Recovering Your Business From a Destructive Cyber Attack

Dell EMC PowerProtect Cyber Recovery

Los ciber ataques son los nuevos desastres.

Panorama de riesgos cibernéticos.

Intentos

cada

39

sec

Source: Security Magazine

verizon

71%

of breaches are financially motivated

verizon

43%

of breaches involved small business

accenture

$13M

Avg cost of Cybercrime for an organization

accenture

$5.2T

of global risk over the next 5 years

Costo promedio por Cyberataques

por Industria

Industry	Avg Cost
Banking	**$18.4M**
Utilities	**$17.8M**
Software	**$16M**
Automotive	**$15.8M**
Insurance	**$15.8M**
High Tech	**$14.7M**
Capital Markets	**$13.9M**
Energy	**$13.8M**
US Federal	**$13.7M**
Consumer Goods	**$11.9M**
Health	**$11.9M**
Retail	**$11.4M**
Life Sciences	**$10.9M**
Media	**$9.2M**
Travel	**$8.2M**
Public Sector	**$7.9M**

accenture

THREAT LANDSCAPE EVOLVING – BIZ @ RISK

71%

of breaches are financially motivated

39%

of detected malware is Ransomware (#1 variety)

93%

CAGR in Ransomware variants from 2010 to 2016

>100

Average dwell time of a cyber-attack in days

24%

Organizations satisfied with their ability to detect and investigate

92%

Organizations cannot detect cyber-attacks quickly

59%

Believe that isolating affected systems and recovering from backups should be the response to ransomware

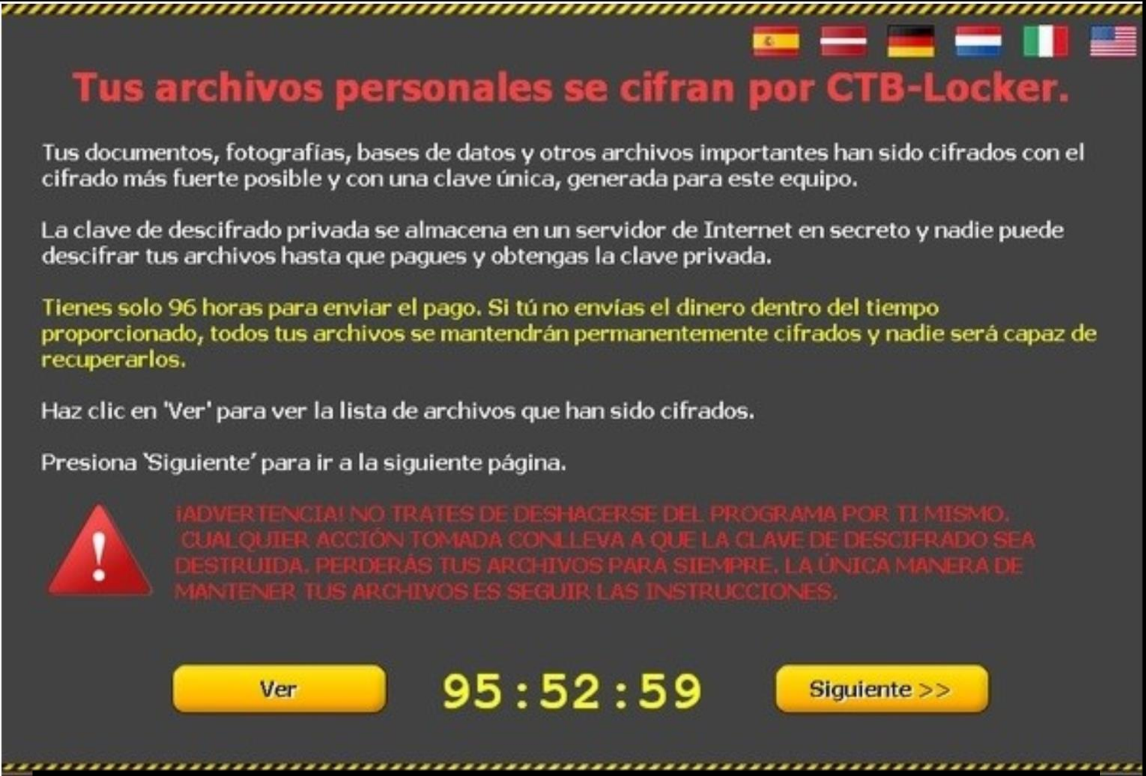
60%

CISOs actively involved in data recovery planning as part of incident response

Los riesgos cibernéticos actualmente

Cyber Threats Continue to Evolve Year after Year

- Amenazas tradicionales
  - Cyber Theft
  - Cyber Attack
    - Denial of Service
- Amenazas emergentes
  - Cyber Destruction
    - Primary and Secondary Storage
  - Cyber Extortion/Blackmail
    - Ransomware



Tus archivos personales se cifran por CTB-Locker.

Tus documentos, fotografías, bases de datos y otros archivos importantes han sido cifrados con el cifrado más fuerte posible y con una clave única, generada para este equipo.

La clave de descifrado privada se almacena en un servidor de Internet en secreto y nadie puede descifrar tus archivos hasta que pagues y obtengas la clave privada.

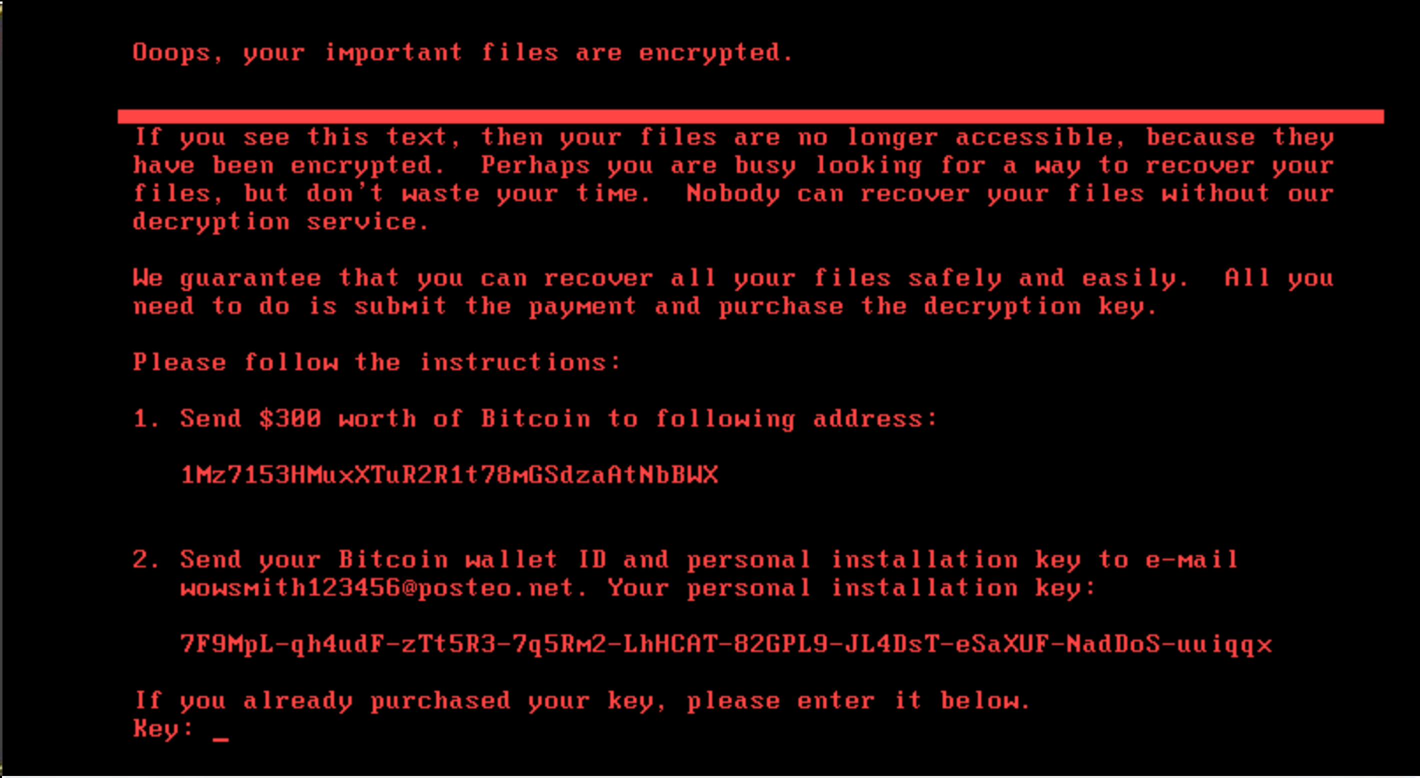
Tienes solo 96 horas para enviar el pago. Si tú no envías el dinero dentro del tiempo proporcionado, todos tus archivos se mantendrán permanentemente cifrados y nadie será capaz de recuperarlos.

Haz clic en 'Ver' para ver la lista de archivos que han sido cifrados.

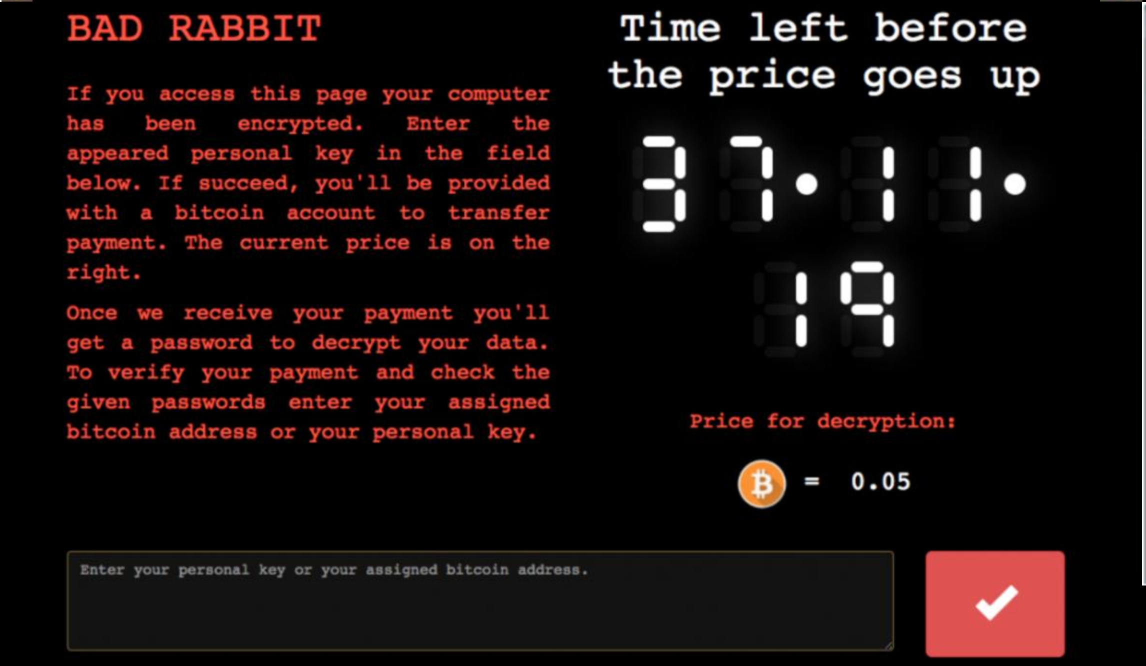
Presiona 'Siguiente' para ir a la siguiente página.

¡ADVERTENCIA! NO TRATES DE DESHACERSE DEL PROGRAMA POR TI MISMO. CUALQUIER ACCIÓN TOMADA CONLLEVA A QUE LA CLAVE DE DESCIFRADO SEA DESTRUIDA. PERDERÁS TUS ARCHIVOS PARA SIEMPRE. LA ÚNICA MANERA DE MANTENER TUS ARCHIVOS ES SEGUIR LAS INSTRUCCIONES.

95:52:59



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   7F9MpL-qh4udF-zTt5R3-7q5Rm2-LhHCAT-82GPL9-JL4DsT-eSaXUF-NadDoS-uuiqqx

If you already purchased your key, please enter it below.
Key: _
```



BAD RABBIT

If you access this page your computer has been encrypted. Enter the appeared personal key in the field below. If succeed, you'll be provided with a bitcoin account to transfer payment. The current price is on the right.

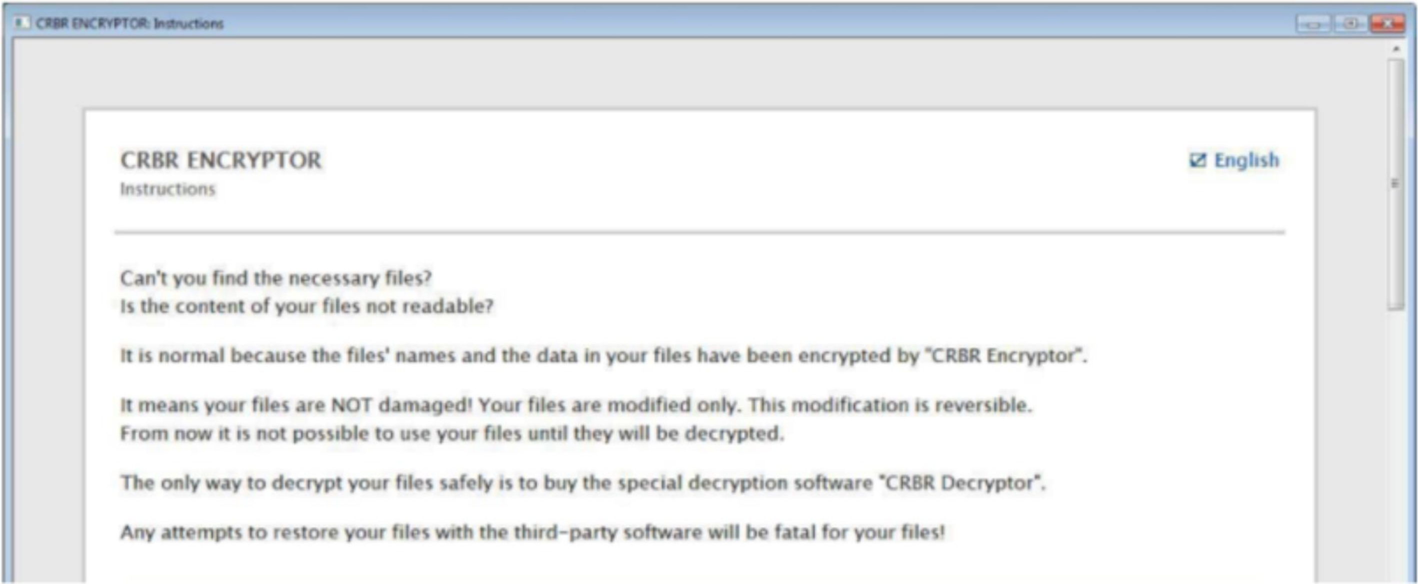
Once we receive your payment you'll get a password to decrypt your data. To verify your payment and check the given passwords enter your assigned bitcoin address or your personal key.

Time left before the price goes up

37·11·19

Price for decryption:

₿ = 0.05



CRBR ENCRYPTOR: Instructions

CRBR ENCRYPTOR

Instructions

Can't you find the necessary files?
Is the content of your files not readable?

It is normal because the files' names and the data in your files have been encrypted by "CRBR Encryptor".

It means your files are NOT damaged! Your files are modified only. This modification is reversible.
From now it is not possible to use your files until they will be decrypted.

The only way to decrypt your files safely is to buy the special decryption software "CRBR Decryptor".

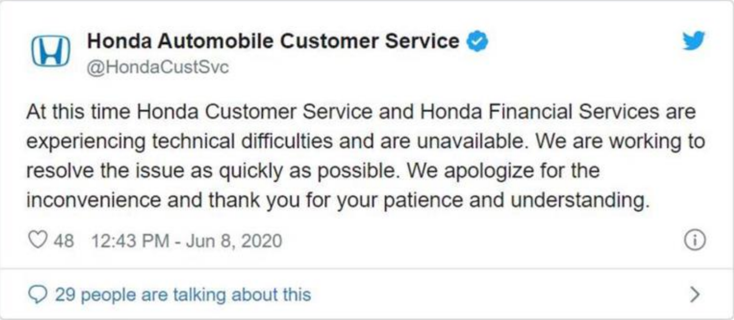
Any attempts to restore your files with the third-party software will be fatal for your files!

Honda – Manufacturing DOWN

https://techcrunch.com/2020/06/09/honda-ransomware-snake/

https://jalopnik.com/honda-seems-to-be-the-victim-of-a-ransomware-attack-1843953940

https://www-bloomberg-com.cdn.ampproject.org/c/s/www.bloomberg.com/amp/news/articles/2020-06-09/honda-suspends-vehicle-shipments-after-suspected-cyberattack

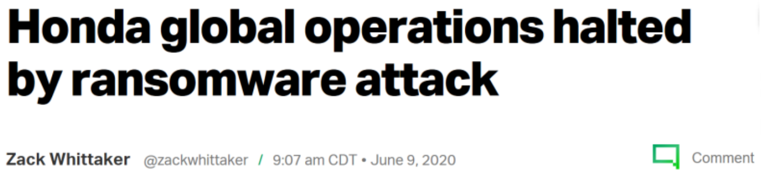


Honda Automobile Customer Service @HondaCustSvc

At this time Honda Customer Service and Honda Financial Services are experiencing technical difficulties and are unavailable. We are working to resolve the issue as quickly as possible. We apologize for the inconvenience and thank you for your patience and understanding.

♡ 48 12:43 PM - Jun 8, 2020

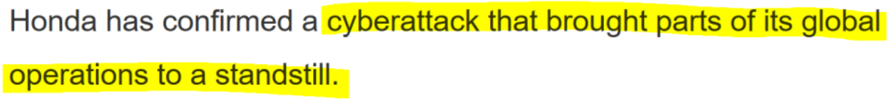
29 people are talking about this



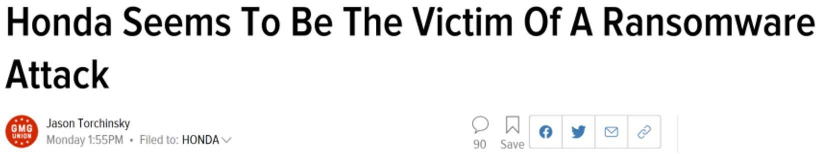
Honda global operations halted by ransomware attack

Zack Whittaker @zackwhittaker / 9:07 am CDT • June 9, 2020

Comment



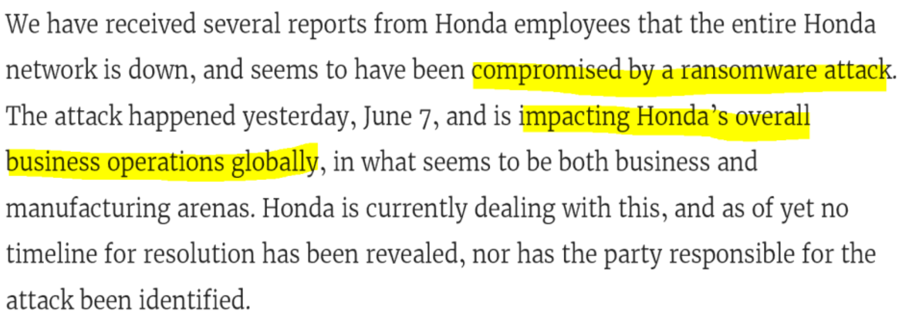
Honda has confirmed a cyberattack that brought parts of its global operations to a standstill.



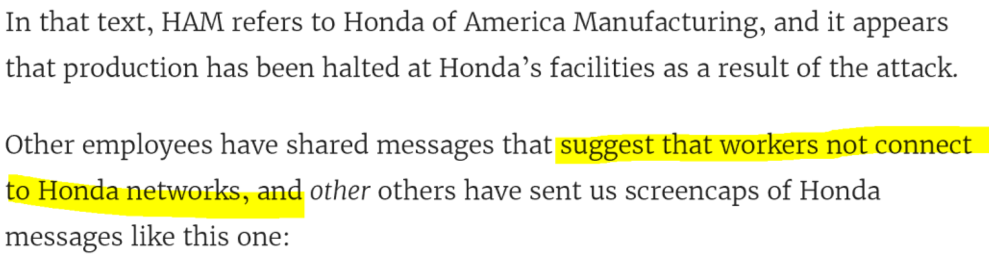
Honda Seems To Be The Victim Of A Ransomware Attack

Jason Torchinsky
Monday 1:55PM • Filed to: HONDA

90 Save

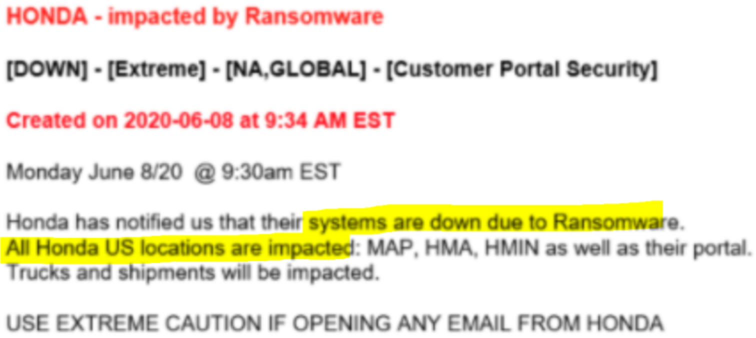


We have received several reports from Honda employees that the entire Honda network is down, and seems to have been compromised by a ransomware attack. The attack happened yesterday, June 7, and is impacting Honda's overall business operations globally, in what seems to be both business and manufacturing arenas. Honda is currently dealing with this, and as of yet no timeline for resolution has been revealed, nor has the party responsible for the attack been identified.



In that text, HAM refers to Honda of America Manufacturing, and it appears that production has been halted at Honda's facilities as a result of the attack.

Other employees have shared messages that suggest that workers not connect to Honda networks, and *other* others have sent us screencaps of Honda messages like this one:



HONDA - impacted by Ransomware

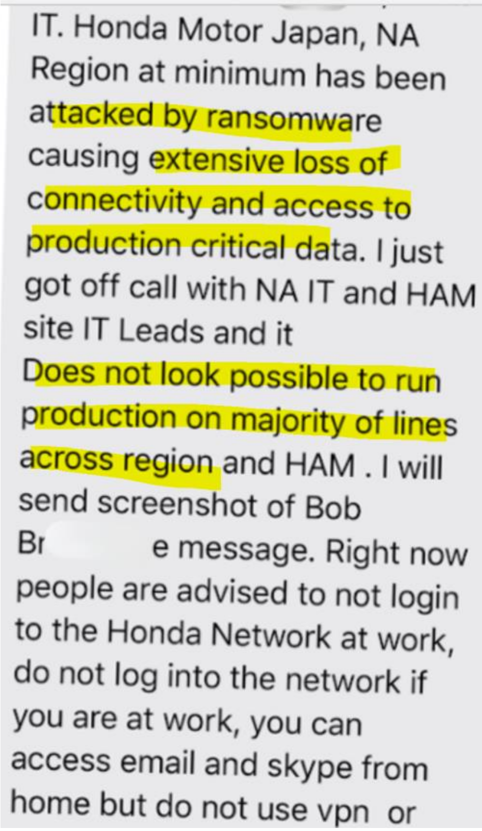
[DOWN] - [Extreme] - [NA,GLOBAL] - [Customer Portal Security]

Created on 2020-06-08 at 9:34 AM EST

Monday June 8/20 @ 9:30am EST

Honda has notified us that their systems are down due to Ransomware.
All Honda US locations are impacted: MAP, HMA, HMIN as well as their portal.
Trucks and shipments will be impacted.

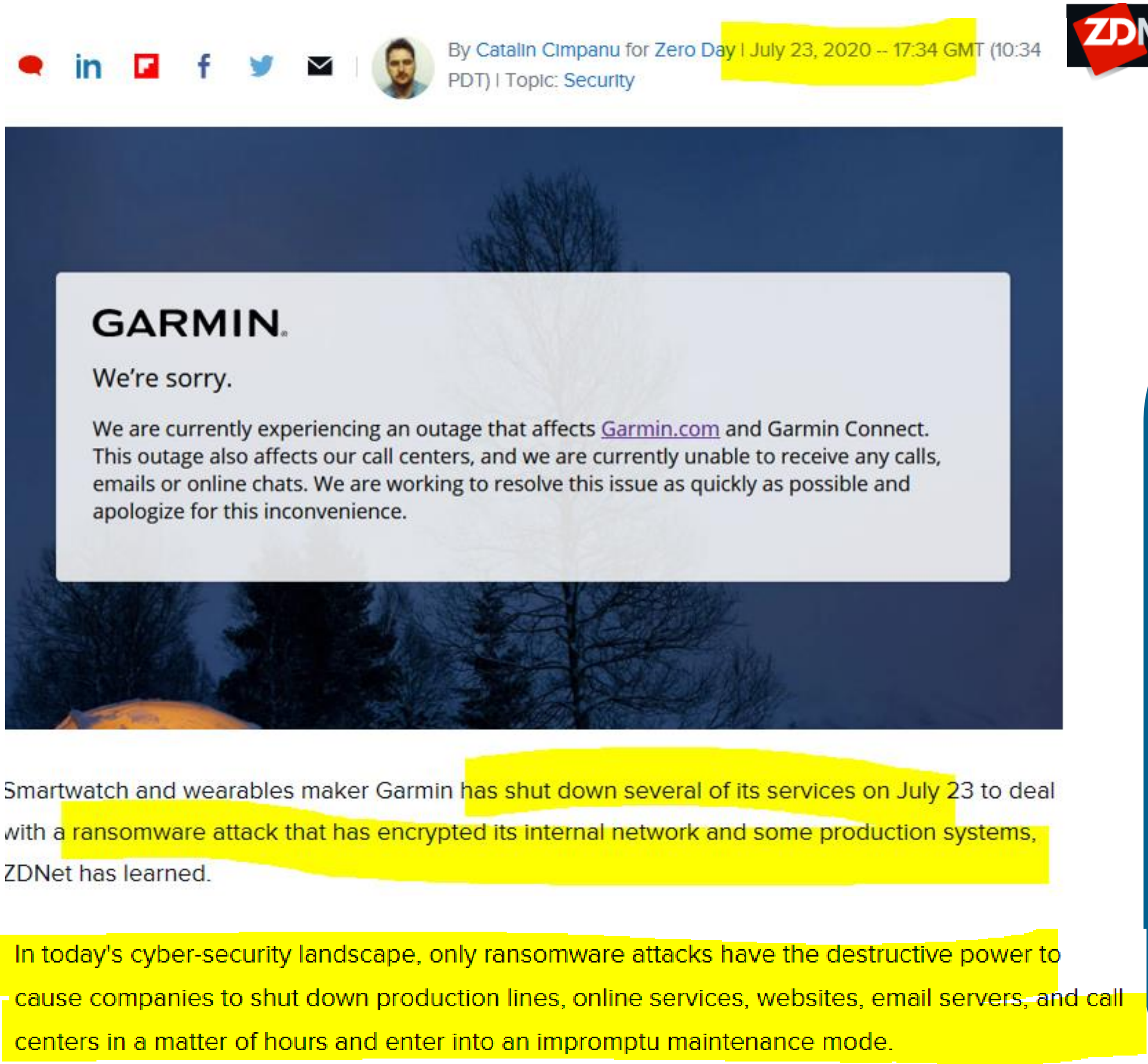
USE EXTREME CAUTION IF OPENING ANY EMAIL FROM HONDA



IT. Honda Motor Japan, NA Region at minimum has been attacked by ransomware causing extensive loss of connectivity and access to production critical data. I just got off call with NA IT and HAM site IT Leads and it Does not look possible to run production on majority of lines across region and HAM . I will send screenshot of Bob Br [redacted] e message. Right now people are advised to not login to the Honda Network at work, do not log into the network if you are at work, you can access email and skype from home but do not use vpn or

Garmin hit by Ransomware

https://www.zdnet.com/article/garmin-services-and-production-go-down-after-ransomware-attack/



By Catalin Cimpanu for Zero Day | July 23, 2020 -- 17:34 GMT (10:34 PDT) | Topic: Security

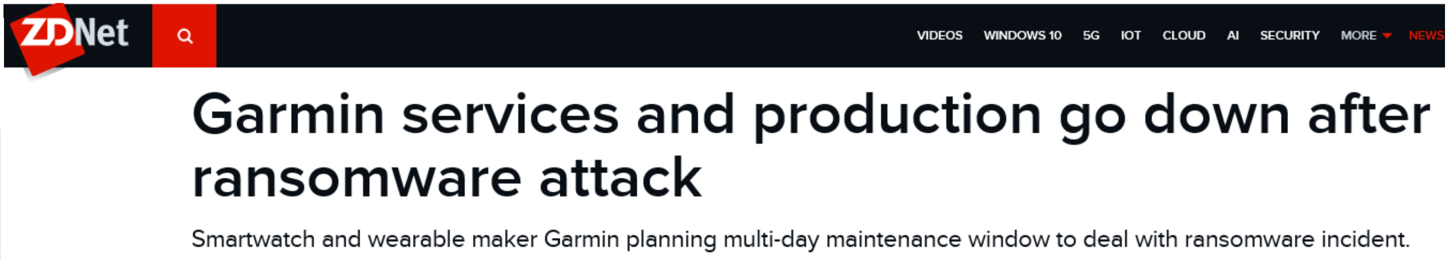
GARMIN.

We're sorry.

We are currently experiencing an outage that affects Garmin.com and Garmin Connect. This outage also affects our call centers, and we are currently unable to receive any calls, emails or online chats. We are working to resolve this issue as quickly as possible and apologize for this inconvenience.

Smartwatch and wearables maker Garmin has shut down several of its services on July 23 to deal with a ransomware attack that has encrypted its internal network and some production systems, ZDNet has learned.

In today's cyber-security landscape, only ransomware attacks have the destructive power to cause companies to shut down production lines, online services, websites, email servers, and call centers in a matter of hours and enter into an impromptu maintenance mode.



Garmin services and production go down after ransomware attack

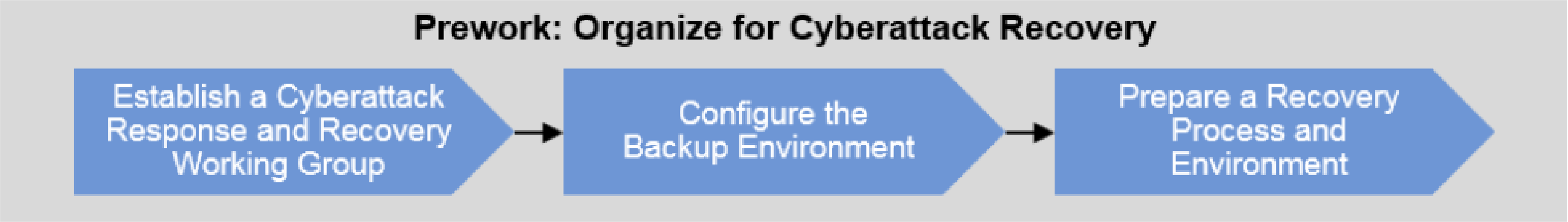
Smartwatch and wearable maker Garmin planning multi-day maintenance window to deal with ransomware incident.

Impacted Services – Financial Cost to the business?!?

- Internal network / prod systems
- Call Center – phone/email/chat DOWN
- Official website – DOWN
- Garmin Connect (global end-user service) – DOWN
- Production lines (Asia) – DOWN minimum 2 days
- Aviation Database Services – DOWN
  - Impacts pilots and is an FAA requirement
  - flyGarmin (web service) – DOWN
- Garmin Pilot App – DOWN
  - Pilot scheduling & flight plans - DOWN

Gartner
Technical Professional Advice

Backup and Recovery Best Practices for Cyberattacks



Prework: Organize for Cyberattack Recovery

Establish a Cyberattack Response and Recovery Working Group → Configure the Backup Environment → Prepare a Recovery Process and Environment

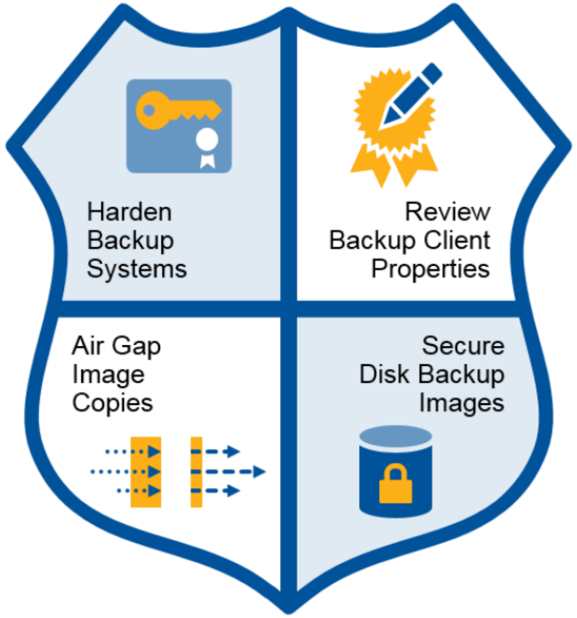
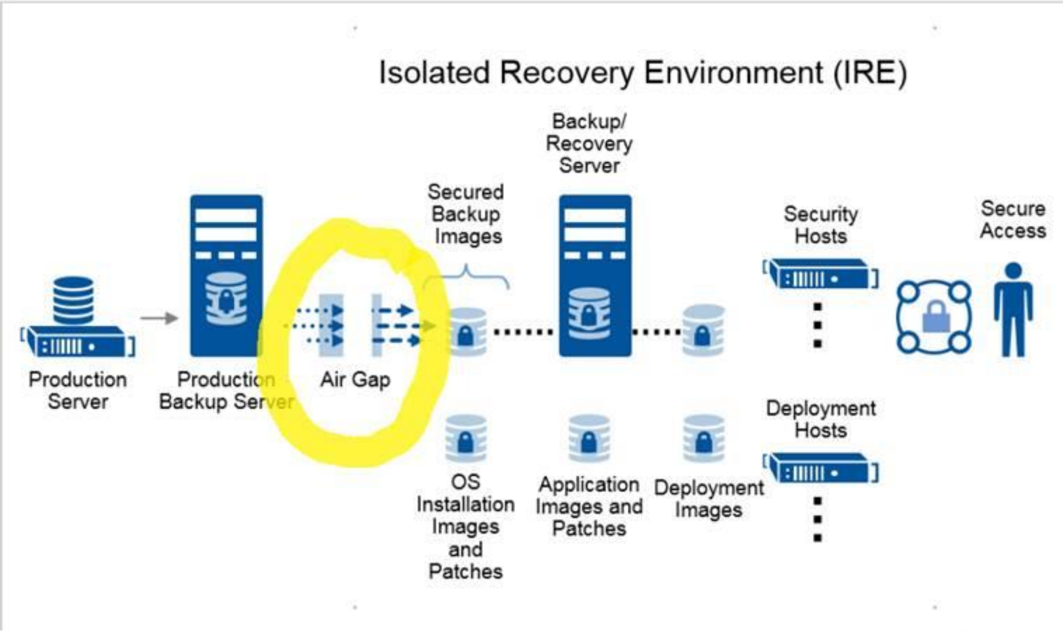
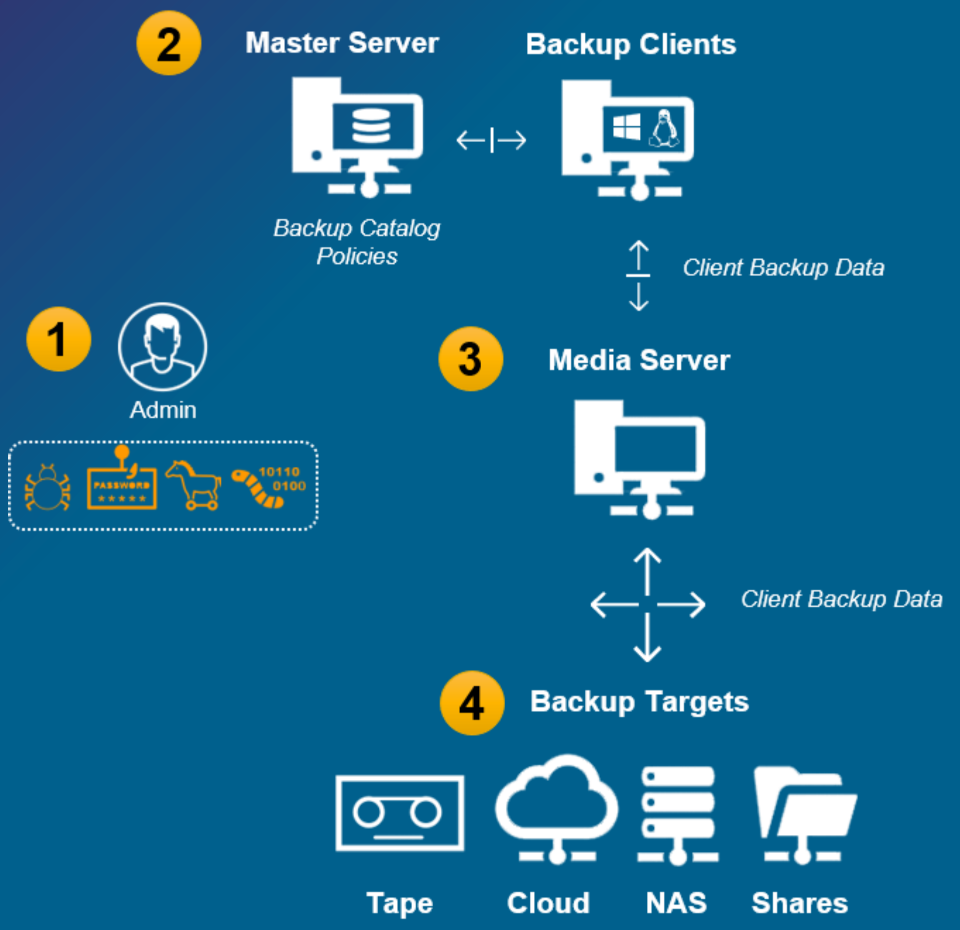


Figure 6. Secured Isolated Recovery Environment



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



1 **IT and Backup admins are main targets for compromise**

2 **Master Server (Backup Catalog):** Backup master server is targeted and infected resulting in encrypted/wiped backup catalog, or pre-mature policy expiration

3 **Media Server:** All mounted filesystems on the media server are targeted and encrypted/wiped

4 **Backup Targets:**

Disk / NAS: Filesystems on the media server are targeted and encrypted/wiped. Backup repositories can become encrypted/wiped from ransomware crawling network file shares

Tape: Provides a better chance to recover from the destructive event if threat was removed from the environment prior to attack. However, if backup catalog is held hostage or destroyed, recovering from the tape will be increasingly difficult

Cloud: General-purpose or Public Cloud offer the advantage of remote protection but are inherently less secure due to reliance on internet (always on) or unsecure networks, leaving data, backups and catalogs exposed

Dell Technologies

Power Protect Cyber Recovery Solution

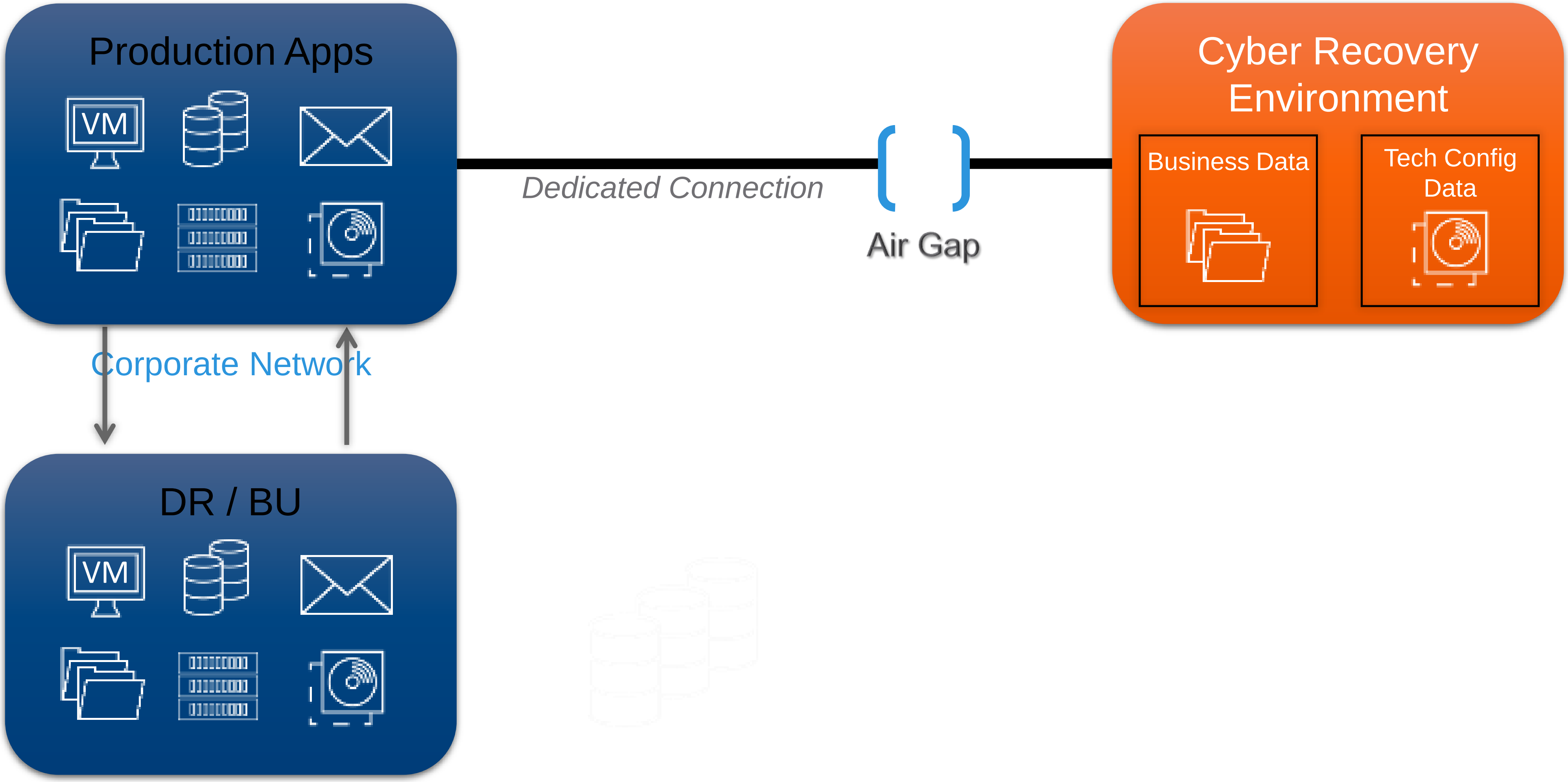
DELL Technologies

DISASTER RECOVERY [IS NOT] CYBER RECOVERY

This is a much different challenge which requires a different approach and architecture

	Disaster Recovery	Cyber Recovery
Recovery Time	Close to Instant	Reliable & Fast
Recovery Point	Ideally Continuous	1 Day Average
Nature of Disaster	Flood, Power Outage, Weather	Cyber Attack, Targeted
Impact of Disaster	Regional; Typically Contained	Global; Spreads Quickly
Topology	Connected, Multiple Targets	Isolated; Addition to DR
Data Volume	Comprehensive, All Data	Selective, Includes Foundation SVCs
Recovery	Standard DR (e.g. Failback)	Iterative, Selective Recovery; Part of IR

Cyber Recovery



Production Apps

Dedicated Connection

Air Gap

Cyber Recovery Environment

Business Data

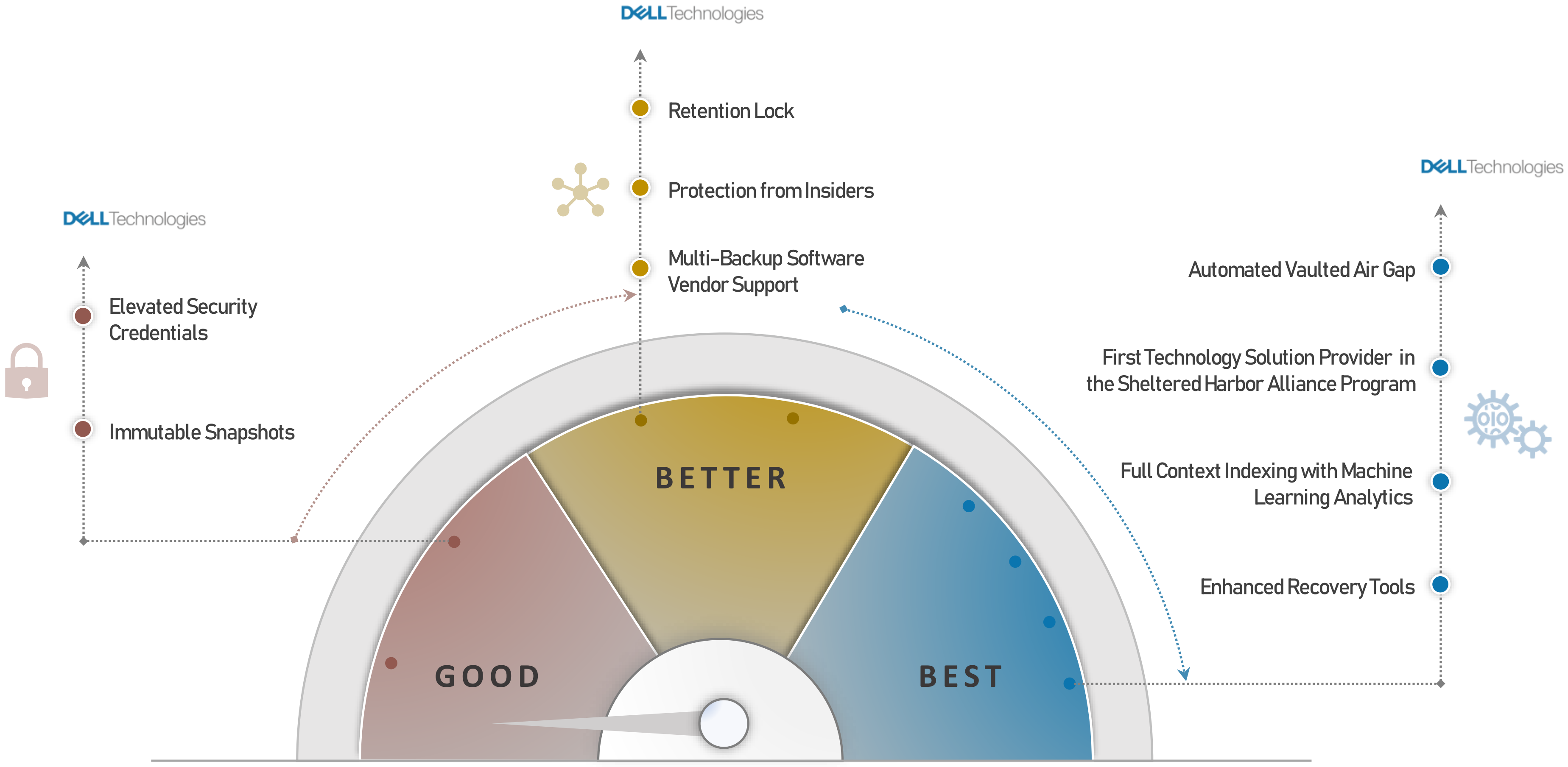
Tech Config Data

Corporate Network

DR / BU

Cyber Recovery: Moving the Needle

Cyber Vault Technical Capabilities and Competitive Market Differentiators


DELL Technologies
Elevated Security Credentials
Immutable Snapshots
DELL Technologies
Retention Lock
Protection from Insiders
Multi-Backup Software Vendor Support
DELL Technologies
Automated Vaulted Air Gap
First Technology Solution Provider in the Sheltered Harbor Alliance Program
Full Context Indexing with Machine Learning Analytics
Enhanced Recovery Tools
GOOD
BETTER
BEST

Dell Technologies Cyber Recovery is the only data protection solution providing **all** described technical capabilities.

» No other technology company provides a complete cyber resilience solution architecture anywhere.

PowerProtect DD

The next generation of Data Domain backup appliances delivering enterprise performance, efficiency, scale, and cloud support

Cloud Tier
Long-term Retention

Cloud DR
Simple and
Cost Effective

PowerProtect DD
Virtual Edition
Software Defined

Up to 38%

faster backups with up to 94 TB per hour[3]

Up to 45%

faster restores[4]

50%[5]

faster instant access/ restore with up to 60k IOPS and up to 64 VMs

Up to 1.5PB

in a single rack

Up to 228PB

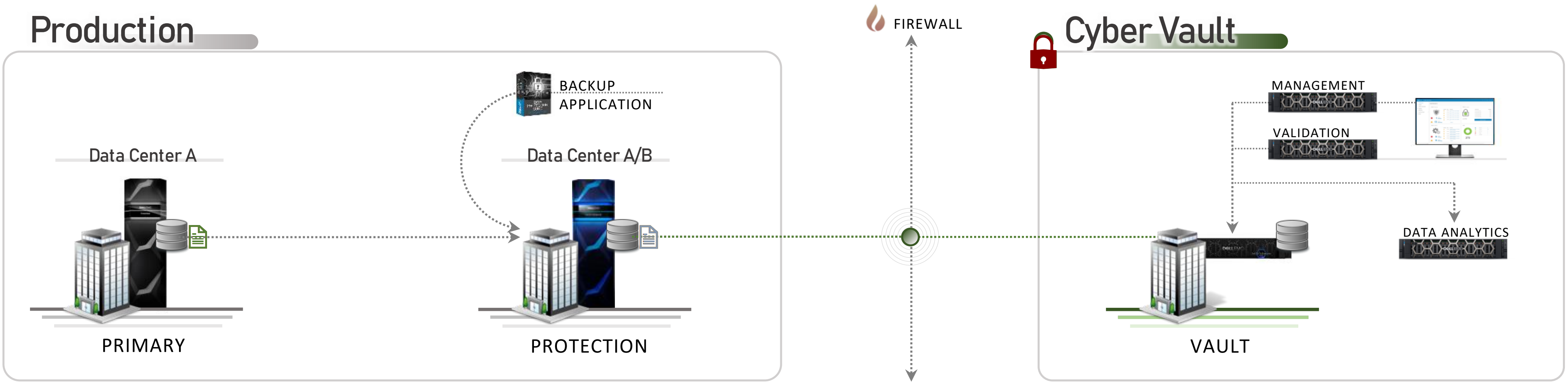
logical capacity with Cloud Tier

Recover

backups from Cyber Recovery Vault

Cyber Recovery: Use Case

Understanding the Data Center and Cyber Vault Workflow



CRITICAL REBUILDS

- Authentication, Identity, Security
- Intellectual Property
- Networking
- Host & Build Tools
- Storage
- Documentation

VAULT WORKFLOW

- Management host enables the management network interface
- Management enables data transfer network in both PROD and VAULT
- **Data pull initiated by Vault; *Data transfer commences***
- During data transfer management host disables management network
- Data transfer completes and management network enabled
- Management host disables data transfer network in both PROD and VAULT
- Retention lock applied to vaulted data
- Validation host ensures viability of data and alerts any data corruption
- Deep forensic analysis commences on vaulted data

WORKLOADS

Microsoft SQL Server

IBM DB2

SAP

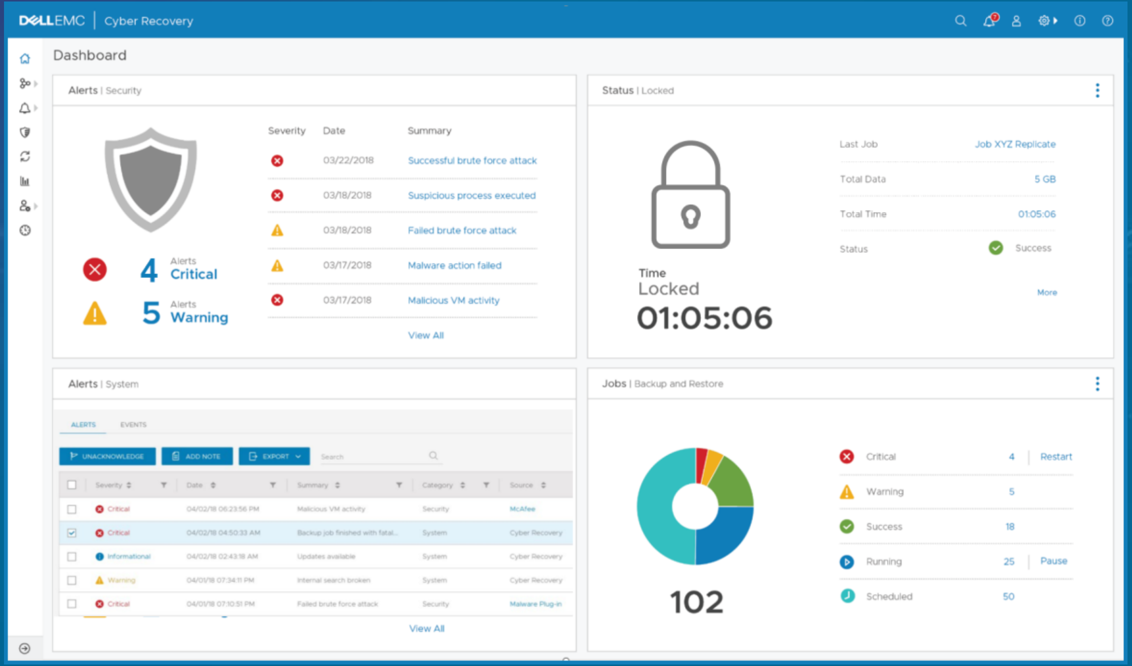
ORACLE DATABASE

vmware

CyberSense Analytics:

Machine Learning Enables Early Detection & Rapid Recovery from a Cyber Attack

Dell EMC Cyber Recovery w/ CyberSense



DELLEMC | Cyber Recovery

Dashboard

Alerts | Security

4 Alerts Critical

5 Alerts Warning

Severity	Date	Summary
☒	03/22/2018	Successful brute force attack
☒	03/18/2018	Suspicious process executed
⚠	03/18/2018	Failed brute force attack
⚠	03/17/2018	Malware action failed
☒	03/17/2018	Malicious VM activity

View All

Status | Locked

Time Locked 01:05:06

Last Job	Job XYZ Replicate
Total Data	5 GB
Total Time	01:05:06
Status	✓ Success

More

Alerts | System

ALERTS EVENTS

UNACKNOWLEDGE ADD NOTE EXPORT Search

□	Severity	Date	Summary	Category	Source
□	Critical	04/02/18 06:23:56 PM	Malicious VM activity	Security	McAfee
☑	Critical	04/02/18 04:50:33 AM	Backup job finished with fatal...	System	Cyber Recovery
□	Informational	04/02/18 02:43:18 AM	Updates available	System	Cyber Recovery
□	Warning	04/01/18 07:34:11 PM	Internal search broken	System	Cyber Recovery
□	Critical	04/01/18 07:10:51 PM	Failed brute force attack	Security	Malware Plug-in

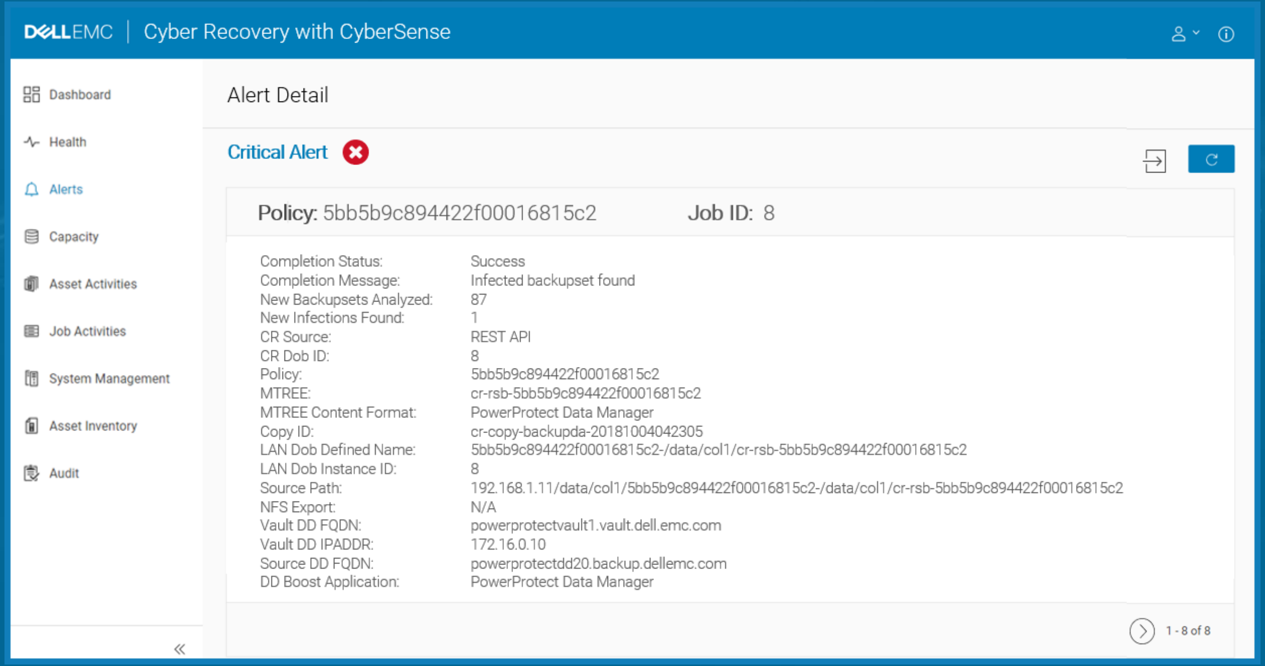
View All

Jobs | Backup and Restore

102

Critical	4	Restart
Warning	5	
Success	18	
Running	25	Pause
Scheduled	50	

CyberSense Alert Example



DELLEMC | Cyber Recovery with CyberSense

Alert Detail

Critical Alert ☒

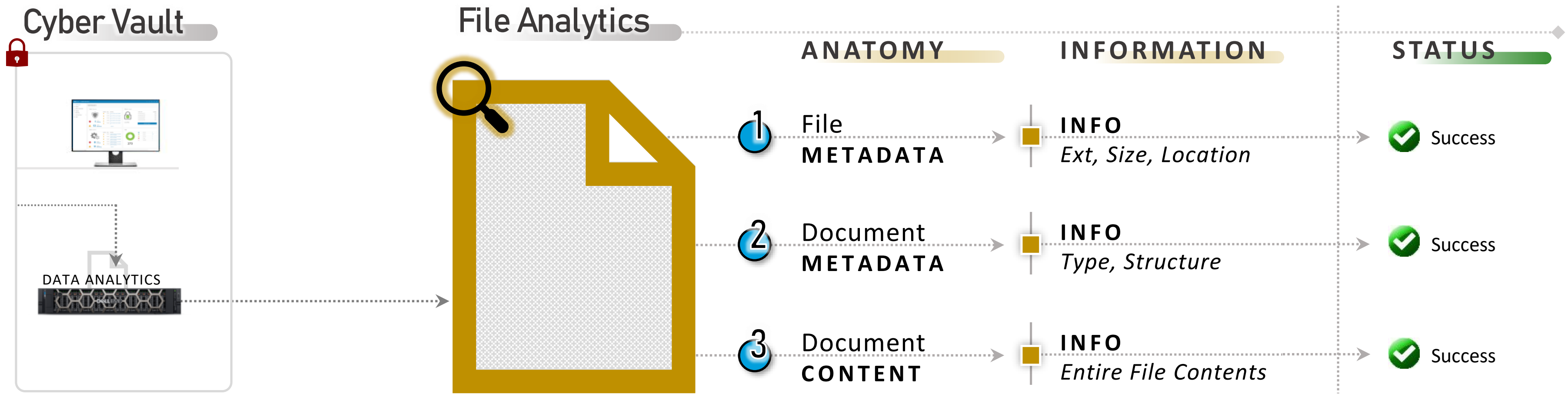
Policy: 5bb5b9c894422f00016815c2 **Job ID:** 8

Completion Status:	Success
Completion Message:	Infected backupset found
New Backupsets Analyzed:	87
New Infections Found:	1
CR Source:	REST API
CR Dob ID:	8
Policy:	5bb5b9c894422f00016815c2
MTREE:	cr-rsb-5bb5b9c894422f00016815c2
MTREE Content Format:	PowerProtect Data Manager
Copy ID:	cr-copy-backupda-20181004042305
LAN Dob Defined Name:	5bb5b9c894422f00016815c2-/data/col1/cr-rsb-5bb5b9c894422f00016815c2
LAN Dob Instance ID:	8
Source Path:	192.168.1.11/data/col1/5bb5b9c894422f00016815c2-/data/col1/cr-rsb-5bb5b9c894422f00016815c2
NFS Export:	N/A
Vault DD FQDN:	powerprotectvault1.vault.dell.emc.com
Vault DD IPADDR:	172.16.0.10
Source DD FQDN:	powerprotectdd20.backup.dellemc.com
DD Boost Application:	PowerProtect Data Manager

1 - 8 of 8

Cyber Recovery: Vault Forensics

Understanding File Anatomy and the Forensic Analytics Workflow



	ANATOMY	INFORMATION	STATUS
1	File **METADATA**	**INFO** *Ext, Size, Location*	✓ Success
2	Document **METADATA**	**INFO** *Type, Structure*	✓ Success
3	Document **CONTENT**	**INFO** *Entire File Contents*	✓ Success

VAULT ANALYTICS WORKFLOW

Scan
» Deep data scan of critical data sources archived in the vault

Analytics
» Deep scan generates 100+ statistics from each observation

Analysis
» Machine learning algorithms applied to analyze for any attacks

Repeat
» Workflow repeats as new backup data is pulled to the vault

Investigate
» Forensic tools used to identify any file corruption & diagnose its specific type

✓ 99.5% Confidence – First Pass Scan & Analysis

Cyber Recovery: Critical Rebuild

An Suggested List of Critical Rebuild Materials in the Cyber Vault

CRITICAL REBUILD MATERIALS

1 Authentication, Identity, Security

- Certificates
- Active Directory / LDAP
- DNS Dumps
- Event Logs (including SIEM data)

2 Intellectual Property

- Source Code
- Proprietary Algorithms
- Developer Libraries

3 Networking

- Switch & Router Configurations
- Firewall & Load Balancer Settings
- IP Services Design
- Access Control Configuration
- Firmware, Microcode, Patches

4 Host and Build Tools

- Physical & Virtual Platform Builds
- Dev/Ops Tools & Automation Scripts
- Firmware, Microcode, Patches
- Vendor Software
  - Binaries (Gold Images)
  - Configurations and Settings

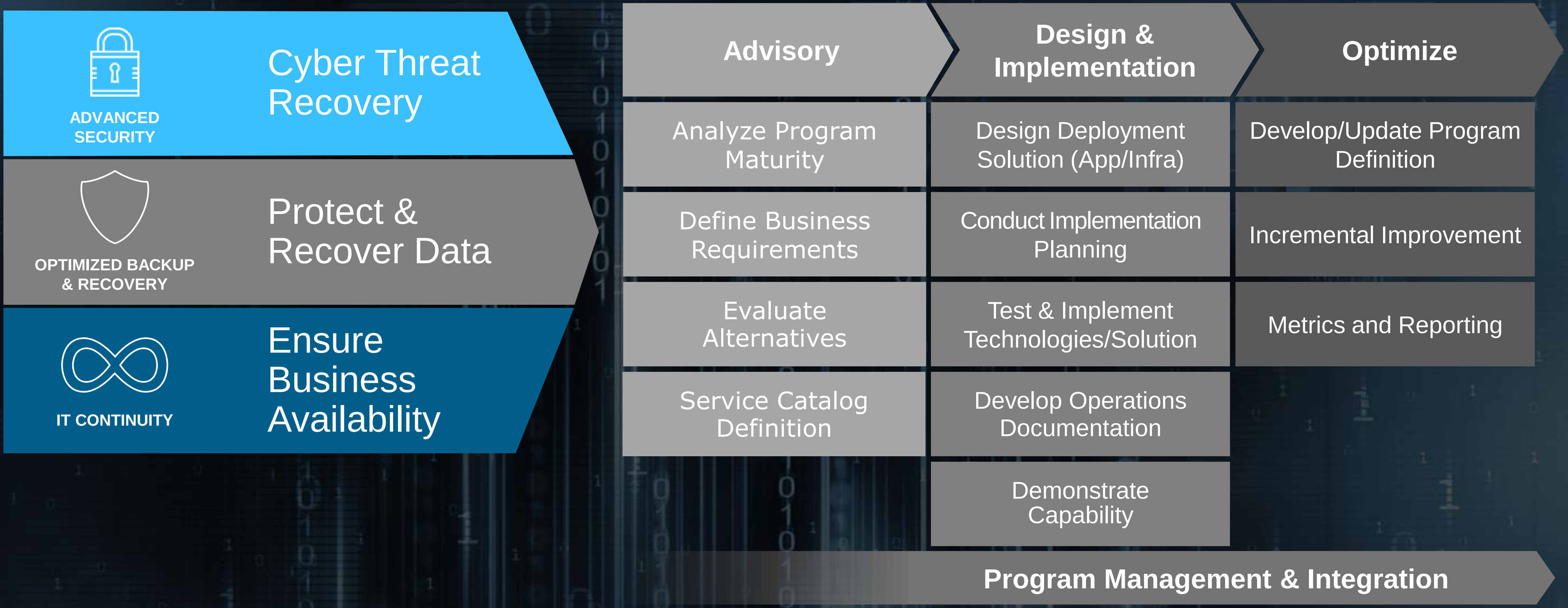
5 Storage

- SAN / Array Configurations
- Storage Abstraction Settings
- Backup Hardware Configuration
- Firmware, Microcode, Patches

6 Documentation

- CMDB & Asset Management Extracts
- D/R / Cyber Recovery Runbooks and Checklists
- HR Resources and Contact Lists
- Incident Response Plan

Dell EMC’s Resiliency Methodology



Cyber Threat Recovery

Protect & Recover Data

Ensure Business Availability

Advisory	Design & Implementation	Optimize
Analyze Program Maturity	Design Deployment Solution (App/Infra)	Develop/Update Program Definition
Define Business Requirements	Conduct Implementation Planning	Incremental Improvement
Evaluate Alternatives	Test & Implement Technologies/Solution	Metrics and Reporting
Service Catalog Definition	Develop Operations Documentation	
	Demonstrate Capability	

Program Management & Integration

DELL EMC