Cyber Recovery afstemmen op NIS2

Marius Vasilache
Dell Technologies

Cyber Recovery afstemmen op NIS2:
een nieuwe norm voor bedrijfskritische veerkracht

Marius Vasilache

Cyber Recovery & Data Protection Specialist

DELL Technologies

Broad spectrum of sophisticated cyber threats

Motivations, techniques and goals

- Crime
- Espionage
- Terrorism
- Insider
- Hacktivism
- Warfare

DELL Technologies

Confidence in recovery

67%

are not very confident that all business-critical data can be recovered in the event of a destructive cyberattack.[1]

Global Data Protection Index Survey
2022 Snapshot

[1] Based on research by Vanson Bourne commissioned by Dell Technologies, “Global Data Protection Index 2022 Snapshot,” carried out August – October 2022. Results were derived from a total of 1,000 IT decision makers worldwide from both private and public organizations with 250+ employees.

DELL Technologies

The time for resilience is now!

Gartner®

“Transforming cybersecurity into cyber-resilience involves prioritizing resilience over defense, and elevating the native disciplines and skills used by the business continuity management office above cybersecurity teams’ traditionally defensive strategies.”

Gartner, You Will Be Hacked, So Embrace the Breach!

"Implement at least an immutable backup copy by selecting write lock or WORM media before starting any other initiative, as **having an immutable copy of the backup is the most important item to start protecting backup data."**

Gartner, Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults

DELL Technologies

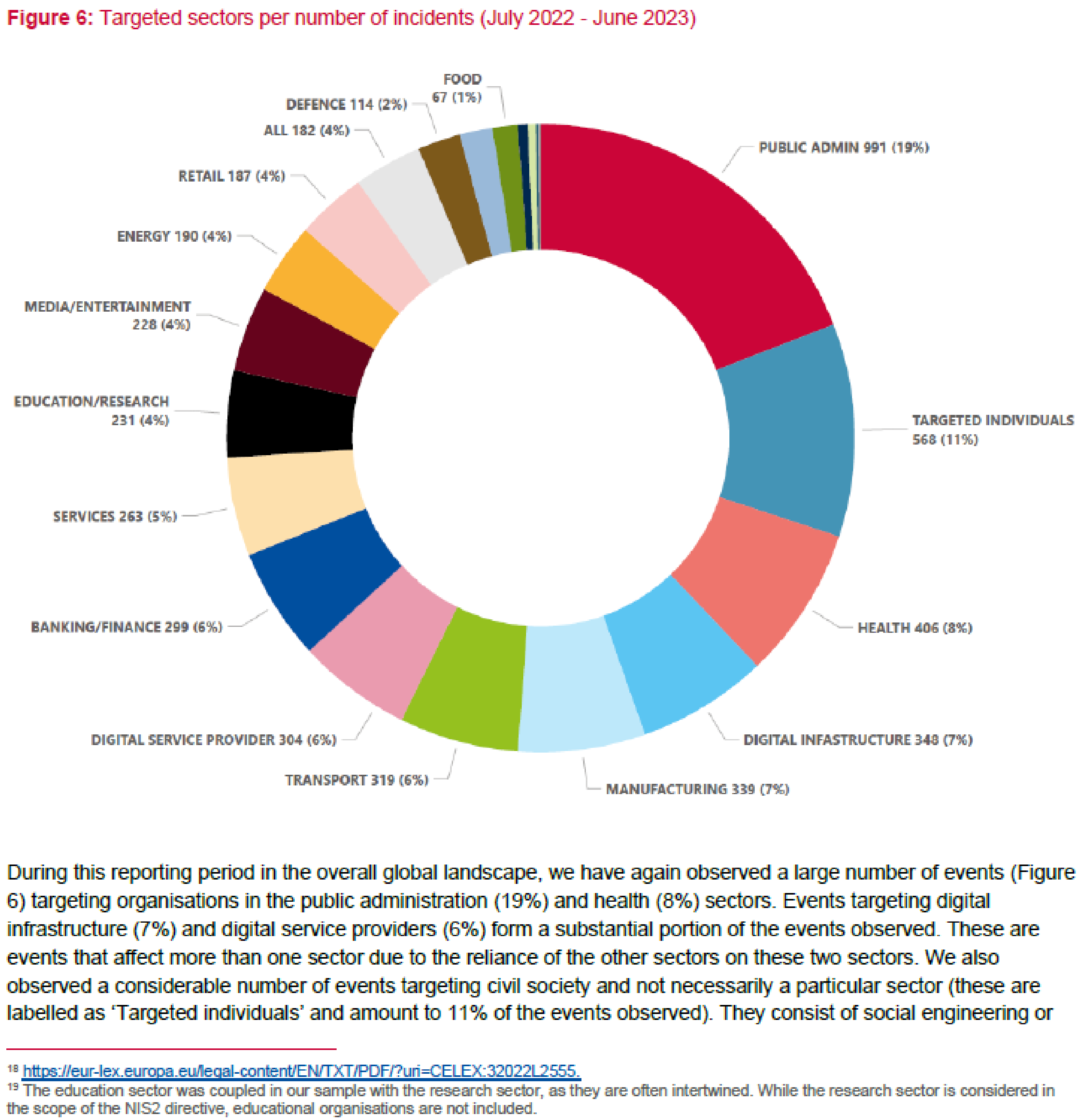


Figure 6: Targeted sectors per number of incidents (July 2022 - June 2023)

During this reporting period in the overall global landscape, we have again observed a large number of events (Figure 6) targeting organisations in the public administration (19%) and health (8%) sectors. Events targeting digital infrastructure (7%) and digital service providers (6%) form a substantial portion of the events observed. These are events that affect more than one sector due to the reliance of the other sectors on these two sectors. We also observed a considerable number of events targeting civil society and not necessarily a particular sector (these are labelled as 'Targeted individuals' and amount to 11% of the events observed). They consist of social engineering or

[18] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555.

[19] The education sector was coupled in our sample with the research sector, as they are often intertwined. While the research sector is considered in the scope of the NIS2 directive, educational organisations are not included.

ENISA THREAT LANDSCAPE 2023

Upcoming & Current Regulation

THE NIS 2 DIRECTIVE

Legislated Autumn 2023 enforced mid-2024

*‘Essential and important entities will be required to take appropriate and proportionate technical, operational and organizational measures … **to prevent or minimise the impact of incidents** on recipients of their services and on other services.’*

Managing directors will be held personally liable for implementing resilience and will be fined if they are unable to prove this.

Estimated 81,000 businesses to be impacted both directly and as part of the wider **supply chain** for critical entities across aligned regions.

DORA

- Jan 16th, 2023, DORA in force - 2 Year implementation period: Jan 17th 2025
- Test the ICT business continuity plans and the ICT response and recovery plans at least yearly,
- Use ICT systems that are physically and logically segregated from the source ICT system
- Penalties
  - Financial institutions not fixed yet
  - Potential criminal sanctions
  - ICT providers: 1% of average worldwide turnover in proceeding year, applied daily until compliance is achieved for 6 months

EUROPEAN CENTRAL BANK
EUROSYSTEM

- Plan for how to operate in a diminished capacity
- Backups should be tested regularly to verify their availability and integrity.
- Store backup copies at an alternate site with a different risk profile

EBA EUROPEAN BANKING AUTHORITY

- Financial institutions should develop response and recovery plans for critical ICT systems and services

CYBER

is the new

DISASTER

PowerProtect the foundation of data protection

Cyber recovery requirements

Immutability
Preserve original integrity of data

Isolation
Physical and logical separation of data

Intelligence
Machine learning and analytics identify threats

Modern threats require modern solutions to ensure cyber resilience

DELLTechnologies

PowerProtect DD

The foundation of resilience

Fast, secure, efficient storage

Multicloud resiliency

Operational simplicity

PowerProtect DD - Zero Trust Architecture

Immutability

Retention Lock Compliance Mode (2012)

Cohasset Associates (2013)

- SEC 17a-4(f) Compliance
- FDA 21 Part II
- Sarbanes-Oxley Act

Dual Role Authorization (2017)

Admin & Security Officer

- Sensitive & Destructive Commands (95+)

End to End Encryption

- Data in Flight: TL2 1.2 256 Bit
- Data at Rest: FIPS 140-2 Crypto Libraries

Multi-factor Authentication (MFA) – RSA

- Web UI, CLI, Security Officer, and iDRAC

Integrated Lights Out Mgt Hardening (iDRAC)

Local or External Key Management (KMIP)

Security Logs to SIEM / SOAR

PowerProtect Data Domain

Secure System Clock
NTP Clock Tamper Controls (2019)

- Change, Drift, Sync

Custom System OS - DDOS

- Restricted BASH Access
- Can’t restart in Single User Mode

File System – DDFS

- Hashed containers – not recognized by malware

Secure Transport - DDBoost

- Encrypted, Secure, Authorized, Not Open

Data Invulnerability Architecture

- Continuously checks that data written is data stored – Self Healing

Secure AD / LDAP Authentication

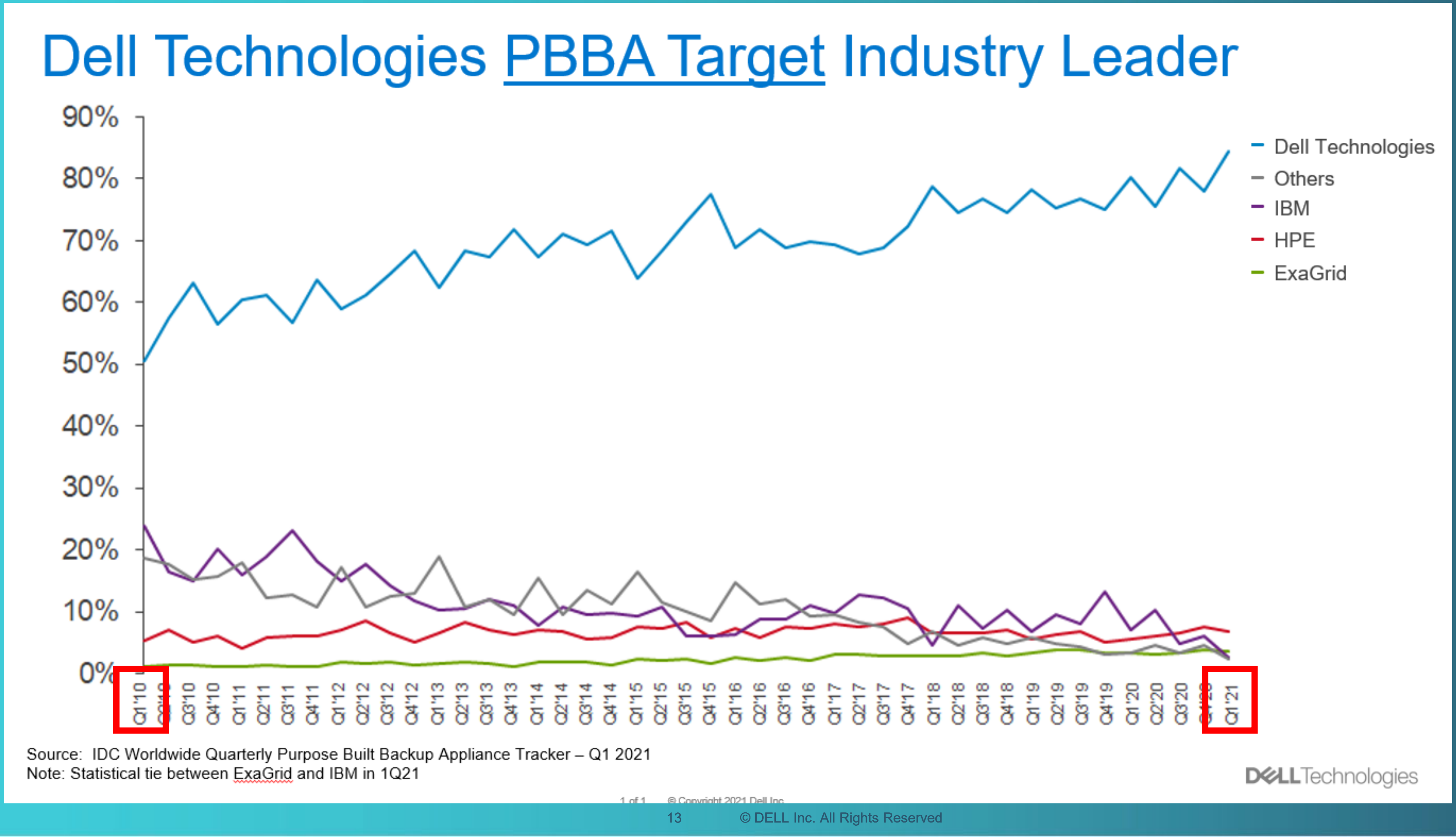
Secure Remote Support Services

Role Based Access

- Limited Admin, Operator, Security Officer

DELL Technologies

What does **IDC** show when looking at the PPBA target market?



Dell Technologies PBBA Target Industry Leader

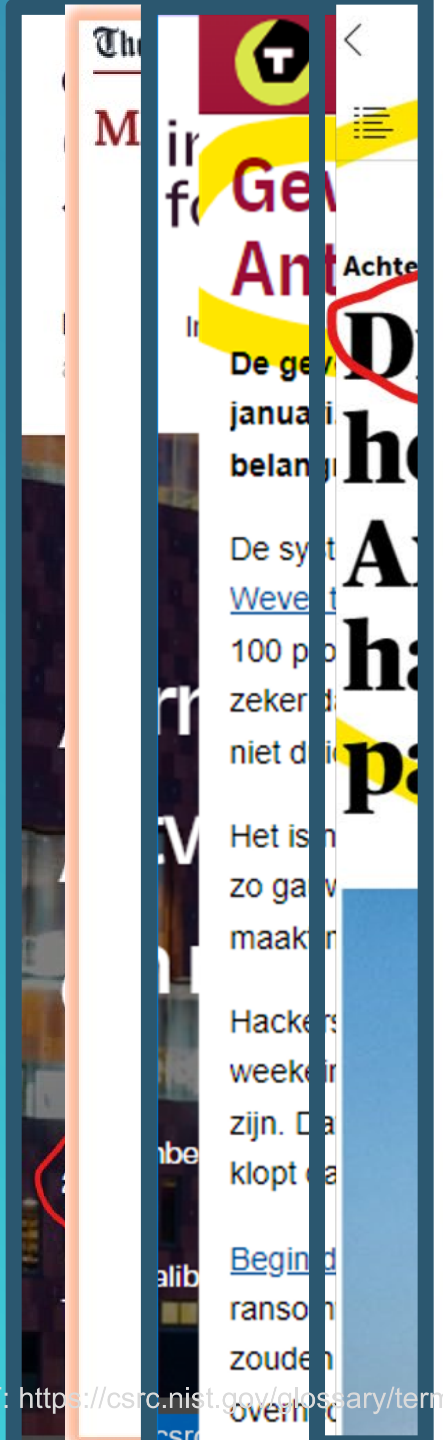
Source: IDC Worldwide Quarterly Purpose Built Backup Appliance Tracker – Q1 2021
Note: Statistical tie between ExaGrid and IBM in 1Q21

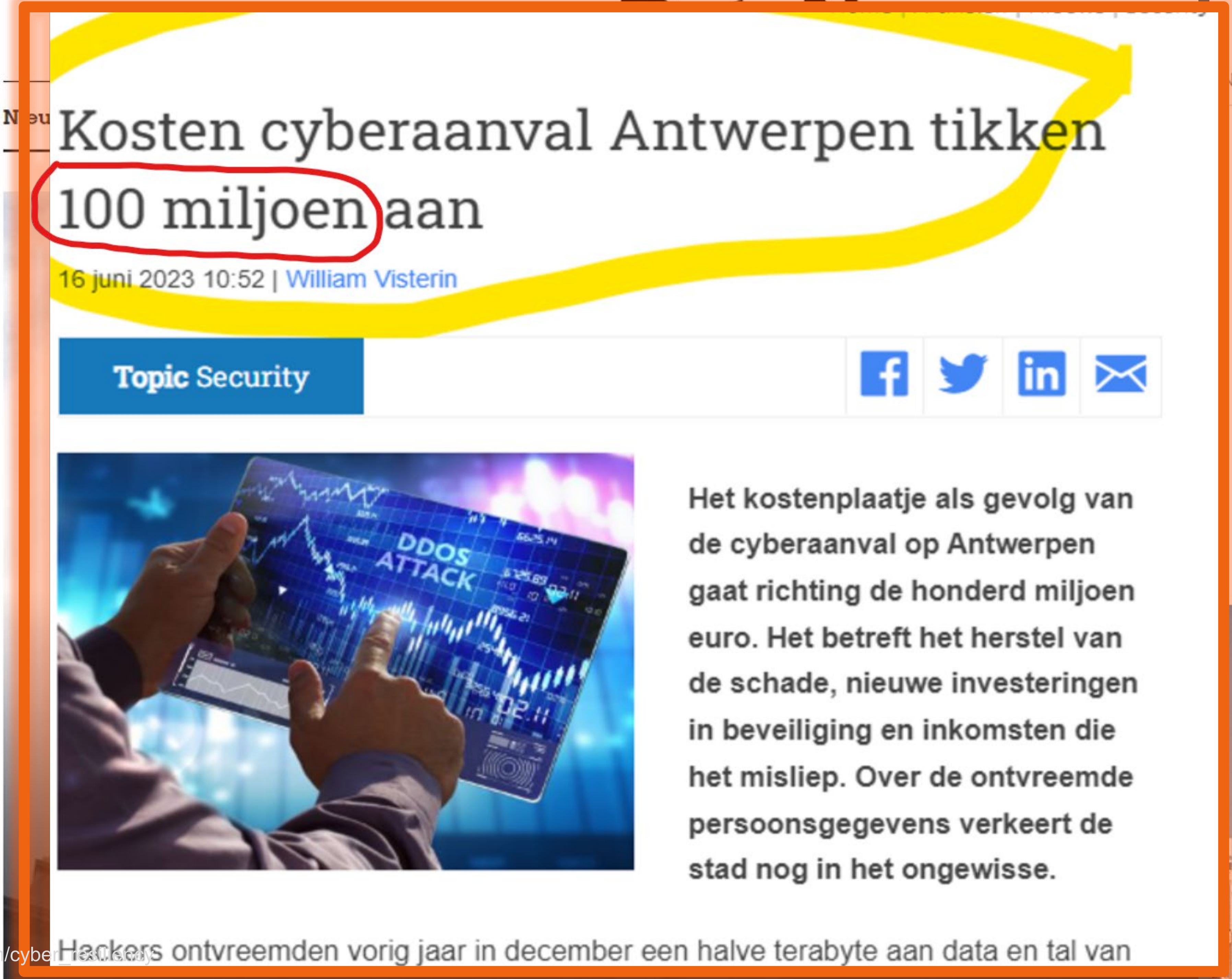
DELL Technologies

1 of 1 © Copyright 2021 Dell Inc.

DELL Technologies

PowerProtect Cyber Recovery





Kosten cyberaanval Antwerpen tikken 100 miljoen aan

16 juni 2023 10:52 | William Visterin

Topic Security

Het kostenplaatje als gevolg van de cyberaanval op Antwerpen gaat richting de honderd miljoen euro. Het betreft het herstel van de schade, nieuwe investeringen in beveiliging en inkomsten die het misliep. Over de ontvreemde persoonsgegevens verkeert de stad nog in het ongewisse.

Hackers ontvreemden vorig jaar in december een halve terabyte aan data en tal van

NIST: https://csrc.nist.gov/glossary/term/cyber_resiliency

es

Cyber recovery requirements

Immutability
Preserve original integrity of data

Isolation
Physical and logical separation of data

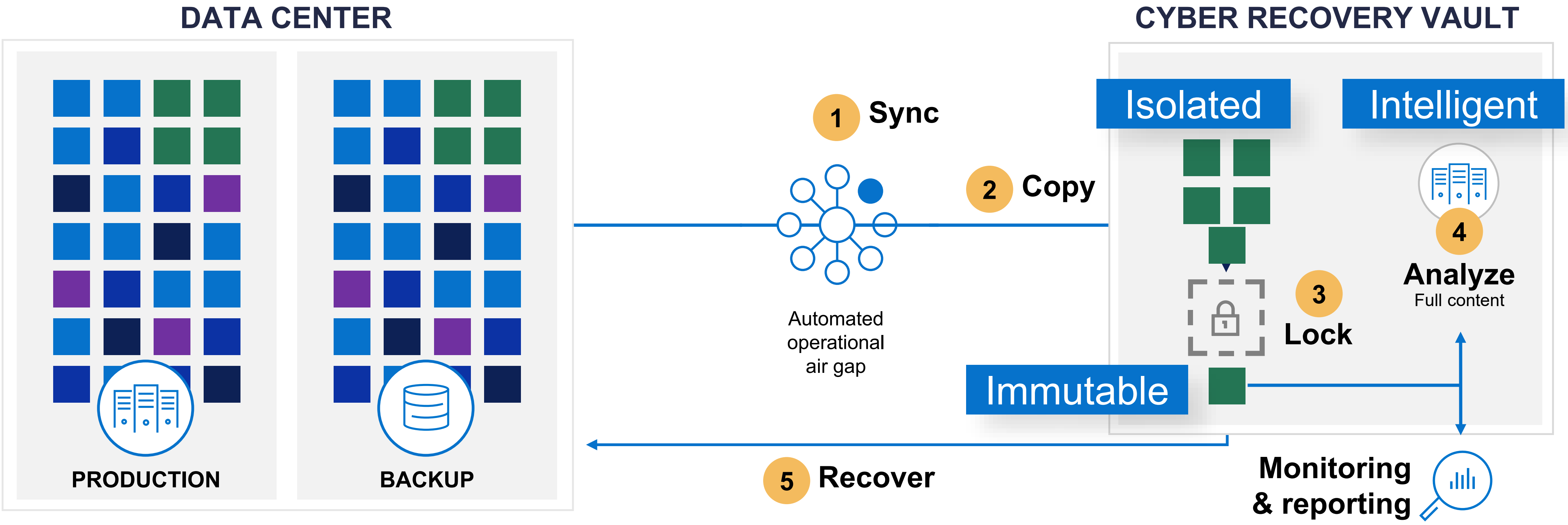
Intelligence
Machine learning and analytics identify threats

Modern threats require modern solutions to ensure cyber resilience

DELLTechnologies

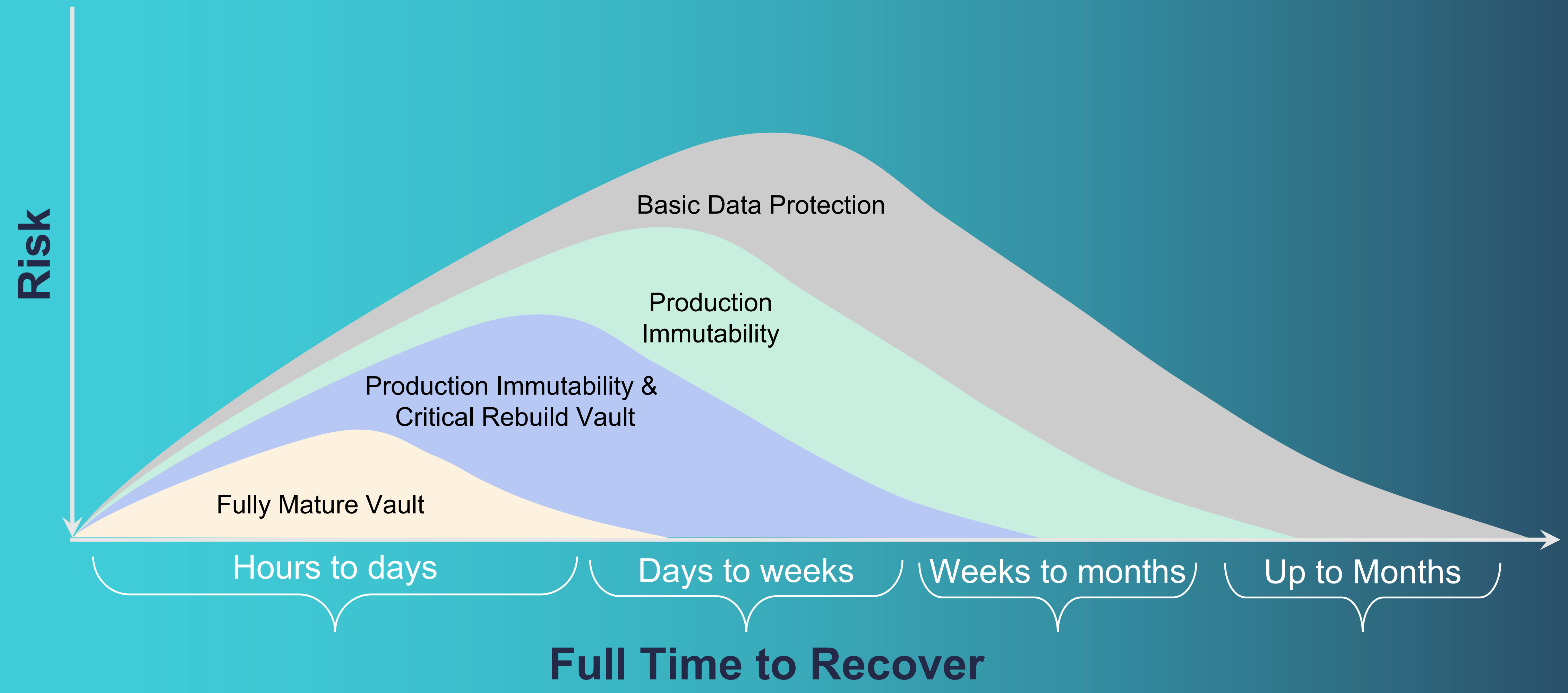
PowerProtect Cyber Recovery

Data vaulting critical business data



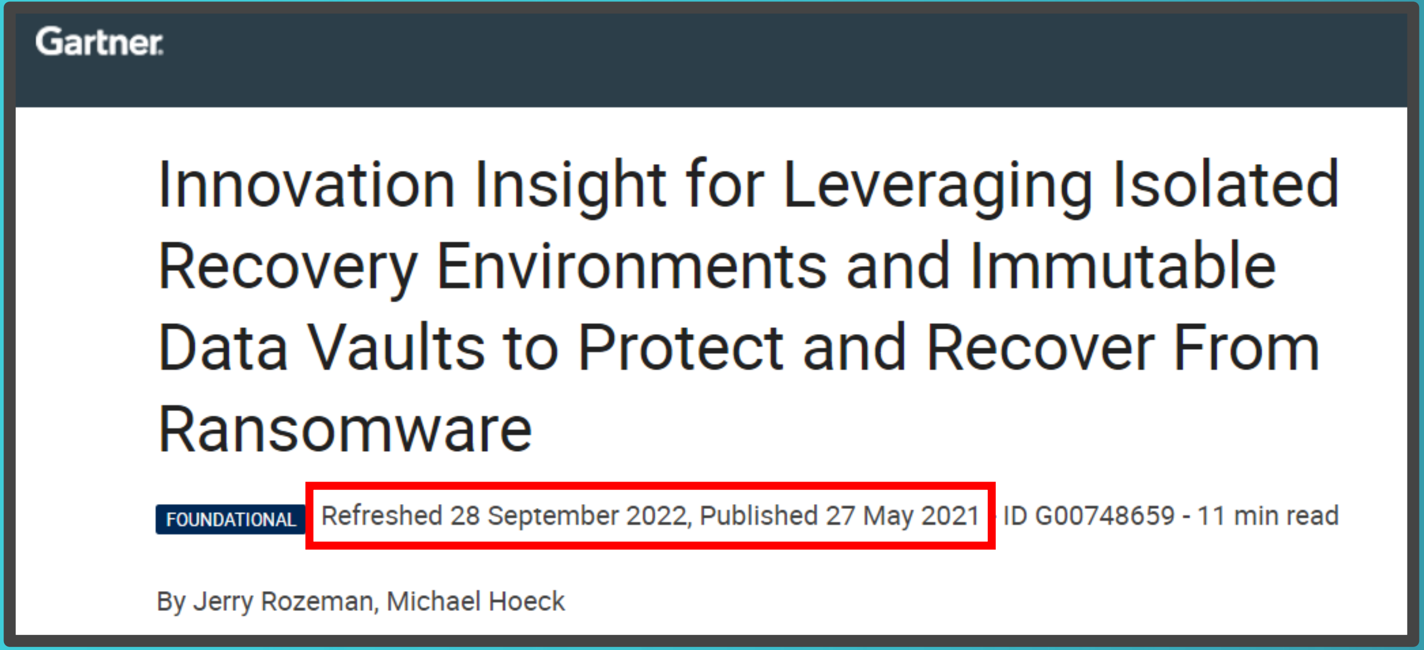
Stronger Resilience. Better Outcomes.

Reduce Risk, Speed Recovery, and Lower Costs



DELL Technologies

Gartner analyzing the market on Cyber Recovery

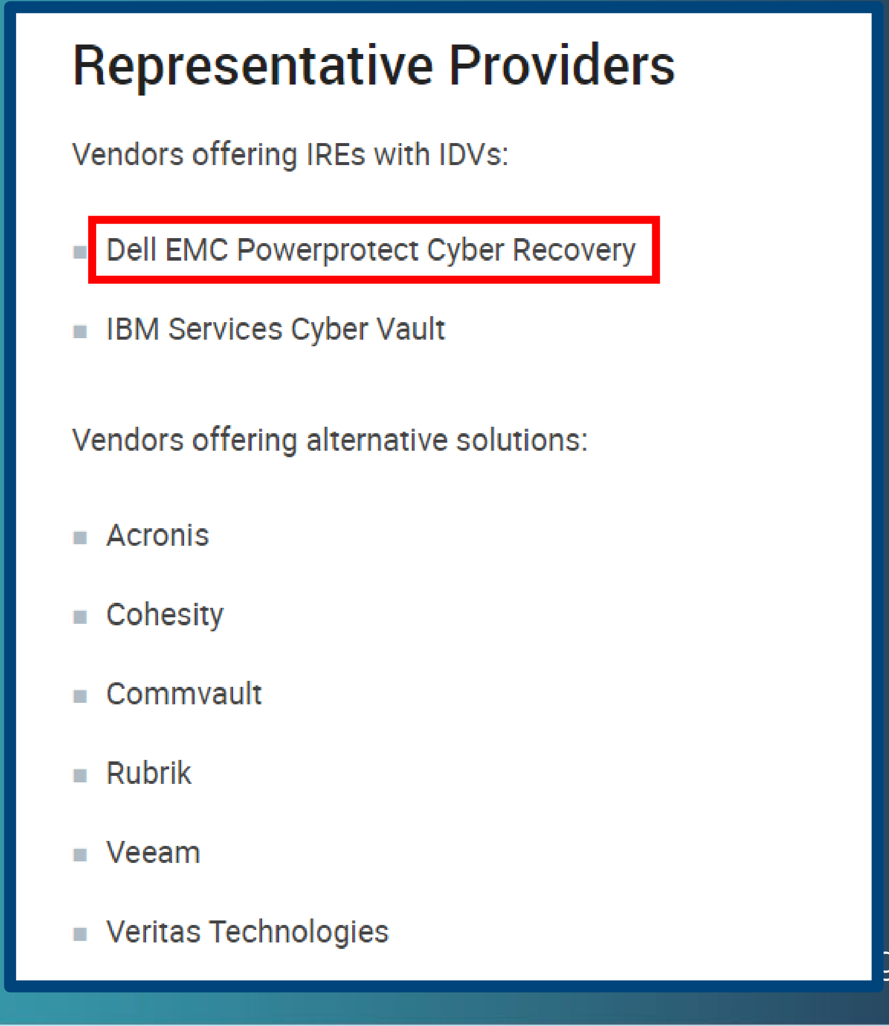


Gartner

Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware

FOUNDATIONAL Refreshed 28 September 2022, Published 27 May 2021 ID G00748659 - 11 min read

By Jerry Rozeman, Michael Hoeck



Representative Providers

Vendors offering IREs with IDVs:

- Dell EMC Powerprotect Cyber Recovery
- IBM Services Cyber Vault

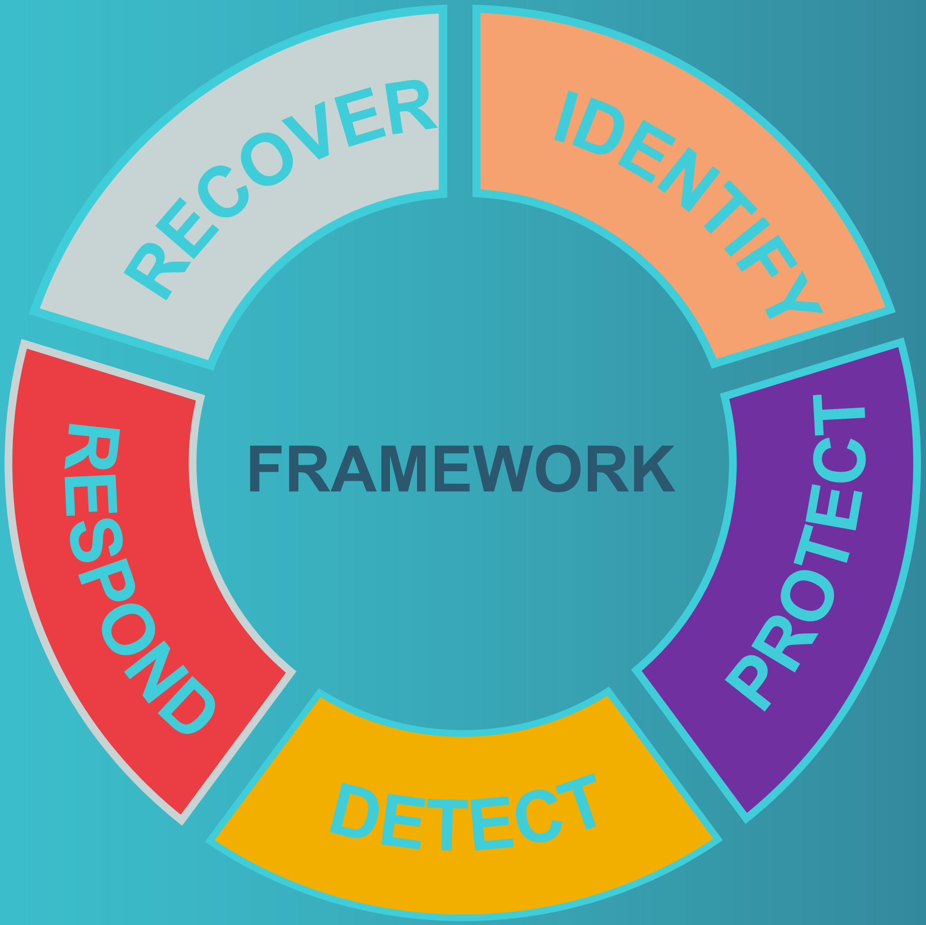
Vendors offering alternative solutions:

- Acronis
- Cohesity
- Commvault
- Rubrik
- Veeam
- Veritas Technologies

Cyber Resilience is a Strategy | Dell Cyber Recovery is a Solution

Cyber Resilience

- *“The ability (for a business / organization) to continuously deliver the intended outcome despite adverse cyber events.”* *
- A high-level holistic strategy that includes cyber security standards, guidelines, people, business processes and technology solutions
- Example: NIST Cybersecurity Framework



Cyber Recovery

- Dell Cyber Recovery is a critical component of an overall Cyber Resilience strategy
- Dell Cyber Recovery is a data protection solution that isolates business-critical data away from attack surfaces
- Critical data is stored immutably in a hardened vault enabling recovery with assured data availability, integrity and confidentiality

*https://en.wikipedia.org/wiki/Cyber_resilience

Extensive Dell Security and Resiliency Services

Professional Services

- Cyber Assessments
- Deploy & Implement
- Runbook & Validation
- Advisory & Design
- Operate & Manage

Incident Recovery & Retainer Service

- Evaluate & Plan
- Strengthen Readiness
- Incident Response & Recovery
- Tabletop Exercises

APEX Cyber Recovery

- Manage day-to-day vault operations
- Drive consistent procedures & testing
- Monitored 24x7x365 by global operations team
- Support recovery operations

>35K
Service & Support Professionals

Certified Cyber Security Experts

20+ years of
resiliency services innovation

DELL Technologies

Data protection & data resilience leadership

1500+

Cyber Recovery customers*

17 EB+

Data protected in the cloud

#1

Data Protection appliances & software**

2012	First “Immutable” data protection appliance
2015	First “Isolated” recovery solution with custom deployment
2016	zDP: 1st z/OS implementation of logical corruption protection
2018	Introduced PowerProtect Cyber Recovery solution
2019	First technology vendor in Sheltered Harbor Alliance Partner Program
2020	First Endorsed Sheltered Harbor Solution – PowerProtect Cyber Recovery
2021	Introduced PowerProtect Cyber Recovery for Multi-Cloud & AWS
2021	Formal support for PowerProtect Cyber Recovery for DLM
2022	Introduced PowerProtect Cyber Recovery for Azure and Google Cloud
2022	Managed as-a-Service Dell APEX Cyber Recovery Services

>35k
Service & support professionals

241m+
Assets supported

94%
Technical support CSAT rating

10,000+
Transformation projects completed

*Based on Dell Technologies analysis, February 2023

**Based on combined revenue from the IDC 4Q22 Purpose-Built Backup Appliance (PBBA) Tracker, with select Storage Software segments from the 4Q22 Storage Software and Cloud Services Tracker.

DELL Technologies

Thank you!

DELL Technologies