Resumo da solução

CyberSense® para Dell PowerProtect Cyber Recovery

Ferramentas forenses e lógica analítica com IA para detectar, diagnosticar e se recuperar com mais inteligência de ataques cibernéticos

A VANTAGEM DO CYBERSENSE

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

- Automatiza a verificação regular de dados de backup para validar a integridade dos dados e alertar quando um comportamento suspeito é detectado.
- Verifica diretamente o conteúdo nas imagens de backup do Dell Avamar, NetWorker, Commvault, NetBackup e PowerProtect Data Manager, sem a necessidade de reidratar os dados.
- Oferece análise profunda de conteúdo completo com cada verificação de dados para detectar até mesmo os mais sofisticados ataques de ransomware.
- Emite alertas personalizados para assinaturas de malware e regras de YARA a fim de detectar comportamentos conhecidos de ransomware ou agentes mal-intencionados internos.
- Facilita a recuperação mais inteligente e rápida com relatórios forenses pós-ataque para entender a profundidade e a amplitude do ataque. Além disso, ele lista os últimos conjuntos de backups em boas condições antes da corrupção.

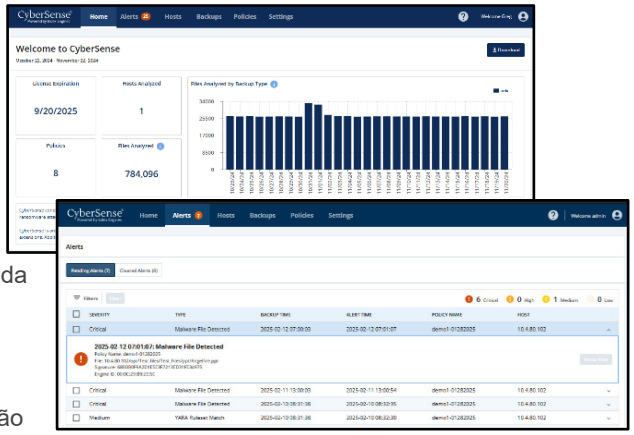
O CyberSense se destaca de outras abordagens de lógica analítica de dados e oferece um nível mais alto de confiança de que os dados de backup permanecem íntegros e podem ser recuperados rapidamente após a ocorrência de um ataque.

À medida que a frequência dos ataques virtuais continua a aumentar e os criminosos virtuais se tornam mais resilientes, as ferramentas de segurança convencionais não protegem os dados contra ataques cibernéticos.

O **CyberSense®** entra em ação para detectar corrupção de dados após um ataque com 99,99% de precisão* e facilita a restauração inteligente e rápida. Atuando como a primeira linha de recuperação para milhares de organizações em todo o mundo, o CyberSense garante a integridade dos ativos de dados, incluindo infraestrutura de núcleo, bancos de dados e documentos essenciais, inspirando confiança de que os dados estão protegidos contra corrupção mal-intencionada.

O CyberSense verifica os backups de dados em um cofre do Cyber Recovery para observar como os dados mudam com o tempo. Em seguida, ele utiliza o aprendizado de máquina e a IA para detectar sinais de corrupção que indicam um ataque de ransomware. Os dados são comparados com mais de 200 lógicas analíticas baseadas em conteúdo para identificar a corrupção com 99,99% de confiança*, ajudando você a proteger a infraestrutura e o conteúdo essenciais para os negócios. O CyberSense detecta exclusões em massa, criptografia e outras alterações suspeitas, resultantes de ataques sofisticados, na infraestrutura de núcleo (como Active Directory, DNS etc.), nos repositórios de arquivos, nos file systems e nos bancos de dados essenciais.

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 em boas condições é disponibilizada para dar suporte a rápidas recuperações selecionadas, que ajudam a minimizar a interrupção dos negócios e a perda de dados, reduzindo os custos da recuperação cibernética.

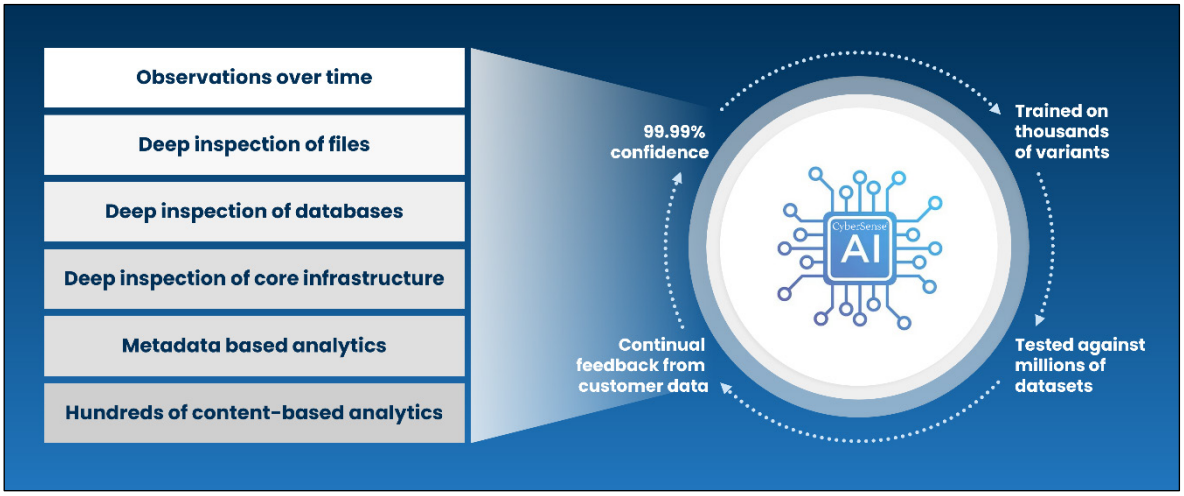


O fluxo de trabalho do Cyber Recovery

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. O CyberSense rastreia meticulosamente as alterações nos arquivos ao longo do tempo, descobrindo com eficiência a corrupção de dados até mesmo pelas ameaças cibernéticas mais sofisticadas.

Lógica analítica de conteúdo completo

O CyberSense é o único produto no mercado que oferece lógica analítica e indexação de conteúdo completo em todos os dados protegidos. A análise de IA profunda do CyberSense é executada em todos os dados, e uma decisão probabilística é gerada com 99,99% de precisão* a respeito da integridade dos dados ou da corrupção por ransomware. 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 e detecta corrupção de dados usando a lógica analítica de conteúdo completo. Ele faz a auditoria de arquivos e bancos de dados para verificar alterações indicativas de um ataque, incluindo corrupção total ou parcial de arquivos. A análise tradicional deixa essas ameaças passarem, gerando uma falsa segurança. Alertas de limite personalizados podem ser definidos com base em alterações de arquivos regulares, arquivos adicionados ou arquivos excluídos. As assinaturas de malware e as regras personalizadas de YARA também podem ser implementadas para a detecção, prospectiva ou retrospectiva, de malware em backups.

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 analisa seus dados no cofre e detecta indicadores comportamentais 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 diagnóstico e recuperação rápidos, a fim de reduzir 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

* Com base em um relatório de ESG encomendado pela Index Engines: "Index Engines' CyberSense Validated 99.99% Effective in Detecting Ransomware Corruption". Junho de 2024

DELL Technologies