Validação técnica

Proteção de dados essenciais contra ameaças cibernéticas, como ransomware, com uma solução de cofre digital abrangente

Dell EMC PowerProtect Cyber Recovery com CyberSense

Por Vinny Choinski, analista de validação sênior, e Christophe Bertrand, analista sênior

Outubro de 2020

Esta validação técnica do ESG foi encomendada pela Dell Technologies e distribuída sob licença do ESG.

© 2020 by The Enterprise Strategy Group, Inc. Todos os direitos reservados.

Conteúdo

Introdução 3
Informações gerais 3
Solução Dell EMC PowerProtect Cyber Recovery 4
Validação técnica do ESG 5
Cofre do PowerProtect Cyber Recovery 5
Lacuna de ar do Cyber Recovery 7
CyberSense 8
A grande verdade 10

Validações técnicas do ESG

O objetivo das validações técnicas da ESG é educar os profissionais de TI sobre as soluções de tecnologia da informação para empresas de todos os tipos e tamanhos. As validações técnicas do ESG não são destinadas a substituir o processo de avaliação que deve ser realizado antes de tomar decisões de compra, mas sim para oferecer informações sobre essas tecnologias emergentes. Nossos objetivos são explorar alguns dos recursos e funções mais valiosos das soluções de TI, mostrar como eles podem ser utilizados para resolver problemas reais do cliente e identificar as áreas que precisam de melhorias. A perspectiva dos especialistas terceirizados da equipe de validação da ESG é baseada em nossos próprios testes práticos, bem como em entrevistas com clientes que utilizam esses produtos em ambientes de produção.

© 2020 by The Enterprise Strategy Group, Inc. Todos os direitos reservados.

Introdução

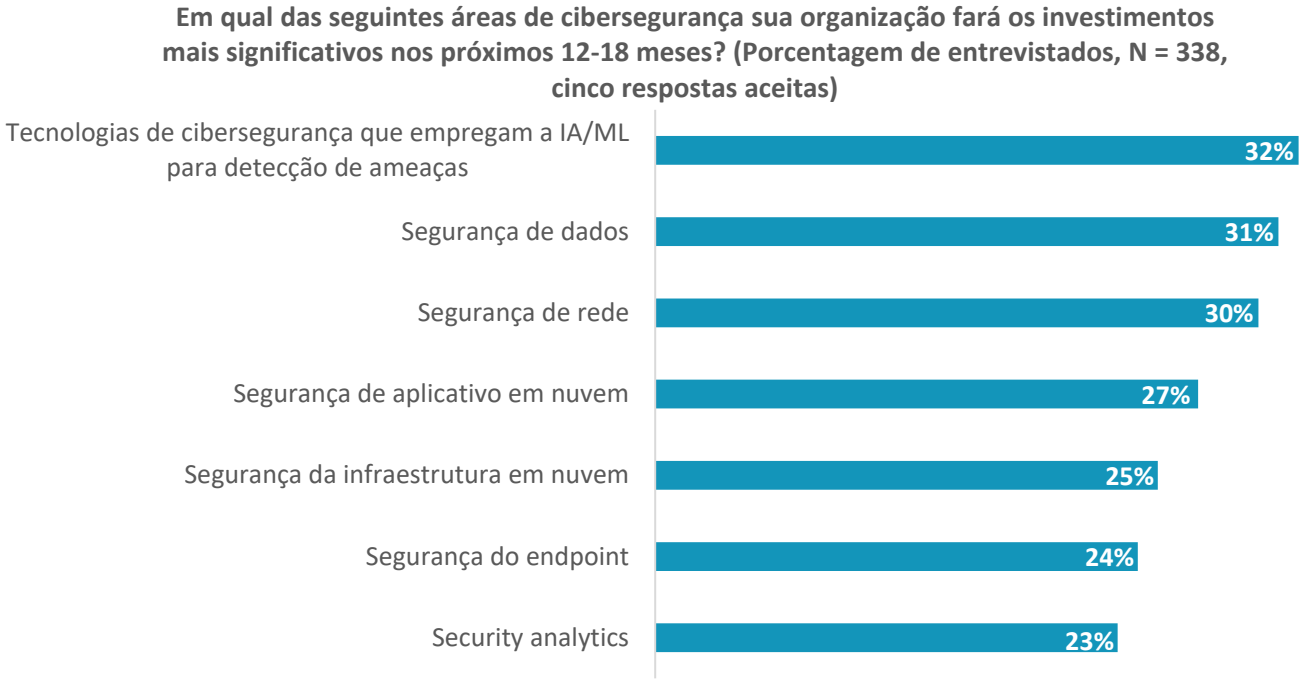
Esta validação técnica do ESG documenta a validação prática da solução Dell EMC PowerProtect Cyber Recovery com CyberSense da Dell Technologies. A ESG realizou análises e auditorias de todos os principais elementos da solução Cyber Recovery, incluindo o cofre do mesmo e suas várias camadas de segurança e proteção para dados essenciais, a lacuna de ar operacional e o mecanismo de análise do CyberSense.

Informações gerais

Independentemente do setor ou do porte da organização, os ataques cibernéticos expõem continuamente os negócios e os governos a dados comprometidos, perda de receita devido ao tempo de inatividade, danos à reputação e multas de regulamentação dispendiosas.

A pesquisa da ESG confirma que a maioria das organizações aumentará os gastos com cibersegurança em 2020, impulsionado pelo desejo de proteger os processos de negócios e neutralizar ameaças perigosas. Embora a maioria possa investir em análises baseadas em IA/ML, segurança de dados, segurança de rede e segurança de aplicativos, os CISOs distribuirão os dólares orçamentários em várias áreas (veja a Figura 1). Os dados indicam que muitas organizações estão no processo de reengenharia de toda a infraestrutura de cibersegurança em uma tentativa de melhorar a eficácia, simplificar as operações de segurança e oferecer suporte a novos processos de negócios orientados pela tecnologia.[1]

Figura 1. As 7 principais áreas de investimento em cibersegurança de 2020



Fonte: Enterprise Strategy Group

Os ransomware e atores ruins descobriram que têm uma chance maior de atingir seu objetivo: receber um resgate ou destruir dados, se nenhum backup estiver disponível para recuperação. Isso colocou os sistemas de backup e os dados sob ataque direto. Infelizmente, há vários pontos vulneráveis, pois os backups foram projetados para a acessibilidade, não necessariamente para a segurança. Os sistemas de backup de dados e aplicativos tornam-se alvos de comprometimento, pois o acesso a esses sistemas é confiável e, portanto, pode ser mais fácil e rapidamente infiltrado. Além disso, os sistemas

[1] Fonte: ESG Brief, *Tendências de gastos com cibersegurança de 2020*, março de 2020.

© 2020 by The Enterprise Strategy Group, Inc. Todos os direitos reservados.

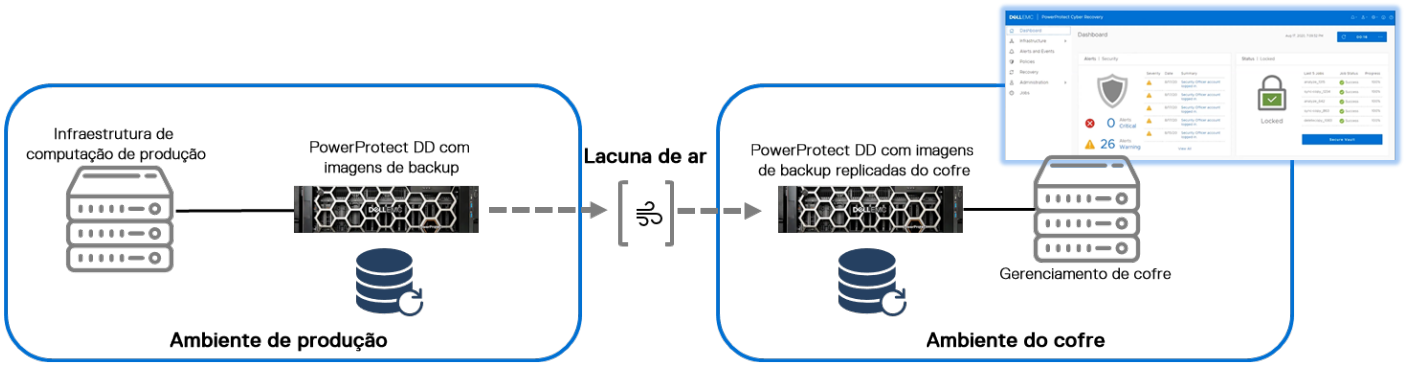
de backup geralmente contêm catálogos de dados, e a criptografia ou exclusão de dados do catálogo podem fazer a recuperação de um backup demorar muito mais tempo, ou até mesmo impedir que o backup seja usado para recuperação.

Solução Dell EMC PowerProtect Cyber Recovery

O Cyber Recovery fornece uma solução abrangente para combater ransomware e ataques cibernéticos destrutivos. É uma solução madura com cinco anos de mercado e centenas de clientes. O software Cyber Recovery automatiza a sincronização de dados entre os sistemas de produção e o cofre, criando cópias com lacuna de ar e imutáveis com políticas de retenção bloqueadas. Se ocorrer um ataque cibernético, os usuários poderão identificar rapidamente uma cópia limpa dos dados, recuperar sistemas essenciais e fazer com que os negócios sejam operados novamente.

O PowerProtect Cyber Recovery conta com o conceito de "cofre" de dados, que geralmente é fisicamente isolado, dentro de uma gaiola ou sala bloqueada, e sempre logicamente isolado por meio de uma lacuna de ar operacional. O cofre não é um data center extra, ele geralmente está localizado no data center de produção ou corporativo ou, às vezes, com um fornecedor de soluções terceirizado. Os componentes do cofre nunca são acessíveis da produção. O acesso ao cofre é fornecido por uma "lacuna de ar operacional", como mostrado na Figura 2.

Figura 2. Visão geral da solução Dell EMC PowerProtect Cyber Recovery



Fonte: Enterprise Strategy Group

Os principais elementos da solução Cyber Recovery incluem:

- Somente a solução PowerProtect Cyber Recovery tem uma lacuna de ar lógica automatizada e orquestrada para proteger os dados. Algumas outras soluções afirmam ter uma "lacuna de ar", pois os dados podem ser separados da rede de produção (por exemplo, uma cópia dos dados armazenados na nuvem); no entanto, com essa abordagem, os dados ainda podem ser acessíveis a atores ruins e uma cópia fora do local não fornece uma lacuna total do ar.

- O cofre do Cyber Recovery em si é isolado fisicamente e logicamente. Ele não pode ser aberto ou controlado do lado da produção nem acessado, a menos que a pessoa esteja fisicamente no cofre.

- O recurso de bloqueio de retenção de conformidade do PowerProtect DD está em conformidade com a norma 17a-4(f)(ii). Ele não pode ser desativado sem uma senha separada do agente de segurança e somente para dados armazenados recentemente. Esse recurso foi fortalecido ainda mais para proteger contra ataques ainda mais avançados, como manipulação de NTP.

© 2020 by The Enterprise Strategy Group, Inc. Todos os direitos reservados.

- O Cyber Recovery pode proteger e habilitar a recuperação de conjuntos de backup de qualquer fornecedor que possam gravar no equipamento PowerProtect.

- Em agosto de 2020, o PowerProtect Cyber Recovery tornou-se a primeira e, no momento em que este documento foi publicado, a única solução a receber o endosso por atender a todos os requisitos de armazenamento de dados do padrão do Sheltered Harbor.

Como parte do PowerProtect Data Manager e para usuários que executam o Dell EMC NetWorker, o PowerProtect Cyber Recovery permite a recuperação automatizada do cofre. A Dell e seus parceiros de ecossistemas fornecem uma metodologia abrangente para a proteção de dados, bem como a realização de avaliações de danos e a perícia para recuperar sistemas ou corrigir e remover o malware ofensivo.

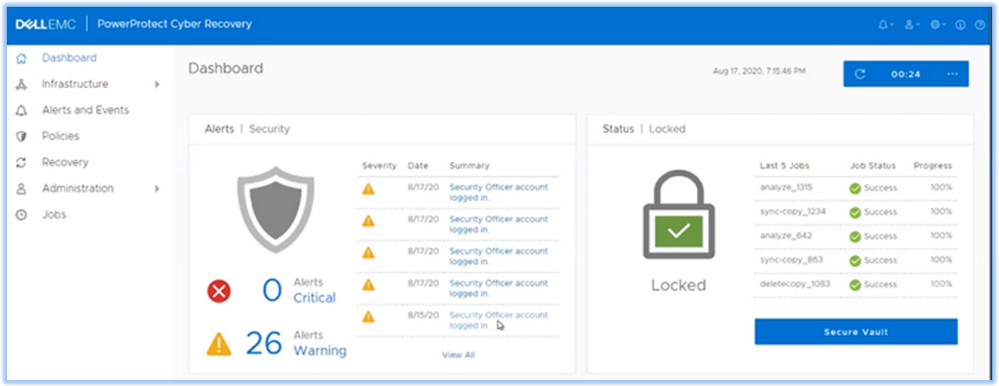
Validação técnica do ESG

O ESG executou a validação e o teste da solução Cyber Recovery do PowerProtect usando o laboratório de engenharia de prova de conceito da Dell. Os testes foram projetados para validar todos os principais elementos da solução Cyber Recovery, incluindo o cofre do Cyber Recovery, a lacuna de ar operacional e o mecanismo de análise do CyberSense.

Cofre do PowerProtect Cyber Recovery

A solução PowerProtect Cyber Recovery baseia-se na implantação e operação de um "cofre" do Cyber Recovery como elemento fundamental. O cofre oferece várias camadas de proteção para fornecer resiliência contra ataques cibernéticos, até mesmo de uma ameaça interna. Ele transfere dados essenciais da superfície de ataque, isolando-os fisicamente em uma parte protegida do data center e requer credenciais de segurança separadas e autenticação de vários fatores para acesso. As proteções adicionais incluem uma lacuna de ar operacional automatizada para fornecer isolamento de rede, além da eliminação de interfaces de gerenciamento acessíveis à produção que podem ser comprometidas. Como ilustrado na Figura 3, o Cyber Recovery é gerenciado por meio de uma interface intuitiva, acessível somente do cofre, completa com painéis de status de solução abrangentes. Uma interface de CLI e APIs também estão disponíveis para o gerenciamento. O software Cyber Recovery implantado dentro da segurança do ambiente do cofre automatiza a sincronização de dados entre os sistemas de produção e o cofre e, em seguida, cria cópias imutáveis com políticas de retenção bloqueadas. Se ocorrer um ataque cibernético, uma cópia de dados limpa pode ser rapidamente identificada e os sistemas críticos para os negócios são recuperados.

Figura 3. Painéis de interface do gerenciamento do PowerProtect Cyber Recovery



Fonte: Enterprise Strategy Group

O ESG exercitou e validou os fluxos de dados operacionais padrão e o desempenho dos aplicativos dos sistemas relacionados à solução Cyber Recovery, bem como aqueles que estão dentro do próprio cofre. Os usuários fariam backup de aplicativos e dados de produção em uma solução, como o ambiente do PowerProtect DD e do NetWorker, mostrados

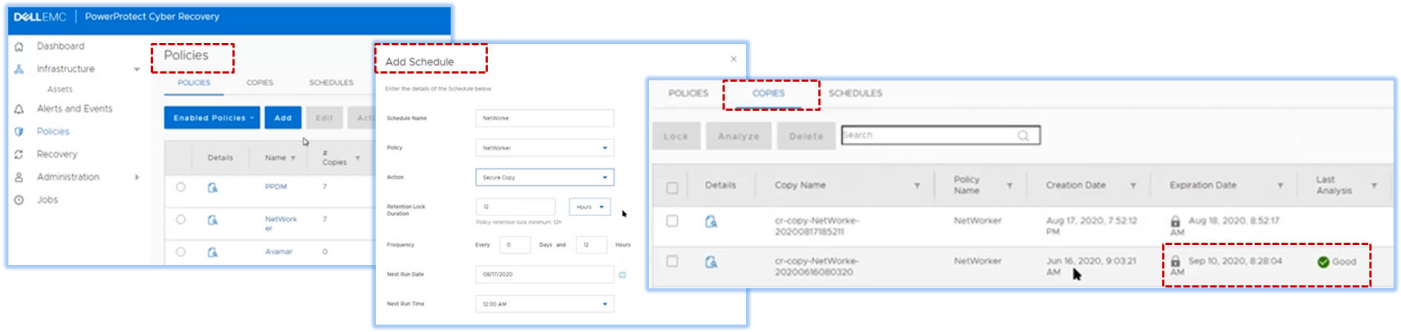
© 2020 by The Enterprise Strategy Group, Inc. Todos os direitos reservados.

na arquitetura de referência, embora o Cyber Recovery possa interagir com muitos aplicativos de backup de diferentes fornecedores.

O recurso de lacuna de ar será discutido em mais detalhes na próxima seção deste relatório, mas essencialmente, uma porta específica e pré-configurada no firewall do cofre é designada para a ingestão de dados e, em seguida, o software Cyber Recovery ativa a porta em intervalos curtos e orientados por políticas. Os dados são "puxados" pelos sistemas do cofre da solução de backup, pela lacuna de ar e pelo destino do PowerProtect DD do cofre. Uma vez que a cópia de dados tenha sido ingerida, a porta designada será desativada, fechando efetivamente o cofre. Com a utilização de uma trava de retenção em conformidade com a SEC 17a-4(f)(ii) e a imutabilidade de WORM, e a necessidade de credenciais de acesso de vários fatores e de segurança separadas, o design da solução Cyber Recovery faz com que seja essencialmente impossível que o cofre seja hackeado. O ESG verificou que o Cyber Recovery incorpora várias camadas de segurança para proteger contra intrusos, incluindo internos. O cofre não pode ser aberto ou controlado do lado da produção. As implantações de cofre utilizam isolamento físico e lógico — os sistemas de cofre implantados adequadamente não podem ser acessados, a menos que a pessoa esteja fisicamente no cofre. As travas de retenção de dados não podem ser desativadas sem uma senha separada do agente de segurança.

Como ilustrado na Figura 3, o ESG utilizou a IU de gerenciamento para criar facilmente políticas automatizadas do Cyber Recovery. Assim que o destino do PowerProtect DD ingere os dados e a lacuna de ar foi fechada, o Cyber Recovery faz com que a cópia e o catálogo relacionado sejam imutáveis ao colocar uma trava de retenção orientada por políticas nos arquivos para protegê-los contra exclusão acidental ou intencional. Como observado, a retenção do cofre é configurável, mas a maioria dos usuários mantém cerca de um mês de cópias.

Figura 4. Gerenciamento de políticas do PowerProtect Cyber Recovery



Fonte: Enterprise Strategy Group

Depois que os dados forem protegidos, eles poderão ser verificados pelo mecanismo de análise CyberSense integrado para descobrir anomalias. O ESG validou que o CyberSense emprega análises completas de conteúdo de arquivos e aprendizado de máquina (ML) treinados em vários vetores de ataque para identificar possíveis comprometimentos de dados. Ele opera de maneira segura no cofre, onde ele avalia os dados armazenados lá, ocupando mais de 100 observações por arquivo todos os dias. Em seguida, esses dados são avaliados no cofre por um mecanismo de ML/IA para gerar um veredicto sobre a validade dos dados. Assim como ocorre com o recurso de lacuna de ar, os recursos e a funcionalidade de análise do CyberSense serão discutidos em mais detalhes posteriormente neste relatório.

A recuperação de dados do cofre em caso de ataques cibernéticos ou simplesmente para os procedimentos de teste de recuperação é essencial. O ESG verificou que a solução Cyber Recovery oferece várias maneiras de realizar a recuperação. A solução inclui ferramentas de inteligência no cofre para acelerar a recuperação de cópias "limpas". O CyberSense processa um veredicto em cada conjunto de dados para determinar se ele está "OK" ou "suspeito". Os dados rotulados como "suspeitos" incluem informações sobre o conteúdo que estão em risco, de modo que o restante dos dados "limpos" pode ser usado para recuperação. Isso permite a recuperação mais rápida e segura possível, além de potencialmente

© 2020 by The Enterprise Strategy Group, Inc. Todos os direitos reservados.

ajudar a controlar a origem do ataque. A Dell afirma que nenhuma solução competitiva oferece informações específicas, durante uma análise de primeira passagem, em porções do conjunto de dados que podem ter sido impactadas; além disso, as soluções de vários concorrentes contam com as informações enviadas ou extraídas de um plano SaaS de nuvem pública que provavelmente não estarão disponíveis no ambiente de produção, o que normalmente é encerrado após o ataque.

Por que isso é importante

Muitas organizações aceitaram o fato de que elas experimentarão um ataque cibernético bem-sucedido em algum momento em um futuro não muito distante. Essas organizações mudaram suas ideias de prevenção para a resiliência — desejam recuperar sistemas essenciais para os negócios da forma mais rápida e eficiente possível após um incidente cibernético.

A solução PowerProtect Cyber Recovery faz uma abordagem de "cofre" para a resiliência cibernética prática. O ESG validou que a implantação e a operação da solução de cofre e seus vários componentes são relativamente simples, especialmente com a ajuda dos serviços de consultoria da Dell EMC.

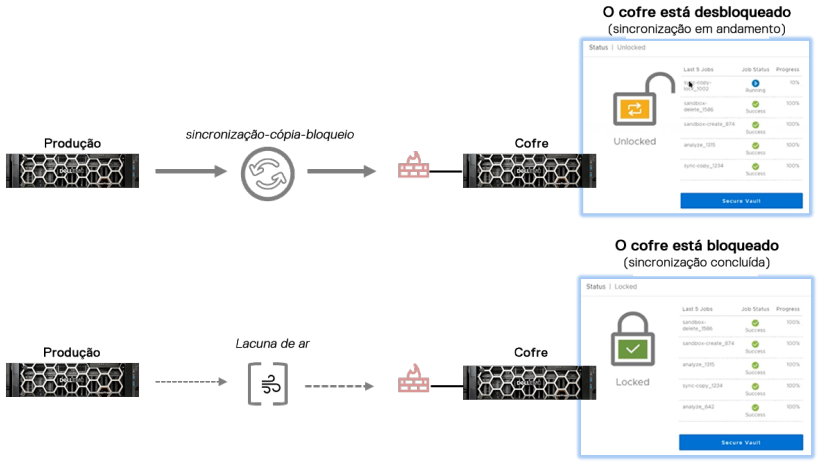
Lacuna de ar do Cyber Recovery

O conceito de "lacuna de ar" é essencial para a abordagem de "cofre" utilizada pela solução PowerProtect Cyber Recovery. A criação de uma lacuna de ar bem-sucedida que realmente isole o ambiente de cofre de sistemas externos e conectividade requer engenharia cuidadosa e design de solução inovador. A Dell chama sua implementação de "lacuna de ar operacional" para diferenciar-se da definição de "lacuna de ar" mais antiga, que identifica uma rede que nunca está conectada externamente. A lacuna de ar do Cyber Recovery também é "operacional", pois a ingestão de dados e o gerenciamento do processo são automatizados e orientados por políticas, e não requer intervenção manual.

Conforme ilustrado na figura 5 e verificado pelo ESG, o cofre, seus sistemas e dados são isolados física e logicamente, exceto durante o processo de ingestão de dados real. Com base na segurança do cofre, o software PowerProtect Cyber Recovery inicia uma transferência de dados agendada, designando, configurando e ativando brevemente uma única porta de rede em uma interface dedicada para essa finalidade. No laboratório de engenharia de prova de conceito da Dell, os dados foram transferidos entre um sistema PowerProtect DD 9900 usado como um dispositivo de backup no lado da produção, em uma conexão de rede ativada brevemente, para um sistema de destino PowerProtect DD 9900 no cofre. Os dados foram "extraídos" do sistema de backup no lado da produção, portanto, não participaram do gerenciamento ou da operação da conexão de rede. Assim que a transferência de dados foi concluída, a conexão de rede não foi apenas fechada, mas a própria interface foi desativada, reestabelecendo o isolamento completo do cofre por meio de uma lacuna de ar operacional. O gerenciamento de lacunas de ar foi inteiramente controlado pelo software Cyber Recovery de dentro do cofre. E mesmo quando a lacuna de ar foi desbloqueada brevemente, o acesso é extremamente limitado — apenas o destino de replicação está sempre acessível, para aceitar os dados atualizados e os componentes do cofre, incluindo cópias de dados anteriores, que nunca estão acessíveis.

© 2020 by The Enterprise Strategy Group, Inc. Todos os direitos reservados.

Figura 5. Lacuna de ar operacional do PowerProtect Cyber Recovery



Fonte: Enterprise Strategy Group

Por que isso é importante

O cofre do Cyber Recovery é uma solução eficiente que aprimora a resiliência cibernética organizacional. Mas o cofre é tão eficaz quanto a tecnologia e a abordagem da lacuna de ar usadas para estabelecer e manter o isolamento. O ESG confirmou que a solução de lacuna de ar operacional usada pelo Cyber Recovery é de última geração, realiza sua função pretendida e oferece uma solução segura para proteger dados essenciais contra ataques cibernéticos, ransomware, malware e outras ameaças que o ESG tem visto no mercado.

Para todas as organizações e tomadores de decisões de TI que avaliam várias soluções de resiliência cibernética, ter confiança na capacidade de isolar dados contra invasões cibernéticas contínuas é um ingrediente importante em uma solução bem-sucedida de resiliência cibernética.

CyberSense

O ESG validou a configuração e a operação básicas do mecanismo de análise do CyberSense e da funcionalidade no ambiente da solução PowerProtect Cyber Recovery, conforme implementado no laboratório de engenharia de prova de conceito da Dell. o CyberSense é integrado à solução Cyber Recovery geral e adiciona uma camada de proteção inteligente para ajudar a encontrar a corrupção de dados se um ataque cibernético penetrar os ambientes de produção ou de backup. O mecanismo de análise do CyberSense oferece indexação total de conteúdo e usa o aprendizado de máquina para analisar mais de 100 estatísticas baseadas em conteúdo para detectar sinais de corrupção devido a invasões cibernéticas. A Dell afirma que o CyberSense encontra corrupção com até 99,5% de confiança, ajudando os usuários a identificar ameaças e a diagnosticar vetores de ataque e, ao mesmo tempo, proteger o conteúdo essencial para os negócios, tudo isso dentro da segurança do cofre. A Figura 6 ilustra as etapas básicas envolvidas no processo de análise e geração de relatórios do CyberSense.

© 2020 by The Enterprise Strategy Group, Inc. Todos os direitos reservados.

Figura 6. Processo de análise e geração de relatórios do CyberSense

Fonte: Enterprise Strategy Group

- Os dados são verificados no formato em que foram armazenados no cofre (por exemplo, os backups permanecem no formato de backup).
- As análises assumem mais de 100 observações por arquivo, incluindo medições como entropia e semelhança.
- Essas observações são coletadas e avaliadas por uma ferramenta de aprendizado de máquina que identificou padrões que indicam que os dados foram corrompidos. Como ela está em busca de padrões, não de assinaturas, a análise é mais eficaz e não precisa ser atualizada com frequência. O processo é repetido cada vez que um novo conjunto de dados é colocado no cofre.
- As ferramentas de análise e geração de relatórios podem ajudar a identificar rapidamente dados corrompidos e a origem de um ataque, permitindo uma recuperação mais rápida e mais segura.

Depois que os dados são replicados para o cofre do Cyber Recovery e um bloqueio de retenção é aplicado, o CyberSense verifica os dados de backup, criando observações pontuais de arquivos e bancos de dados. A execução de análises nos dados no cofre é um componente importante para manter a integridade desses dados e possibilitar uma recuperação rápida após um ataque. A análise ajuda a determinar se um conjunto de dados é válido e utilizável para recuperação ou se, de alguma forma, foi incorretamente alterado ou corrompido para que seja “suspeito” e potencialmente inutilizável.

O CyberSense detecta exclusões em massa, criptografia e outros tipos de alterações em arquivos e bancos de dados que resultam de ataques cibernéticos comuns. Essa verificação ocorre diretamente nos dados da imagem de backup sem a necessidade do software de backup original. As análises geradas incluem incompatibilidade de tipo de arquivo, corrupção, extensões de resgate conhecidas, exclusões, entropia, semelhança e muito mais. Os resultados da análise são, então, utilizados pelos algoritmos de aprendizado de máquina para tomar uma decisão determinística sobre a corrupção de dados que é um indicativo de um ataque cibernético. Os algoritmos de aprendizado de máquina foram treinados para todos os cavalos de troia e ransomware mais recentes e podem ser atualizados à medida que novos vetores de ataque forem descobertos. As análises CyberSense são particularmente eficientes porque (a) podem ler o formato de backup, portanto, não há necessidade de restaurar dados, o que é difícil de automatizar e pode expor o cofre a riscos potenciais; e (b) eles avaliam o conteúdo completo do arquivo, não apenas seus metadados, para fornecer informações superiores.

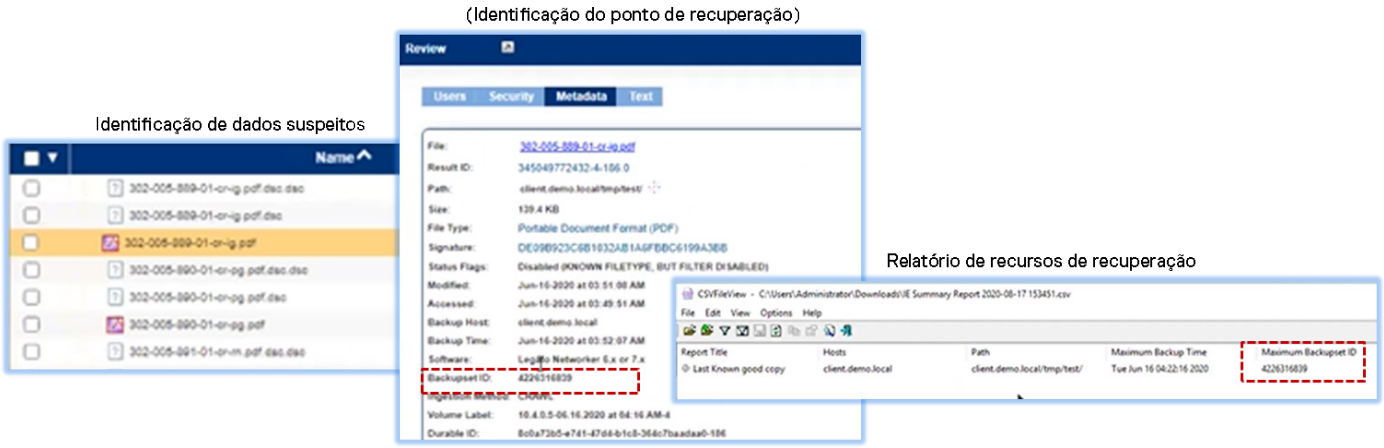
O CyberSense vai além das soluções somente de metadados, pois baseia-se na análise do conteúdo completo dos arquivos no cofre, o que proporciona um alto grau de confiança na detecção de corrupção de dados. Ele audita arquivos e bancos de dados para ataques que incluem corrupção baseada somente no conteúdo da estrutura de arquivos ou criptografia parcial dentro de um documento ou página de um banco de dados. Esses ataques não podem ser encontrados usando análises que não são digitalizadas no arquivo para comparar a mudança ao longo do tempo. Sem análise completa baseada em conteúdo, o número de falsos negativos será significativo, fornecendo um falso senso de confiança na integridade e na segurança dos dados.

© 2020 by The Enterprise Strategy Group, Inc. Todos os direitos reservados.

As observações contínuas dos dados permitem que o CyberSense controle como o conteúdo dos arquivos muda ao longo do tempo. O CyberSense gera análises de uma ampla variedade de tipos de dados, incluindo infraestrutura básica, como DNS, LDAP e Active Directory; arquivos de dados não estruturados, como documentos, contratos e acordos; propriedade intelectual; e bancos de dados, como Oracle, DB2, SQL, Epic Caché e outros.

Se o CyberSense detectar sinais de corrupção, será gerado um alerta que inclua o vetor de ataque e a listagem de arquivos afetados. Um alerta crítico é exibido no painel do Cyber Recovery e, em seguida, os relatórios forenses pós-ataque do CyberSense estão disponíveis para diagnosticar e recuperar-se rapidamente do ataque de ransomware. Como ilustrado na Figura 7, com o CyberSense, as organizações podem auditar proativamente seus arquivos e bancos de dados para determinar quando um ataque começou e, em seguida, recuperar rapidamente com a última versão boa dos dados, talvez até mesmo antes que haja interrupções nos negócios.

Figura 7. Correção do CyberSense



Fonte: Enterprise Strategy Group

Por que isso é importante

Uma coisa é isolar as cópias de dados cruciais do restante do data center. É muito diferente ter certeza de que essas cópias podem ser usadas para recuperar de maneira segura as operações de negócios. A confiança que os conjuntos de dados específicos realmente podem ser utilizados para recuperar sistemas essenciais para os negócios é o que mais importa para as organizações que implantam soluções de resiliência cibernética, como o PowerProtect Cyber Recovery.

A análise do CyberSense conclui o processo do Cyber Recovery, oferecendo confiança aos usuários de que os dados contidos no cofre do Cyber Recovery são "limpos" e utilizáveis para fins de recuperação reais. O conteúdo completo e a análise de dados orientada por máquina são de última geração para esse tipo de operação. Portanto, as organizações que dependem do PowerProtect Cyber Recovery acreditam que estão fazendo tudo o que podem para aumentar a resiliência cibernética e reduzir os riscos e os custos de ataques cibernéticos e invasões.

A grande verdade

As organizações estão se afastando de um foco na cibersegurança e colocando-o em direção a uma abordagem mais abrangente, conhecida como resiliência cibernética. Em vez de esperar que elas possam derrotar as ameaças cibernéticas 100% do tempo, estão supondo que um ataque cibernético eventualmente será bem-sucedido e que a organização precisará se recuperar do ataque e retomar as operações da maneira mais rápida e econômica possível.

© 2020 by The Enterprise Strategy Group, Inc. Todos os direitos reservados.

Para recuperar com êxito os dados e os sistemas essenciais para os negócios depois de um incidente cibernético, cópias não afetadas ou “limpas” de aplicativos e conjuntos de dados devem estar disponíveis. O desafio se torna a forma como uma organização garante que os dados limpos e os aplicativos não afetados existam. Para muitas organizações, a resposta é isolar de maneira física e lógica as cópias de dados de todos os sistemas de produção e backup normais e, em seguida, digitalizar e analisar esses dados dentro do ambiente de “cofre” seguro para detectar qualquer corrupção e identificar cópias limpas que podem ser usadas com confiança para recuperação operacional.

A solução PowerProtect Cyber Recovery da Dell Technologies atende a um requisito importante no mercado de resiliência cibernética em rápida expansão, fornecendo um cofre digital completo, análise de dados e solução de recuperação cibernética. O Cyber Recovery integra os principais elementos de uma solução geral, incluindo uma proteção de “lacuna de ar” automatizada e de última geração, além de um mecanismo de análise comprovado e orientado por IA que opera a partir da segurança do ambiente do cofre.

As estratégias de resiliência cibernética geralmente empregam termos como “confiança” e “confiabilidade” para descrever os níveis de eficácia oferecidos por uma solução ou outra. A avaliação prática do ESG confirmou que as organizações que implantaram a solução PowerProtect Cyber Recovery podem, de fato, dizer aos acionistas que têm um alto grau de confiança de que os sistemas podem ser recuperados com êxito após um ataque cibernético e que os negócios estarão operacionais e lucrativos novamente com a menor quantidade de interações.

A confiança é fundamental no mercado. Isso é o que o PowerProtect Cyber Recovery oferece: proteção de dados moderna e comprovada que melhora a resiliência cibernética. É exatamente o que muitas organizações estão procurando.

Todos os nomes de marcas comerciais são propriedade de suas respectivas empresas. As informações contidas nesta publicação foram obtidas por fontes que o Enterprise Strategy Group (ESG) considera confiáveis, mas não são garantidas pelo mesmo. Esta publicação pode conter opiniões do ESG, que estão sujeitas a alterações de tempos em tempos. Esta publicação possui direitos autorais do Enterprise Strategy Group, Inc. Qualquer reprodução ou redistribuição desta publicação, no todo ou em parte, seja em formato de cópia impressa, eletronicamente ou de outra forma, a pessoas não autorizadas a recebê-la, sem o consentimento expresso do Enterprise Strategy Group, Inc., viola a lei de direitos autorais dos Estados Unidos e estará sujeita a uma ação por danos civis e, se aplicável, a processos criminais. Em caso de dúvidas, entre em contato com Relacionamento com o cliente do ESG em 508.482.0188.

Enterprise Strategy Group é uma empresa de estratégia, validação, pesquisa e análise de TI que oferece inteligência de mercado e percepções práticas à comunidade global de TI.

© 2020 by The Enterprise Strategy Group, Inc. Todos os direitos reservados.