DELL Technologies

Resumen de la solución

CyberSense® para Dell PowerProtect Cyber Recovery

Análisis y herramientas forenses con IA para detectar, diagnosticar y recuperarse de ataques cibernéticos de manera más inteligente

LA VENTAJA DE CYBERSENSE

CyberSense® está completamente integrado con la solución de vault de Dell PowerProtect Cyber Recovery.

- Automatiza el escaneo regular de los datos de respaldo para validar la integridad de los datos y alertar cuando se detecta un comportamiento sospechoso.
- Escanee directamente el contenido dentro de las imágenes de respaldo de Dell Avamar, NetWorker, CommVault, NetBackup y PowerProtect Data Manager sin la necesidad de rehidratar los datos.
- Ofrece un análisis profundo de contenido completo con cada escaneo de datos para detectar incluso los ataques de ransomware más sofisticados.
- Alertas personalizadas para que las reglas YARA y las firmas de malware detecten comportamiento conocido de ransomware o agentes internos maliciosos.
- Facilita una recuperación más rápida e inteligente con informes forenses posteriores al ataque para obtener información valiosa y detallada sobre la profundidad y la amplitud del ataque y proporciona una lista de los últimos conjuntos de respaldo en buen estado antes de que se produzcan daños.

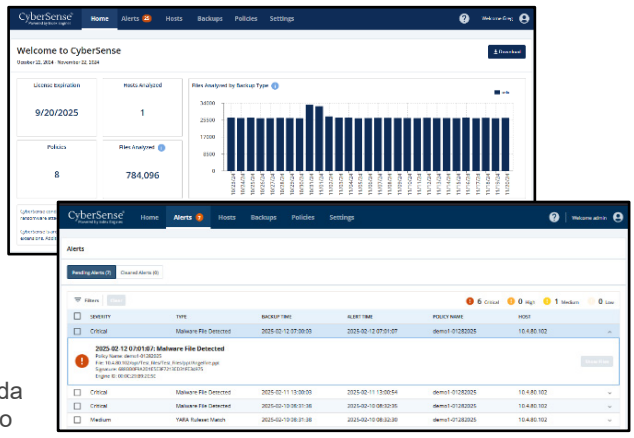
CyberSense se distingue de otros enfoques de análisis de datos y proporciona un mayor nivel de confianza de que los datos de respaldo tienen integridad y se pueden recuperar rápidamente después de que ocurre un ataque.

A medida que la frecuencia de los ataques cibernéticos continúa aumentando y los delincuentes cibernéticos se vuelven más resilientes, las herramientas de seguridad convencionales no alcanzan para proteger los datos contra los ataques cibernéticos.

CyberSense® interviene para detectar daños en los datos después de un ataque con una precisión del 99,99 %* y facilita la restauración inteligente y rápida. Como la primera línea de recuperación para miles de organizaciones en todo el mundo, CyberSense garantiza la integridad de los recursos de datos, incluida la infraestructura principal, las bases de datos y los documentos fundamentales, lo que infunde la confianza de que los datos están limpios de daños maliciosos.

CyberSense escanea los respaldos de datos en una vault de Cyber Recovery para observar cómo cambian los datos con el tiempo. Luego, utiliza el aprendizaje automático y la IA para detectar signos de corrupción que indican un ataque de ransomware. Los datos se comparan con más de 200 análisis basados en contenido para identificar la corrupción con un 99,99 % de confianza*, lo que lo ayuda a proteger la infraestructura y el contenido esencial de su negocio. CyberSense detecta eliminaciones masivas, cifrado y otros cambios sospechosos en la infraestructura central (incluidos Active Directory, DNS, etc.), los repositorios de archivos, los sistemas de archivos y las bases de datos fundamentales que surgen de los ataques sofisticados.

Cuando se produce un comportamiento sospechoso, CyberSense proporciona informes forenses posteriores al ataque para diagnosticar el radio de efecto del ataque cibernético. Cuando se detectan daños en los datos, está disponible una lista de los últimos conjuntos de datos de respaldo en buen estado para admitir recuperaciones selectivas que ayudan a minimizar la interrupción del negocio y la pérdida de datos, lo que disminuye el costo de la recuperación cibernética.

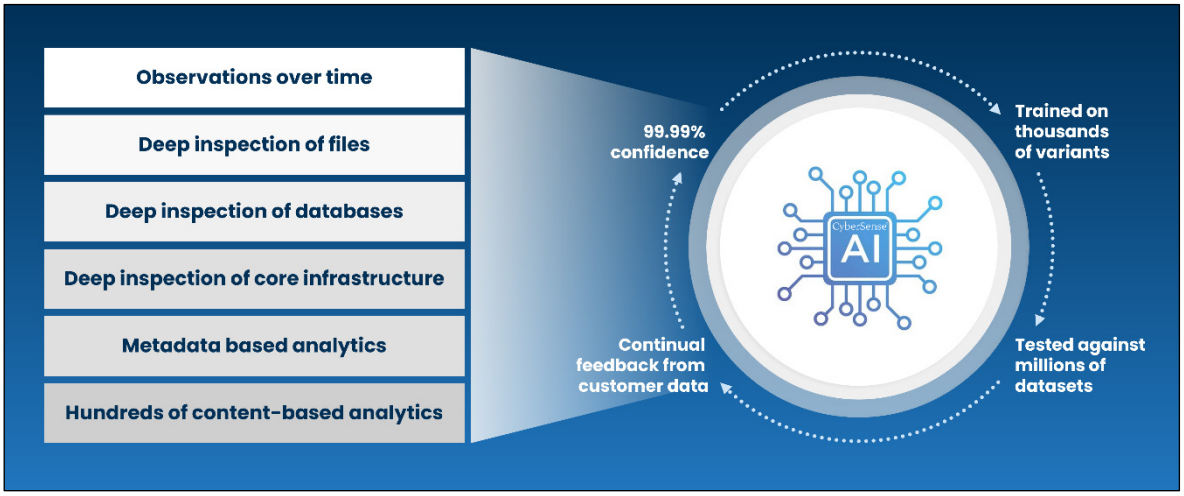


El flujo de trabajo de Cyber Recovery

CyberSense se integra sin inconvenientescon Dell PowerProtect Cyber Recovery, monitoreando activamente archivos y bases de datos para detectar daños de ransomware mediante el análisis de la integridad de los datos. Una vez que los datos se replican en el vault de Cyber Recovery y se aplica el bloqueo de retención, CyberSense inicia automáticamente un análisis integral de los datos de respaldo y crea observaciones de un punto en el tiempo de archivos, bases de datos e infraestructura principal. CyberSense realiza un seguimiento meticuloso de los cambios en los archivos a lo largo del tiempo, lo que permite descubrir de manera eficaz los daños en los datos, incluso por parte de las amenazas cibernéticas más sofisticadas.

Análisis de contenido completo

CyberSense es el único producto en el mercado que ofrece indexación de contenido completo y análisis sobre todos los datos protegidos. El análisis profundo de IA de CyberSense abarca la totalidad de los datos y genera una decisión probabilística con una precisión del 99,99 %* en cuanto a si los datos tienen integridad o si han sido dañados por ransomware. Esta funcionalidad distingue a CyberSense de otras soluciones que adoptan una vista general de los datos y utilizan análisis que buscan signos evidentes de corrupción en función de los metadatos. Los daños en el nivel de metadatos no son difíciles de detectar; por ejemplo, cambiar una extensión de archivo a .encrypted o cambiar radicalmente el tamaño del archivo. Estos tipos de ataques no representan los ataques sofisticados que los delincuentes cibernéticos utilizan en la actualidad.



CyberSense va más allá de las soluciones que solo se basan en metadatos y detecta daños en los datos mediante análisis de contenido completo. Audita archivos y bases de datos en busca de cambios que indiquen un ataque, incluida la corrupción total o parcial de archivos. El análisis tradicional omite estas amenazas, lo que genera una falsa confianza. Las alertas de umbral personalizadas se pueden configurar en función de los cambios en los archivos, los archivos agregados o los archivos eliminados. Las reglas personalizadas de YARA y las firmas de malware también se pueden implementar para la detección de malware tanto hacia delante como hacia atrás en los respaldos.

Tipos de datos compatibles

CyberSense genera análisis a partir de una amplia variedad de tipos de datos. Entre ellos se incluye infraestructura central como DNS, LDAP, Active Directory, archivos no estructurados como documentos, contratos, propiedad intelectual y bases de datos como Oracle, DB2, SQL, PostgreSQL, Epic Caché, etc.

Resumen

CyberSense, completamente integrado con Dell PowerProtect Cyber Recovery, analiza sus datos de vault y detecta indicadores de comportamiento de compromiso y daños. CyberSense le permite comprender proactivamente el radio de efecto de un ataque cibernético en curso y facilitar la implementación de un plan para diagnosticar y recuperarse rápidamente a fin de mitigar la interrupción del negocio y los costos significativos asociados.

Obtenga más información sobre Dell PowerProtect Cyber Recovery

Póngase en contacto con un experto de Dell Technologies

Más información sobre CyberSense

Únase a la conversación con #PowerProtect

* Información basada en un informe de ESG encargado por Index Engines, “CyberSense de Index Engines demostró una eficacia del 99,99 % en la detección de daños causados por ransomware”. Junio de 2024