Cyber Resilience:
Are your ready for 2025?

Sam Taher
Global Account Manager
Data Protection & Cyber Resiliency
Dell Technologies

Steve Koss
Distinguished Engineer and Global Lead,
ClearPath Forward® Solution Architects,
Unisys

SEPTEMBER 28, 2023

unisys

DELL Technologies
PLATINUM PARTNER

The Time for Resilience is Now!

Cyber Resiliency - The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

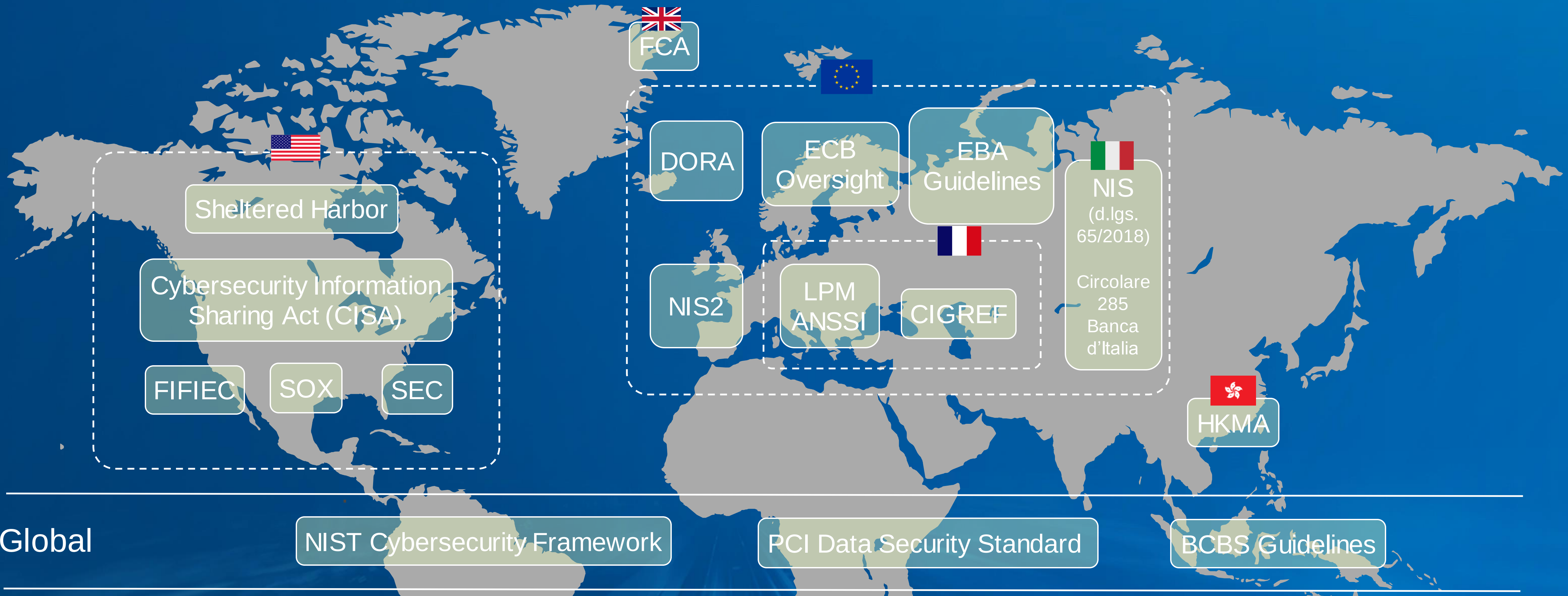
Can your organization withstand a cyber attack?

“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!

Some Cyber Security Regulations…

A common concern, multiple answers…



FCA

DORA

ECB Oversight

EBA Guidelines

NIS2

LPM ANSSI

CIGREF

NIS (d.lgs. 65/2018)

Circolare 285 Banca d'Italia

Sheltered Harbor

Cybersecurity Information Sharing Act (CISA)

FIFIEC

SOX

SEC

HKMA

Global

NIST Cybersecurity Framework

PCI Data Security Standard

BCBS Guidelines

Note: Applicable regulation depends on where a bank operates, not where they are headquartered
A US bank operating in the EU must comply with EU regulation for its EU operation (and conversely)

Cyber Resilience Regulations in the EU & UK

A quick overview of the regulatory frameworks

- **NIS2 Directive - Network and Information Systems V2**
  - Directive (EU) 2022/2555, published 14 December 2022, 21 months to incorporate in national laws
  - Sectors covered:
    - **Essential**: Healthcare, Digital infrastructure, Transport, Water supply, Digital service providers, Banking, Financial market infrastructure, Energy, Wastewater, Health (pharmaceuticals, R&D, critical medical devices), Space, Public administration
    - **Important**: Providers of public electronic communications networks or services, Chemicals, Food producers, processors and distributors, Manufacturing of critical products (medical devices, computers, electronics, motor vehicles), Digital providers (social networking platforms, search engines, online marketplaces), Postal and courier services
    - Member states can levy fines of up to EUR 10 million or 2% of annual turnover (revenue) for certain violations or breaches. In addition, critical entity management bodies (i.e., executive teams) can be held personally liable for infringements.
- **DORA - Digital Operational Resilience Act**
  - EU 2022/2554 – published 14 December 2022, applicable 17 January 2025
  - For all Financial Institutions operating in the European Union
    - Must protect, detect, contain, **recover and repair** against Information Communication Technologies (ICT) related events in a timely manner. This explicitly includes ICT risk management, incident reporting, and operational resilience testing. A lack of operational resiliency jeopardizes the entire financial system. Entered in to force: 17 Jan 2025.

- **Financial Conduct Authority in UK** – Focus on IBS and follow EBA guidelines
- **European Banking Authority** – ICT Guidelines

- **Basel Committee on Banking Supervision** – Principals for operational resilience
- **Loi de Programmation Militaire in France** – Aims to strengthen national security in the field of cyber security

- **European Central Bank** – Cyber resilieny oversight
- **ANSSI**
- **Italy Best Practices**
  - Comunicato Stampa
  - CERTFin Ransomware Playbook 2023

Cyber Resilience Maturity…

Where we stand..

- While regulators often do not require a specific cyber strategy or product, **all expect institutions to maintain adequate capability in this area**
- In most jurisdictions, broader IT and operational risk management practices are quite mature and are used to address cyber-risk and supervise cyber-resilience
- Banks nonetheless generally still **lack a cyber strategy that defines clear tolerance and appetite levels for cyber risk and that has been approved at board level**
- Cyber resilience is not always clearly articulated across the technical, business and strategic defense lines
- Protection and detection testing is evolving and prevalent - **response and recovery less so**
- Incident recovery preparation and testing is still typically done through tabletop exercises, and broader continuity testing. **Things need to improve in this area.**

PowerProtect Cyber Recovery Advantage

Transforming Data Protection to Data Resilience

DELL Technologies

Key Enabler of Mature Cyber Resiliency Plan

Focus on increasing confidence in the ability to recover from a cyber attack through key technologies and processes

Isolation, Immutability & Automation

Intelligence: AI/ML based security analytics tools

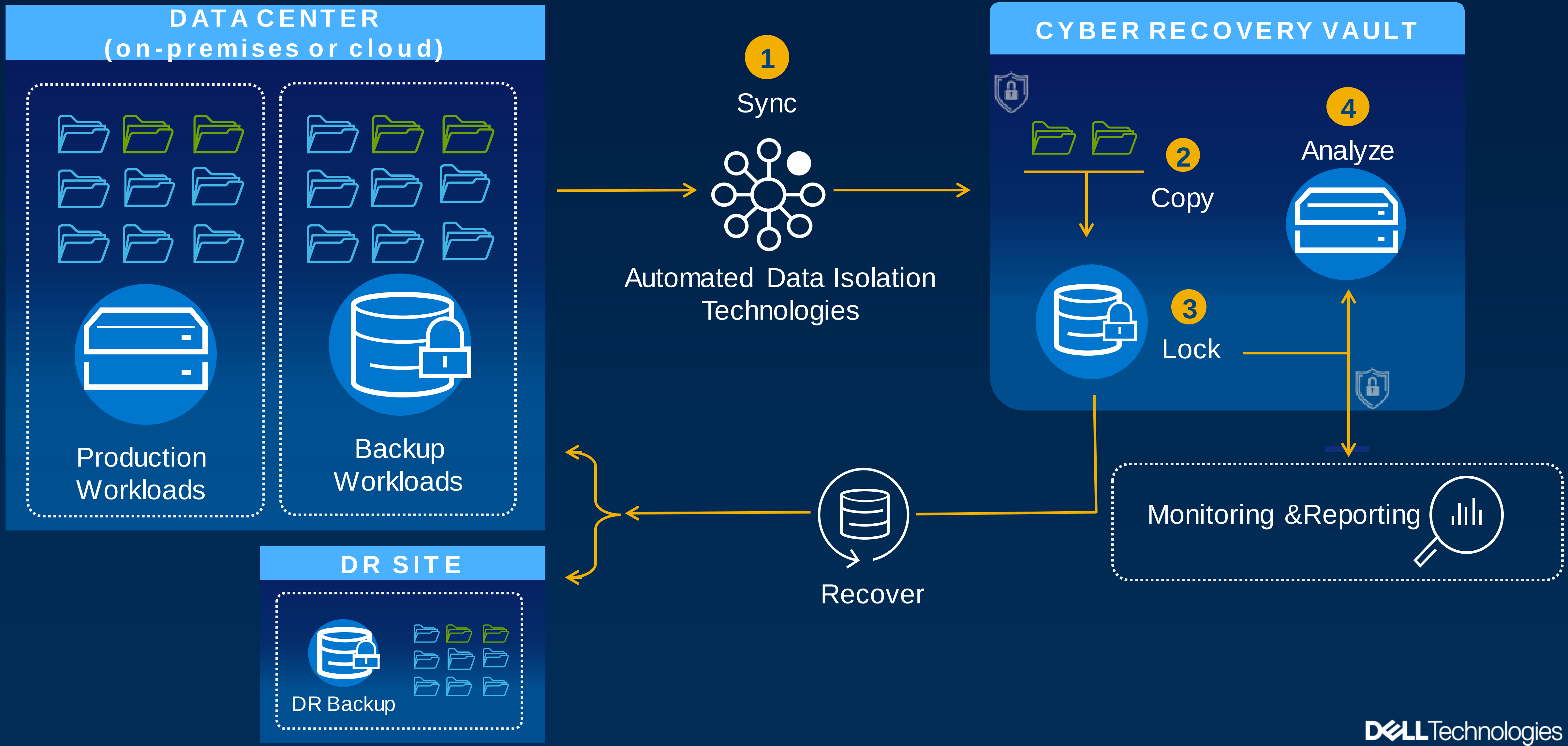
Runbooks and recovery process

Business Recovery At speed and scale

Cross functional enablement

Dell PowerProtect Cyber Recovery

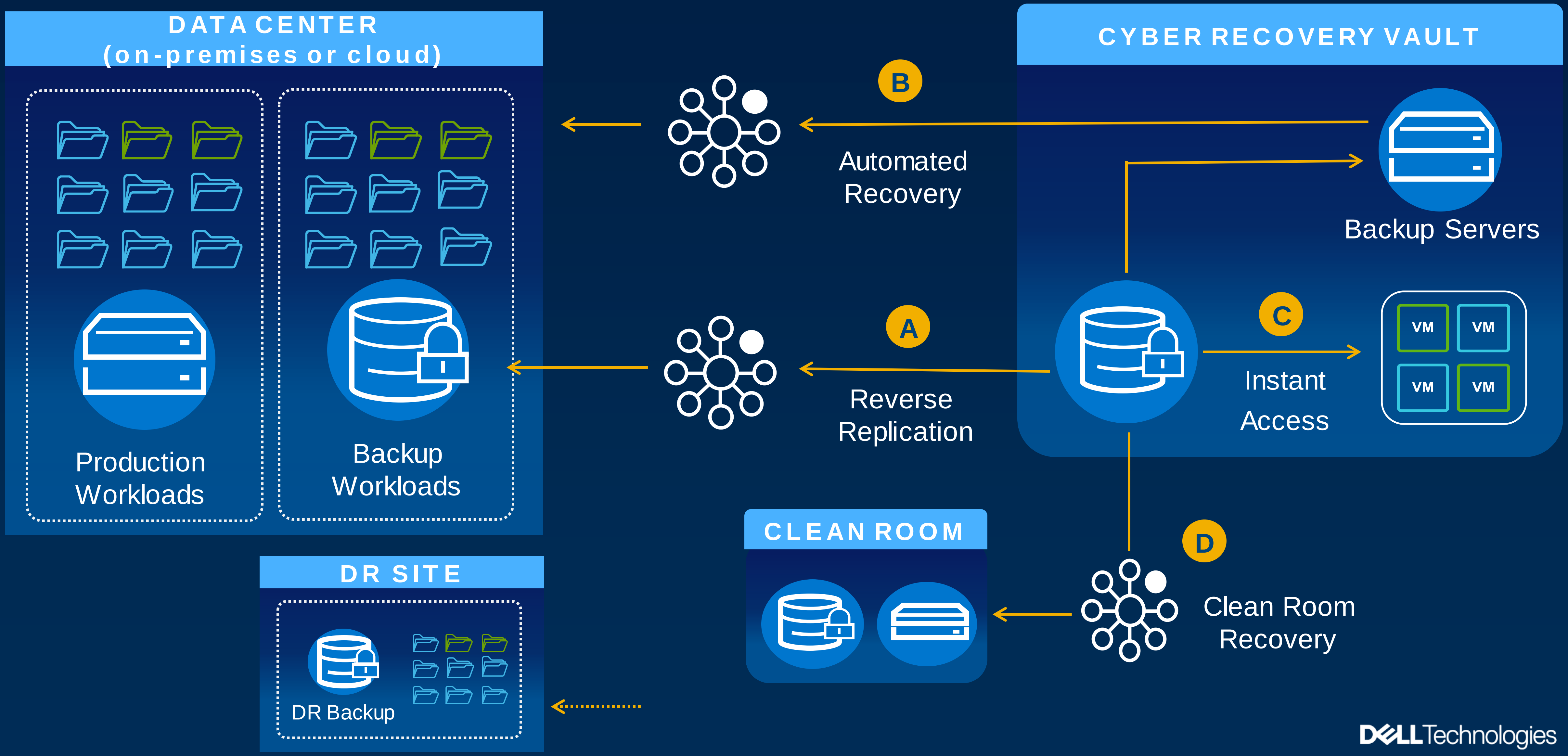
Ensuring the Recovery of Critical Rebuild Data in case of Cyber Threats



DELL Technologies

Recovery Options with PowerProtect Cyber Recovery

Flexible Recovery options



DELL Technologies

PowerProtect Cyber Recovery Deployment

Modern protection and recovery for critical rebuild data from ransomware and cyber threats to **enable cyber resiliency and ensure business continuity**.

ON-PREMISES

Optional Managed Services

COLOCATION/CLOUD ADJACENT

PUBLIC CLOUD

aws
Google Cloud

The Power of PowerProtect Cyber Recovery

Reduce Risk, Speed Recovery and Lower costs to recovery from Destructive Cyberattacks

PowerProtect DD and DDVE are the foundation of Data Protection – fast, storage efficient and highly secured for resilience

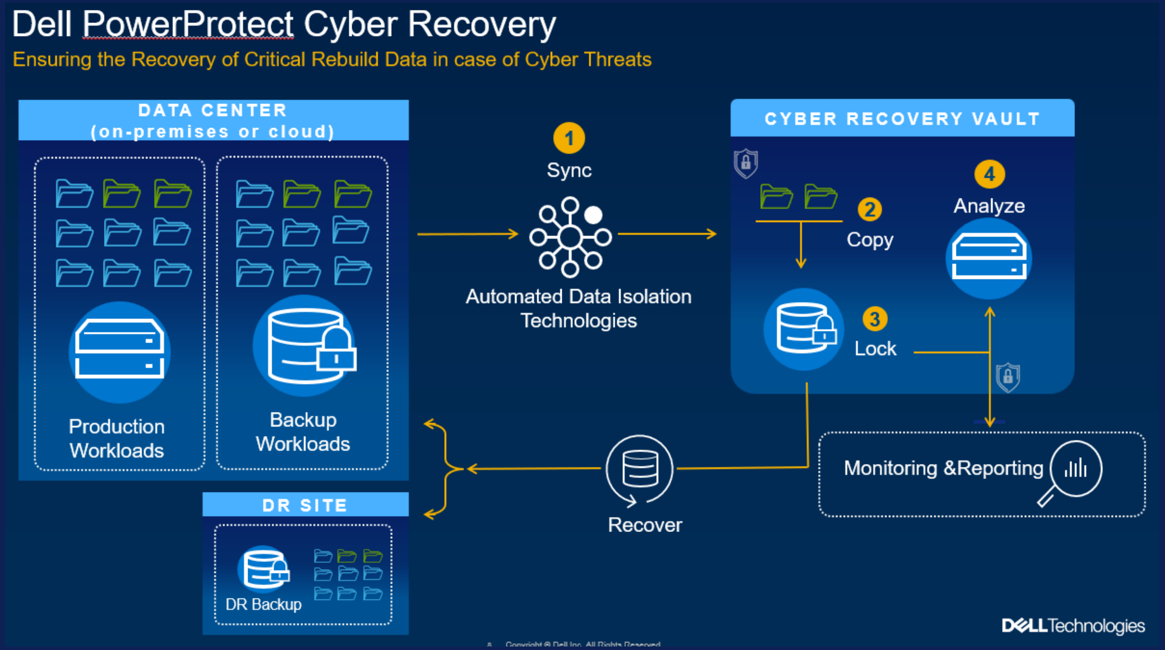
Immutability & multi-layered security design protects against a full spectrum of threats, including insiders

Physical and logical **Isolation** technologies protect the data vault from unauthorized access

Intelligent analytics & ML help to enable confident recovery with data integrity

First and **Only** Sheltered Harbor endorsed turnkey data vaulting solution to confidently recover financial data

2,200^{+} customers[1]



Dell PowerProtect Cyber Recovery

Ensuring the Recovery of Critical Rebuild Data in case of Cyber Threats

On-premises – Colocation - Public Cloud

Whether on-premises, colocation or public cloud, Dell PowerProtect Cyber Recovery protects critical data from cyberattacks with flexible deployments and streamlined recovery options.

[1] Based on Dell Technologies analysis, February 2023

What about ClearPath…

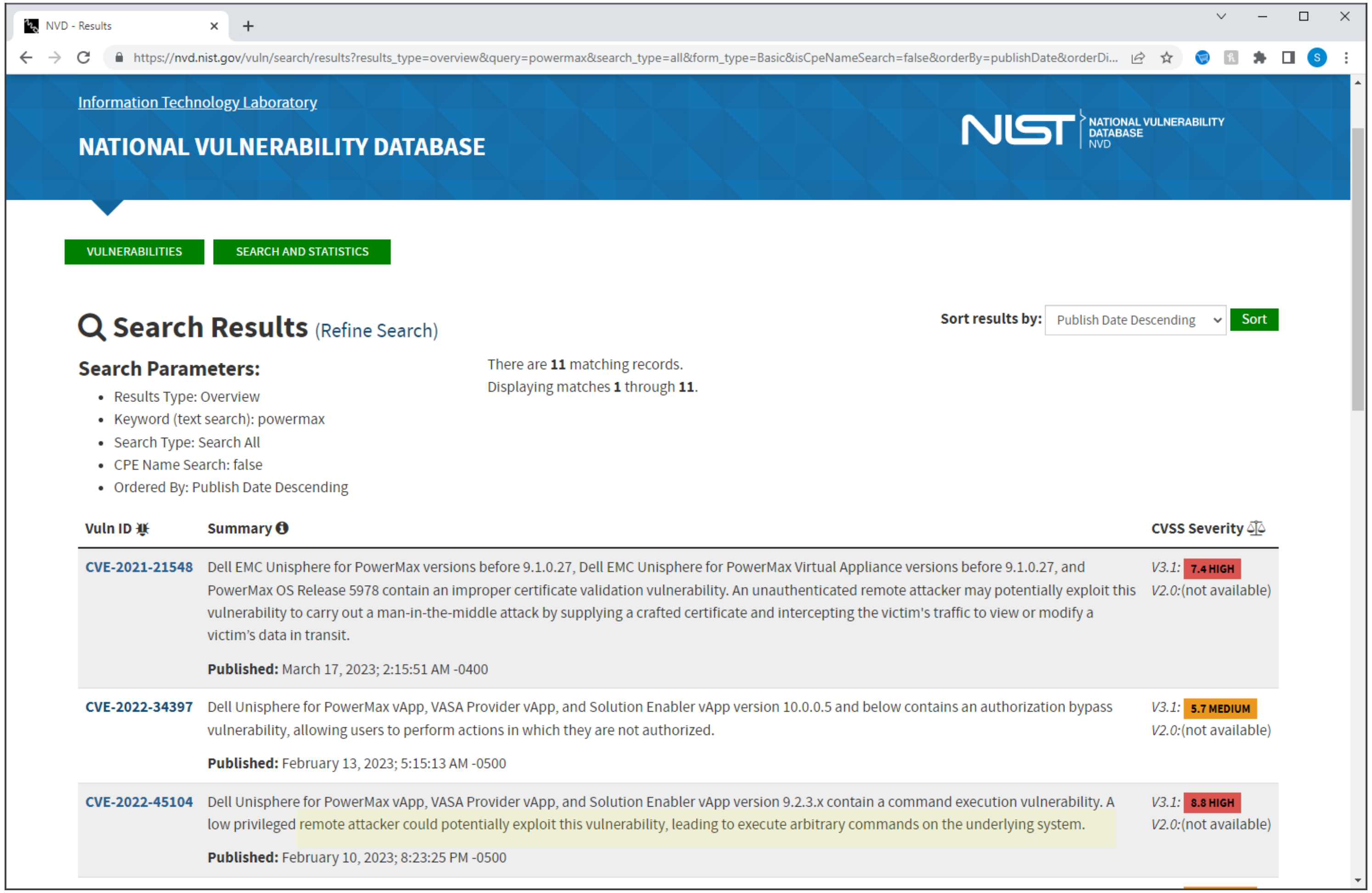
Today’s ClearPath Ecosystem – Why Cyber Vault

- Minimal ClearPath “Vulnerabilities” – DoS, Software Crash – No Data access.

- Storage Replication is for Datacenter/Storage Failure – not Malware
- Storage Snapshots are for Software Problems

- TAPE isn’t really TAPE, it’s another computer
- DISK isn’t really DISK, it’s another computer
- Libra/Dorado vs. MCP/OS 2200 Software Series / Developer Studio
- Surrounding Servers critical to running (OpCon)
- MCP: External Software directly accessing MCP disks, bypassing MCP security

Example: Storage Vulnerabilities(Dell PowerMax – Unisphere)


NVD - Results
https://nvd.nist.gov/vuln/search/results?results_type=overview&query=powermax&search_type=all&form_type=Basic&isCpeNameSearch=false&orderBy=publishDate&orderDi...
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NIST NATIONAL VULNERABILITY DATABASE NVD
VULNERABILITIES
SEARCH AND STATISTICS

Search Results (Refine Search)

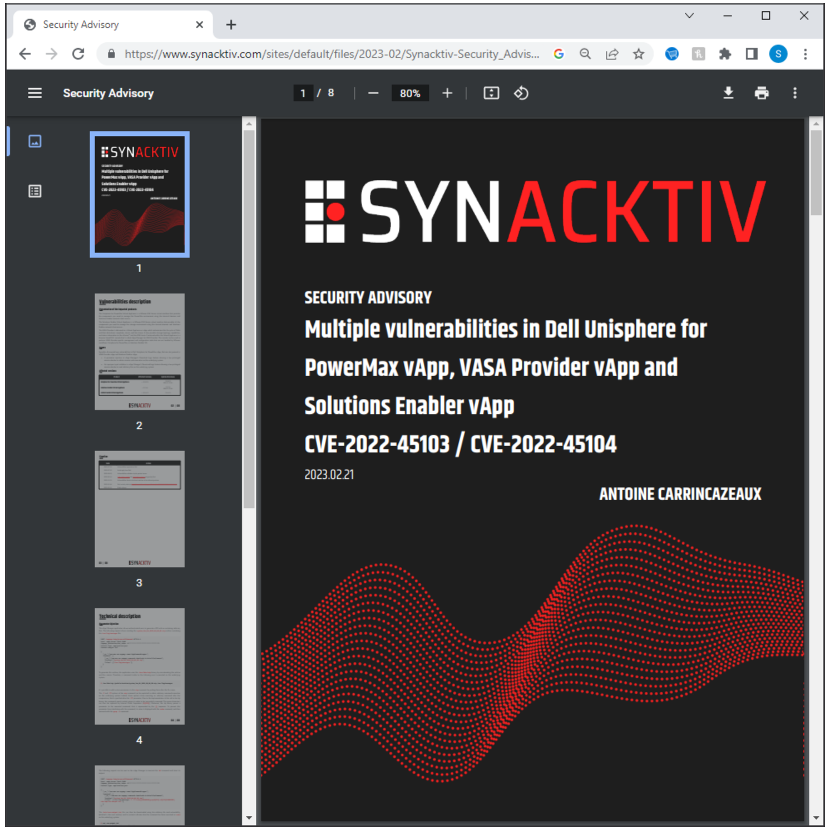
Sort results by: Publish Date Descending Sort

Search Parameters:

- Results Type: Overview
- Keyword (text search): powermax
- Search Type: Search All
- CPE Name Search: false
- Ordered By: Publish Date Descending

There are **11** matching records.
Displaying matches **1** through **11**.

Vuln ID	Summary	CVSS Severity
CVE-2021-21548	Dell EMC Unisphere for PowerMax versions before 9.1.0.27, Dell EMC Unisphere for PowerMax Virtual Appliance versions before 9.1.0.27, and PowerMax OS Release 5978 contain an improper certificate validation vulnerability. An unauthenticated remote attacker may potentially exploit this vulnerability to carry out a man-in-the-middle attack by supplying a crafted certificate and intercepting the victim's traffic to view or modify a victim's data in transit. **Published:** March 17, 2023; 2:15:51 AM -0400	V3.1: 7.4 HIGH V2.0:(not available)
CVE-2022-34397	Dell Unisphere for PowerMax vApp, VASA Provider vApp, and Solution Enabler vApp version 10.0.0.5 and below contains an authorization bypass vulnerability, allowing users to perform actions in which they are not authorized. **Published:** February 13, 2023; 5:15:13 AM -0500	V3.1: 5.7 MEDIUM V2.0:(not available)
CVE-2022-45104	Dell Unisphere for PowerMax vApp, VASA Provider vApp, and Solution Enabler vApp version 9.2.3.x contain a command execution vulnerability. A low privileged remote attacker could potentially exploit this vulnerability, leading to execute arbitrary commands on the underlying system. **Published:** February 10, 2023; 8:23:25 PM -0500	V3.1: 8.8 HIGH V2.0:(not available)


Security Advisory
https://www.synacktiv.com/sites/default/files/2023-02/Synacktiv-Security_Advis...
Security Advisory
1 / 8
80%
SYNACKTIV

SECURITY ADVISORY

Multiple vulnerabilities in Dell Unisphere for PowerMax vApp, VASA Provider vApp and Solutions Enabler vApp

CVE-2022-45103 / CVE-2022-45104

2023.02.21

ANTOINE CARRINCAZEAUX

https://www.synacktiv.com/sites/default/files/2023-02/Synacktiv-Security_Advisory-Dell_EMC_vApp_Manager-Multiple_Vulnerabilities.pdf

The criminals are finding that data extortion is more effective than system extortion via encryption.

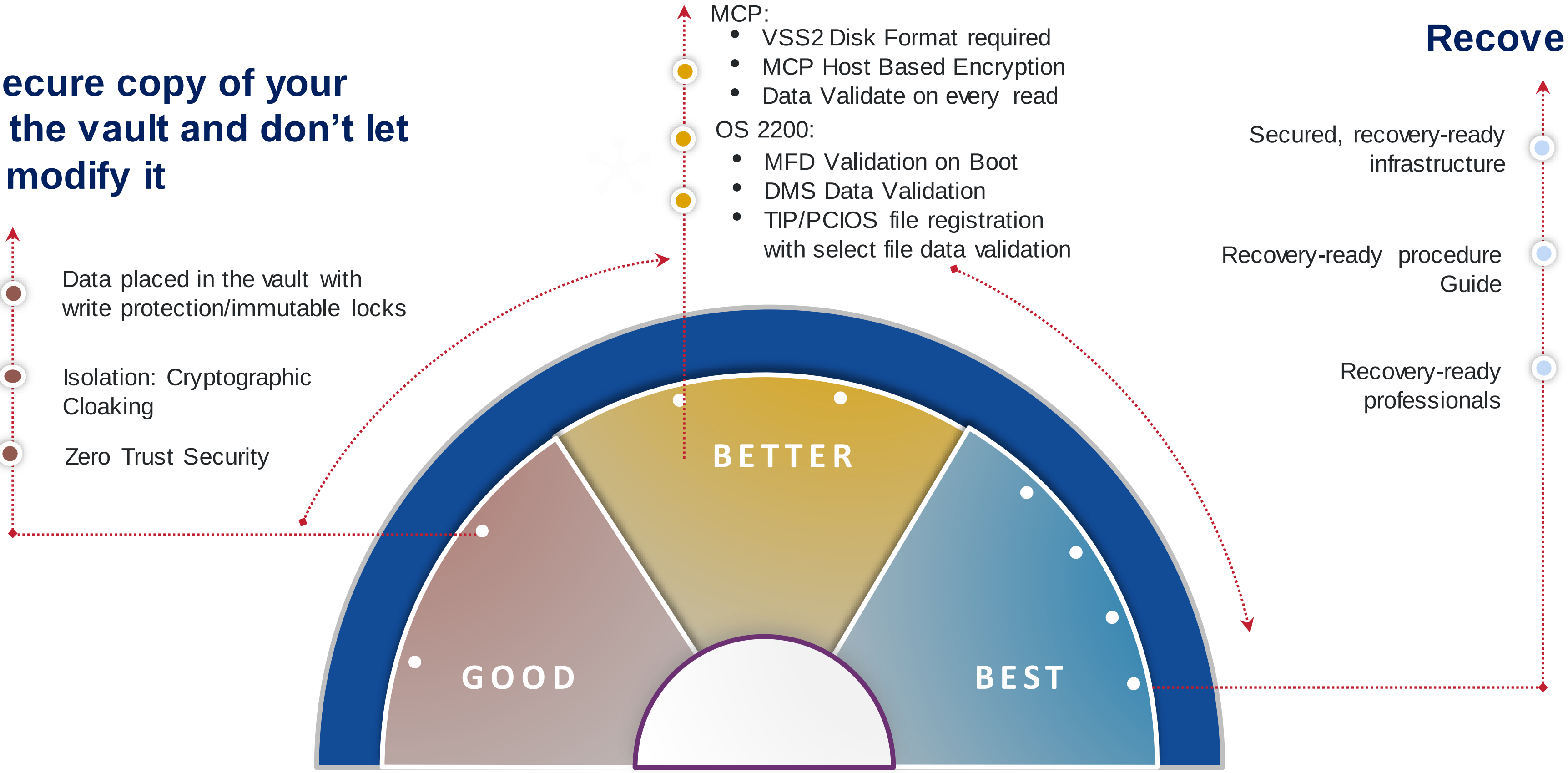
In 2023, we'll see ransomware attacks focusing on corrupting data rather than encrypting it.

Since almost all ransomware operators already engage in double extortion, meaning they exfiltrate the data before encrypting it.

Andrew Hollister, CISO LogRhythm

DELL Technologies PLATINUM PARTNER

Cyber Recovery for ClearPath: What Unisys Adds



Place a secure copy of your data into the vault and don’t let anybody modify it

- Data placed in the vault with write protection/immutable locks
- Isolation: Cryptographic Cloaking
- Zero Trust Security

Validate the data

MCP:

- VSS2 Disk Format required
- MCP Host Based Encryption
- Data Validate on every read

OS 2200:

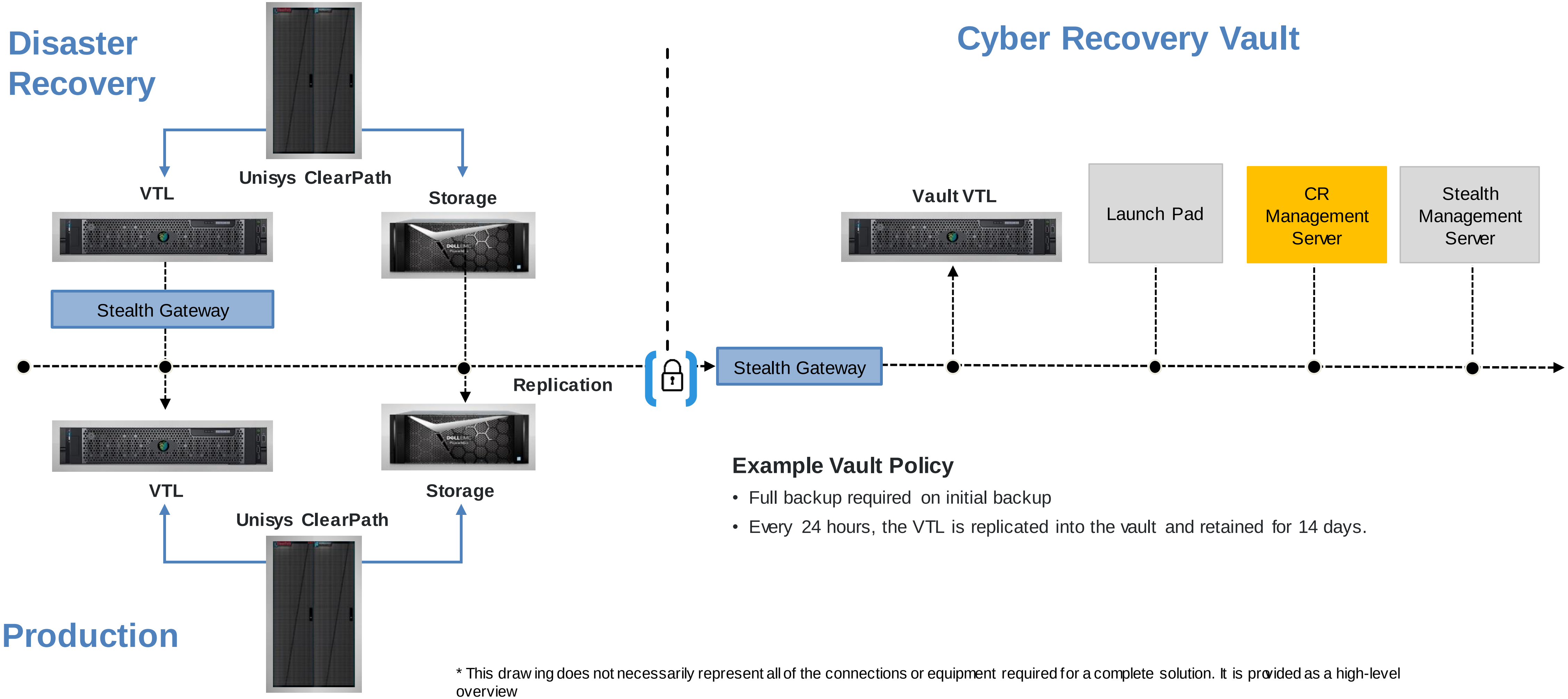
- MFD Validation on Boot
- DMS Data Validation
- TIP/PCIOS file registration with select file data validation

Recovery Ready

- Secured, recovery-ready infrastructure
- Recovery-ready procedure Guide
- Recovery-ready professionals

DELLTechnologies PLATINUM PARTNER

Unisys ClearPath VTL Cyber Recovery – Conceptual Example

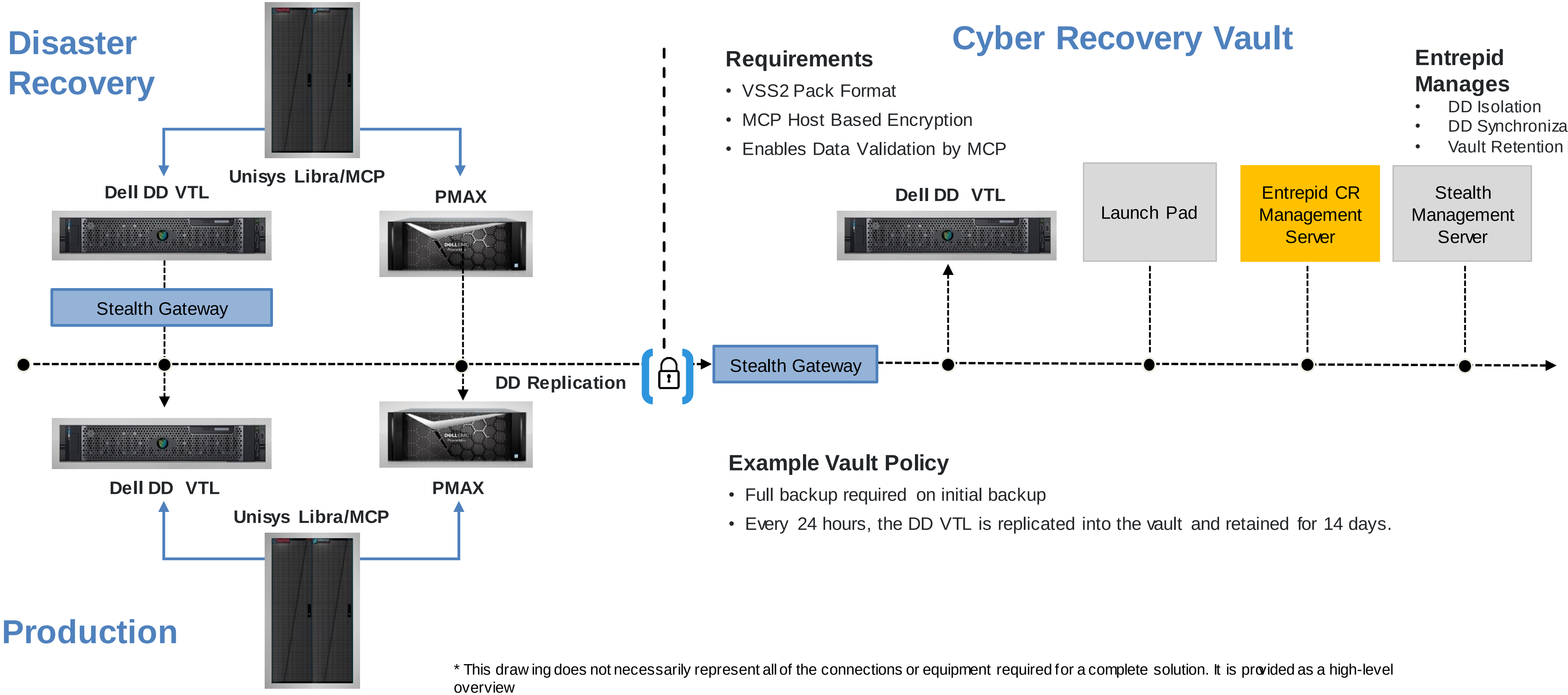


Example Vault Policy

- Full backup required on initial backup
- Every 24 hours, the VTL is replicated into the vault and retained for 14 days.

* This drawing does not necessarily represent all of the connections or equipment required for a complete solution. It is provided as a high-level overview

Unisys ClearPath MCP Dell DD VTL Cyber Recovery



Requirements

- VSS2 Pack Format
- MCP Host Based Encryption
- Enables Data Validation by MCP

Entrepid Manages

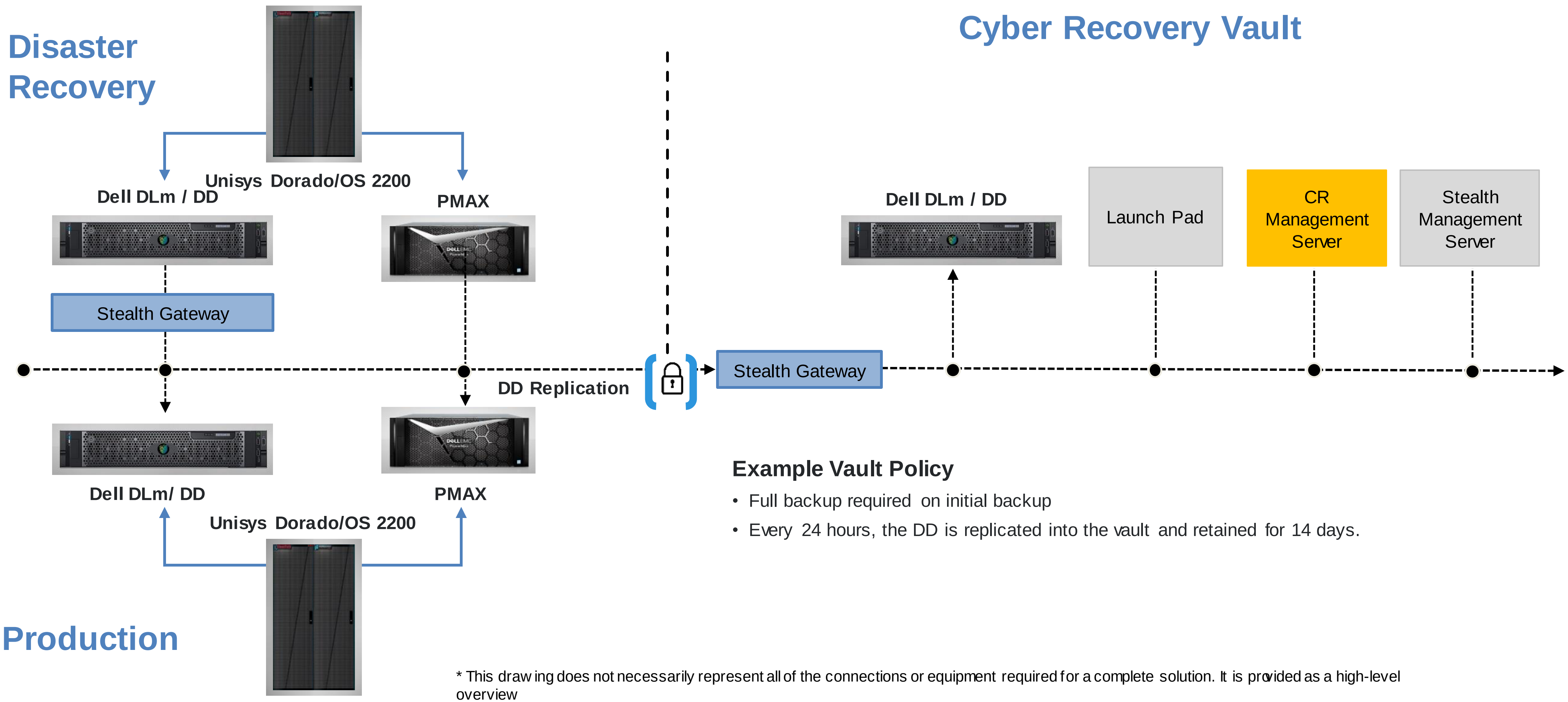
- DD Isolation
- DD Synchronization
- Vault Retention Lock

Example Vault Policy

- Full backup required on initial backup
- Every 24 hours, the DD VTL is replicated into the vault and retained for 14 days.

* This drawing does not necessarily represent all of the connections or equipment required for a complete solution. It is provided as a high-level overview

Unisys ClearPath OS 2200 Dell DLm Cyber Recovery

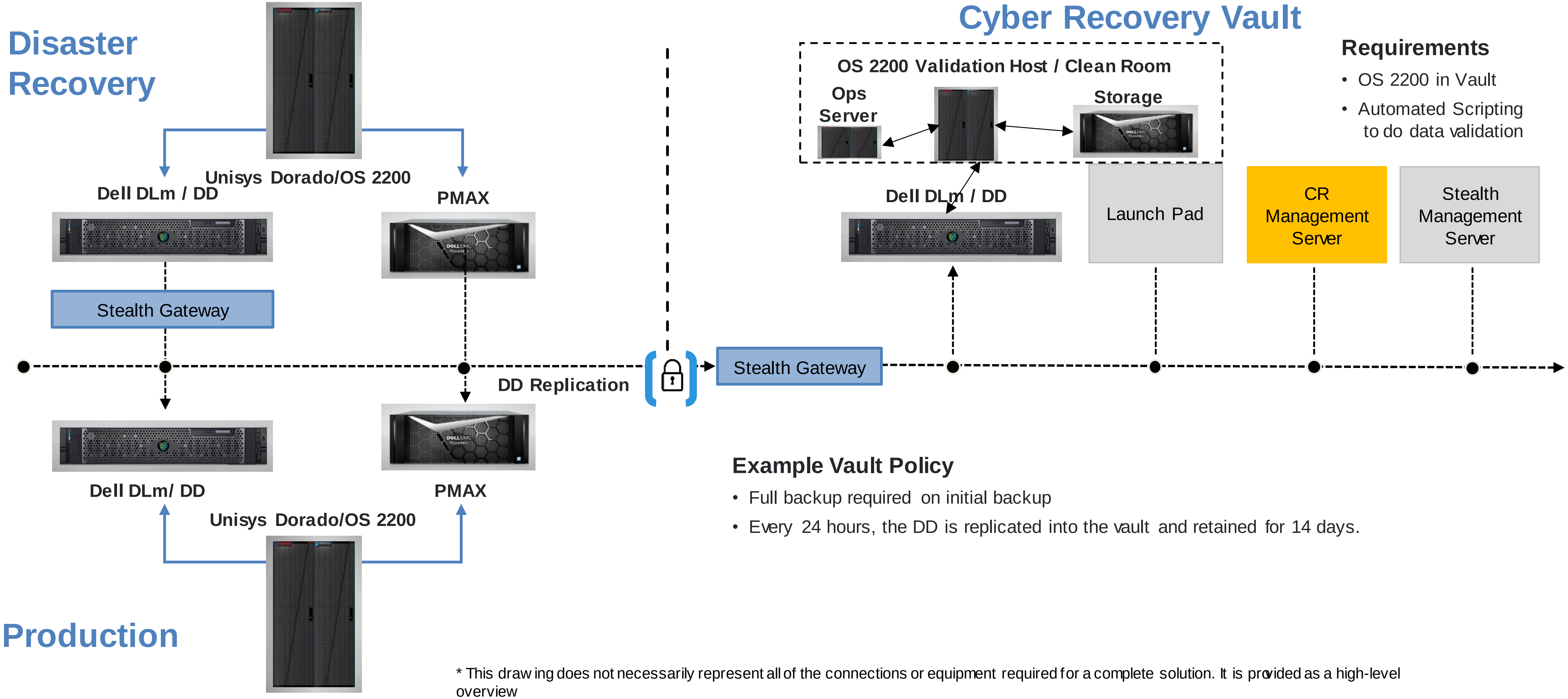


Example Vault Policy

- Full backup required on initial backup
- Every 24 hours, the DD is replicated into the vault and retained for 14 days.

* This drawing does not necessarily represent all of the connections or equipment required for a complete solution. It is provided as a high-level overview

Unisys ClearPath OS 2200 Dell DLm Cyber Recovery – Data Validation



Requirements

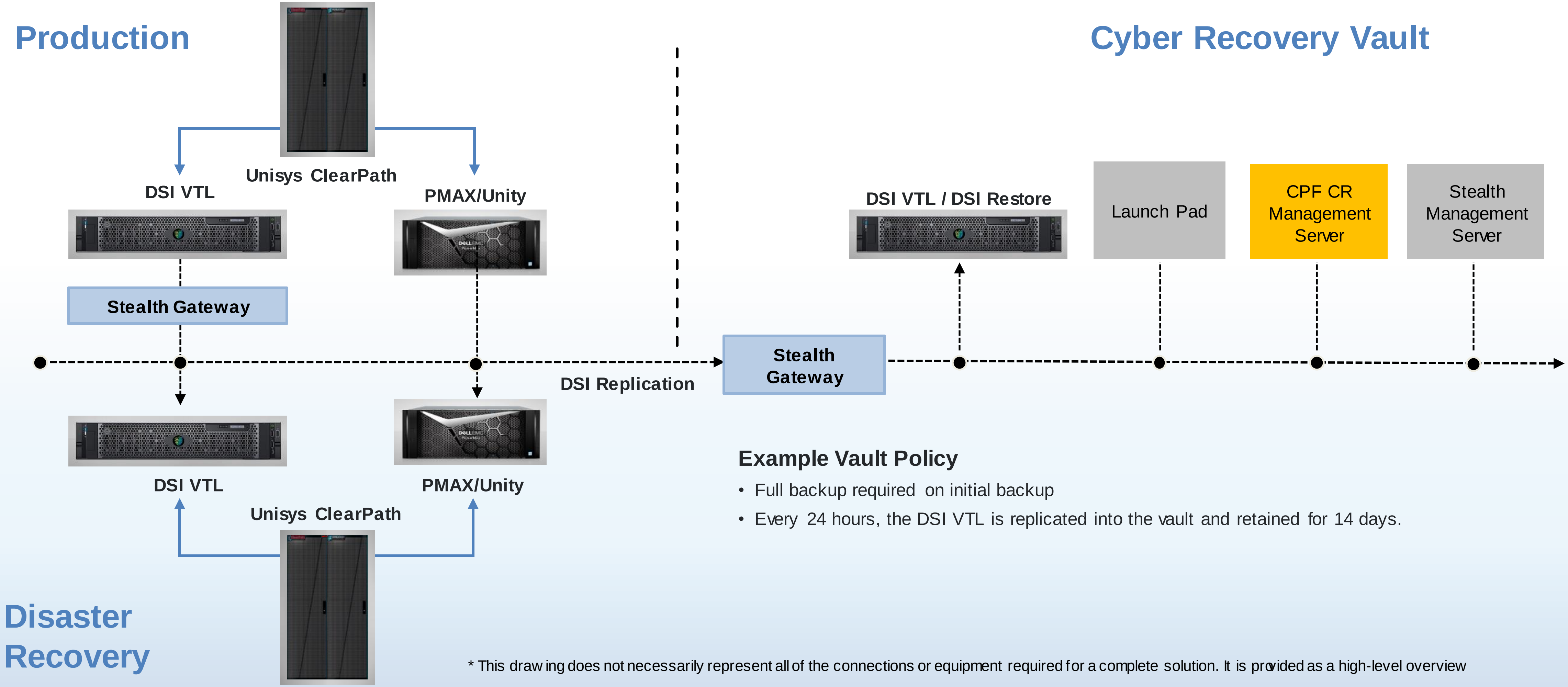
- OS 2200 in Vault
- Automated Scripting to do data validation

Example Vault Policy

- Full backup required on initial backup
- Every 24 hours, the DD is replicated into the vault and retained for 14 days.

* This drawing does not necessarily represent all of the connections or equipment required for a complete solution. It is provided as a high-level overview

Unisys ClearPath DSI VTL Cyber Recovery

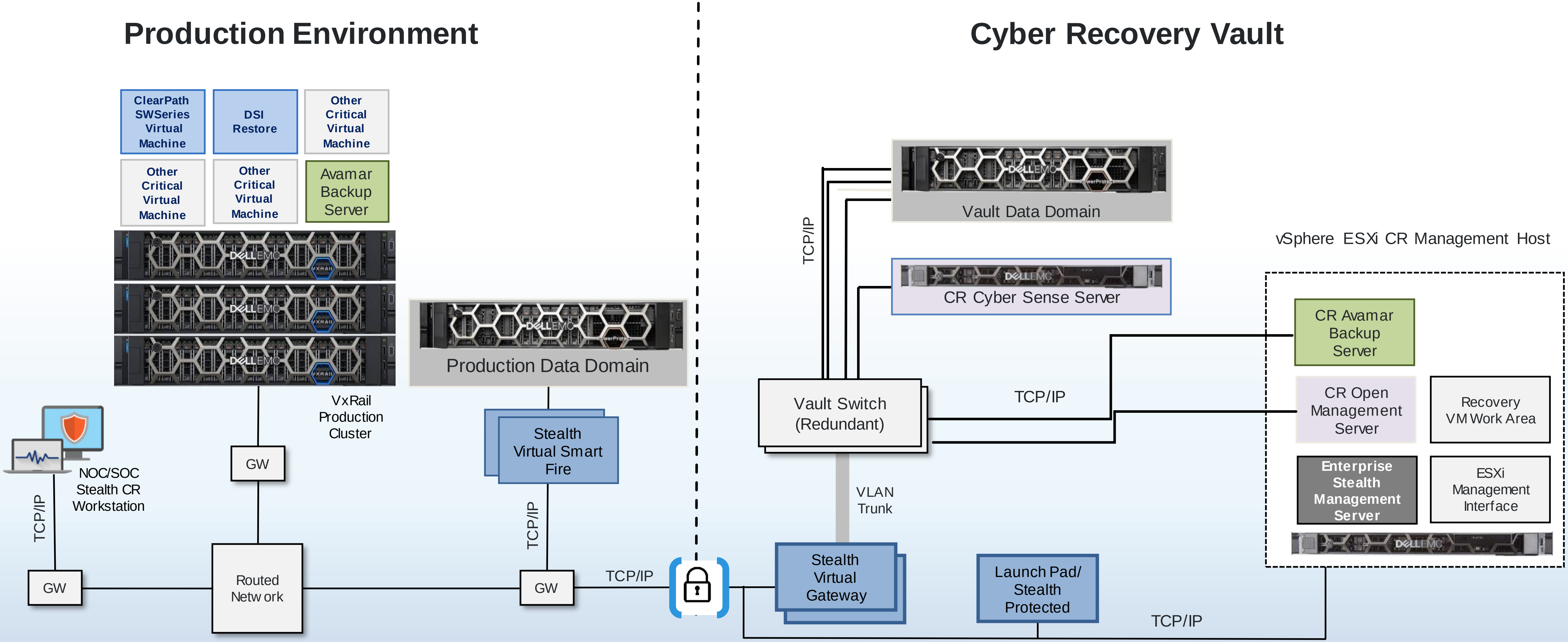


Example Vault Policy

- Full backup required on initial backup
- Every 24 hours, the DSI VTL is replicated into the vault and retained for 14 days.

* This drawing does not necessarily represent all of the connections or equipment required for a complete solution. It is provided as a high-level overview

Unisys ClearPath Virtualized Software Series Example Cyber Recovery Solution


Production Environment
Cyber Recovery Vault
ClearPath SWSeries Virtual Machine
DSI Restore
Other Critical Virtual Machine
Other Critical Virtual Machine
Other Critical Virtual Machine
Avamar Backup Server
VxRail Production Cluster
Production Data Domain
NOC/SOC Stealth CR Workstation
TCP/IP
GW
GW
Routed Network
Stealth Virtual Smart Fire
TCP/IP
GW
TCP/IP
Vault Data Domain
TCP/IP
CR Cyber Sense Server
Vault Switch (Redundant)
TCP/IP
VLAN Trunk
Stealth Virtual Gateway
Launch Pad/ Stealth Protected
TCP/IP
vSphere ESXi CR Management Host
CR Avamar Backup Server
CR Open Management Server
Recovery VM Work Area
Enterprise Stealth Management Server
ESXi Management Interface

Unisys Cyber Recovery Services

- Unisys Data Stored in the Vault
  - Conduct a one-day workshop to review the data that is required in the vault
  - Ensure all files/data are identified that is required for a full rebuild of the Unisys environment
  - Review backup process to ensure that the required data is being backed up
  - Review the process to load the vault, ensure all Unisys files/data are making it into the vault
- Unisys Data Validation Services
  - MCP: Move to VSS2 format. if needed, turn on MCP host-based encryption, ensure data validation occurs
  - OS 2200: Install OS 2200 SS in vault, automation scripting to load and boot OS 2200, verify
- Unisys Recovery Procedures
  - Conduct a workshop to develop the procedure to recover the Unisys system should a Cyber event occur
  - Document the process in a Unisys Recovery Procedure Guide
  - Assist client in testing the procedure guide. Provide training to ensure your team can do the bare metal rebuild allows them to start the recovery process without waiting on Unisys resources to arrive.
- Create a Zero-Trust Cryptographic Isolation
  - Unisys Stealth Services

Let’s Discuss Next Steps.

Keep In Mind:

- Start early. Don’t wait until a cyber event occurs!
- Are you currently looking at or do you have a Cyber Vault?
- Don’t forget ClearPath.
- Will it need to be added to your budget?

This will be a process; every environment is unique.

Getting Started:

- White Paper Available
- Reach out directly to your Client Executive
- Email: ClearPathServices@unisys.com

Thank you

unisys

DELL Technologies
PLATINUM PARTNER

Backup slides

PCI DSS : 12 requirements

https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

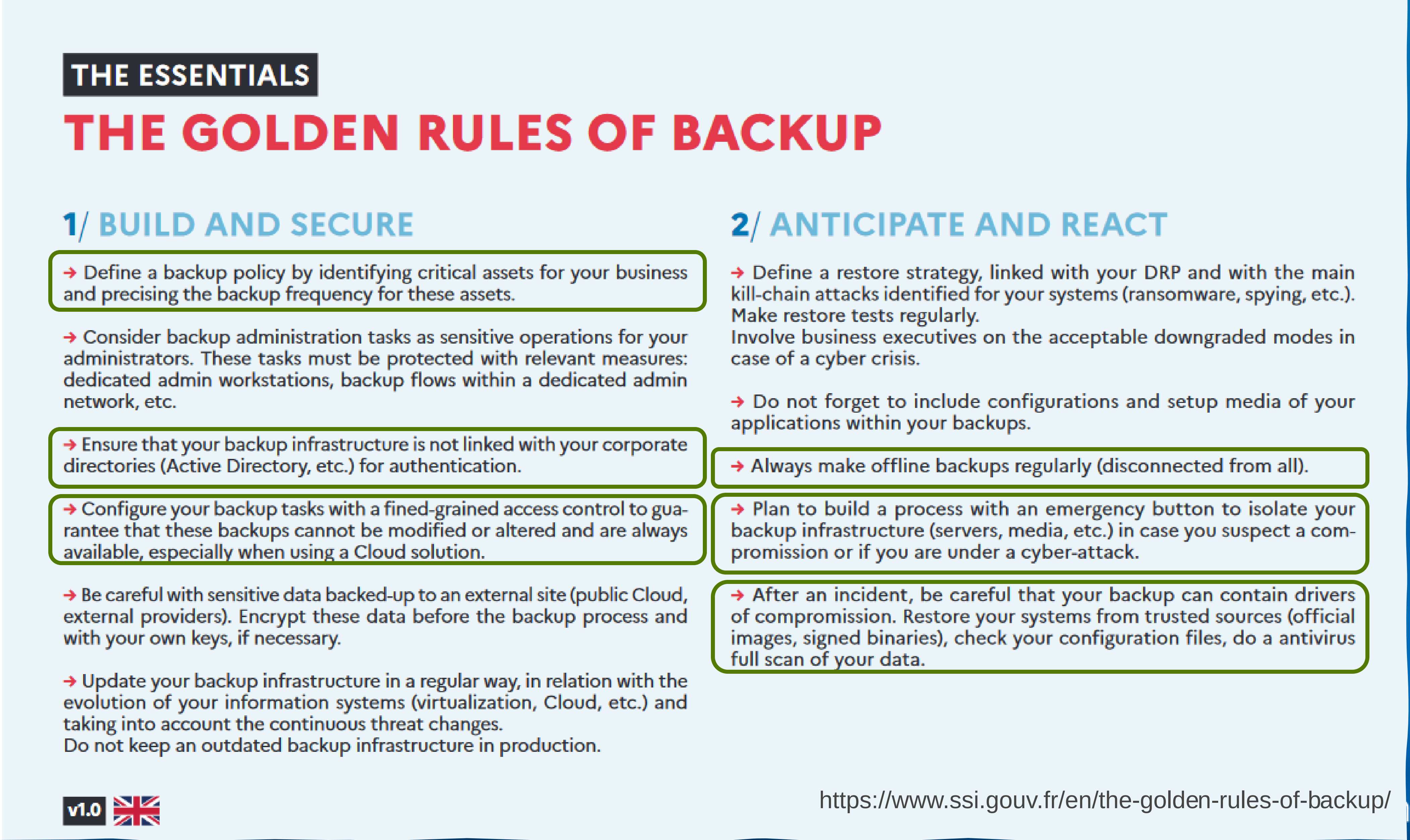
1. Install and maintain a secure network: Implement firewalls and restrict access to cardholder data based on a need-to-know basis.
2. Protect cardholder data: Encrypt cardholder data when stored or transmitted across public networks and never store sensitive card data such as the CVV/CVC.
3. Maintain a vulnerability management program: Keep security software updated and run frequent scans to identify vulnerabilities in the system.
4. Implement strong access control measures: Limit access to cardholder data to authorized personnel and use unique credentials for each user.
5. Regularly monitor and test networks: Regularly monitor all access to cardholder data and perform regular security testing to identify vulnerabilities.
6. Maintain an information security policy: Develop and maintain policies and procedures that address information security for employees, contractors, and third-party vendors.
7. Restrict physical access to cardholder data: Limit physical access to cardholder data and implement controls to monitor and track access.
8. Regularly test security systems and processes: Conduct regular penetration testing and vulnerability scans to identify and address security issues.
9. Maintain an incident response plan: Establish and maintain a plan to respond to security incidents.
10. Educate employees on information security: Provide regular training to employees to ensure they are aware of information security policies and procedures.
11. Regularly monitor and test security controls: Monitor and test security controls and processes regularly to ensure they are effective.
    File monitoring is a necessity, too. The system should perform file comparisons each week to detect changes that may have otherwise gone unnoticed
12. Implement strict access controls for cardholder data: Limit access to cardholder data on a need-to-know basis and restrict physical access to systems that store cardholder data.

(warning: to be updated with V4.0 requirements)

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ANSSI

Agence nationale de la sécurité des systèmes d'information



THE ESSENTIALS

THE GOLDEN RULES OF BACKUP

1/ BUILD AND SECURE

→ Define a backup policy by identifying critical assets for your business and precising the backup frequency for these assets.

→ Consider backup administration tasks as sensitive operations for your administrators. These tasks must be protected with relevant measures: dedicated admin workstations, backup flows within a dedicated admin network, etc.

→ Ensure that your backup infrastructure is not linked with your corporate directories (Active Directory, etc.) for authentication.

→ Configure your backup tasks with a fined-grained access control to guarantee that these backups cannot be modified or altered and are always available, especially when using a Cloud solution.

→ Be careful with sensitive data backed-up to an external site (public Cloud, external providers). Encrypt these data before the backup process and with your own keys, if necessary.

→ Update your backup infrastructure in a regular way, in relation with the evolution of your information systems (virtualization, Cloud, etc.) and taking into account the continuous threat changes.
Do not keep an outdated backup infrastructure in production.

2/ ANTICIPATE AND REACT

→ Define a restore strategy, linked with your DRP and with the main kill-chain attacks identified for your systems (ransomware, spying, etc.).
Make restore tests regularly.
Involve business executives on the acceptable downgraded modes in case of a cyber crisis.

→ Do not forget to include configurations and setup media of your applications within your backups.

→ Always make offline backups regularly (disconnected from all).

→ Plan to build a process with an emergency button to isolate your backup infrastructure (servers, media, etc.) in case you suspect a compromission or if you are under a cyber-attack.

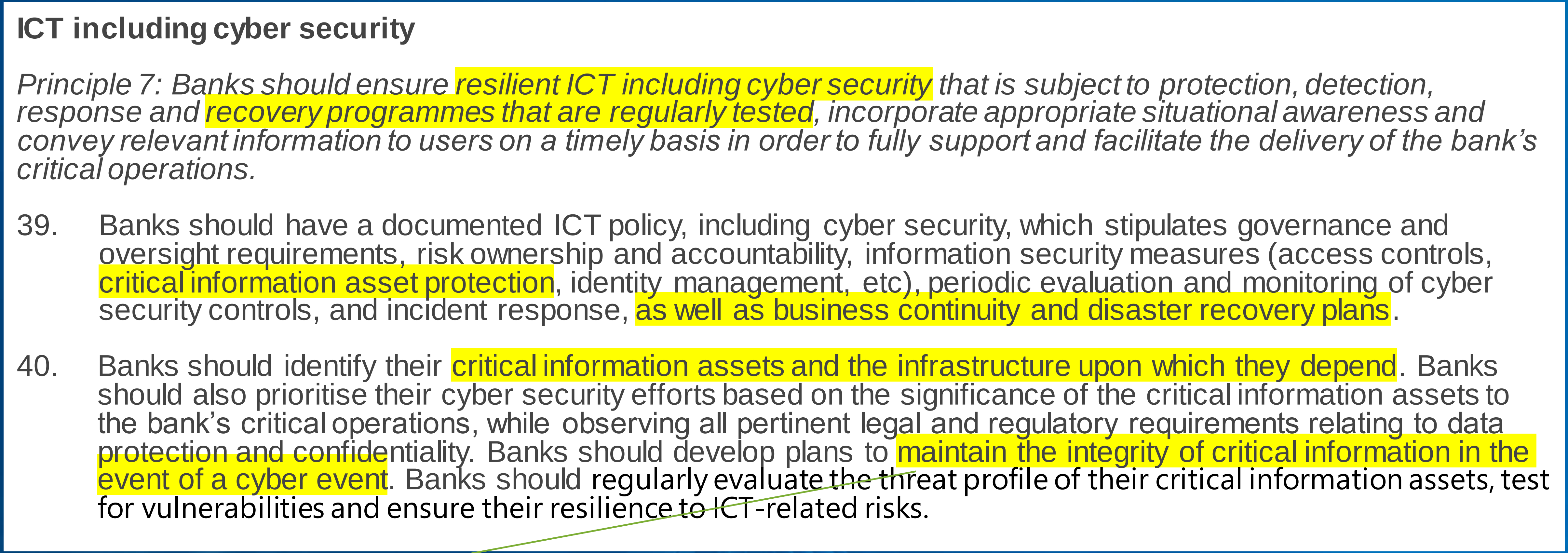
→ After an incident, be careful that your backup can contain drivers of compromission. Restore your systems from trusted sources (official images, signed binaries), check your configuration files, do a antivirus full scan of your data.

v1.0

https://www.ssi.gouv.fr/en/the-golden-rules-of-backup/

Basel Committee on Banking Supervision

Principles for operational resilience – November 2020



ICT including cyber security

Principle 7: Banks should ensure resilient ICT including cyber security that is subject to protection, detection, response and recovery programmes that are regularly tested, incorporate appropriate situational awareness and convey relevant information to users on a timely basis in order to fully support and facilitate the delivery of the bank's critical operations.

39. Banks should have a documented ICT policy, including cyber security, which stipulates governance and oversight requirements, risk ownership and accountability, information security measures (access controls, critical information asset protection, identity management, etc), periodic evaluation and monitoring of cyber security controls, and incident response, as well as business continuity and disaster recovery plans.

40. Banks should identify their critical information assets and the infrastructure upon which they depend. Banks should also prioritise their cyber security efforts based on the significance of the critical information assets to the bank's critical operations, while observing all pertinent legal and regulatory requirements relating to data protection and confidentiality. Banks should develop plans to maintain the integrity of critical information in the event of a cyber event. Banks should regularly evaluate the threat profile of their critical information assets, test for vulnerabilities and ensure their resilience to ICT-related risks.

Isolation	Immutability	Intelligence	Independance

European Central Bank (ECB)

EUROPEAN CENTRAL BANK
EUROSYSTEM

Cyber resilience oversight expectations for financial market infrastructures – December 2018

2.5.2.1 The Financial Market Infrastructures (FMIs) should – based on the identification of its critical functions, key roles, processes, information assets, third-party service providers and interconnections – plan for how to operate in a diminished capacity or how to safely restore services over time, based on services' relative priorities, and with accurate data. In order to make the best decisions about its recovery objectives following a cyber incident, the FMI must first define its recovery point objectives (RPOs) and its recovery time objectives (RTOs), commensurate to its business needs and systemic role in the ecosystem.

2.5.2.2 The FMI should develop a formal backup policy specifying the minimum frequency and scope of data, based on data sensitivity and the frequency with which that new information is introduced.

Backups should be protected at rest and in transit to ensure the confidentiality, integrity and availability of data. Backups should be tested regularly to verify their availability and integrity.

The FMI should store backup copies at an alternate site with a different risk profile to the main site, and with transfer rates consistent with actual RPOs. The alternate site and backups should be safeguarded by stringent protective and detective controls.

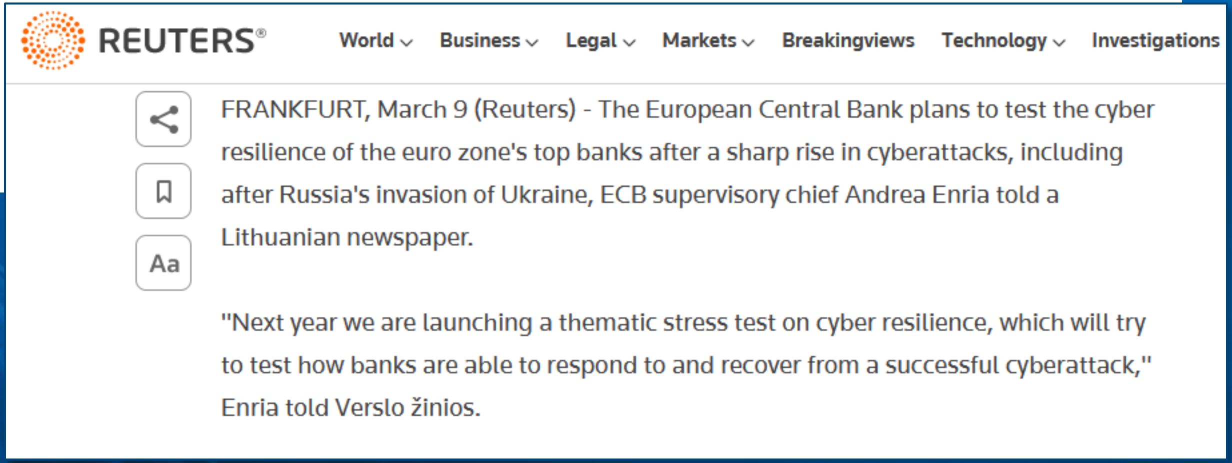
2.6.2 The FMI should establish and maintain a comprehensive testing programme as an integral part of its cyber resilience framework. The testing programme should consist of a broad spectrum of methodologies, practices and tools for monitoring, assessing and evaluating the effectiveness of the core components of the cyber resilience framework.

The FMI should ensure that the tests are undertaken by independent parties, whether internal or external.

The FMI should test critical systems, applications and data recovery plans at least annually.

The FMI should perform penetration tests, engaging all critical internal and external stakeholders in the penetration testing exercises: system owners, business continuity, and incident and crisis response teams.

Reuters, 9 March 2023:



FRANKFURT, March 9 (Reuters) - The European Central Bank plans to test the cyber resilience of the euro zone's top banks after a sharp rise in cyberattacks, including after Russia's invasion of Ukraine, ECB supervisory chief Andrea Enria told a Lithuanian newspaper.

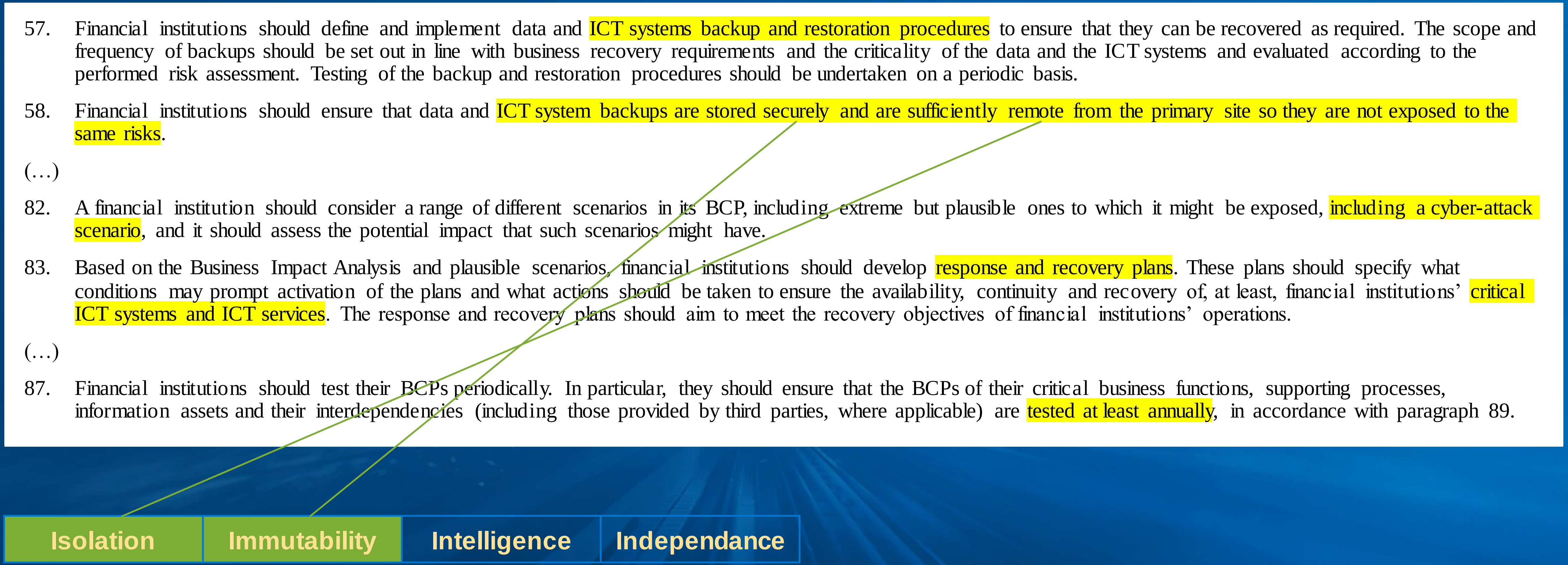
"Next year we are launching a thematic stress test on cyber resilience, which will try to test how banks are able to respond to and recover from a successful cyberattack," Enria told Verslo žinios.

Isolation	Immutability	Intelligence	Independance

European Banking Authority (EBA)

Guidelines on ICT and security risk management

EBA/GL/2019/04 – published 29 November 2019



57. Financial institutions should define and implement data and ICT systems backup and restoration procedures to ensure that they can be recovered as required. The scope and frequency of backups should be set out in line with business recovery requirements and the criticality of the data and the ICT systems and evaluated according to the performed risk assessment. Testing of the backup and restoration procedures should be undertaken on a periodic basis.

58. Financial institutions should ensure that data and ICT system backups are stored securely and are sufficiently remote from the primary site so they are not exposed to the same risks.

(…)

82. A financial institution should consider a range of different scenarios in its BCP, including extreme but plausible ones to which it might be exposed, including a cyber-attack scenario, and it should assess the potential impact that such scenarios might have.

83. Based on the Business Impact Analysis and plausible scenarios, financial institutions should develop response and recovery plans. These plans should specify what conditions may prompt activation of the plans and what actions should be taken to ensure the availability, continuity and recovery of, at least, financial institutions' critical ICT systems and ICT services. The response and recovery plans should aim to meet the recovery objectives of financial institutions' operations.

(…)

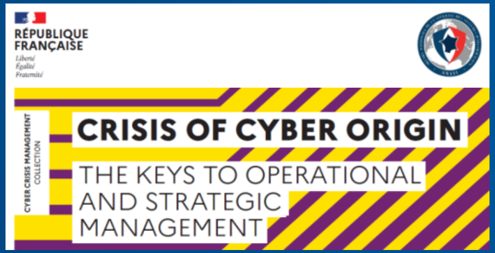
87. Financial institutions should test their BCPs periodically. In particular, they should ensure that the BCPs of their critical business functions, supporting processes, information assets and their interdependencies (including those provided by third parties, where applicable) are tested at least annually, in accordance with paragraph 89.

Isolation | Immutability | Intelligence | Independance

Loi de Programmation Militaire in France

- LPM is a law that aims to strengthen national security, particularly in the field of cyber security
- Large French banks are considered as OIV (Opérateurs d'Importance Vitale) : companies or organizations that play an essential role in France. They are subject to specific obligations in terms of IT security under the LPM
- The obligations imposed on OIVs under the LPM include :
  - Identification and declaration: OIVs must be identified and declared to ANSSI (Agence nationale de la sécurité des systèmes d'information). They must also inform ANSSI of any security incident.
  - The implementation of security measures: OIVs must implement appropriate security measures to protect their information systems against attacks, intrusions and cyber attacks
  - Incident reporting: In the event of a security incident, OIVs must notify ANSSI as soon as possible so that appropriate response measures can be taken
  - Cooperation with ANSSI : The OIV must cooperate with the ANSSI in the framework of investigations and security audits
  - Staff training: OIVs must ensure adequate training of their staff in computer security
  - Obligation of result: OIVs are required to ensure a high level of security of their information systems and are responsible in case of violation of these security measures
- These obligations are intended to guarantee the protection against cyber threats of the country's critical infrastructures, such as communication networks, financial services, energy systems and transportation infrastructures

ANSSI Best Practices


RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER CRISIS MANAGEMENT COLLECTION

CRISIS OF CYBER ORIGIN

THE KEYS TO OPERATIONAL AND STRATEGIC MANAGEMENT

Crisis of cyber origin
The keys to operational and strategic management
May 2022

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

RANSOMWARE ATTACKS, ALL CONCERNED

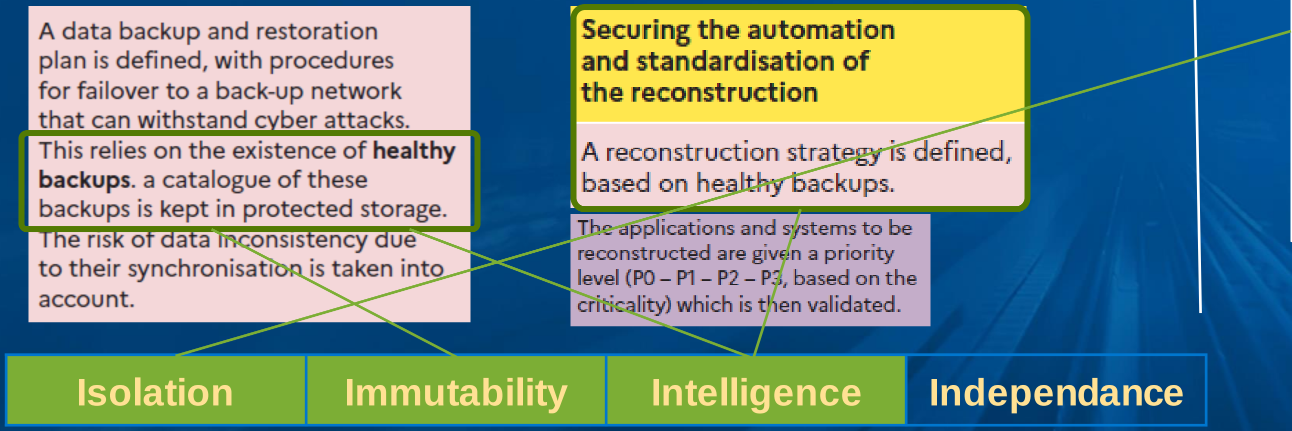
HOW TO PREVENT THEM AND RESPOND TO AN INCIDENT

Ransomware attacks, all concerned
How to prevent them and respond to an incident
August 2021

An organisation is considered resilient if, in the event of a cyber crisis, it is able to maintain its most critical activities (…) and restart them in a controlled manner so as to limit the impacts of the attack on the organisation, its activity sector and its customers, thus retaining the trust of the ecosystem.

Regular backups of all data, including data on file, infrastructure and critical business application servers, must be made. Keep in mind that these backups can also be affected by ransomware. Indeed, more and more cyber criminals are looking to attack backups in order to reduce the victim's ability to retrieve their data, thereby maximizing the chances that they will pay the ransom. These backups, at least for the most critical ones, must be disconnected from the information system to prevent them from being encrypted like other files (…)

In this respect, it is important to note that backup-less architectures effectively protect against the destruction of isolated data, when this is due to a hardware failure. However, they do not protect against targeted ransomware attacks, since attackers attempt to encrypt the data on all servers.


A data backup and restoration plan is defined, with procedures for failover to a back-up network that can withstand cyber attacks. This relies on the existence of **healthy backups**. a catalogue of these backups is kept in protected storage. The risk of data inconsistency due to their synchronisation is taken into account.

Securing the automation and standardisation of the reconstruction

A reconstruction strategy is defined, based on healthy backups.

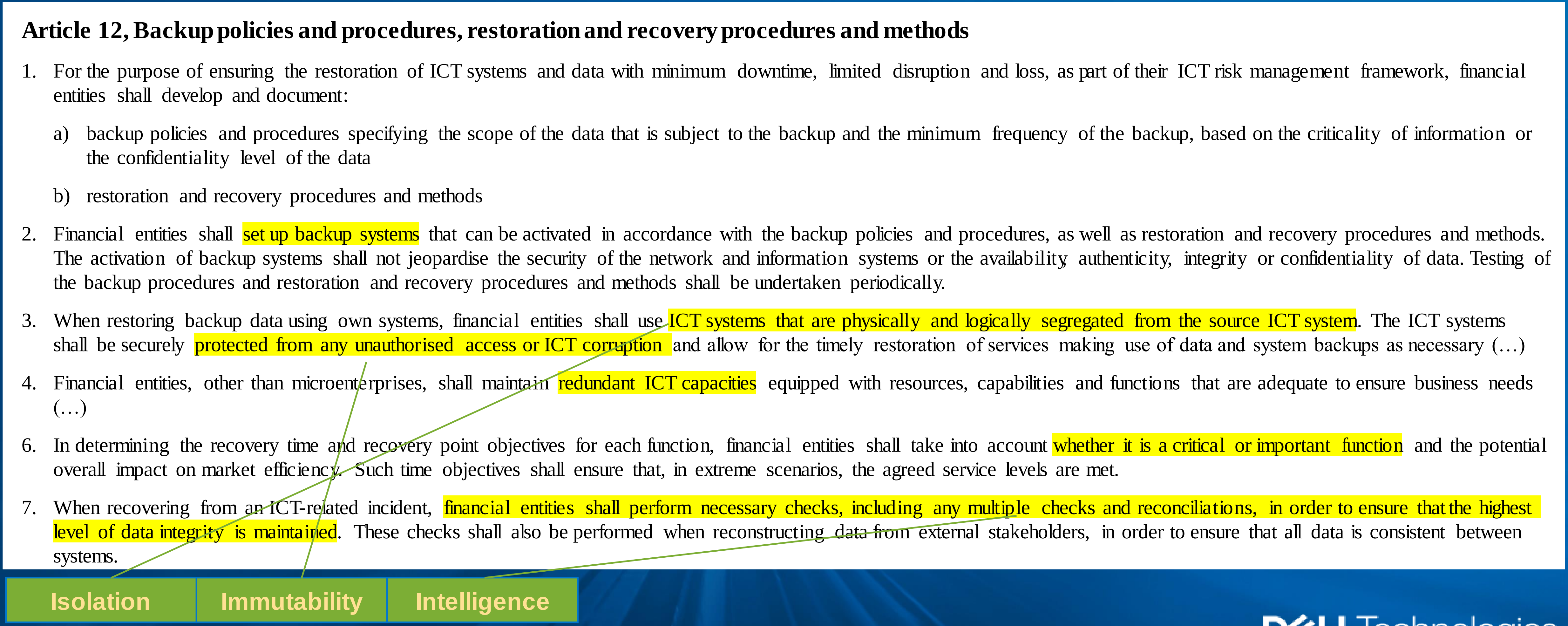
The applications and systems to be reconstructed are given a priority level (P0 – P1 – P2 – P3, based on the criticality) which is then validated.

Isolation	Immutability	Intelligence	Independance

DORA - Digital Operational Resilience Act

For all Financial Institutions operating in the European Union

EU 2022/2554 – published 14 December 2022, applicable 17 January 2025



Article 12, Backup policies and procedures, restoration and recovery procedures and methods

1. For the purpose of ensuring the restoration of ICT systems and data with minimum downtime, limited disruption and loss, as part of their ICT risk management framework, financial entities shall develop and document:

   a) backup policies and procedures specifying the scope of the data that is subject to the backup and the minimum frequency of the backup, based on the criticality of information or the confidentiality level of the data

   b) restoration and recovery procedures and methods

2. Financial entities shall set up backup systems that can be activated in accordance with the backup policies and procedures, as well as restoration and recovery procedures and methods. The activation of backup systems shall not jeopardise the security of the network and information systems or the availability, authenticity, integrity or confidentiality of data. Testing of the backup procedures and restoration and recovery procedures and methods shall be undertaken periodically.

3. When restoring backup data using own systems, financial entities shall use ICT systems that are physically and logically segregated from the source ICT system. The ICT systems shall be securely protected from any unauthorised access or ICT corruption and allow for the timely restoration of services making use of data and system backups as necessary (…)

4. Financial entities, other than microenterprises, shall maintain redundant ICT capacities equipped with resources, capabilities and functions that are adequate to ensure business needs (…)

6. In determining the recovery time and recovery point objectives for each function, financial entities shall take into account whether it is a critical or important function and the potential overall impact on market efficiency. Such time objectives shall ensure that, in extreme scenarios, the agreed service levels are met.

7. When recovering from an ICT-related incident, financial entities shall perform necessary checks, including any multiple checks and reconciliations, in order to ensure that the highest level of data integrity is maintained. These checks shall also be performed when reconstructing data from external stakeholders, in order to ensure that all data is consistent between systems.

NIS2 Directive - Network and Information Systems V2

Directive (EU) 2022/2555, published 14 December 2022, 21 months to incorporate in national laws

More sectors covered:

- **Essential**: Healthcare, Digital infrastructure, Transport, Water supply, Digital service providers, Banking, Financial market infrastructure, Energy, Wastewater, Health (pharmaceuticals, R&D, critical medical devices), Space, Public administration
- **Important**: Providers of public electronic communications networks or services, Chemicals, Food producers, processors and distributors, Manufacturing of critical products (medical devices, computers, electronics, motor vehicles), Digital providers (social networking platforms, search engines, online marketplaces), Postal and courier services

Member states can levy fines of up to EUR 10 million or 2% of annual turnover (revenue) for certain violations or breaches. In addition, critical entity management bodies (i.e., executive teams) can be held personally liable for infringements.

Article 21 - Cybersecurity risk-management measures

1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. (…)
2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

   (a) policies on risk analysis and information system security;

   (b) incident handling;

   (c) business continuity, such as backup management and disaster recovery, and crisis management; (…)

   (f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

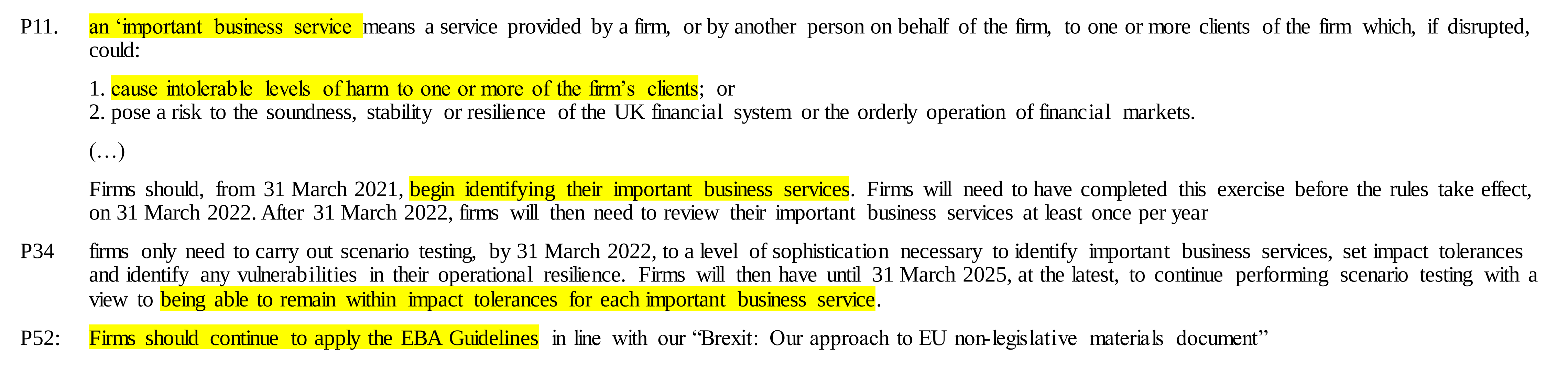
   (g) basic cyber hygiene practices and cybersecurity training;

   (i) human resources security, access control policies and asset management;

Financial Conduct Authority in UK

(in partnership with Bank of England and Prudential Regulation Authority)

See https://www.fca.org.uk/firms/operational-resilience
and Policy Statement PS21/3 – published March 2021, fully applicable March 2025



P11. an ‘important business service means a service provided by a firm, or by another person on behalf of the firm, to one or more clients of the firm which, if disrupted, could:

1. cause intolerable levels of harm to one or more of the firm’s clients; or
2. pose a risk to the soundness, stability or resilience of the UK financial system or the orderly operation of financial markets.

(…)

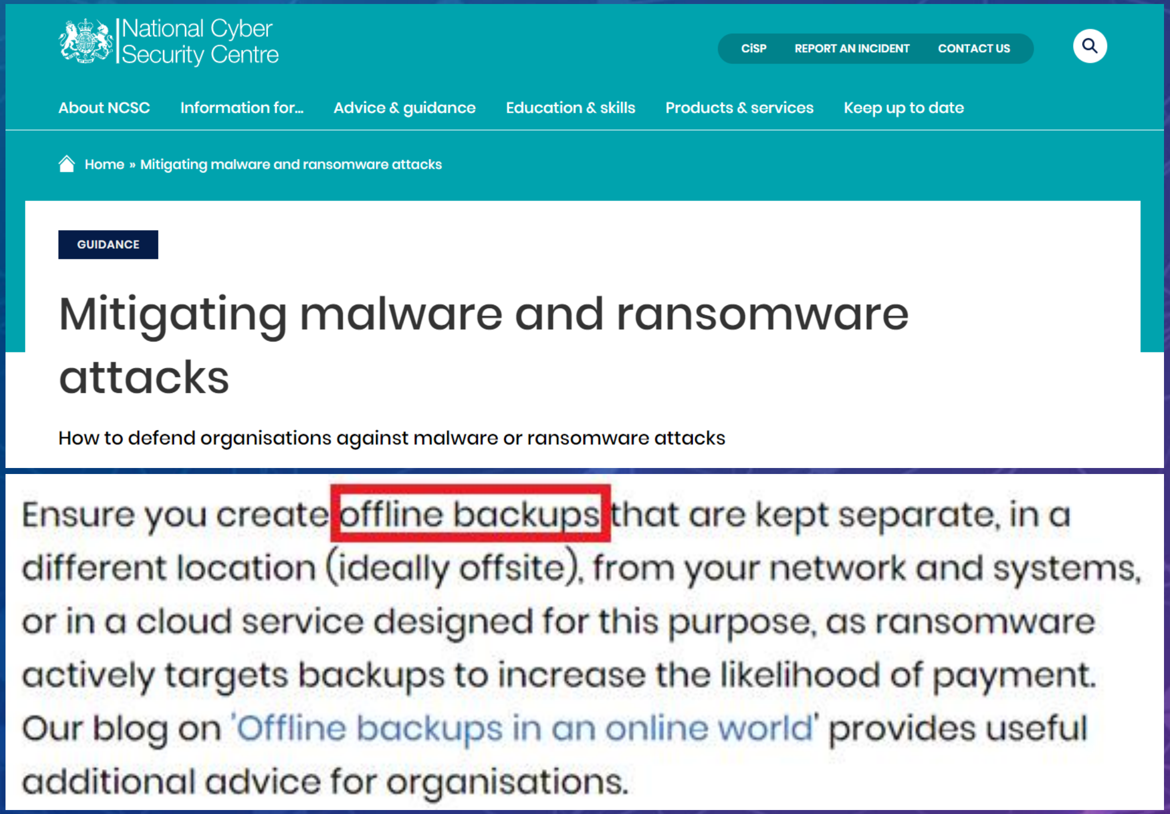
Firms should, from 31 March 2021, begin identifying their important business services. Firms will need to have completed this exercise before the rules take effect, on 31 March 2022. After 31 March 2022, firms will then need to review their important business services at least once per year

P34 firms only need to carry out scenario testing, by 31 March 2022, to a level of sophistication necessary to identify important business services, set impact tolerances and identify any vulnerabilities in their operational resilience. Firms will then have until 31 March 2025, at the latest, to continue performing scenario testing with a view to being able to remain within impact tolerances for each important business service.

P52: Firms should continue to apply the EBA Guidelines in line with our “Brexit: Our approach to EU non-legislative materials document”

UK Guidelines

- National Cyber Security Centre NCSC
- Cyber Essentials Framework – Data Security Protection Toolkit
- Cyber Assessment Framework alignment
- HSE Report Recommendation Page 13:
“Offline backups (or backups that are verified as inaccessible to attackers with full control of production IT)”



Mitigating malware and ransomware attacks

How to defend organisations against malware or ransomware attacks

Ensure you create offline backups that are kept separate, in a different location (ideally offsite), from your network and systems, or in a cloud service designed for this purpose, as ransomware actively targets backups to increase the likelihood of payment. Our blog on 'Offline backups in an online world' provides useful additional advice for organisations.

<u>CAF Requirement</u>

Protect data in accordance with the risks to essential functions posed by compromises of data integrity and/or availability. In addition to effective data access control measures, other relevant security measures might include maintaining up-to-date, **isolated (e.g. offline) back-up copies of data**, combined with the **ability to detect data integrity failures** where necessary. Software and/or hardware used to access critical data may also require protection.

7.3.5	Removed from cat 3	When did you last successfully restore from a backup?	Backups should be tested frequently. The example provided may relate to a live or test environment.
7.3.6	New	Are your backups kept separate from your network ('offline'), or in a cloud service designed for this purpose	Cloud synching services, such as OneDrive, SharePoint or Google Drive, should not be used as your only backup and stored backup should not be permanently connected to your network. Further guidance is available from the [National Cyber Security Centre](https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world)
5.1.1	New for cat 3 and 4	Root cause analysis is conducted routinely as a key part of your lessons learned activities following a data security incident, with findings acted upon.	Explain, in the comments, how any incident response and management tests findings have informed the immediate future technical protection and remediated any systemic vulnerabilities of the system or service, to ensure identified issues cannot arise in the same way again.