de todos os conselhos de administração terão um comitê de segurança cibernética dedicado para criar relatórios adicionais e expectativas estratégicas sobre políticas, execução e recuperação de segurança cibernética[1]. O crescimento exponencial do crime cibernético está custando milhões de dólares e horas que as organizações estão lutando para reduzir e recuperar. Com um ataque cibernético ocorrendo a cada 15 segundos em 2022[2], tornou-se uma corrida contra o relógio para garantir que você esteja preparado com uma estratégia que reduza seu risco, elimine sua incerteza e mantenha o controle de seu ambiente.

A confiança em um plano de resiliência e recuperação vem da implementação de uma estrutura de segurança cibernética confiável, com a tecnologia e os processos certos. Você tem um plano de resposta a incidentes de segurança cibernética que possa comunicar com confiança ao seu gerente e à alta administração? De acordo com o Gartner[3], até 2025, 70% dos CEOs exigirão uma cultura de resiliência organizacional contra o cibercrime. Agora é a hora de entender as tendências de segurança cibernética e os componentes críticos de um plano de recuperação bem-sucedido. Seja capaz de interromper um ataque de ransomware imediatamente e demonstrar ao seu conselho de administração com confiança que você implementou as ferramentas certas para recuperação.

O que é air gap e por que devo me importar?

À medida que os ataques cibernéticos se tornam cada vez mais sofisticados, os hackers não visam apenas seu armazenamento de dados principal, mas também seu armazenamento de dados de backup. É fundamental contar com isso em sua estratégia de recuperação de desastres. Na maioria dos casos, os hackers ficam inativos em seu sistema até que possam acessar e comprometer seus dados primários e de backup. Se eles podem acessá-lo, eles podem criar problemas.

Um air gap, de acordo com o Instituto Nacional de Padrões e Tecnologia (NIST), é uma interface entre dois sistemas na qual (a) eles não estão conectados fisicamente e (b) nenhuma conexão lógica é automatizada (ou seja, os dados são transferidos através da interface apenas manualmente, sob controle humano)[4]. No passado, as folgas de ar eram o padrão ouro para proteger a tecnologia operacional, como um termostato ou eletrodomésticos. Agora que quase tudo está conectado por meio de uma rede sem fio ou com fio, a necessidade de um rigoroso processo de air gap é fundamental para manter uma boa cópia dos dados disponíveis para recuperação.

Em ambientes de rede, os hackers podem explorar praticamente qualquer ponto de entrada, mesmo por meio de um sistema com todos os sinais sem fio e com fio desativados. Nos sistemas mais fechados para dados altamente seguros, alguns departamentos de TI desativam todas as portas USB e usam uma gaiola de Faraday para bloquear todas as transmissões sem fio e evitar vazamentos eletromagnéticos.

A replicação automática de imagem (AIR) permite replicar dados de backup entre domínios de backup que podem estar no mesmo ou em sites diferentes, incluindo nuvem pública. AIR também permite cópias offline de seus backups, para reduzir ainda mais a ameaça de acesso a dados por fontes não intencionais. À medida que os dados se expandem em seus data centers próprios e na nuvem pública, é importante ter uma solução de backup e recuperação que implemente uma estrutura de intervalo de ar para manter uma última cópia boa conhecida dos dados críticos.

Dados em nuvem e Air Gap

O cloud-first está crescendo: 85% das organizações relatam que serão cloud-first até 2025, com 94% implementando uma estratégia multi-cloud[5]. Vimos um aumento acentuado na aceleração de estratégias de nuvem, o que pode resultar em ferramentas e autoridade de tomada de decisão díspares. Assim como você diversifica e otimiza seu repositório de dados primário com diferentes opções de nuvem pública, é importante otimizar sua abordagem de recuperação de dados com as melhores soluções criadas para que você volte a funcionar.

Recomendamos a funcionalidade de um ambiente de recuperação isolado (IRE) como a melhor opção possível. As soluções com Air Gap oferecidas em um IRE criam uma cópia segura de seus dados críticos, fornecendo aos administradores um conjunto limpo de arquivos sob demanda para neutralizar o impacto de um ataque de ransomware em um ambiente multinuvem.

Ambientes de recuperação isolados

As soluções tradicionais de isolamento de rede interrompem fisicamente ou logicamente a conectividade entre locais seguros, impossibilitando toda a comunicação de entrada ou saída. Isso limita a transferência de dados para o ambiente isolado e coloca em risco os objetivos de tempo de recuperação (RTOs) e os objetivos de ponto de recuperação (RPOs) se a cópia terciária for necessária. Comumente referido como envio de dados de replicação da origem para o destino, o domínio de origem processa e envia de forma independente uma tarefa de replicação para um domínio de destino. Essa abordagem tradicional limita o tempo disponível para replicar dados críticos em um ambiente seguro quando a conexão está inativa ou bloqueada.

Por outro lado, o modelo de replicação pull inicia a solicitação de replicação do destino. A Veritas oferece a solução IRE do NetBackup, que otimiza a movimentação de dados oferecendo um modelo de replicação pull em que a solicitação para enviar dados vem do pool de eliminação de duplicações do servidor de mídia (MSDP) do IRE e a conexão reversa oferece melhor controle do fluxo de dados para proteger ainda mais o ambiente lógica e fisicamente. As replicações para o IRE agora podem ser totalmente controladas de dentro do IRE, incluindo o suporte de uma janela específica, conforme definido no cronograma de intervalo de ar do IRE.

O NetBackup IRE é impenetrável durante a transferência de dados devido a várias camadas de segurança, incluindo mecanismos de prevenção contra invasões e criptografia de dados em trânsito e em repouso. Ao longo da jornada de dados, os dados estão seguros, independentemente de onde residam, o armazenamento não é comprometido e não há risco de usuários mal-intencionados ou não autorizados lerem ou modificarem os dados. A Veritas oferece opções de isolamento de dados no local e na nuvem com o NetBackup Recovery Vault — um armazenamento como serviço em nuvem perfeito, air gap para proteção contra ransomware, otimizado para escala e garantindo portabilidade de dados com custos previsíveis.

A Veritas oferece um fluxo de trabalho simples que permite transformar qualquer NetBackup — no local ou na nuvem — em uma estrutura IRE, fornecendo resiliência de ransomware com foco em três princípios principais:

- **Proteger**: incorpore facilmente o recurso de recuperação isolada com suporte para autenticação multifator (MFA) e controle de acesso baseado em função (RBAC) que se alinha com a estratégia de segurança Veritas Zero Trust.
- **Detectar**: o NetBackup IT Analytics fornece detecção de anomalias que pode detectar ransomware em tempo real. O recurso integrado de varredura de malware do NetBackup fornece varredura de malware antes da recuperação que pode ser priorizada com base em pontuações de anomalias.
- **Recuperar**: Orquestre a recuperação de um conjunto de dados inteiro em um ambiente isolado, na nuvem ou no local, com a capacidade de gerenciar uma ampla variedade de requisitos de RPO e RTO.

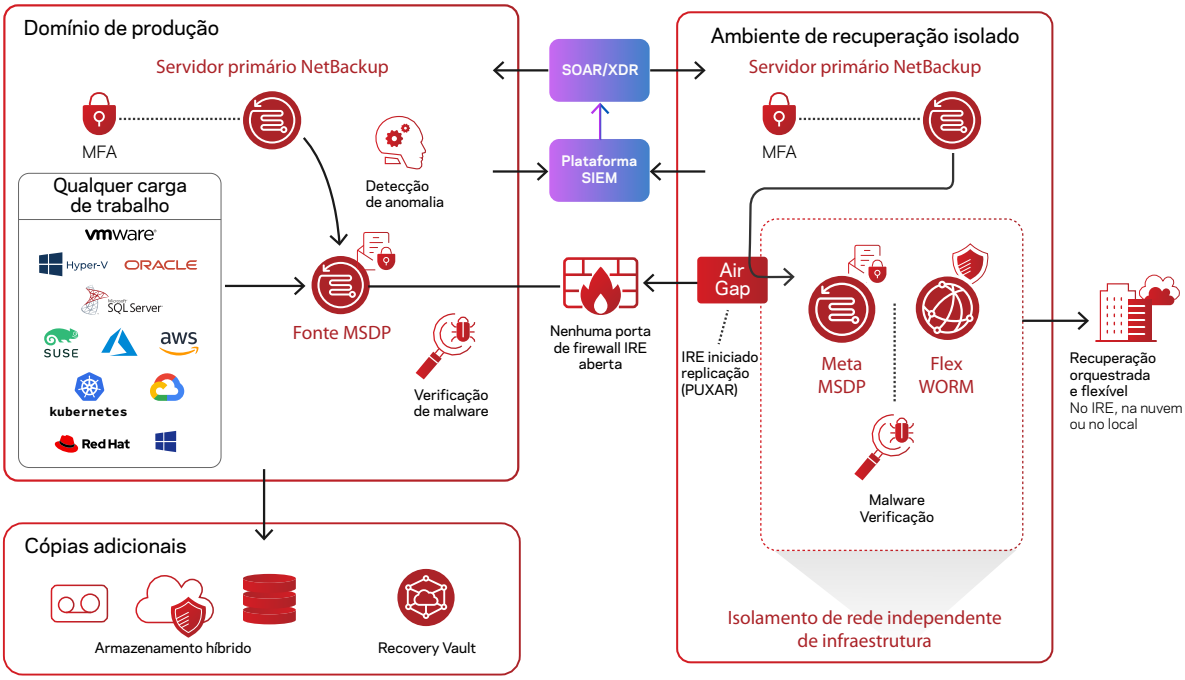

Figura 1: Ambiente de recuperação isolado do NetBackup

Um ambiente isolado fornece outra camada de resiliência para combater ransomware e malware.

Aumente a proteção com confiança zero

Uma política Zero Trust oferece proteção ainda maior. Foi comprovado que a adoção de uma mentalidade de confiança zero em toda a empresa reduz o risco de um ataque devastador.

O Veritas IRE é baseado no armazenamento WORM (escrever uma vez, ler diversas - write once read many) multilocatário baseado em contêiner dos dispositivos Flex com sistema operacional de proteção e uma arquitetura Zero Trust. Ao fortalecer seu gerenciamento de identidade e acesso (IAM) com MFA e RBAC para usuários, ferramentas e máquinas, você limita o acesso a dados e backups altamente confidenciais. Somente os usuários que precisam acessar os dados devem ser permitidos. Higiene de senhas também é uma prioridade.

Você pode impedir o acesso a essas áreas com fortes controles de IAM, controles de privilégio, proteção e hardware seguro, todos construídos em Zero Trust. Se ocorrer uma violação, ela reduz a superfície de ataque ou o raio de explosão porque fornece várias camadas de segurança que minimizam o impacto. Uma vez em seus sistemas, os cibercriminosos geralmente se movem em seu ambiente em busca de dados críticos para os negócios, informações confidenciais e sistemas de backup.

Detecção de anomalias e verificação de malware

Com visibilidade completa, detecção inteligente de anomalias e verificação de malware, você pode saber com segurança onde estão todos os seus dados, reduzindo a complexidade operacional e otimizando o gerenciamento de custos. A detecção de anomalias baseada em IA da Veritas reconhece dados fora do comum e atividades do usuário em todo o seu ambiente e alerta você sobre atividades suspeitas, quase em tempo real. Esse recurso garante que seus dados sejam sempre recuperáveis e permite que você tome medidas imediatas quando o ransomware ataca, isolando backups com malware e limitando o impacto do malware em seus dados de backup. Você pode restaurar imagens completas que foram digitalizadas e validadas como seguras ou pode restaurar arquivos individuais. Se um arquivo marcado para restauração estiver infectado, você poderá restaurá-lo a partir de um backup não infectado. Isso oferece uma maneira segura e eficaz de recuperar dados sem nenhum risco de infectar novamente a máquina de destino.

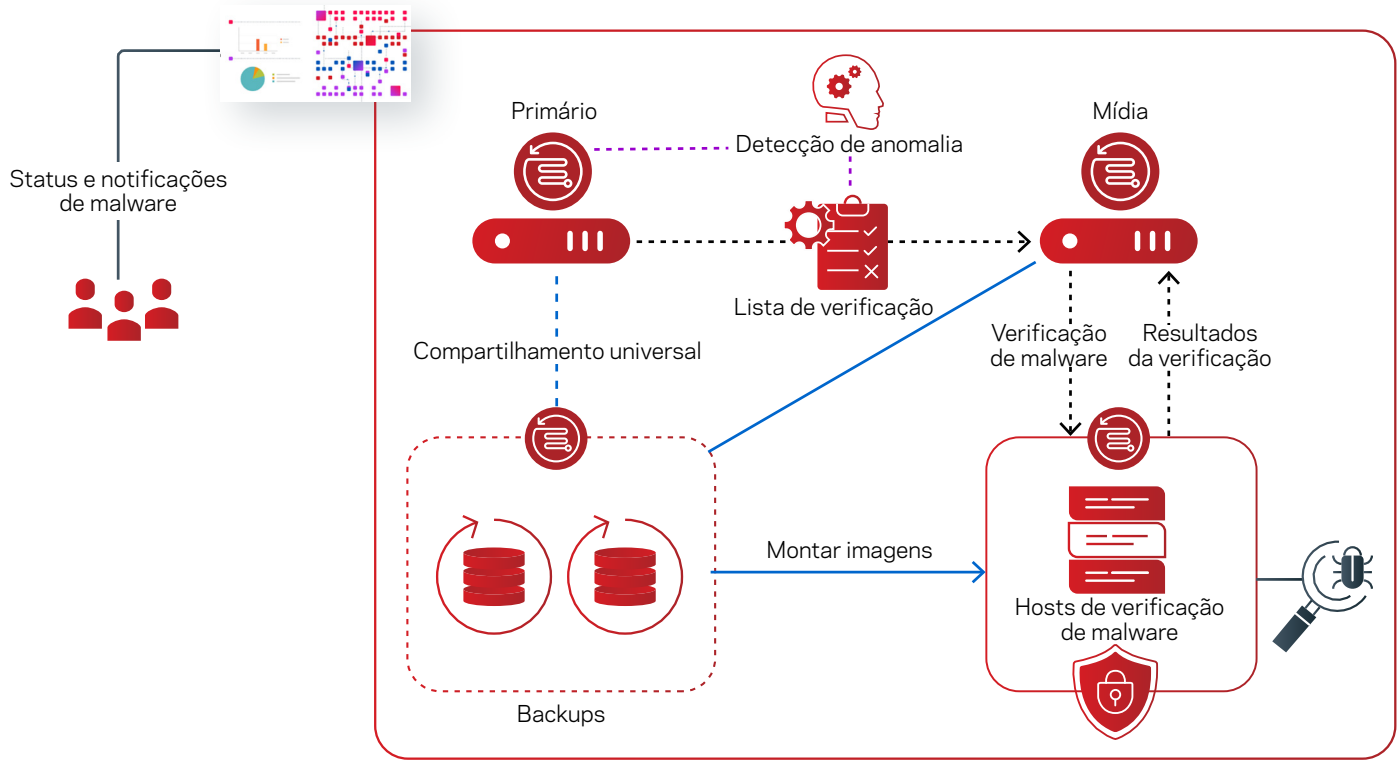

Figura 2: Verificação de malware integrada do NetBackup

Recuperar usando armazenamento imutável e indelével

O armazenamento imutável e indelével garante que ninguém ou nada possa alterar, criptografar ou excluir dados por um determinado período de tempo (ou de forma alguma). Também evita adulteração de dados e acesso não autorizado. Como parte de sua estratégia de IRE, o NetBackup Recovery Vault fornece uma solução de armazenamento imutável e indelével baseada em nuvem que pode ser ampliada ou reduzida dependendo de suas necessidades.

Recupere com confiança com IRE

Reduza o risco, elimine a incerteza e mantenha o controle com o NetBackup Isolated Recovery Environment. Visite Veritas.com ou entre em contato com nossa equipe para saber mais sobre como nossa solução pode garantir a resiliência de seu ransomware em seu ambiente multinuvem.

Feche as lacunas em sua estratégia de resiliência corporativa.
Saiba mais >

1. www.gartner.com/en/newsroom/press-releases/2021-01-28
2. www.sonicwall.com/resources/white-papers/2023-sonicwall-cyber-threat-report/
3. www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022
4. csrc.nist.gov/glossary/term/air_gap
5. www.gartner.com/en/newsroom/press-releases/2021-11-10

Sobre a Veritas

A Veritas Technologies é líder em gerenciamento de dados em várias nuvens. Mais de 80 mil clientes, incluindo 95% das empresas da Fortune 100, confiam na Veritas para ajudar a garantir a proteção, capacidade de recuperação e conformidade de seus dados. A Veritas tem uma reputação de confiabilidade em escala, o que oferece a resiliência de que seus clientes precisam contra as interrupções ameaçadas por ataques cibernéticos, como ransomware. Nenhum outro fornecedor é capaz de igualar a capacidade de execução da Veritas, com suporte para mais de 800 fontes de dados, mais de 100 sistemas operacionais, mais de 1.400 destinos de armazenamento e mais de 60 nuvens por meio de uma abordagem única e unificada. Com tecnologia de escala de nuvem, a Veritas está entregando hoje sua estratégia de gerenciamento autônomo de dados, que reduz a sobrecarga operacional e, ao mesmo tempo, oferece maior valor. Saiba mais em www.veritas.com/pt/br. Siga-nos no Twitter em @veritastechllc.

VERITAS

www.veritas.com/pt/br

Para obter informações de contato globais, visite:
veritas.com/pt/br/company/contact

V1626 05/22