DEMONSTRAÇÃO DO ESG

A resiliência cibernética é imprescindível ao armazenamento essencial

Data: outubro de 2022 **Autores:** Scott Sinclair, diretor de práticas, e Monya Keane, analista sênior de pesquisas

RESUMO: O ambiente de TI mudou. Como agora os dados são um ativo de alto valor, as ameaças cibernéticas também se tornaram generalizadas. Portanto, a resiliência cibernética deve ser um princípio fundamental ao escolher o armazenamento essencial. Com o PowerMax, a Dell Technologies consolidou-se ainda mais como líder em armazenamento essencial, criando e integrando recursos indispensáveis de resiliência cibernética diretamente nesses sistemas.

Visão geral

Os dados são um ativo de negócios vital e altamente valioso. A pesquisa do ESG mostra que, para 59% das organizações, os dados são a essência dos negócios, e a expectativa é de que essa porcentagem aumente para 81% em dois anos.[1] A função de uma infraestrutura de armazenamento essencial é preservar, proteger e entregar dados que sustentam cargas de trabalho e aplicativos que simplesmente não podem ficar inativos.

Durante décadas, implementar "armazenamento essencial" significava fornecer desempenho e escala indispensáveis, além de garantir disponibilidade contínua para proteção contra falhas de componentes, falhas no local, erros do usuário e desastres naturais. Agora, os ataques mal-intencionados estão ganhando supremacia. Por esse motivo, os princípios fundamentais do armazenamento essencial devem evoluir além desses recursos tradicionais para incluir também o aprimoramento da postura de resiliência cibernética da organização.

A Dell Technologies, líder em armazenamento empresarial, continua a desenvolver sua principal plataforma de armazenamento — PowerMax — para atender às necessidades essenciais dos ambientes de TI mais exigentes. As recentes iniciativas de inovação da Dell visam colocar na linha PowerMax uma série de recursos robustos para aprimorar a postura de resiliência cibernética de qualquer organização que esteja interessada em proteger mais adequadamente os dados e aplicativos vitais, preservar a reputação da marca e alcançar o sucesso no longo prazo.

A era das ameaças cibernéticas constantes aos dados

Com o aumento das ameaças cibernéticas, a complexidade da TI também aumentou. Quase metade (46%) das organizações entrevistadas na pesquisa do ESG afirma que a TI é mais complexa hoje do que há dois anos. A rápida evolução do ambiente de segurança cibernética (citada por 37%) e as iniciativas de adesão às novas normas de privacidade e segurança dos dados (citadas por 32%) foram dois dos motivadores mais identificados com relação a essa complexidade da TI.[2]

Infelizmente, hoje as organizações estão encontrando dificuldade para contratar talentos de segurança cibernética qualificados o bastante para superar frontalmente essa complexidade: 48% das organizações pesquisadas relatam não ter especialistas suficientes em segurança cibernética na equipe. Essa é a área de déficit de habilidades mais citada na TI empresarial no momento.[3]

[1] Fonte: ESG Research Report, *Data Infrastructure Trends*, novembro de 2021.
[2] Fonte: ESG Complete Survey Results, *2022 Technology Spending Intentions Survey*, novembro de 2021.
[3] Ibid.

Esta demonstração da pesquisa do ESG foi encomendada pela Dell Technologies e é distribuída sob licença da TechTarget, Inc.
© 2022 TechTarget, Inc. Todos os direitos reservados.

Ransomware e malware são predominantes

Entre as várias ameaças enfrentadas pelas empresas, os ataques externos de ransomware e malware tornaram-se praticamente inescapáveis. Em uma pesquisa recente do ESG junto a profissionais de TI e segurança cibernética que supervisionam tecnologias e processos associados à proteção da empresa contra ransomware, 79% relataram ter experimentado uma tentativa de ataque de ransomware nos últimos 12 meses. E 30% dos entrevistados disseram que esses ataques estão ocorrendo semanalmente ou até em uma frequência maior.[4]

Entre as organizações que sofreram uma tentativa de ataque, 73% experimentaram pelo menos uma que teve êxito. No entanto, nessas circunstâncias, o pagamento de resgate não é uma estratégia ideal nem sequer inteligente: 56% das organizações pagaram resgate por um ataque bem-sucedido. No entanto, entre aquelas que pagaram o resgate exigido:

- **87%** enfrentaram tentativas adicionais de extorquir mais dinheiro. Na verdade, 61% das que pagaram inicialmente acabaram pagando ainda mais depois.[5]
- Apenas **14%** obtiveram 100% de seus dados de volta, mesmo depois de enviar o dinheiro do resgate.
- E **61%** obtiveram apenas 75% ou menos dos dados de volta após o pagamento.

Sem dúvida, a proteção completa contra ransomware exige uma estratégia mais multifacetada, uma que incorpore várias tecnologias e ferramentas direcionadas à detecção, prevenção e recuperação.

Agora, muitas organizações estão modelando suas estratégias de resiliência cibernética conforme a orientação fornecida pelo NIST Cybersecurity Framework, que recomenda que as organizações identifiquem recursos essenciais, protejam esses recursos, detectem falhas e violações e tenham um plano de resposta e recuperação de incidentes cibernéticos. Outro componente da estrutura do NIST que as organizações estão adotando amplamente é a arquitetura Zero Trust, que descarta o conceito de borda de rede protetora em favor da filosofia "nunca confie, sempre verifique". Nesse modelo, a configuração de segurança dos usuários (até mesmo de pessoas que trabalham dentro da organização) deve ser validada repetida e rotineiramente para que os usuários possam acessar aplicativos e dados.

Os sistemas de armazenamento devem fazer parte dessa abordagem de segurança cibernética. Afinal de contas, o componente de infraestrutura mais comum visado por ataques de ransomware é o hardware para armazenamento, segundo a pesquisa do ESG. Essa foi a resposta principal, citada por 40% das organizações entrevistadas.

Como o armazenamento essencial melhora a resiliência ao ransomware

Os ataques de ransomware concentram-se em acessar e, em seguida, criptografar dados de negócios importantes. Muitas estratégias de resiliência cibernética baseiam-se em ferramentas e tecnologias que enfatizam a **prevenção** por meio do impedimento de ameaças e da **detecção** antecipada de quaisquer ataques que consigam penetrar no ambiente. Mas, com o ransomware, também é importante enfatizar a **recuperação acelerada**.

Os sistemas de armazenamento essencial residem em um local no caminho de dados que é ideal para ajudar na recuperação rápida de dados após um ataque. Por exemplo, à medida que os ataques bem-sucedidos de ransomware aumentaram, alguns sistemas de armazenamento conseguiram utilizar recursos projetados para ajudar na recuperação rápida salvaguardando e, em seguida, fornecendo cópias seguras e imutáveis de volume de dados.

Esse tipo de suporte é extraordinariamente valioso para acelerar a recuperação. Os snapshots podem ser identificados com rapidez como volumes "válidos" e rapidamente recuperados pela TI para restaurar conjuntos de dados à condição original anterior. No entanto, para ambientes de aplicativos essenciais, a *tecnologia de armazenamento deve fazer ainda mais*.

[4] Fonte: ESG Research Report, *The Long Road Ahead to Ransomware Preparedness*, junho de 2022. Todas as referências da pesquisa do ESG contidas nesta demonstração foram extraídas desse relatório de pesquisa, salvo se indicado de outro modo.
[5] Fonte: ESG Complete Survey Results, *The Long Road Ahead to Ransomware Preparedness*, junho de 2022.

© 2022 TechTarget, Inc. Todos os direitos reservados.

O Dell PowerMax pode melhorar a postura de resiliência cibernética de uma organização

Os nomes dos produtos mudaram e os recursos aumentaram ao longo de várias décadas, mas os sistemas de infraestrutura de armazenamento essencial da Dell Technologies lideraram esse espaço desde que o armazenamento empresarial foi estabelecido como uma categoria separada de TI pela EMC no final da década de 1980. Atualmente, o Dell PowerMax oferece vários recursos projetados para atender aos requisitos exigentes de cargas de trabalho essenciais, inclusive:

- Uma arquitetura scale-out totalmente NVMe com vários controladores para permitir desempenho consistente, extremo e em escala.
- Consolidação maciça de cargas de trabalho, com suporte para diversos ambientes de aplicativos de arquivo e bloco que abrangem cargas de trabalho de mainframe, sistemas bare metal, VMs, contêineres e muito mais.
- Os mais altos níveis de segurança, disponibilidade e resiliência. O PowerMax oferece 99,9999% de disponibilidade com criptografia de dados completa de hosts para o PowerMax, criptografia de dados em repouso e snapshots seguros — especificamente, ele comporta até *64 milhões de snapshots por array*, segundo a Dell. Além disso, o software de recuperação de desastres Symmetrix Remote Data Facility (SRDF) da Dell usa topologias avançadas e recursos de automação a fim de fornecer uma base sólida para resiliência. Com o SRDF, as organizações podem até mesmo criar um cofre com air gap. Nesse cofre, os dados são isolados e a conexão com o cofre é intermitente e altamente restrita.

A Dell projetou o PowerMax para resiliência

Recentemente, a Dell se concentrou em criar e incorporar ainda mais recursos de segurança ao PowerMax. Por exemplo, agora o PowerMax é projetado para ambientes Zero Trust com base nos sete pilares de Zero Trust da Dell, o que inclui segurança e proteção intrínsecas do próprio sistema contra ataques por meio de:

- Recursos imutáveis de raiz de confiança — Esses recursos autenticam alterações de hardware e software em nós, compartimentos de mídia e estação de controle. Chaves criptográficas imutáveis incorporadas em nível de componente são fundidas na memória pela produção da Dell.
- Recursos de cadeia de confiança de inicialização segura — Esses recursos estabelecem e estendem uma "cadeia de confiança" de firmware contra rootkits mal-intencionados de inicialização, kernel e driver. A cadeia de confiança de inicialização segura usa autenticação criptográfica para cargas de firmware/carregadores de inicialização subsequentes com base em assinaturas da Dell.
- Atualizações de firmware assinadas digitalmente — O PowerMax também utiliza a autenticação de assinatura digital da Dell para oferecer proteção contra atualizações de firmware não autorizadas. São realizadas verificações de componentes de nó, mídia e estação de controle usando chaves de autenticação criptográficas.

Além de design confiável, o PowerMax oferece recursos adicionais para melhorar a prevenção, detecção e recuperação de ataques de ransomware e outras ameaças de segurança cibernética.

Para prevenção, além de ter segurança de hardware integrada, o PowerMax ajuda a evitar ataques por meio de segurança avançada para impedir acesso não autorizado de um usuário, graças a recursos como Common Criteria, STIG Hardening/APL, certificações de segurança FIPS 140 e suporte para mecanismos confiáveis de controle de acesso do administrador, como:

© 2022 TechTarget, Inc. Todos os direitos reservados.

- Autenticação SecurID baseada em vários fatores para verificar a identidade de um administrador.
- Suporte a Smart Card CAC/PIV que contém um certificado/chave privada para ter acesso a recursos on-line no governo federal dos EUA.
- Controles de acesso baseados em função (RBAC), suporte a LDAP e zDP 2 Actor (que exige que duas pessoas executem determinados comandos zDP), permitindo que apenas usuários autorizados realizem operações designadas, como o provisionamento de armazenamento.

Para **detecção**, o hardware do PowerMax e o software de IA Dell CloudIQ oferecem detecção de anomalias de malware. Trata-se de alertas de conformidade baseados em protocolos de alerta de segurança cibernética, bem como de alertas e exportações Syslog seguros. Mais especificamente, o CloudIQ detecta ataques cibernéticos com rapidez monitorando a utilização incomum do armazenamento do PowerMax e medição de atividades suspeitas. Em seguida, ele alerta os administradores sobre quaisquer alterações drásticas devido a uma possível criptografia. Ele também pode monitorar continuamente a infraestrutura de armazenamento para identificar automaticamente os riscos de segurança cibernética com base em configurações incorretas do sistema e, em seguida, fornecer recomendações detalhadas para corrigir esses problemas.

E, para **recuperação**, a tecnologia de snapshots seguros do PowerMax elevou o nível de proteção e segurança de dados. Dependendo dos objetivos de nível de serviço da empresa, a TI pode configurar até 64 milhões de cópias de snapshot em cada PowerMax (veja a Figura 1).

Figura 1. Como o PowerMax oferece rápida Cyber Recovery

Fonte: Dell Technologies

Esse recurso permite que o PowerMax atenda a objetivos de ponto de recuperação (RPOs) de poucos minutos antes que um ataque seja bem-sucedido. Além disso, com o suporte para vários snapshots, a TI terá cópias suficientes para proteger até mesmo ambientes grandes e consolidados de armazenamento essencial em pouquíssimo tempo, quase alcançando, assim, uma recuperação instantânea de aplicativos essenciais. Esse nível de flexibilidade de proteção é um divisor de águas para ambientes de produção em escala. Segundo a Dell, o PowerMax oferece a Cyber Recovery mais granular em escala para otimizar o RPO.

© 2022 TechTarget, Inc. Todos os direitos reservados.

A Dell também pode adicionar uma opção de cofre de Cyber Recovery do PowerMax para organizações que precisam de uma opção de recuperação com air gap de cofre remoto (SRDF), com armazenamento em cofre/recuperação orquestrada para sistemas abertos e, da mesma maneira, para armazenamento de mainframe. A oferta do cofre de Cyber Recovery do PowerMax estará disponível no final deste mês e usará a replicação remota do SRDF para criar air gap. Essa solução foi projetada para clientes que precisam de uma cópia dos dados fora da rede de produção com recuperação rápida (RTO). Embora há algum tempo os clientes do PowerMax implementem essa configuração manualmente, o anúncio deste mês incorpora a automação da orquestração de implementação e os Dell Professional Services para simplificar a instalação.

A grande verdade

A Dell geralmente não é o primeiro nome que vem à mente quando as pessoas pensam em fornecedores de segurança. Essa percepção precisa mudar. Os invasores mal-intencionados estão se tornando mais organizados, e suas ameaças estão mais sofisticadas. A Dell fez e continua a fazer investimentos significativos para ajudar a combater essas ameaças, proteger os dados e simplificar todo o gerenciamento da segurança e da resiliência.

Os dados são o ativo mais essencial de uma organização. Eles precisam ser protegidos. Eles precisam estar sempre disponíveis. A ameaça mais recente a essa disponibilidade inclui ransomware, malware e outros ataques cibernéticos. Sim, o PowerMax tem uma linhagem sólida que atende a cargas de trabalho essenciais e de alto nível. A Dell faz isso há anos, mas os novos recursos do PowerMax são particularmente aplicáveis a quase todos os atuais compradores de armazenamento. Todos estão preocupados com ransomware, malware e a possibilidade de aparecer nas próximas manchetes.

E a questão não é combater criminosos que estão tentando ficar ricos. Esses hackers simplesmente podem trabalhar para um governo estrangeiro visando roubar propriedade intelectual para reforçar sua própria segurança nacional ou força militar. Se eles conseguirem criptografar seus dados, além de impedir seu acesso a eles, não há como dizer o que mais eles conseguirão fazer com eles.

Se tiver informações de negócios que de forma alguma você pode deixar cair nas mãos de pessoas mal-intencionadas, você deve ter uma conversa com a Dell sobre a maneira adequada de proteger uma infraestrutura de armazenamento.

Todos os nomes de produtos, logotipos, marcas e marcas registradas pertencem aos respectivos proprietários. As informações contidas nesta publicação foram obtidas de fontes que a TechTarget, Inc. considera confiáveis, mas não são garantidas pela TechTarget, Inc. Esta publicação pode conter opiniões da TechTarget, Inc., que estão sujeitas a alterações. Esta publicação pode incluir previsões, projeções e outras declarações preditivas que representam as suposições e expectativas da TechTarget, Inc. perante as informações atualmente disponíveis. Essas previsões se baseiam nas tendências do setor e envolvem variáveis e incertezas. Consequentemente, a TechTarget, Inc. não oferece nenhuma garantia quanto à precisão das previsões, projeções ou declarações preditivas específicas aqui contidas.

Os direitos autorais desta publicação pertencem à TechTarget, Inc. Qualquer reprodução ou redistribuição desta publicação, no todo ou em parte, seja em formato impresso, eletrônico ou qualquer outro, a pessoas não autorizadas a recebê-la e sem o consentimento expresso da TechTarget, Inc. é uma violação das leis de direitos autorais dos Estados Unidos e estará sujeita a um processo por danos civis e, se necessário, a processo criminal. Em caso de dúvida, entre em contato com o Atendimento ao cliente pelo e-mail cr@esg-global.com.

O **Enterprise Strategy Group** é uma empresa de estratégia, pesquisa e análise de tecnologias integradas, que oferece inteligência de mercado, percepções úteis e serviços de conteúdo de comercialização à comunidade de TI global.

www.esg-global.com contact@esg-global.com +1 508-482-0188

© 2022 TechTarget, Inc. Todos os direitos reservados.