Resumo da solução

CyberSense® para PowerProtect Cyber Recovery

Aprendizado de máquina baseado em IA, lógica analítica e ferramentas forenses para detectar, diagnosticar e se recuperar de ataques cibernéticos

A VANTAGEM DO CYBERSENSE

O CyberSense® é totalmente integrado à solução de cofre Dell PowerProtect Cyber Recovery.

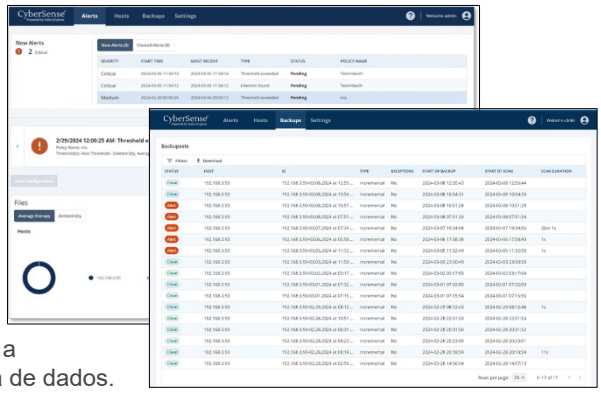
- Essa integração permite uma abordagem automatizada em relação à varredura regular dos dados de backup para validar a integridade dos dados e alertar quando um comportamento suspeito é detectado.
- A capacidade do CyberSense de examinar diretamente as imagens de backup, incluindo Dell NetWorker, Avamar, PowerProtect Data Manager e muito mais, permite que o conteúdo seja analisado sem a necessidade de reidratar os dados.
- Somente o CyberSense oferece lógica analítica de conteúdo completo a cada varredura dos dados para detectar até mesmo os ataques de ransomware mais sofisticados, que podem facilmente passar despercebidos por ferramentas de varredura simples que inspecionam apenas metadados.
- Quando ocorre um ataque, o CyberSense apresenta relatórios forenses pós-ataque para entender a profundidade e a amplitude do ataque e exibe uma lista dos últimos conjuntos de backups válidos antes da corrupção para facilitar o processo de recuperação.

O CyberSense se destaca de outras abordagens de lógica analítica de dados e oferece um nível mais alto de confiança de que os dados de backup permanecem íntegros e podem ser recuperados rapidamente após a ocorrência de um ataque.

Quando as ferramentas de segurança convencionais falham na proteção de dados contra ataques cibernéticos, o **CyberSense®** entra em ação para detectar corrupção de dados após um ataque com 99,5% de precisão e facilita a restauração inteligente e rápida. Servindo como a última linha de defesa e primeira linha de recuperação para milhares de organizações em todo o mundo, o CyberSense garante a integridade de seus ativos de dados, incluindo infraestrutura de núcleo, bancos de dados de produção e documentos essenciais, inspirando confiança de que os dados estão protegidos contra corrupção mal-intencionada.

O CyberSense usa os backups de dados para observar como eles mudam ao longo do tempo e utiliza o aprendizado de máquina baseado em IA para detectar sinais de corrupção indicativos de um ataque de ransomware. Em seguida, o aprendizado de máquina examina essas mais de 200 lógicas analíticas baseadas em conteúdo para encontrar corrupção com 99,5% de confiança, ajudando você a proteger a infraestrutura e o conteúdo essenciais aos negócios. O CyberSense detecta exclusões em massa, criptografia e outras alterações suspeitas na infraestrutura de núcleo (como Active Directory, DNS etc.), arquivos de usuário e bancos de dados de produção essenciais resultantes de ataques sofisticados. Se o CyberSense detectar sinais de corrupção, um alerta será gerado no painel de indicadores com informações adicionais que detalham a escala e o impacto do ataque.

Quando ocorre um comportamento suspeito, o CyberSense apresenta relatórios forenses pós-ataque para diagnosticar o alcance do ataque cibernético. Quando a corrupção de dados é detectada, uma lista dos últimos conjuntos de dados de backup válidos é disponibilizada para dar suporte a uma rápida recuperação selecionada que ajuda a minimizar a interrupção dos negócios e a perda de dados.



O fluxo de trabalho do Cyber Recovery

O CyberSense se integra perfeitamente ao Dell PowerProtect Cyber Recovery, monitorando ativamente arquivos e bancos de dados para detectar a corrupção causada por ransomware e analisar a integridade dos dados. Depois que os dados são replicados para o cofre do Cyber Recovery e o bloqueio de retenção é aplicado, o CyberSense inicia automaticamente uma varredura abrangente dos dados de backup, criando observações pontuais de arquivos, bancos de dados e infraestrutura de núcleo. Essas observações permitem que o CyberSense rastreie meticulosamente as alterações nos arquivos ao longo do tempo, descobrindo com eficiência a corrupção de dados até mesmo pelas ameaças cibernéticas mais sofisticadas.

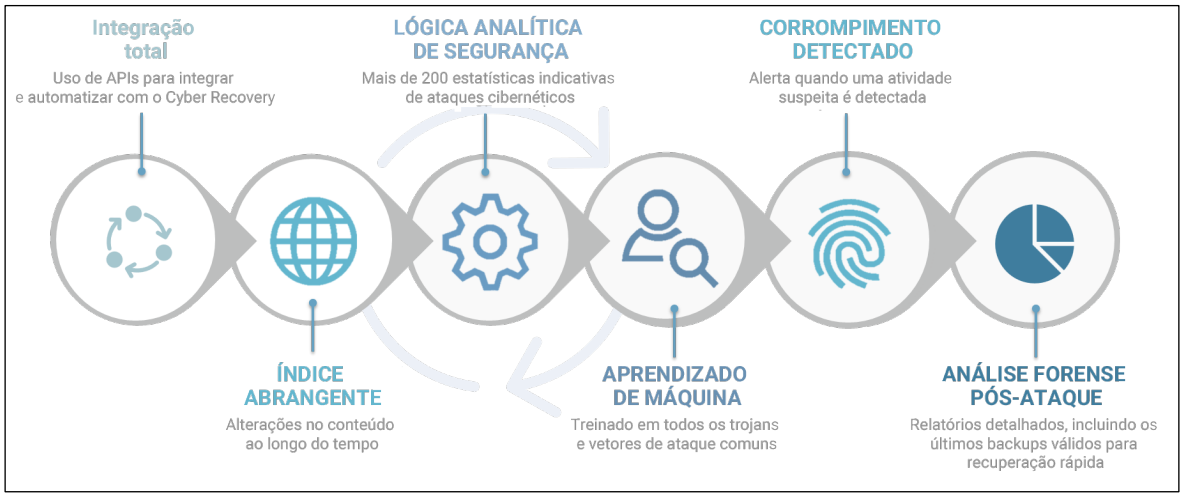
A varredura do CyberSense opera diretamente nos dados dentro da imagem de backup, eliminando a necessidade do software de backup original e a reidratação dos dados. Por meio de lógica analítica avançada, o CyberSense identifica criptografia/corrupção de arquivos ou páginas de banco de dados, reconhece extensões conhecidas de malware, detecta exclusões/criações em massa de arquivos e muito mais.

Utilizando algoritmos de aprendizado de máquina baseado em IA treinados com os mais recentes trojans e ransomware, o CyberSense toma decisões deterministas sobre corrupção de dados indicativas de um ataque cibernético. Em caso de ataque, um alerta crítico é imediatamente exibido no painel de indicadores do Cyber Recovery. Além disso, o CyberSense oferece relatórios forenses pós-ataque, facilitando o diagnóstico rápido e a recuperação de ataques de ransomware para minimizar a perda de dados.

Lógica analítica de conteúdo completo

O CyberSense é o único produto no mercado que oferece lógica analítica baseada em conteúdo completo em todos os dados protegidos. Esse recurso diferencia o CyberSense de outras soluções que têm uma visualização de alto nível dos dados e usam lógica analítica que procura sinais óbvios de corrupção com base nos metadados. A corrupção no nível de metadados não é difícil de detectar; por exemplo, alterar uma extensão de arquivo para .encrypted ou alterar radicalmente o tamanho do arquivo. Esses tipos de ataques não representam os ataques sofisticados que os criminosos cibernéticos usam atualmente.

O



CyberSense vai além das soluções somente de metadados porque se baseia na lógica analítica de conteúdo completo para detectar corrupção de dados. Ele audita arquivos e bancos de dados em busca de ataques que incluem corrupção da estrutura de arquivos baseada apenas em conteúdo ou criptografia parcial dentro de um documento ou página de um banco de dados. Esses ataques não podem ser encontrados usando uma lógica analítica que não examina dentro do arquivo para comparar como ele muda ao longo do tempo. Sem uma lógica analítica baseada em conteúdo completo, o número de falsos negativos será significativo, proporcionando uma falsa sensação de confiança quanto à integridade e segurança dos dados. Além disso, alertas personalizados podem ser criados com base na quantidade ou porcentagem de arquivos alterados ou tipo de arquivo, arquivos adicionados ou excluídos e entropia em um host.

Tipos de dados compatíveis

O CyberSense gera lógica analítica a partir de uma ampla variedade de tipos de dados. Isso inclui a infraestrutura de núcleo, como DNS, LDAP, Active Directory, arquivos não estruturados, como documentos, contratos, propriedade intelectual e bancos de dados, incluindo Oracle, DB2, SQL, PostgreSQL, Epic Caché etc.

Resumo

Totalmente integrado ao Dell PowerProtect Cyber Recovery, o CyberSense audita seus dados e detecta indicadores de violação e corrupção. O CyberSense permite que você compreenda proativamente o alcance de um ataque cibernético em andamento, facilitando a implementação de um plano para diagnosticar e se recuperar rapidamente, reduzindo assim a interrupção dos negócios e suas despesas significativas associadas.

Saiba mais sobre o Dell PowerProtect Cyber Recovery	Entre em contato com um especialista da Dell Technologies	Saiba mais sobre o CyberSense	Participe da conversa com #PowerProtect