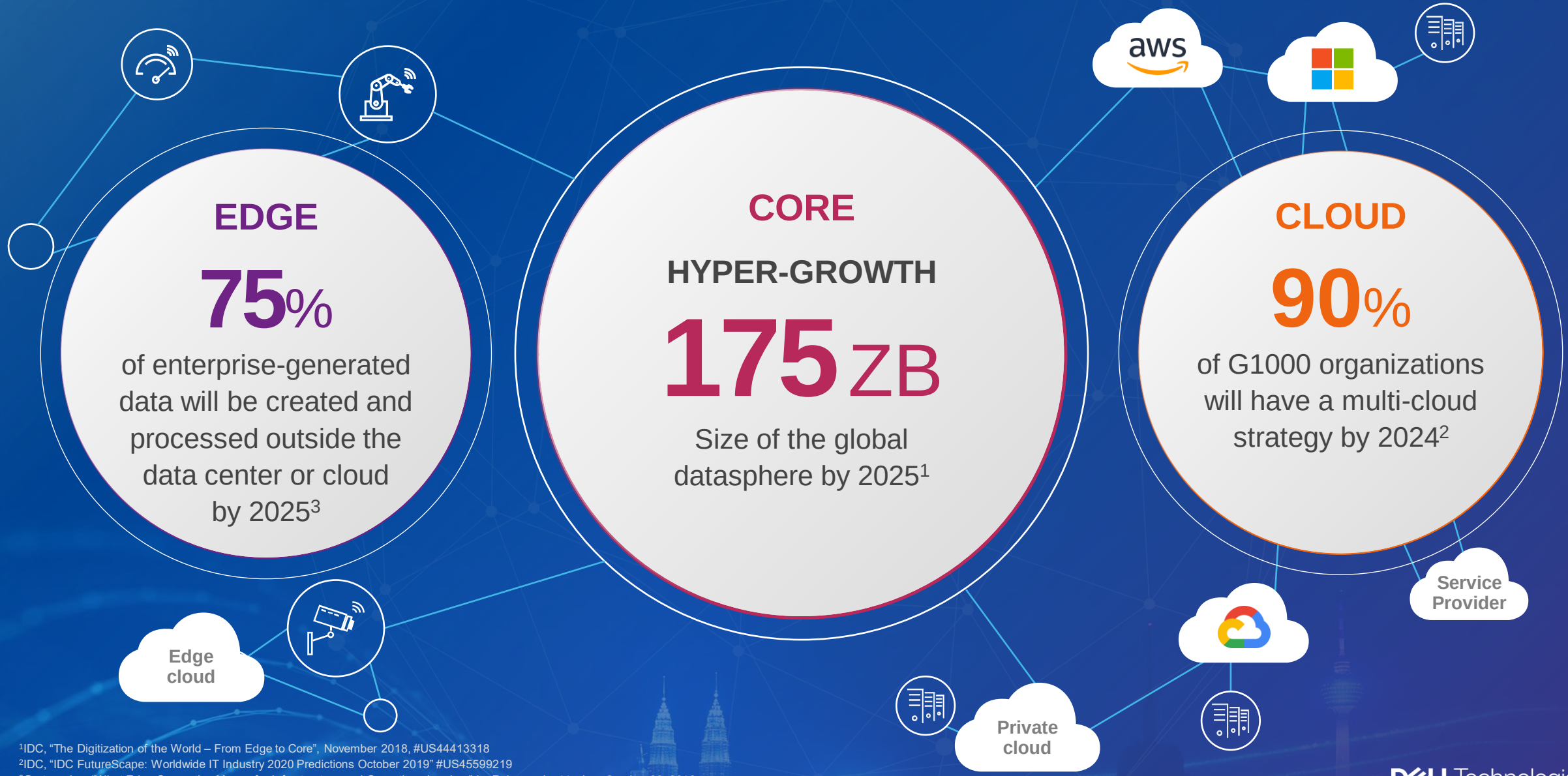
IL DATACENTER MODERNO, L'EVOLUZIONE DELL'INFRASTRUTTURA E LA STRATEGIA PER LA CYBER SECURITY

Maurizio Mercuri
Dell Technologies
Senior Partner Sales Specialist UDS Southern Europe
maurizio.mercuri@dell.com
Mobile: 347.7176876

DELL Technologies

Data growth is everywhere



[1]IDC, "The Digitization of the World – From Edge to Core", November 2018, #US44413318
[2]IDC, "IDC FutureScape: Worldwide IT Industry 2020 Predictions October 2019" #US45599219
[3]Gartner, Inc. "What Edge Computing Means for Infrastructure and Operations Leaders" by Rob van der Meulen, October 28, 2018

DELL Technologies

Cyber attacks: a continuous threat to business

A **cyber attack** happens every …

Source: Security Magazine

Increasing costs of Cyber Attacks

71%

are financially motivated

verizon

43%

Involved small business

verizon

$13M

Avg cost of Cybercrime

accenture

$5.2T

At risk over
the next 5 years

accenture

Avg Cost of Cyber Attack
by Industry

Industry	Average 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

DELL Technologies
PARTNER PROGRAM

DELL Technologies

State of Cybercrime

The Damage & Costs Continue to Rise

Cybercrime To Cost The World $10.5 Trillion Annually By 2025

- If it were measured as a country, then cybercrime, which is predicted to inflict damages totaling $6 trillion USD globally in 2021, would be the world's third-largest economy after the U.S. and China.

Cybercrime Magazine, Nov. 13, 2020

DELL Technologies PARTNER PROGRAM

DELL Technologies

Spectrum of cyber threats

Motivations, techniques and goals

Crime

Theft & extortion for financial gain

Insider

Trusted insiders with malicious intent

Espionage

Corporate or Nation-state actors steal valuable data

Hacktivism

Advance political or social causes

Terrorism

Sabotage & destruction to instil fear

Warfare

With destructive cyber weapons

DELL Technologies

Consequences of cyber attacks

Disrupted Operations

Data theft/breach

Ransom money

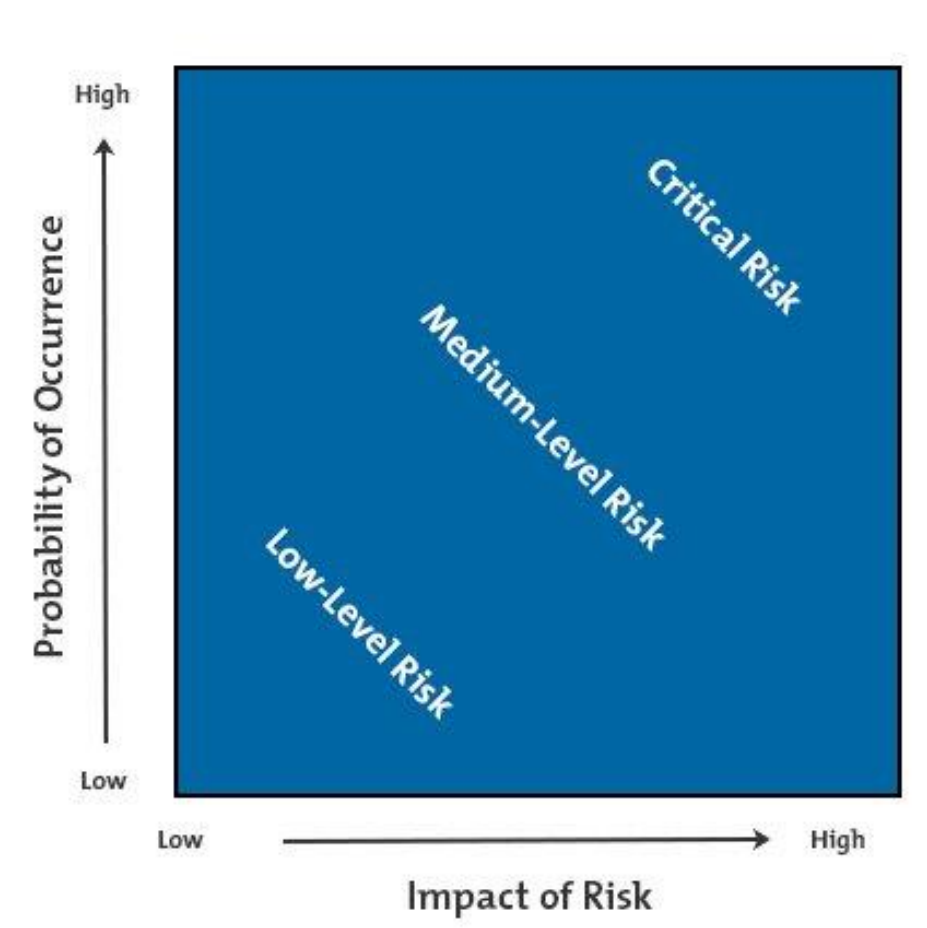
Business reputation

DELL Technologies PARTNER PROGRAM

DELL Technologies

Focus on the Critical Risks of your organization

La domanda non è SE ma Quando avverrà anche a me?



DELL Technologies PARTNER PROGRAM

DELL Technologies

Cyber Resilience Strategy

A high-level holistic strategy that helps organizations:

NIST Cyber Security Framework

(National Institute of Standards and Technology)

DELL Technologies PARTNER PROGRAM

DELL Technologies

BANCA D'ITALIA
EUROSISTEMA

CONSOB
COMMISSIONE NAZIONALE PER LE SOCIETA' E LA BORSA

IVASS
ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI

UIF
Unità di Informazione Finanziaria per l'Italia

Roma, 7 marzo 2022

RICHIAMO AL RISPETTO DELLE MISURE RESTRITTIVE ADOTTATE DALLA UE IN RISPOSTA ALL'AGGRESSIONE MILITARE RUSSA IN UCRAINA

Banca d'Italia, CONSOB, IVASS e UIF richiamano l'attenzione dei soggetti vigilati sul pieno rispetto delle misure restrittive decise dall'Unione europea in risposta alla situazione in Ucraina.

Le misure sono consultabili sui siti della Gazzetta ufficiale dell'Unione europea, del Consiglio europeo, dell'Unità di Informazione Finanziaria – UIF e del Comitato di Sicurezza Finanziaria.

Si ricorda che le misure – adottate dall'Unione europea mediante Regolamenti e Decisioni – sono vincolanti nella loro totalità e sono direttamente e immediatamente applicabili in ciascuno degli Stati Membri.

I soggetti vigilati sono tenuti, pertanto, a rispettarle, mettendo in atto i controlli e i dispositivi necessari, monitorando costantemente l'aggiornamento delle misure in questione.

Ai fini dell'adempimento degli obblighi di comunicazione delle misure di congelamento applicate ai soggetti designati andranno tenute altresì in considerazione le indicazioni fornite dalla UIF con il Comunicato del 4 marzo 2022

Nel contesto attuale, si raccomanda ai soggetti vigilati di esercitare la massima attenzione con riferimento al rischio di attacchi informatici, di intensificare le attività di monitoraggio e difesa in relazione a possibili attività di *malware* e di adottare tutte le misure di mitigazione dei rischi che si rendano necessarie.

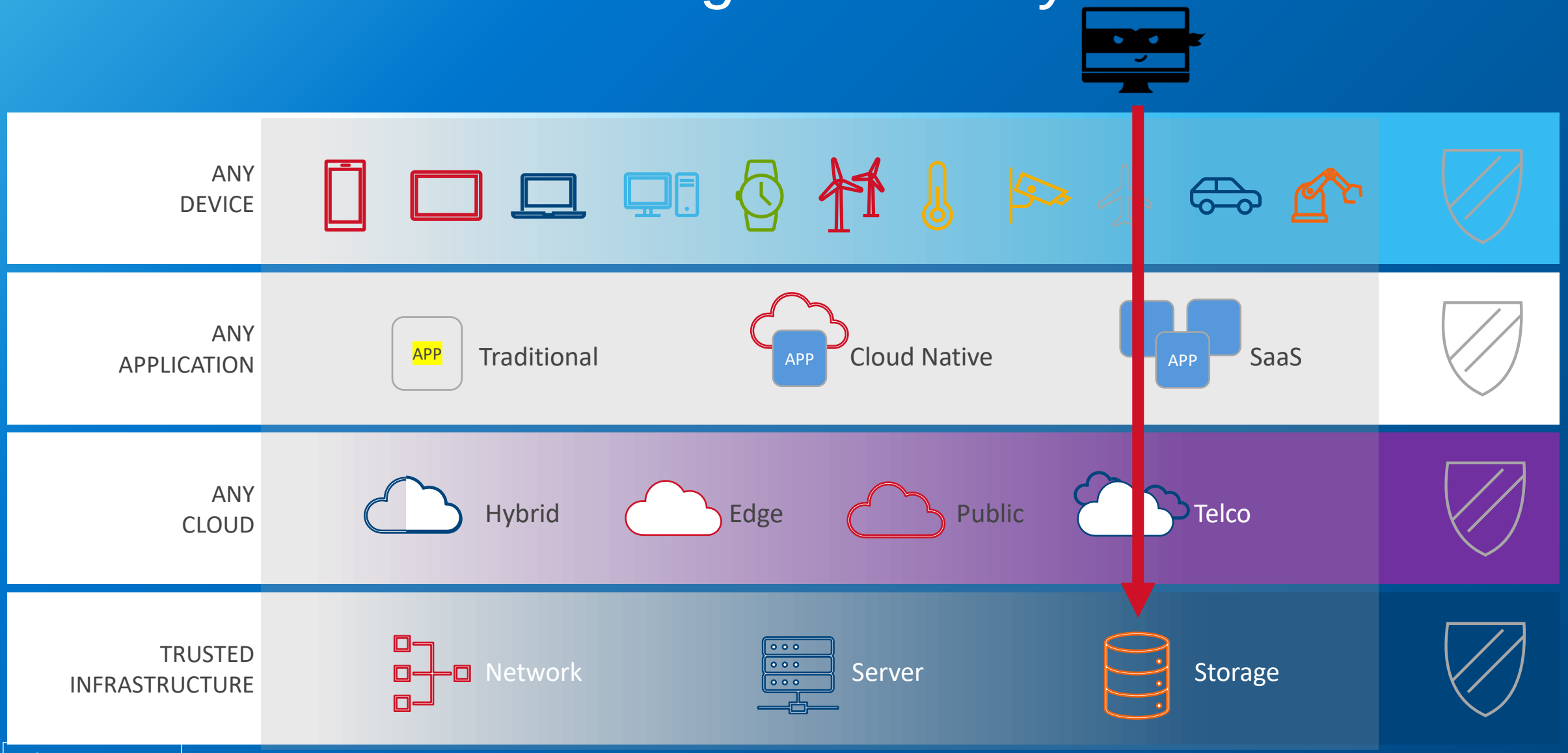
Si invitano, inoltre, i soggetti vigilati a considerare attentamente i piani di continuità aziendale (*business continuity plan*) e a garantire il corretto funzionamento e il pronto ripristino dei *backup*; in tale ambito, si sottolinea l'importanza di garantire la separazione dell'ambiente di *backup* da quello di esercizio, valutando la possibilità di prevedere soluzioni di *backup offline* (ossia che non siano fisicamente o logicamente collegati alla rete) dei sistemi e dei dati essenziali.

Si invitano, infine, i soggetti vigilati a prestare attenzione nel continuo agli aggiornamenti forniti dal Computer Security Incident Response Team - Italia (cfr. https://csirt.gov.it/contenuti?tags=Ucraina).

Si invitano, inoltre, i soggetti vigilati a considerare attentamente i piani di continuità aziendale (business continuity plan) e a garantire il corretto funzionamento e il pronto ripristino dei backup; **in tale ambito, si sottolinea l'importanza di garantire la separazione dell'ambiente di backup da quello di esercizio, valutando la possibilità di prevedere soluzioni di backup offline (ossia che non siano fisicamente o logicamente collegati alla rete) dei sistemi e dei dati essenziali.**

DELL Technologies

Dell Technologies Security Vision



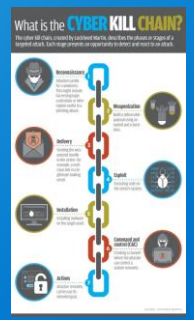
DELL Technologies PARTNER PROGRAM

DELL Technologies

What can happen to your data?

Depends on the motive of the attack

Hackers succeeding the Cyber Kill Chain*



Gain access to critical data

Encrypt and demand ransom

Permanently Delete

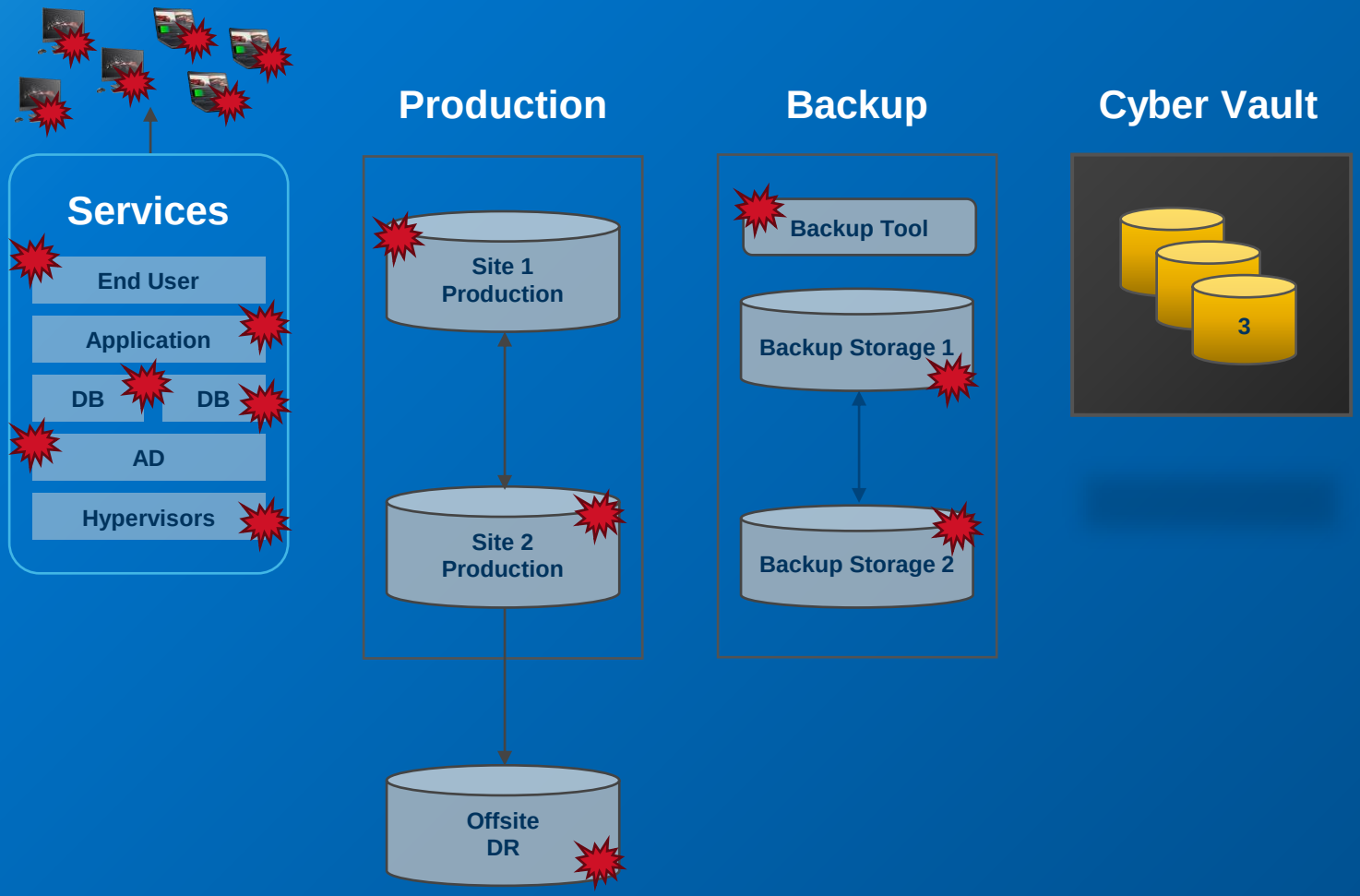
Sell data on the dark net

Trade secrets corporate espionage

* Source: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

The New Data Center Reality

Vaulting your data



DELL Technologies
PARTNER PROGRAM

DELL Technologies

CR is not DR!

	Disaster Recovery site	Cyber Recovery site
Protection against	Disasters	Cyber attacks
Network connection	Connected for Continuous replication	Isolated with intermittent replication
Admin privilege	IT Admins	Restricted to CISO
Recovery purpose	To support most of the business operations	To support only the most critical operations

DELL Technologies PARTNER PROGRAM

DELL Technologies

Covering the data landscape

One strategy

Enterprise databases

ERP Systems

VMware environments

IT Workloads

Archiving

Home directories

Video surveillance

File shares

Emerging Workloads

Artificial intelligence

Data analytics

Assisted driving

Internet of things

Production Workloads

Healthcare

Energy

EDA

Life sciences

Media & entertainment

Financial

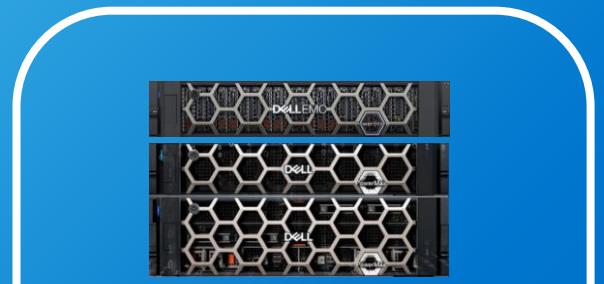
Manufacturing

Structured Data (20%)

Unstructured Data (80%)

DELL Technologies

Dell Technologies: Protecting the World's Data Landscape



Block Storage
PowerStore

Dell DPS

Veritas/IBM

DD Protect

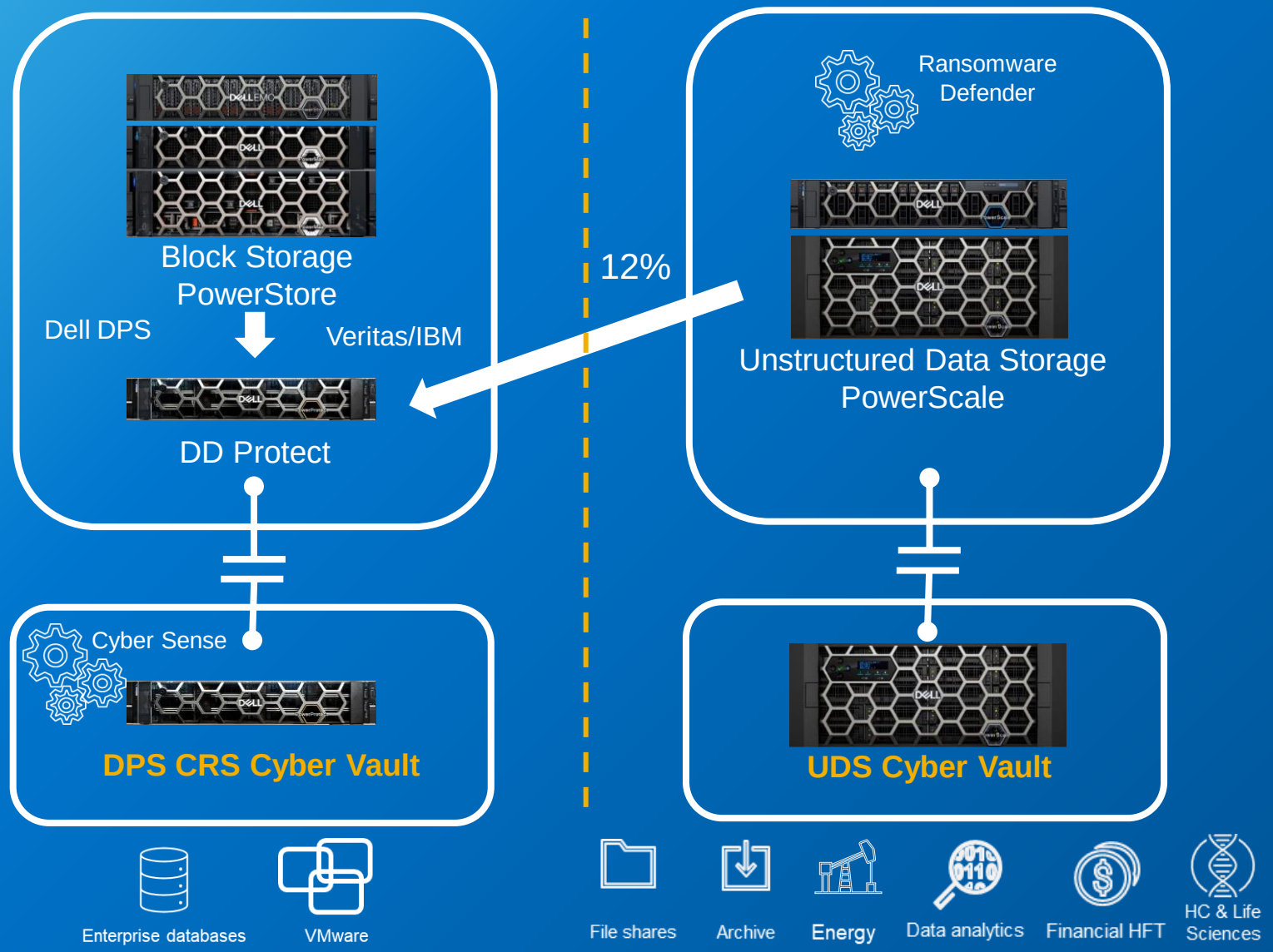
Cyber Sense

DPS CRS Cyber Vault

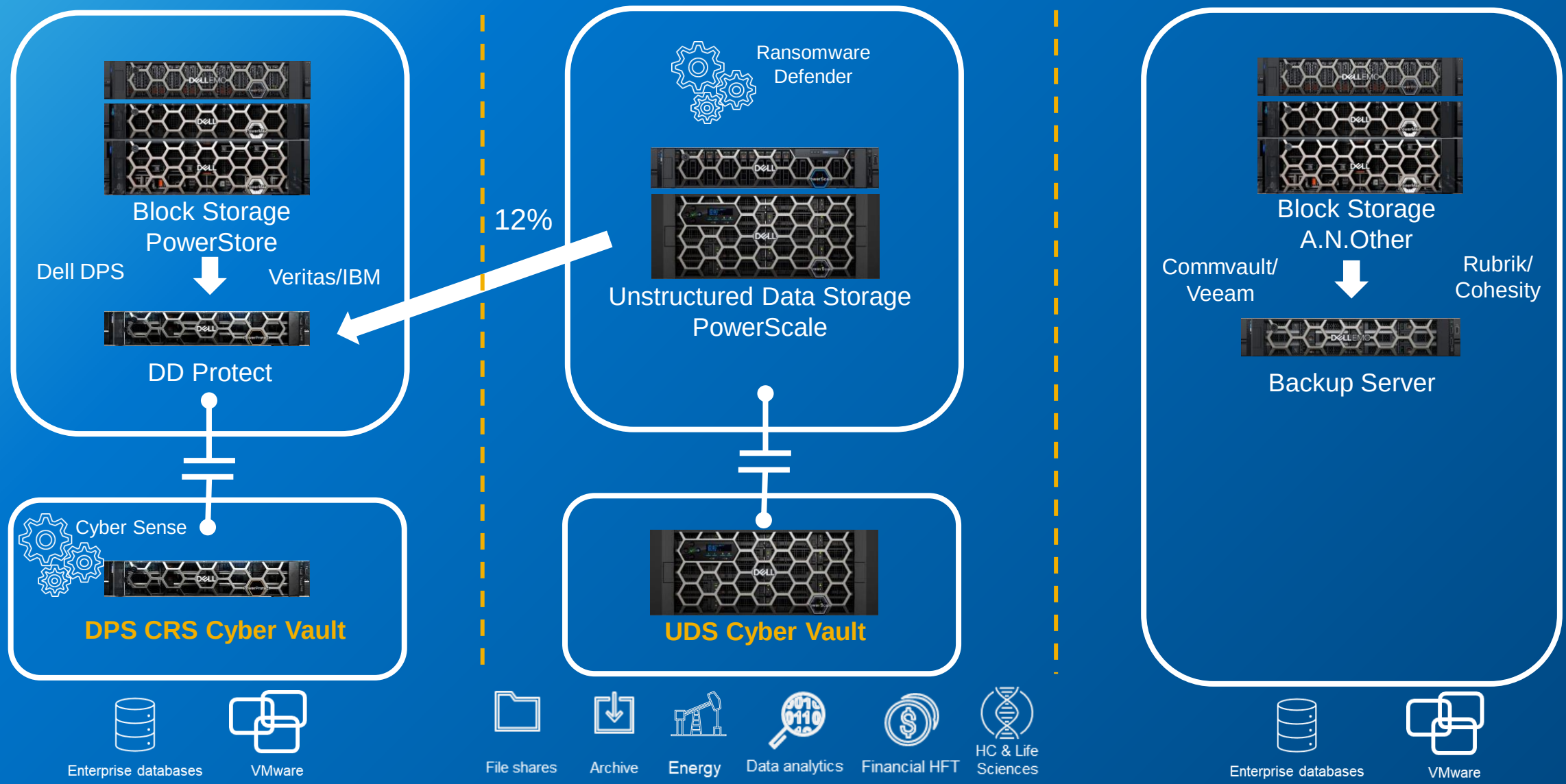
Enterprise databases

VMware

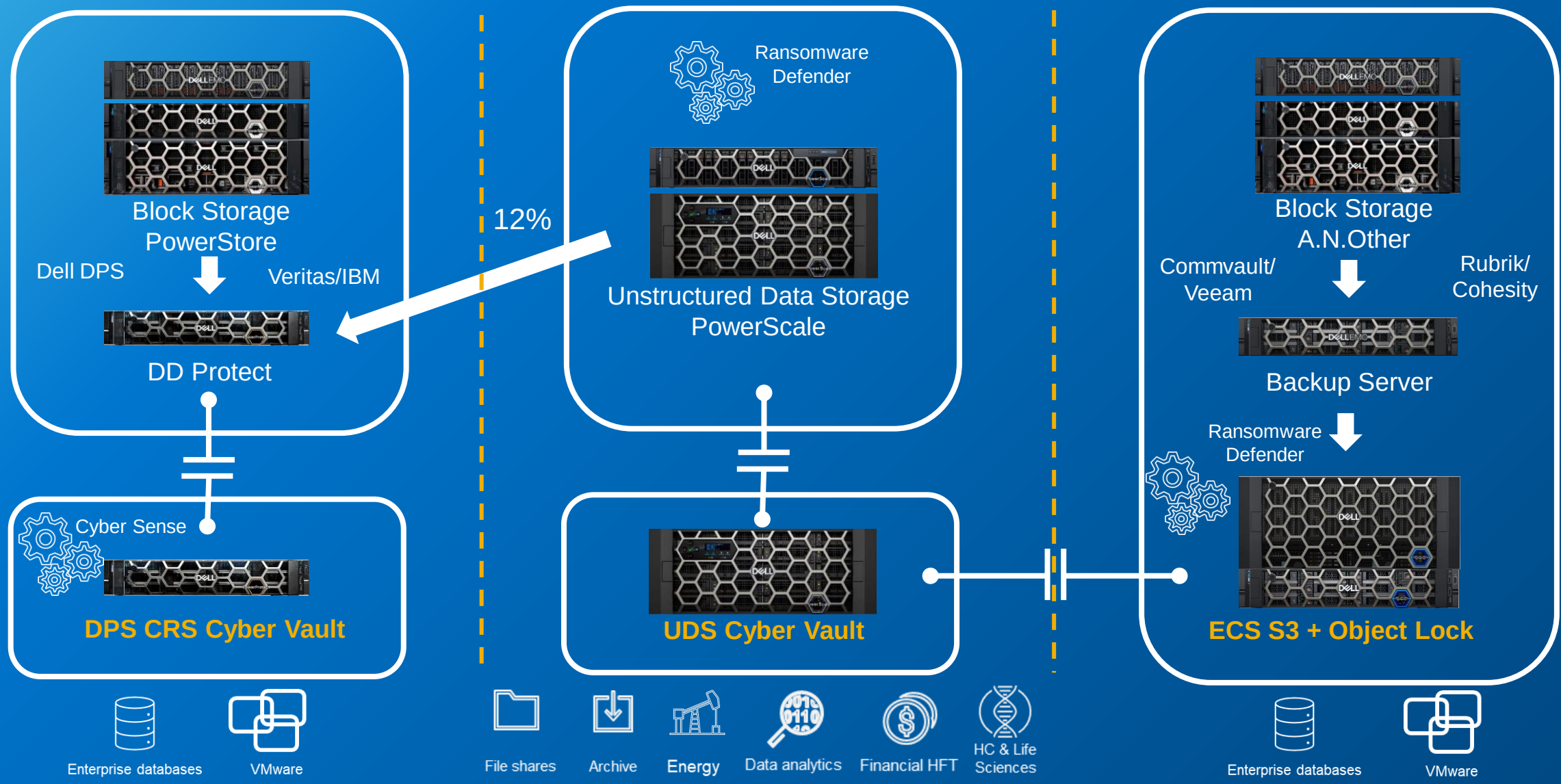
Dell Technologies: Protecting the World's Data Landscape



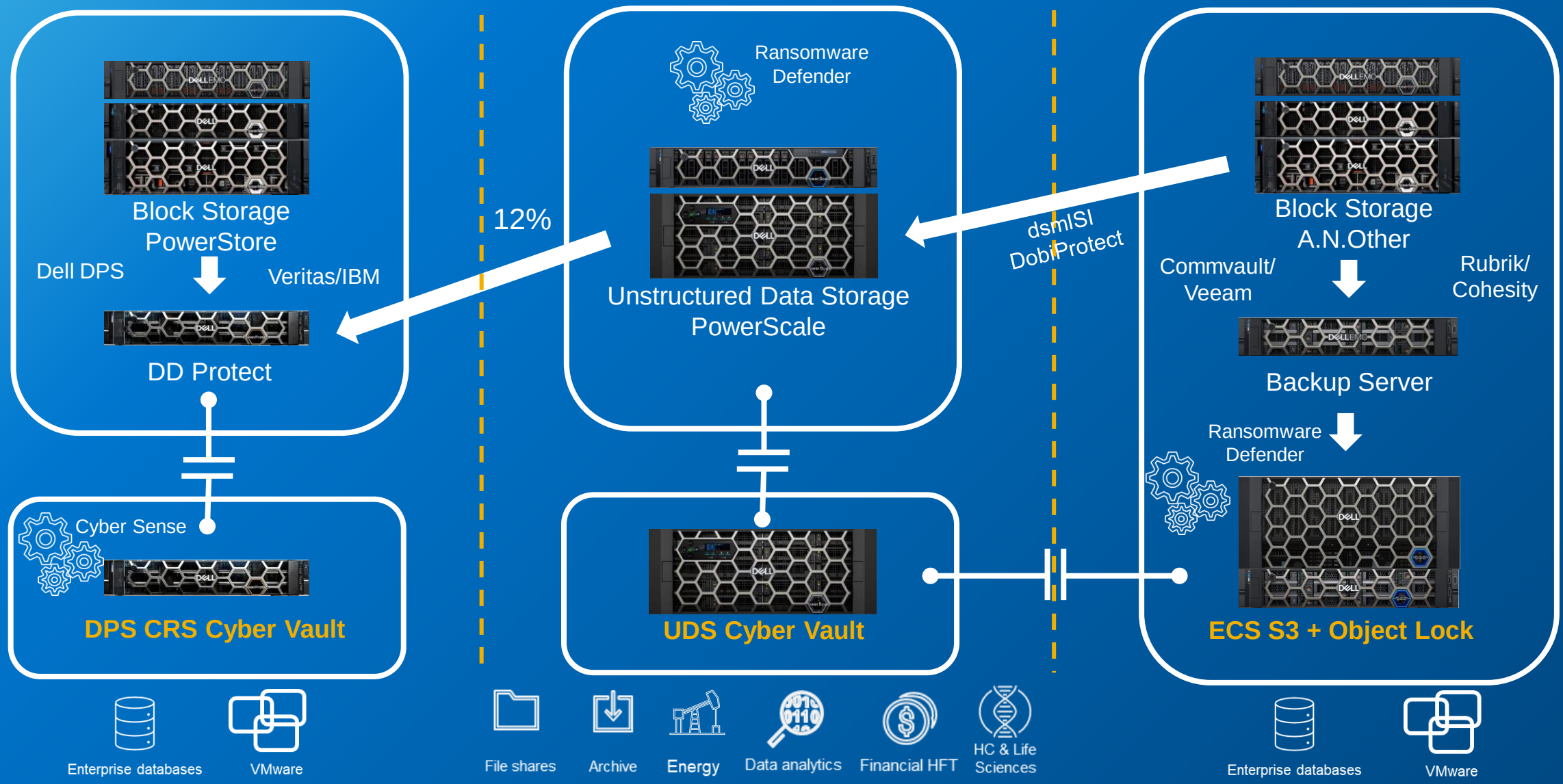
Dell Technologies: Protecting the World's Data Landscape



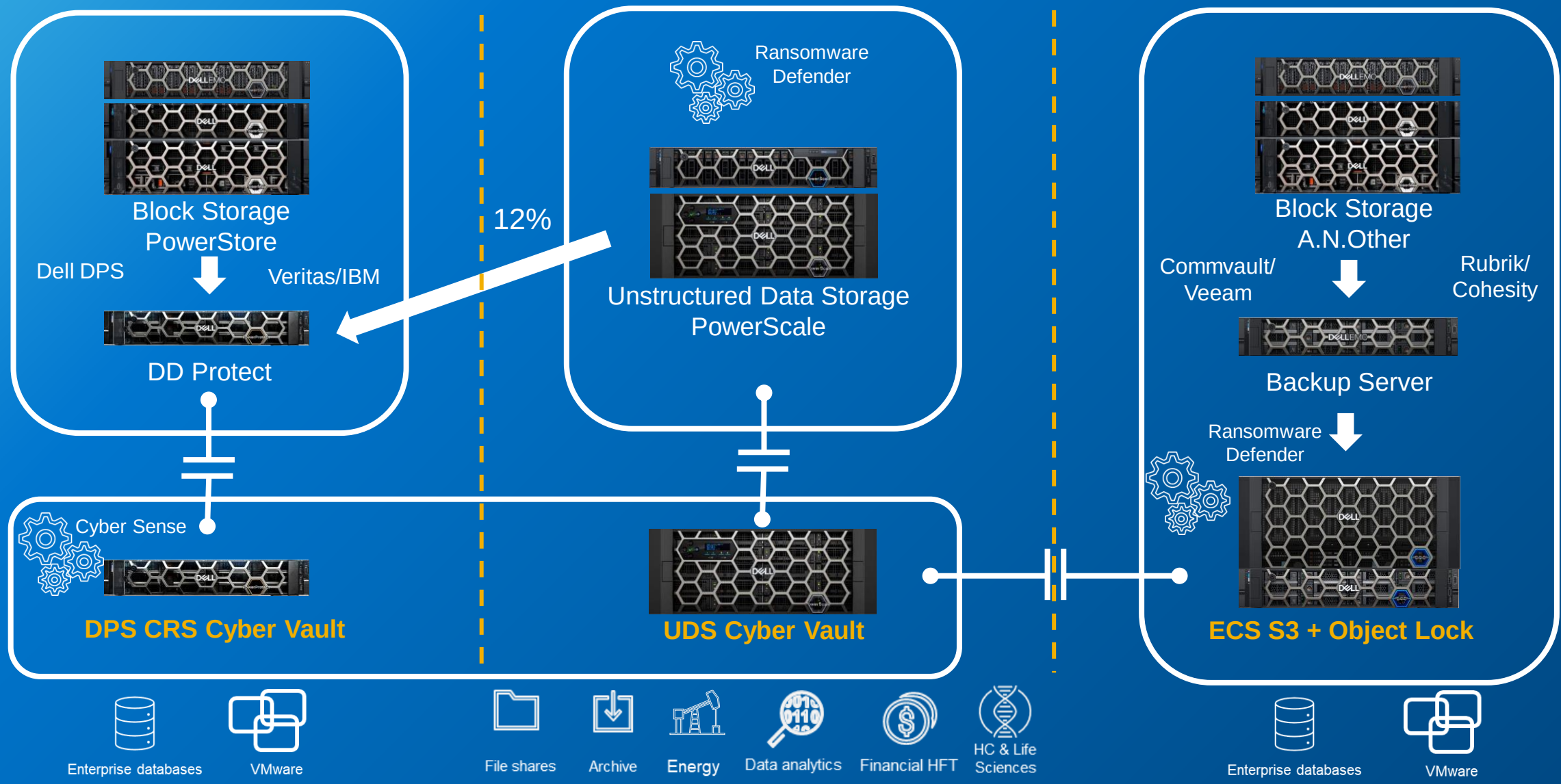
Dell Technologies: Protecting the World's Data Landscape



Dell Technologies: Protecting the World's Data Landscape



Dell Technologies: Protecting the World's Data Landscape



Two solutions based on workloads

PowerProtect Cyber Recovery for
Backup Data

Ransomware Defender for
Unstructured Data

Offering the same solution components

Already adopted by 1000+ Customers

Isolation

Physical & logical separation of data

Immutability

Preserve original integrity of data

Intelligence

Machine learning based threat detection, alerting and reporting

Recovery

Fast recovery for minimal operational impact

DELL Technologies PARTNER PROGRAM

DELL Technologies

Uncover Your Current Environment

Cyber Assessment Tool

What is the Cyber Resiliency Assessment tool?

A quick survey that provides a comprehensive health check on an organization's ability to detect, respond to and recover from threats like ransomware **The output is a detail report on the areas that pose the biggest risk to customers data.**

Cyber Assessment Tool = Cyber Assessment tool

Live Optics

FREE ASSESSMENT per tutti i partecipanti all'evento

Q&A

DELL Technologies PARTNER PROGRAM

DELL Technologies

GRAZIE

DELL Technologies
PARTNER PROGRAM

DELL Technologies

DELL Technologies

PARTNER PROGRAM