DELL EMC
DATA PROTECTION SOLUTIONS

Cyber Recovery:

Enfrentando el reto del siglo 21

Oscar.Lozano@dell.com
+57 317 640 2034
Data Center Channel Leader

DELL Technologies

Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we´ll restart for you.

92% complete

For more information about this issue and posible fixes, visit our website

If you call a support partner, give them this info:

Stop code: 0x0000000

You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with a military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

1. Download the TOR Browser at "https://www.torporject.org/". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

http://petya37h5tbjvsu.onion/N12fvE
http://petya5dsdgdg7ej.onion/N12fvE

1. Enter your personal decryption code there:

https://pety35sdd424fk5.onion/N12fvE

If you already purchased your key, please enter it bellow.

Key: _

DELL EMC
DATA PROTECTION SOLUTIONS

Cyber Recovery:

Enfrentando el reto del siglo 21

Oscar.Lozano@dell.com
+57 317 640 2034
Data Center Channel Leader

DELL Technologies

Los ataques cibernéticos son titulares diarios

Forbes

CYBERSECURITY • EDITORS' PICK

Cisco Hacked: Ransomware Gang Claims It Has 2.8GB Of Data

Davey Winder Senior Contributor
Co-founder, Straight Talking Cyber

Follow

Aug 11, 2022, 04:46am EDT

Sierra Wireless Recovering from Ransomware Attack; Announces Resumption of Production

March 26, 2021 07:00 AM Eastern Daylight Time

GTA

Peel District School Board struggles with fallout from malware attack, leaving parents, teachers in the dark

Incident Of The Week: Garmin Pays $10 Million To Ransomware Hackers Who Rendered Systems Useless

It is believed that Garmin paid the $10 million ransom.

JWN Energy

Colonial Pipeline sued for gas crisis from ransomware attack

30 mins ago

Toronto's Humber River Hospital hit by ransomware

HOWARD SOLOMON JUNE 15, 2021

Classes cancelled and online systems down as GBC grapples with suspected malware infection

News Candice Zhang June 14, 2021

Exagrid pays $2.6m to Conti ransomware attackers

Backup appliance specialist hit by Conti ransomware in May with cyber criminals downloading employee and customer data, confidential contracts and source code

By **Valéry Marchive,** Rédacteur en chef | **Antony Adshead,** Storage Editor

Published: **01 Jun 2021 13:00**

“Los ataques cibernéticos son el crimen de más rápido crecimiento a nivel mundial, y están aumentando en tamaño, sofisticación y costo.”

El número promedio de días que dura un incidente de ransomware ahora es de 16.2 días, frente a los 12.1 días en el tercer trimestre de 2019.
Coveware

El ciclo de vida de la violación de datos (identificar -> contener una violación) es de 279 días
Ponemon Institute / IBM

El costo total del delito cibernético para cada empresa aumentó en un 12% de $ 11.7 millones en 2017 a $ 13.0 millones en 2018
Accenture

Se proyecta que el daño relacionado con el delito cibernético costó $ 21 mil millones anuales en el 2021
Cybersecurity Ventures / Herjavec Group

El 71% de las infracciones fueron motivadas financieramente y el 25% fueron motivadas por el espionaje.
Verizon

Los hackers atacan cada 11 segundos, en promedio 6000 veces al día
University of Maryland

El 52% de las infracciones presentaban piratería, el 28% involucraba malware y el 32-33% incluía phishing o ingeniería social, respectivamente.
Verizon

29.6% RIESGO de verse afectado por una violación de seguridad en los próximos 2 años
Ponemon Institute / IBM Security

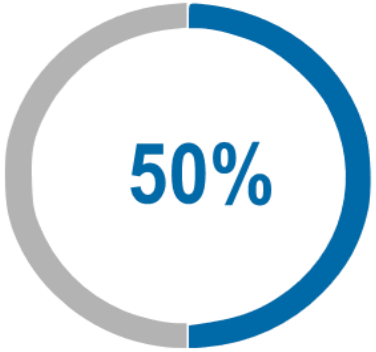
Re.si.lien.cia

[https://dle.rae.es/resiliencia]

- *Del ingl. resilience, y este der. del lat. resiliens, -entis, part. pres. act. de resilīre 'saltar hacia atrás, rebotar', 'replegarse'.*
- 1. f. Capacidad de adaptación de un ser vivo frente a un agente perturbador o un estado o situación adversos.
- 2. f. Capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido.

Por qué es tan importante la Ciber Resiliencia?

Principales retos para los responsables de Ciber Seguridad según el World Economic Forum

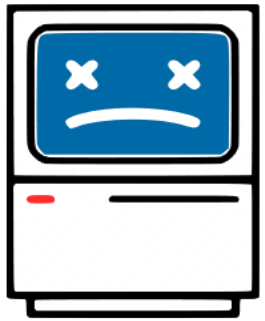


GREATER CONNECTIVITY

5G

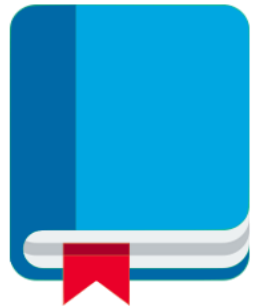
NEW TECHNOLOGY =
NEW THREATS

INCREASE IN
RANSOMWARE ATTACKS



ATTACKS ON CRITICAL
TECHNOLOGY

OUTDATED TECHNOLOGY



LACK OF TRAINING

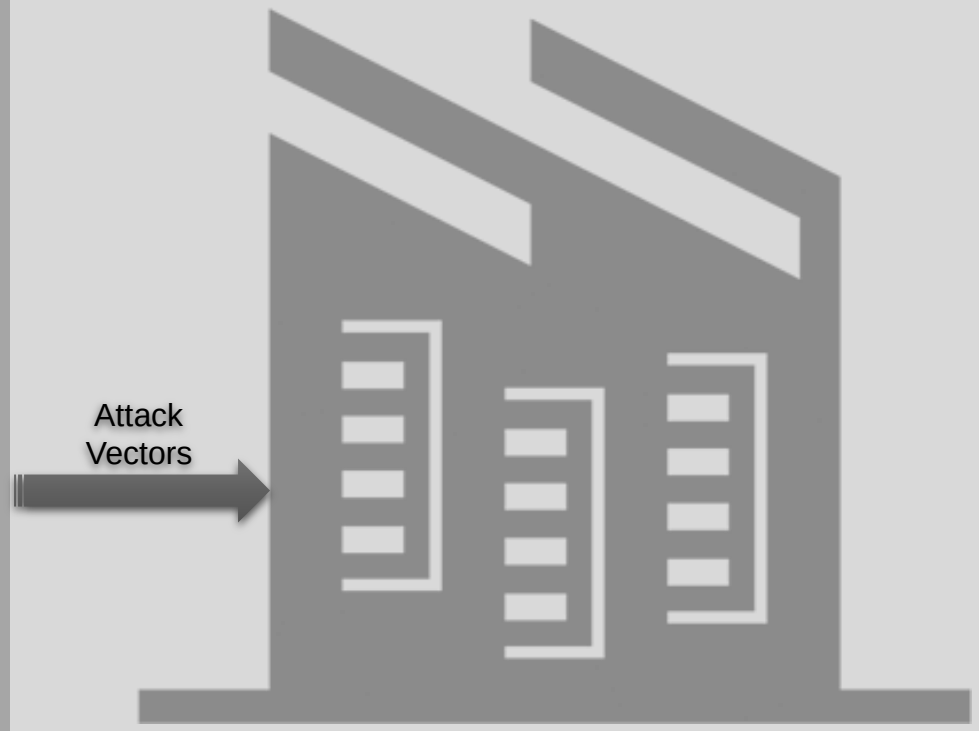
Protección Real-Time Ransomware : Esencial pero puede ser derrotado

Vectores de ataque

Vectores de ataque

Vectores de ataque

Protección contra malware en tiempo real y análisis de comportamiento



La protección en tiempo real no es 100% efectiva.

Algunos ataques penetran en estas defensas y corrompen los datos con el tiempo.

Russia/Ukraine Crisis

Guía Internacional de Ciberseguridad

Asegúrese que todos sepan cómo informar sobre eventos de seguridad sospechosos y por qué es tan importante

Asegúrese de que el SW en todos los dispositivos esté actualizado, los sistemas empresariales estén parcheados

Asegúrese de que todos sepan cómo denunciar correos electrónicos de phishing

Asegúrese de que el software antivirus y el firewall estén instalados y verifique la actividad regularmente

Asegúrese de que las contraseñas sean seguras y únicas, habilite la autenticación multifactor (MFA)

Asegúrese de que las copias de seguridad eficaces y seguras estén en su lugar y que funcionen correctamente

Verifique que su plan de respuesta a incidentes esté actualizado

Compruebe que los registros de su huella a Internet sean correctos y estén actualizados

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

SANS

National Cyber Security Centre

National Cyber Security Centre

CISA CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

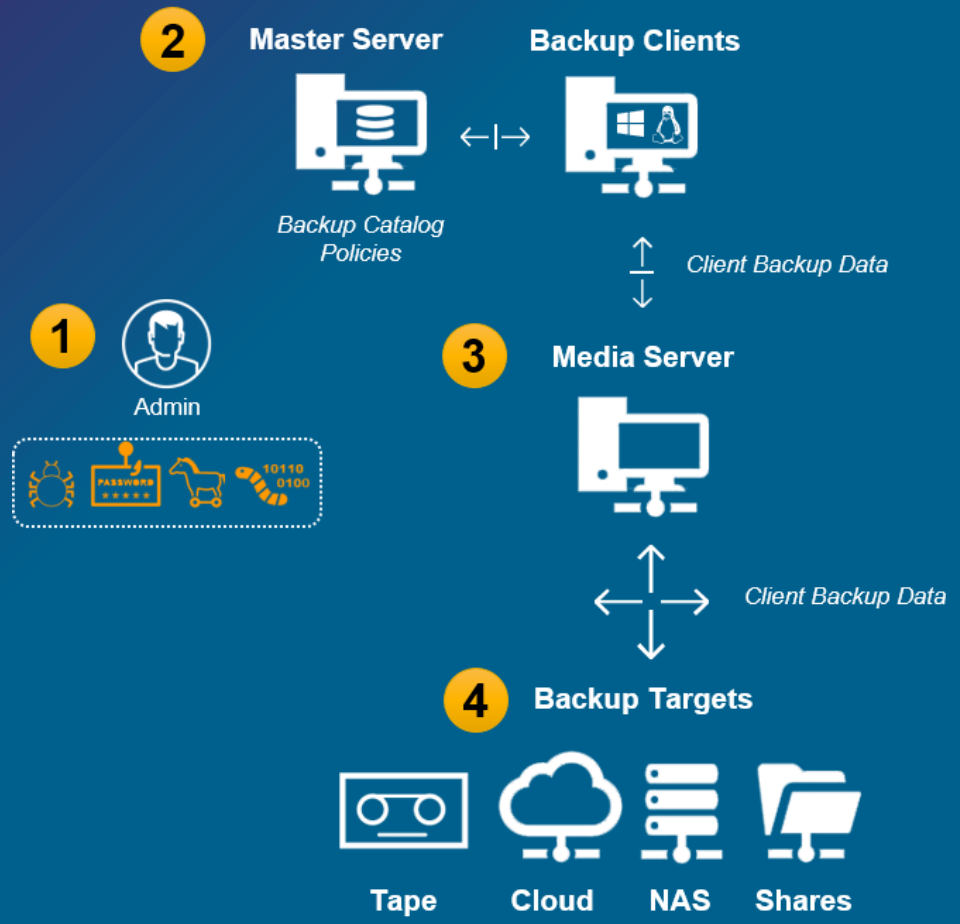
Australian Government Australian Signals Directorate

ACSC Australian Cyber Security Centre

CANADIAN CENTRE FOR CYBER SECURITY

DELL Technologies

Los ataques de Ransomware están apuntando a la infraestructura de Backups.



1. **Los administradores de TI y backup son los principales objetivos de compromiso**

2. **Master Server (Backup Catalog):** El servidor maestro de copia de seguridad está dirigido e infectado, lo que resulta en un catálogo de copia de seguridad cifrado/borrado o en la expiración de la directiva prematura

3. **Media Server:** Todos los sistemas de archivos montados en el servidor de medios son objetivo de cifrados/borrados

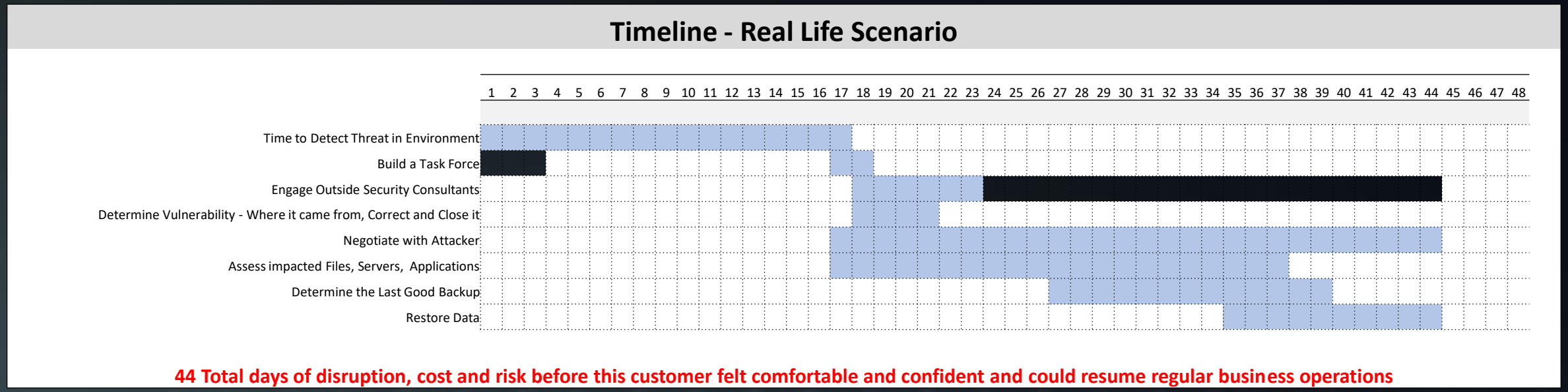
4. **Backup Targets:**

   Disco / NAS: Los sistemas de archivos en el servidor de medios son objetivo de cifrados / borrados. Los repositorios de copia de seguridad pueden cifrarse / borrarse de los recursos compartidos de archivos de red de rastreo de ransomware

   Cinta: proporciona una mejor oportunidad de recuperarse del evento destructivo si la amenaza se eliminó del entorno antes del ataque. Sin embargo, si el catálogo de backup se mantiene como rehén o se destruye, la recuperación de la cinta será cada vez más difícil.

   Nube: La nube de uso general o pública ofrece la ventaja de la protección remota, pero son inherentemente menos seguras debido a la dependencia de Internet (siempre encendida) o redes inseguras, dejando expuestos los datos, las copias de seguridad y los catálogos.

Cronología del cliente - Evento de ransomware



Puntos clave de resumen:

- Los hackers estuvieron en el entorno durante 17 días antes de ser detectados
- Se contrataron costosos consultores externos para ayudar a remediar el ataque cibernético
- El impacto en la organización es peor cuanto más tiempo la amenaza cibernética está en el entorno y pasa desapercibida
- Conversación y negociación continuas del cliente con el hacker cibernético para minimizar el daño adicional

Conceptos erróneos comunes hoy en día

Protección/recuperación limitada contra ataques destructivos o de ransomware

Cifrado de datos

- No hay protección para ataques destructivos o de ransomware
- Para la protección de datos, no para la recuperación

Más seguridad

- No puede tener éxito siempre
- Considere la amenaza interna, el phishing de credenciales, el error humano y la complejidad del sistema

DR tradicional

- Las copias de seguridad son atacadas
- La replicación propaga el problema

Backups en cinta

- Semanas para recuperarse a medida que aumentan las pérdidas cada día
- Los catálogos están expuestos y se pueden eliminar
- Los datos contaminados se pueden escribir en cinta sin visibilidad

"Copias inmutables"

- El bloqueo de retención en producción es una opción cuestionable para ransomware
- Cada sistema en producción es un objetivo
- La "inmutabilidad" a menudo tiene anulaciones de administración que pueden ser explotadas

La única defensa es mantener copias de seguridad sin conexión

"Una arquitectura de copia de seguridad de datos con espacio de aire…"

"Confidencialidad, integridad, disponibilidad y resiliencia"

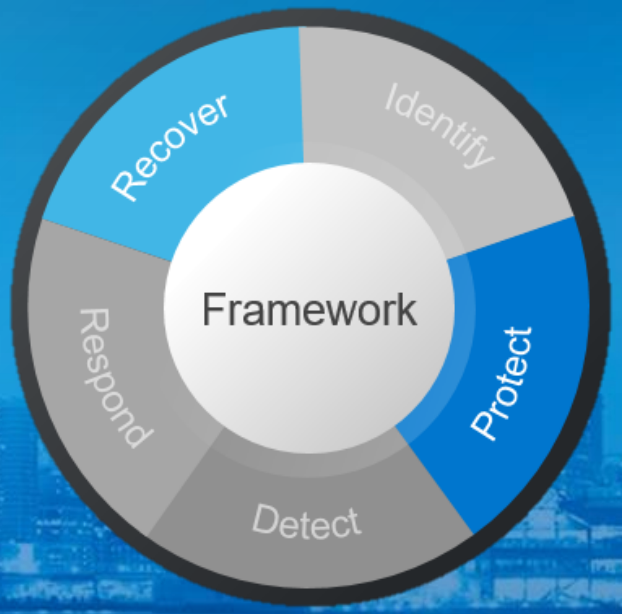
"Considere la posibilidad de mantener las copias de seguridad sin conexión y no disponibles"

"Asegúrarse de que las copias de seguridad no estén conectadas a las redes de las que están realizando copias de seguridad."

Solución Cyber Recovery

DELL Technologies

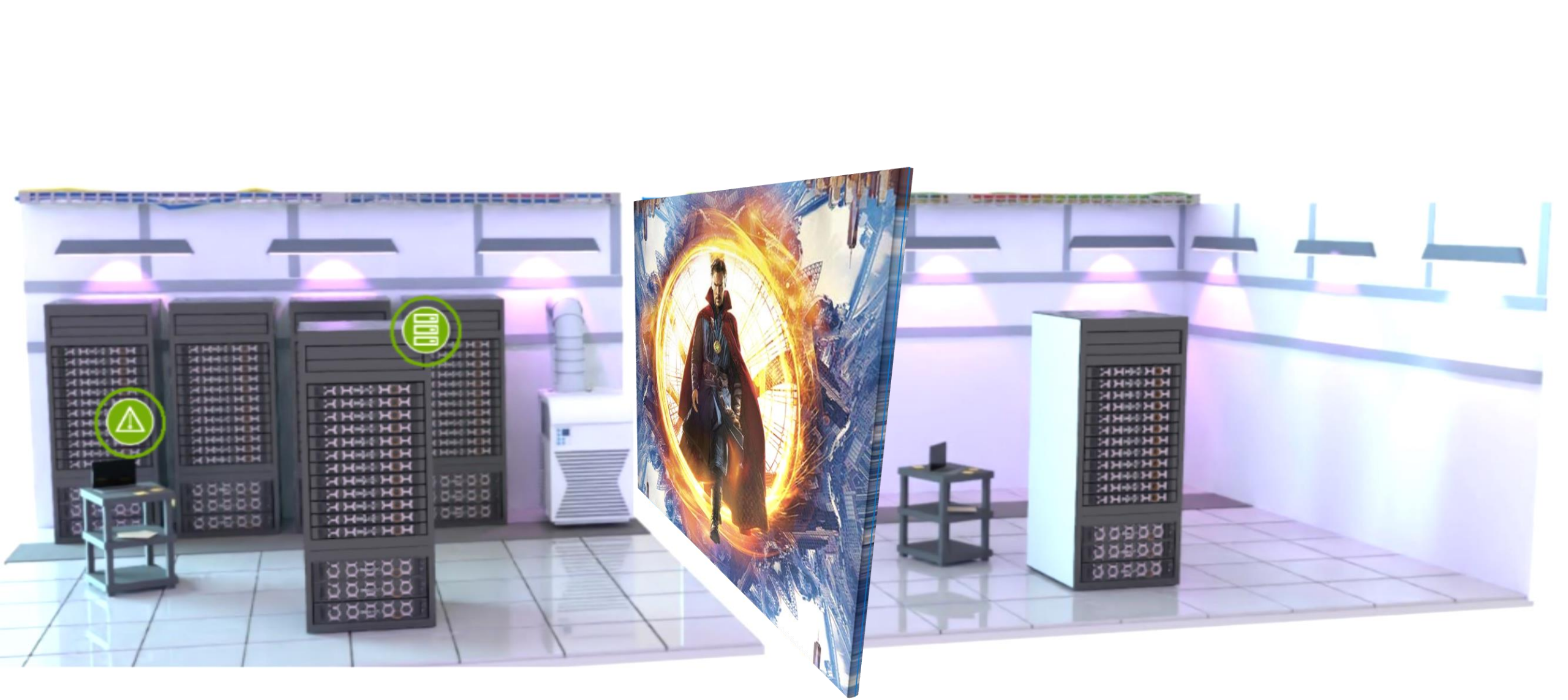
Cyber Recovery



Una solución de protección de datos que aísla los datos críticos para el negocio de las superficies de ataque. Los datos críticos se almacenan inmutablemente en una bóveda reforzada que permite la recuperación con disponibilidad, integridad y confidencialidad de datos garantizadas.

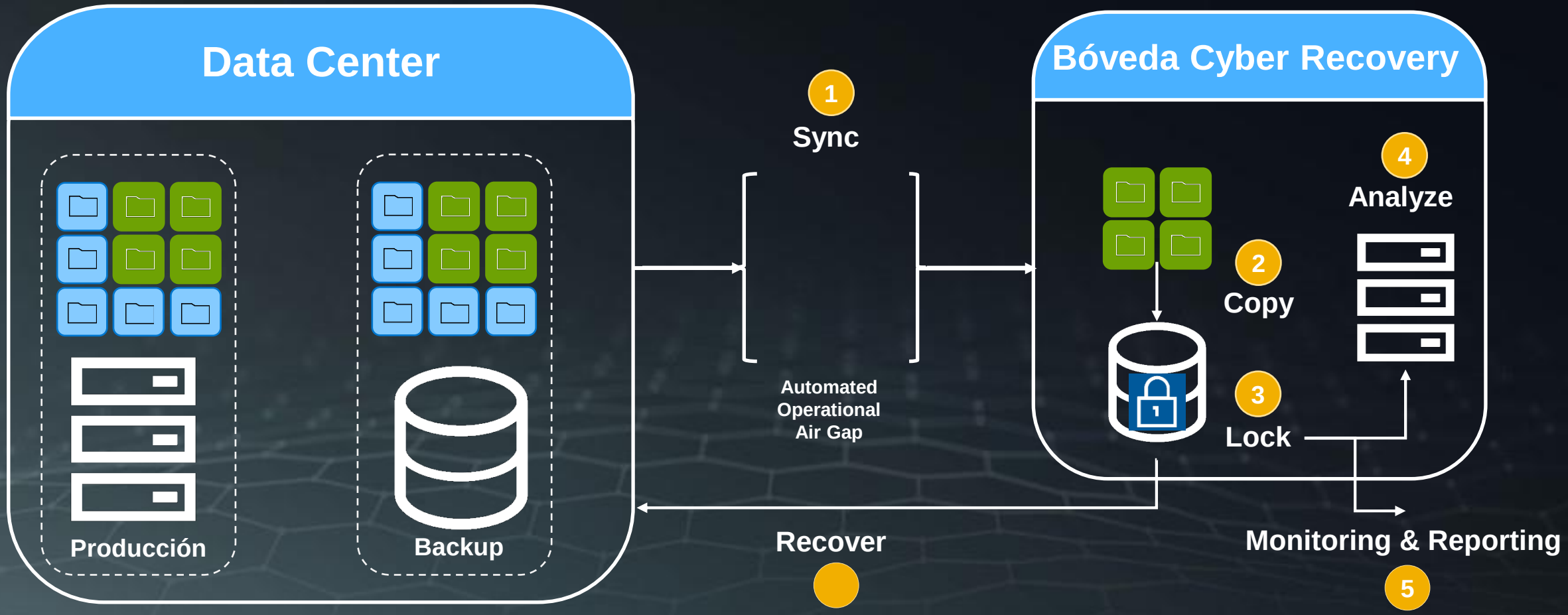
Requerimientos de Cyber Recovery

Las amenazas modernas requieren soluciones modernas

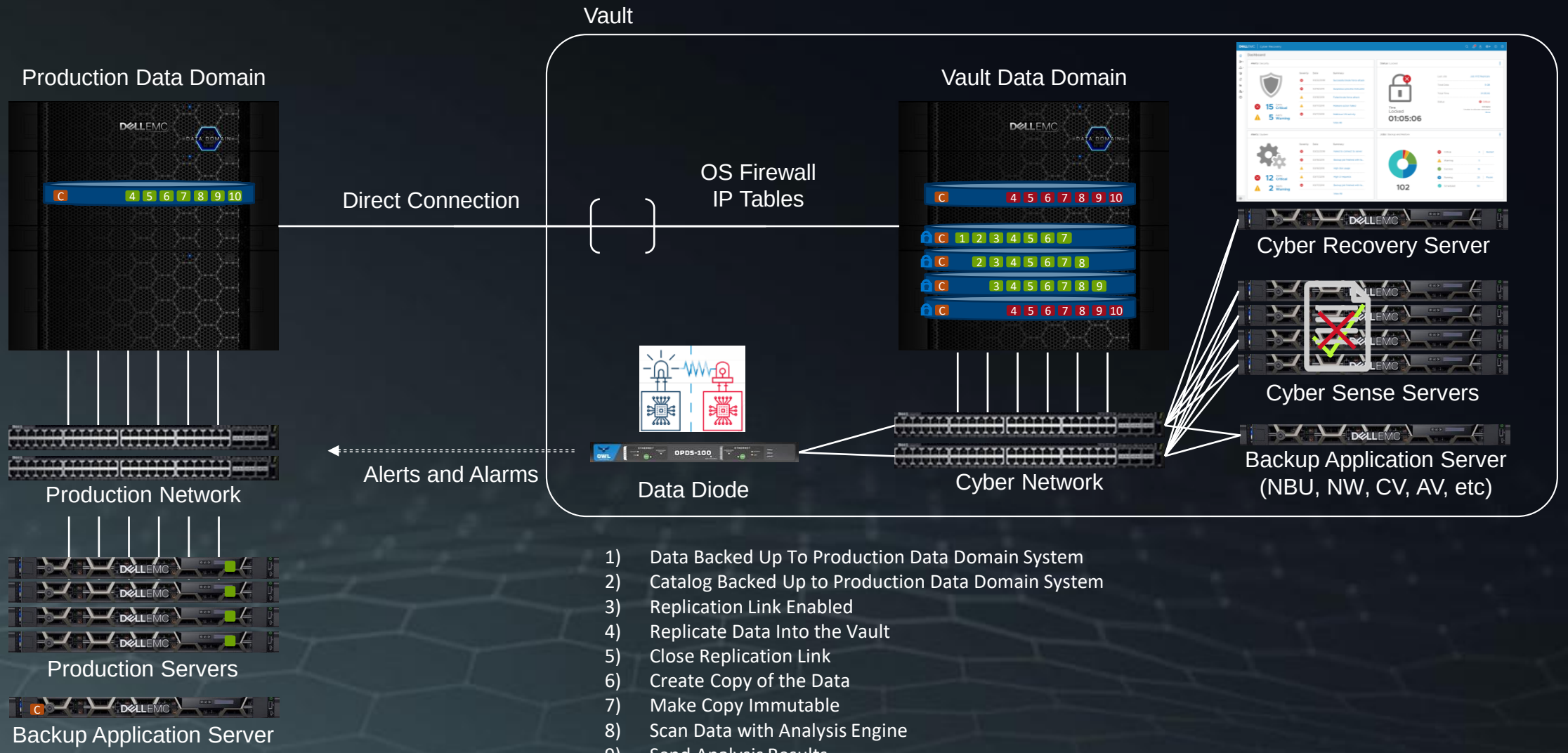


PowerProtect Cyber Recovery

Procesos de bóveda y recuperación de datos

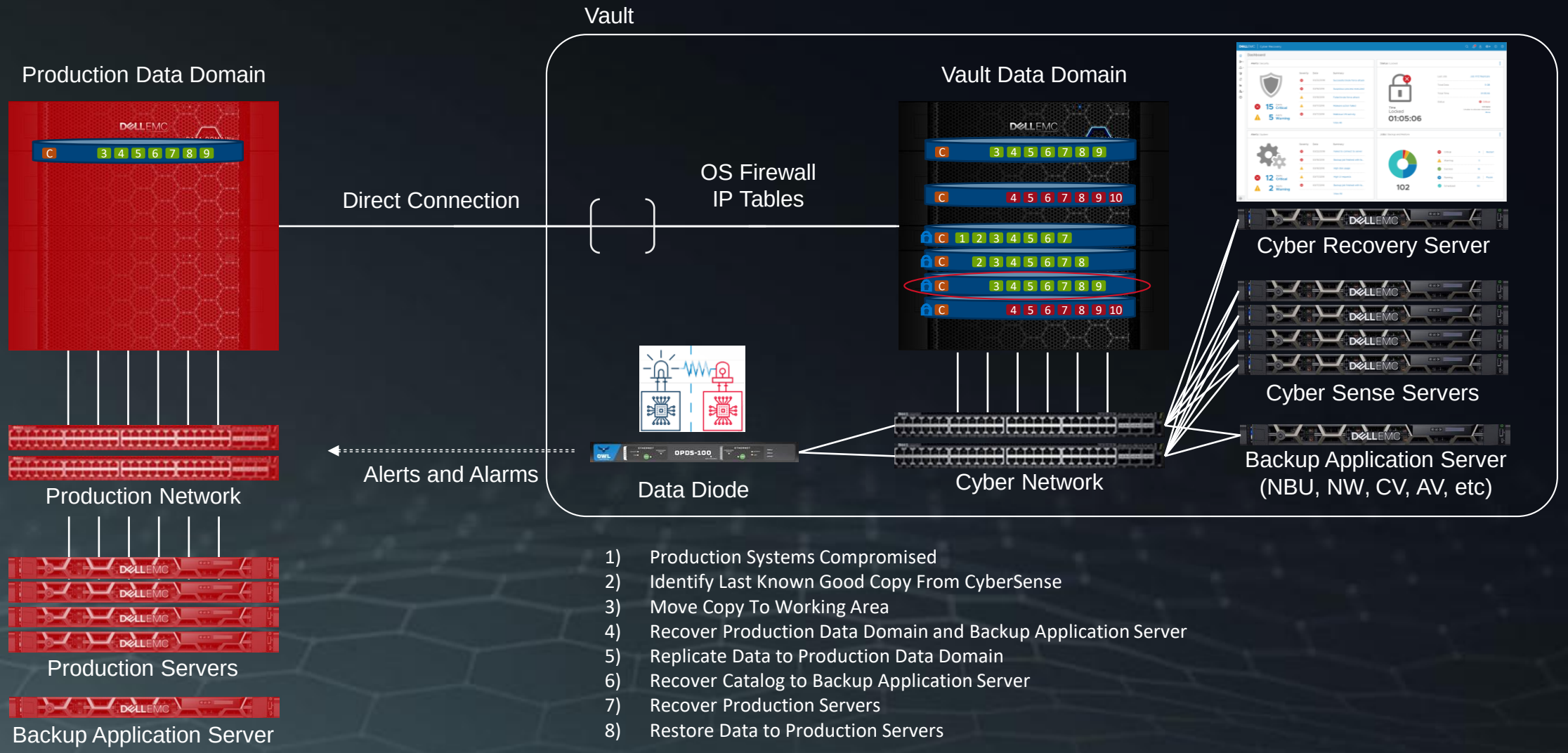


Cyber Recovery Architecture and Data Flow



1) Data Backed Up To Production Data Domain System
2) Catalog Backed Up to Production Data Domain System
3) Replication Link Enabled
4) Replicate Data Into the Vault
5) Close Replication Link
6) Create Copy of the Data
7) Make Copy Immutable
8) Scan Data with Analysis Engine
9) Send Analysis Results
10) Repeat Daily

Recovery From the Vault – Reverse Replication



1) Production Systems Compromised
2) Identify Last Known Good Copy From CyberSense
3) Move Copy To Working Area
4) Recover Production Data Domain and Backup Application Server
5) Replicate Data to Production Data Domain
6) Recover Catalog to Backup Application Server
7) Recover Production Servers
8) Restore Data to Production Servers

Analíticas con CyberSense

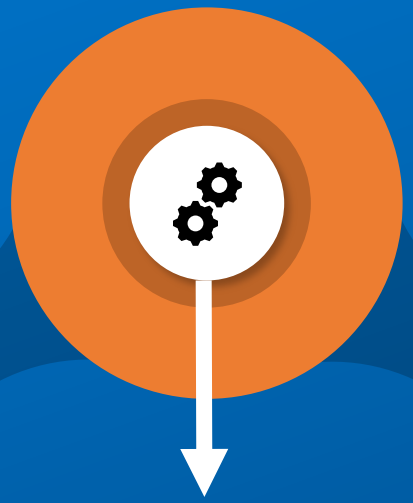
¡Recupere y restaure datos críticos validados con confianza!

Indexar

CyberSense escanea fuentes de datos críticas, incluidos archivos y bases de datos no estructurados para crear una observación. Los datos se pueden ubicar en sistemas de archivos de red o en imágenes de copia de seguridad.

Estadística

Más de 100 estadísticas generadas a partir de cada observación. Las estadísticas incluyen análisis de entropía de archivos, similitud, corrupción, eliminación / creación masiva y mucho más.



Analítica

Los algoritmos de aprendizaje automático se utilizan para analizar las estadísticas para indicar si se ha producido un ataque a los datos..

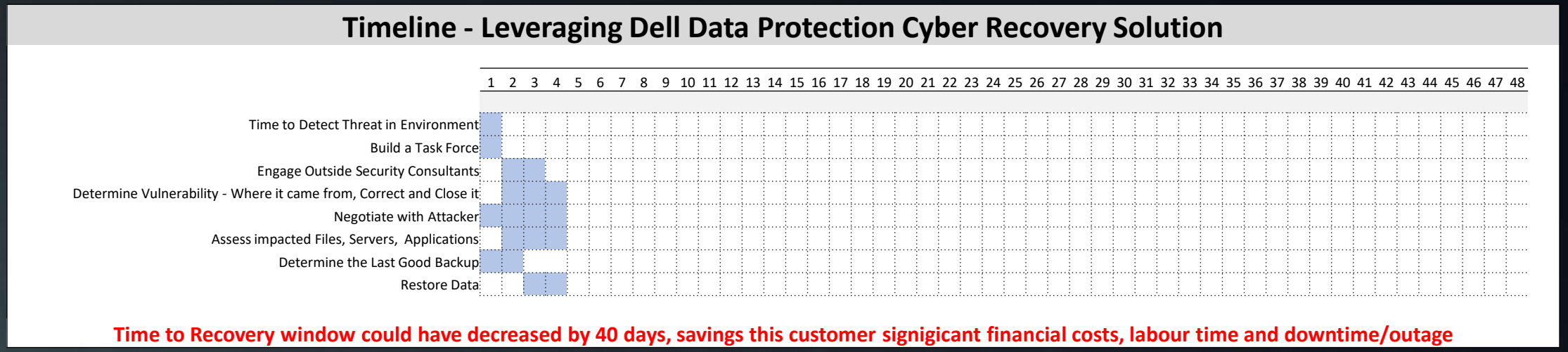
Repetir

El proceso se repite y se crea una nueva observación mediante el escaneo de datos de red o de copia de seguridad. Las nuevas observaciones se comparan con las observaciones anteriores para ver cómo cambian los datos.

Investigar

Las herramientas de informes y análisis forenses están disponibles después de un ataque para encontrar archivos dañados y diagnosticar el tipo de ransomware.

Solución DPS CR – Evento de ransomware

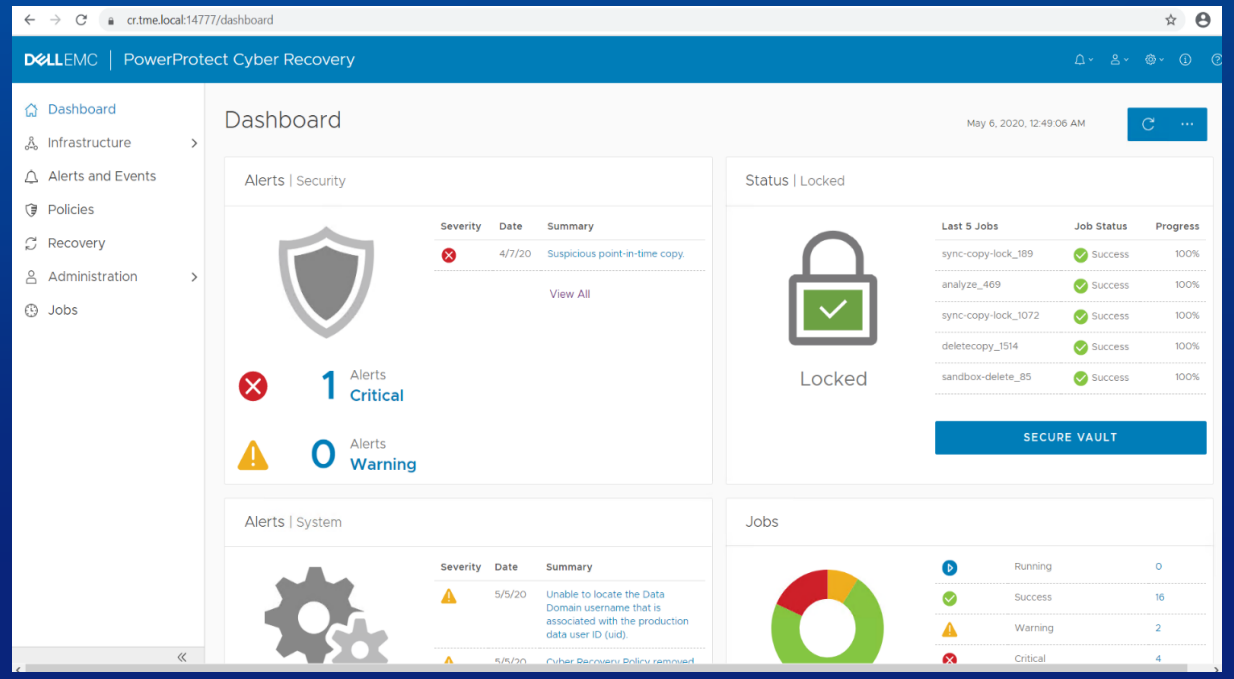


Puntos clave de resumen:

- La solución Dell EMC DPS Cyber Recovery puede detectar amenazas potenciales con cada copia de seguridad
- La capacidad de reducir el tiempo de detección minimiza el impacto de la amenaza / exposición cibernética en el medio ambiente
- Aprovechando la solución DPS Cyber Recovery podemos identificar rápidamente los archivos infectados y aislarlos
- La solución DPS le permite identificar de forma rápida y fiable la última copia de seguridad válida conocida para acelerar los esfuerzos de recuperación
- El tiempo para restaurar datos se redujo significativamente porque hay menos archivos / datos para probar y recuperar

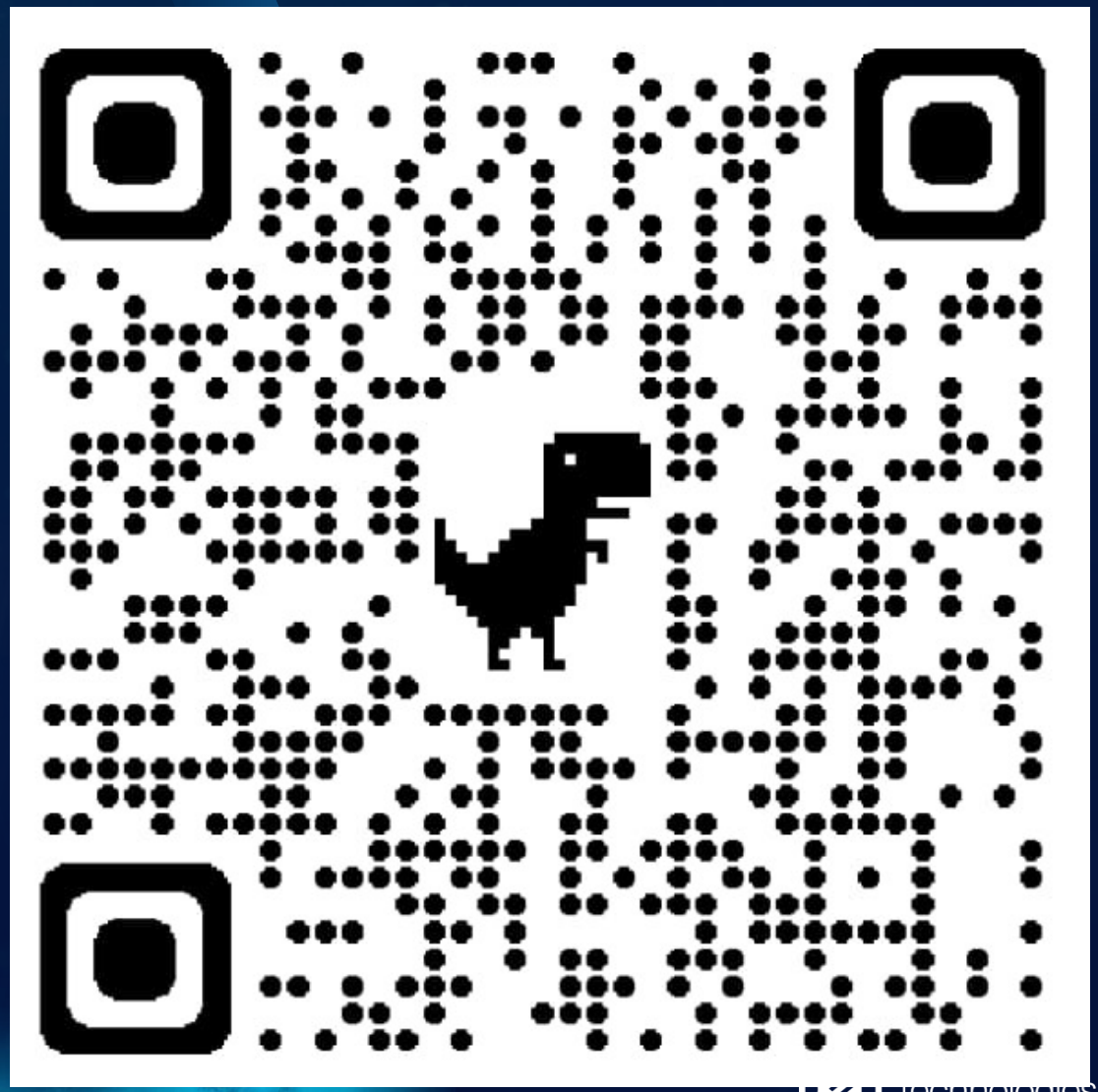
Opciones de consumo

- On-premises
- Public Cloud
- Opciones administradas y alojadas



Siguientes pasos

- Realice un auto-análisis de la robustez de su estrategia Ciber Resilencia en: https://www.dell.com/en-us/dt/data-protection/cyber-resiliency-assessment.htm
- Hagamos un dimensionamiento de una Bóveda para su entidad
- Atienda una demostración en tiempo real de la solución Cyber Recovery



¿Su organización está preparada para resistir un ataque cibernético sofisticado?

DELL Technologies

DELL EMC
DATA PROTECTION SOLUTIONS

Muchas gracias!

Oscar.Lozano@dell.com
+57 317 640 2034
Data Center Channel Leader

DELL Technologies


DELL EMC