Resumen de la solución

# CyberSense® para Dell PowerProtect Cyber Recovery

Análisis basados en IA y herramientas forenses para detectar, diagnosticar y recuperarse de forma más inteligente de ciberataques

## LA VENTAJA DE CYBERSENSE

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

- Automatiza el análisis periódico de los datos de copia de seguridad para validar la integridad de los datos y alertar cuando se detecta un comportamiento sospechoso.
- Analice directamente el contenido de las imágenes de copia de seguridad de Dell Avamar, NetWorker, Commvault, NetBackup y PowerProtect Data Manager sin necesidad de rehidratar los datos.
- Ofrece análisis exhaustivos de contenido completo con cada análisis de datos para detectar incluso los ataques de ransomware más sofisticados.
- Personalice alertas para reglas de YARA y firmas de malware para detectar comportamientos conocidos de ransomware o atacantes internos.
- Facilite un proceso de recuperación más rápido e inteligente mediante informes forenses después del ataque para conocer su alcance, así como una lista de los últimos conjuntos de copias de seguridad correctas previas a la corrupción de datos.

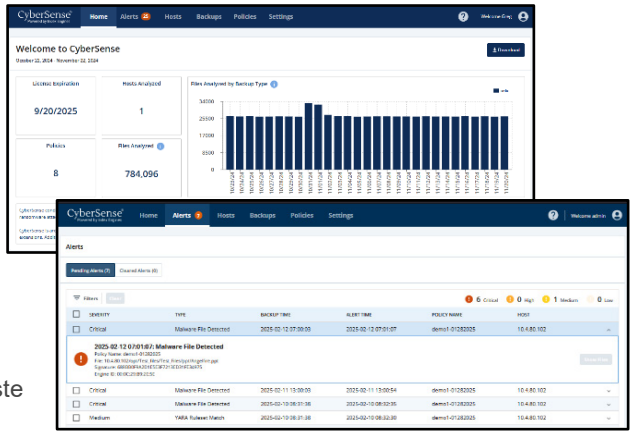
***CyberSense se diferencia de otros enfoques de análisis de datos y proporciona una mayor confianza en la integridad de los datos de copia de seguridad y su rápida recuperación tras un ataque.***

A medida que la frecuencia de los ciberataques continúa aumentando y los ciberdelincuentes se vuelven más resilientes, las herramientas de seguridad convencionales no son suficientes para proteger los datos contra ellos.

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

CyberSense analiza las copias de seguridad de datos en un vault de Cyber Recovery para observar cómo cambian los datos con el tiempo. A continuación, 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 el contenido para identificar corrupción con un 99,99 % de confianza*, lo que ayuda a proteger la infraestructura y el contenido críticos para la empresa. CyberSense detecta eliminaciones masivas, cifrado y otros cambios sospechosos en la infraestructura principal (incluidos Active Directory, DNS, etc.), repositorios de archivos, sistemas de archivos y bases de datos críticas como consecuencia de ataques sofisticados.

Cuando se produce un comportamiento sospechoso, CyberSense proporciona informes forenses tras el ataque para diagnosticar el radio de impacto. Cuando se detectan daños en los datos, se ofrece una lista de los últimos datos de copia de seguridad correctos conocidos para lograr recuperaciones rápidas y organizadas que minimizan las interrupciones comerciales y la pérdida de datos, y reducen el coste de Cyber Recovery.

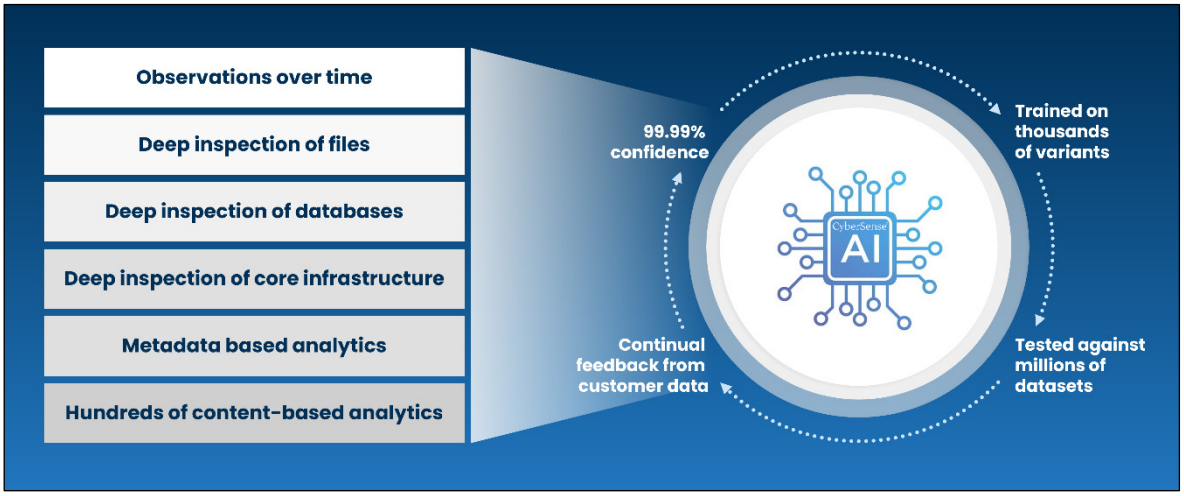



## El flujo de trabajo de Cyber Recovery

CyberSense se integra sin problemas con Dell PowerProtect Cyber Recovery, ya que supervisa activamente los archivos y las bases de datos para detectar corrupción por ransomware mediante el análisis de la integridad de los datos. Una vez que se replican los datos en el vault de Cyber Recovery y se aplica el bloqueo de retención, CyberSense inicia automáticamente un análisis exhaustivo de los datos de copia de seguridad y crea observaciones de un punto en el tiempo de los archivos, bases de datos e infraestructura principal. CyberSense hace un seguimiento meticuloso de los cambios que se producen en los archivos a lo largo del tiempo, con lo que detecta eficazmente la corrupción de datos, incluso por parte de las ciberamenazas más sofisticadas.

## Análisis del contenido completo

CyberSense es el único producto del mercado que ofrece indexación y análisis de contenido completo de todos los datos protegidos. El análisis profundo con IA de CyberSense se ejecuta en la totalidad de los datos y se genera una decisión probabilística con un 99,99 % de precisión* que confirma la integridad de los datos o si han sido dañados por ransomware. Esta capacidad distingue a CyberSense de otras soluciones que adoptan una vista de alto nivel de los datos y utilizan análisis que buscan signos evidentes de corrupción en función de los metadatos. La corrupción a nivel de metadatos no es difícil de detectar. Por ejemplo, cambiar la extensión de un archivo a .encrypted o cambiar radicalmente el tamaño del archivo. Este tipo de ataques no representan los ataques sofisticados que los ciberdelincuentes utilizan hoy en día.




CyberSense va más allá de las soluciones basadas únicamente en metadatos y detecta si los datos han sido dañados mediante análisis de contenido completo. Audita los archivos y las bases de datos para detectar cambios que indiquen un ataque, lo que incluye el daño total o parcial de los archivos. Los análisis tradicionales omiten estas amenazas, lo que genera una falsa confianza. Las alertas personalizadas asociadas a los umbrales se pueden establecer en función de los cambios en los archivos, los archivos añadidos o los archivos eliminados. Las reglas personalizadas de YARA y las firmas de malware también se pueden implementar tanto para la detección hacia adelante como hacia atrás de malware en copias de seguridad.

## Tipos de datos compatibles

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

## Resumen

CyberSense, completamente integrado con Dell PowerProtect Cyber Recovery, analiza los datos de su vault y detecta indicadores de comportamiento de riesgo y corrupción. CyberSense le permite comprender proactivamente el radio de impacto de un ciberataque en curso y facilitar la implementación de un plan para diagnosticar y recuperarse rápidamente. Así se mitigan las interrupciones comerciales y los considerables costes asociados.

| | | | |
|---|---|---|---|
| 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 |

* Datos basados en el informe "Index Engines' CyberSense Validated 99.99% Effective in Detecting Ransomware Corruption" de ESG y encargado por Index Engines. Junio de 2024.



DELL Technologies