Kübervastupidavus kui ettevõtte ellujäämise garantii

Sergei Butenko
Global Specialty Sales, Central & Eastern Europe

DELL Technologies

What is “Resilience”? And why is it needed?

Get the business quickly back to operational mode, whatever incident might have happened.

Traditional

Power outages, natural catastrophes, data center failures

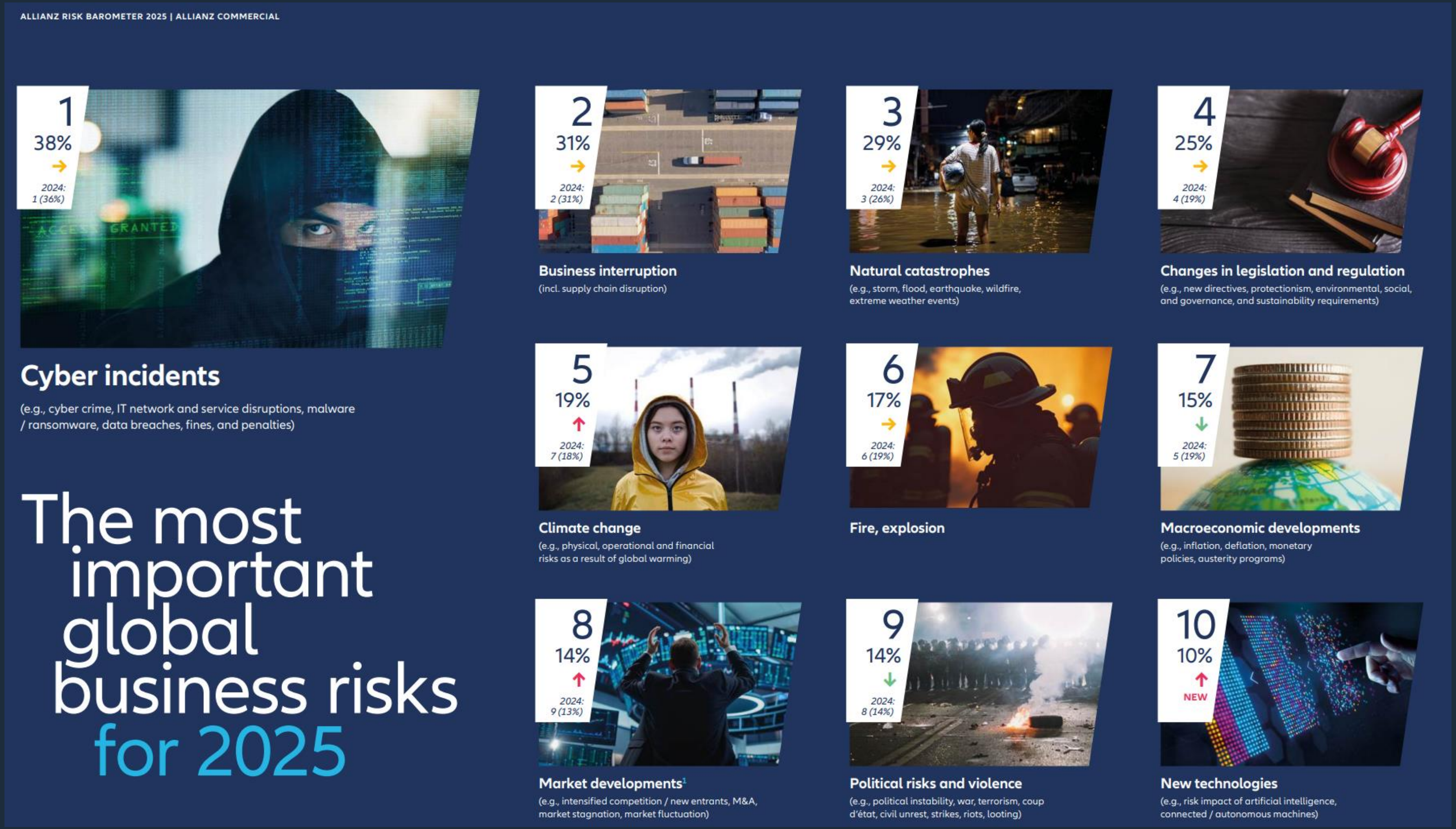
+

Today

Data Theft, Encryption, Poisoning, Wiper attacks

Do you have a risk-based security and resilience strategy?	Do you have an up-to-date picture of your applications and interdependencies?	Does your technology stack enable meeting your resilience goals?	How often do you test recovery from various scenarios?

Allianz Global Risk barometer (2025)



ALLIANZ RISK BAROMETER 2025 | ALLIANZ COMMERCIAL

1
38%
→
2024:
1 (36%)

Cyber incidents

(e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)

The most important global business risks for 2025

2
31%
→
2024:
2 (31%)

Business interruption

(incl. supply chain disruption)

3
29%
→
2024:
3 (26%)

Natural catastrophes

(e.g., storm, flood, earthquake, wildfire, extreme weather events)

4
25%
→
2024:
4 (19%)

Changes in legislation and regulation

(e.g., new directives, protectionism, environmental, social, and governance, and sustainability requirements)

5
19%
↑
2024:
7 (18%)

Climate change

(e.g., physical, operational and financial risks as a result of global warming)

6
17%
→
2024:
6 (19%)

Fire, explosion

7
15%
↓
2024:
5 (19%)

Macroeconomic developments

(e.g., inflation, deflation, monetary policies, austerity programs)

8
14%
↑
2024:
9 (13%)

Market developments[1]

(e.g., intensified competition / new entrants, M&A, market stagnation, market fluctuation)

9
14%
↓
2024:
8 (14%)

Political risks and violence

(e.g., political instability, war, terrorism, coup d'état, civil unrest, strikes, riots, looting)

10
10%
↑
NEW

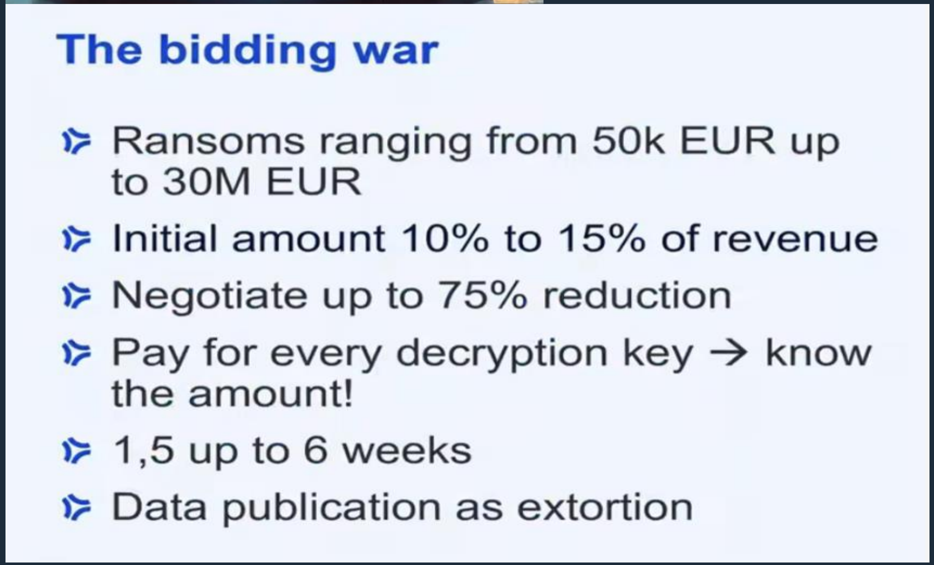
New technologies

(e.g., risk impact of artificial intelligence, connected / autonomous machines)

Cyber Incidents (#1)
for the 4th year in a ROW!

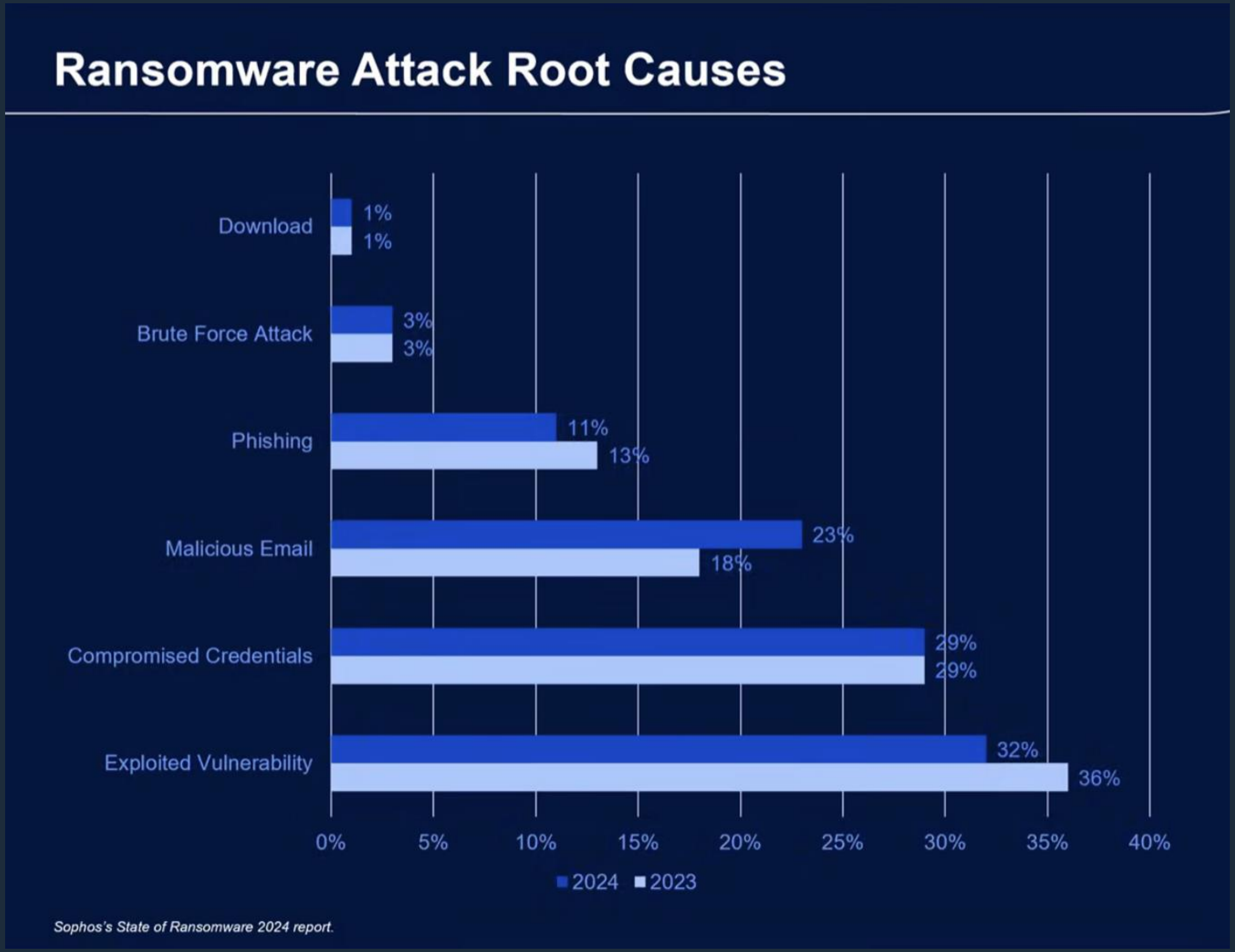
Business interruption (#2)
"Cyber incidents and natural catastrophes are the two Business Interruption exposures companies fear most

Does it even happen to the small business?



The bidding war

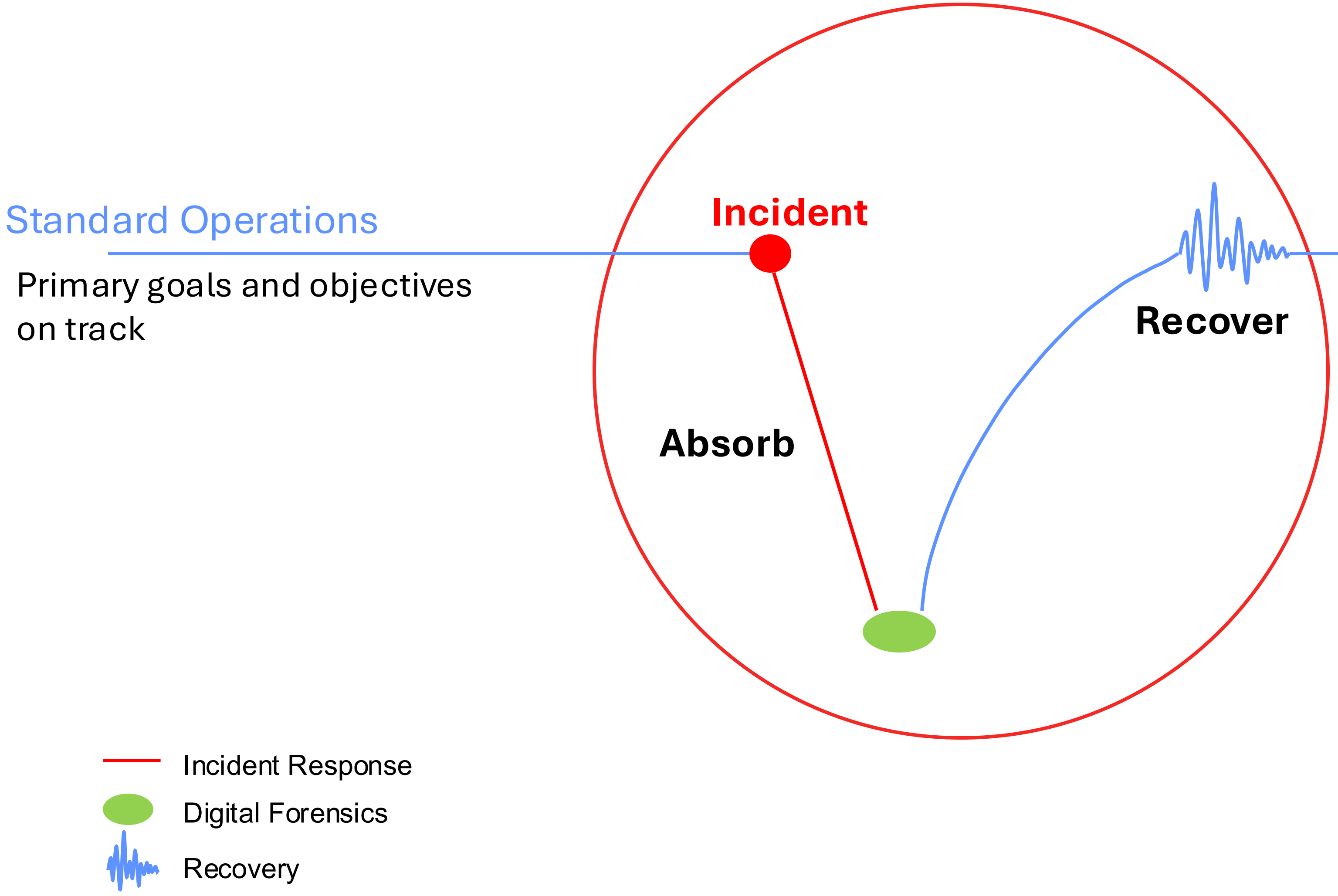
- Ransoms ranging from 50k EUR up to 30M EUR
- Initial amount 10% to 15% of revenue
- Negotiate up to 75% reduction
- Pay for every decryption key → know the amount!
- 1,5 up to 6 weeks
- Data publication as extortion



Ransomware Attack Root Causes

Sophos's State of Ransomware 2024 report.

Cyber Resilience: It’s about getting the business back operational

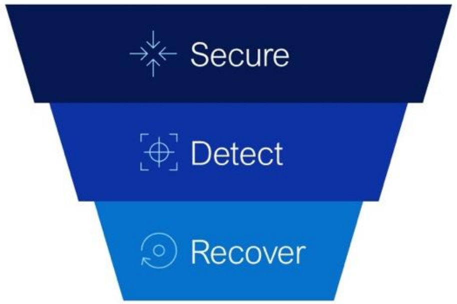


Primary goals and objectives on track

Learn and Adapt

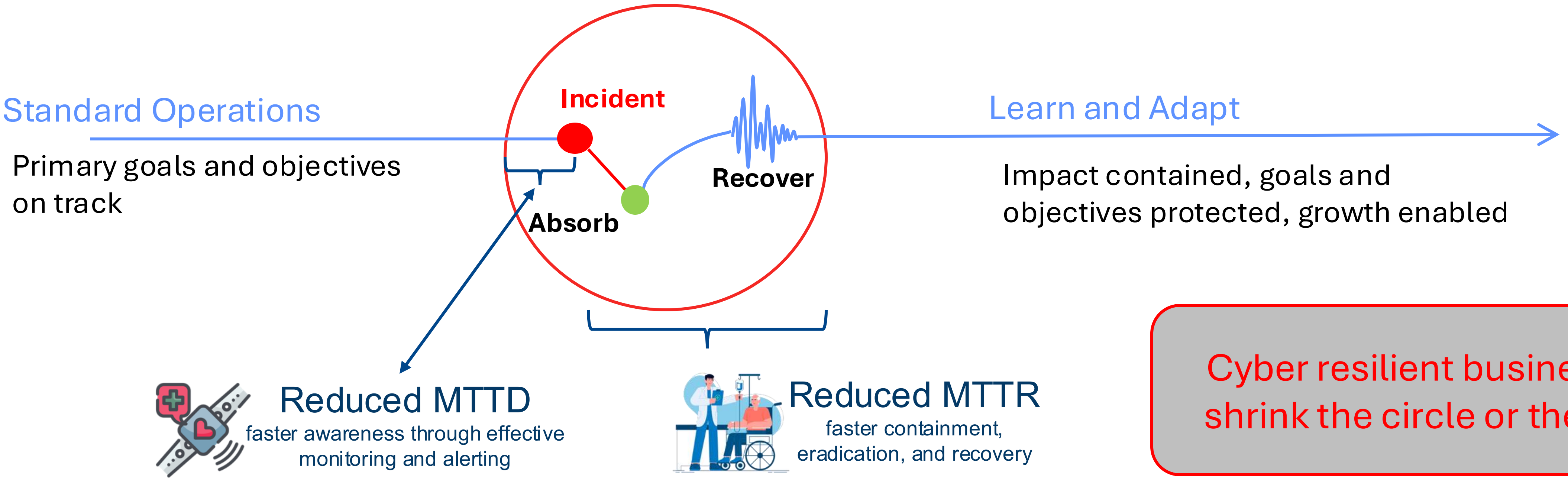
Impact contained, goals and objectives protected, growth enabled

Cyber resilient businesses can shrink the circle or the V-shape



Source WEF: https://www3.weforum.org/docs/WEF_Unpacking_Cyber_Resilience_2024.pdf

Cyber Resilience: It’s about getting the business back operational



Standard Operations

Primary goals and objectives on track

Incident

Absorb

Recover

Learn and Adapt

Impact contained, goals and objectives protected, growth enabled

Reduced MTTD
faster awareness through effective monitoring and alerting

Reduced MTTR
faster containment, eradication, and recovery

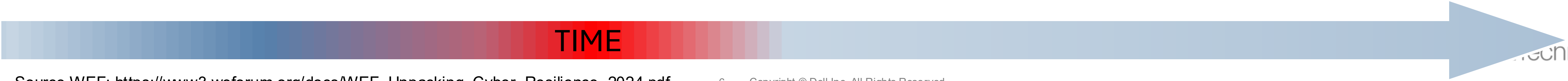
Cyber resilient businesses can shrink the circle or the V-shape

— Incident Response

● Digital Forensics

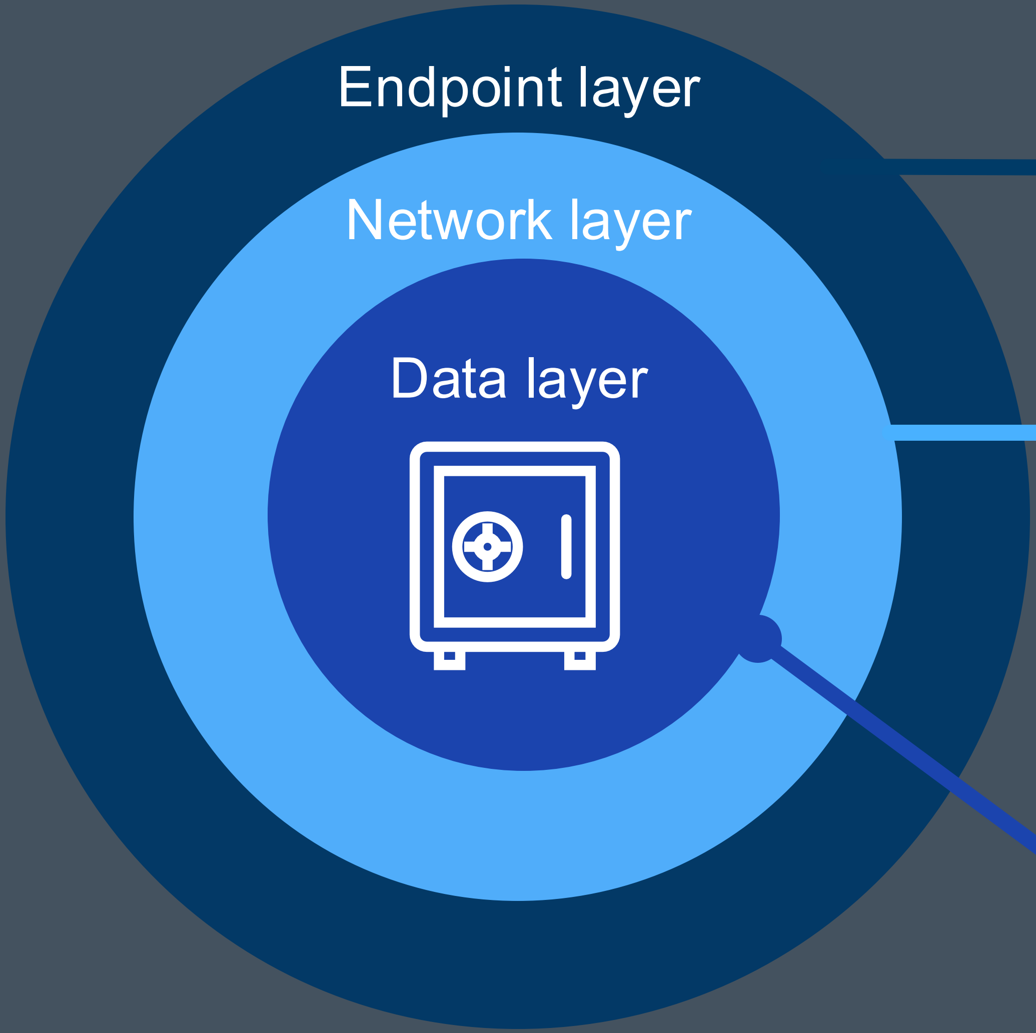
〰 Recovery

MTTD = mean time to detect
MTTR = mean time to recover



Source WEF: https://www3.weforum.org/docs/WEF_Unpacking_Cyber_Resilience_2024.pdf

The Data Layer is the focus of many attacks



Multiple layers of security controls to protect your critical assets

Is your **data layer cyber resilient?**

What can happen to your data?

Depends on the motive of the attack – Multiple types can happen simultaneously

Gain access
to critical data

Information Security Threat

>75%

Permanently
delete

Encrypt and
demand ransom

Operational Disruption
Reputational Damage

Availability

30-60%

Trade secrets
corporate espionage

Sell data on
the dark net

Legal and Regulatory Consequences
Loss of IP
Reputational Damage

Confidentiality

~25%

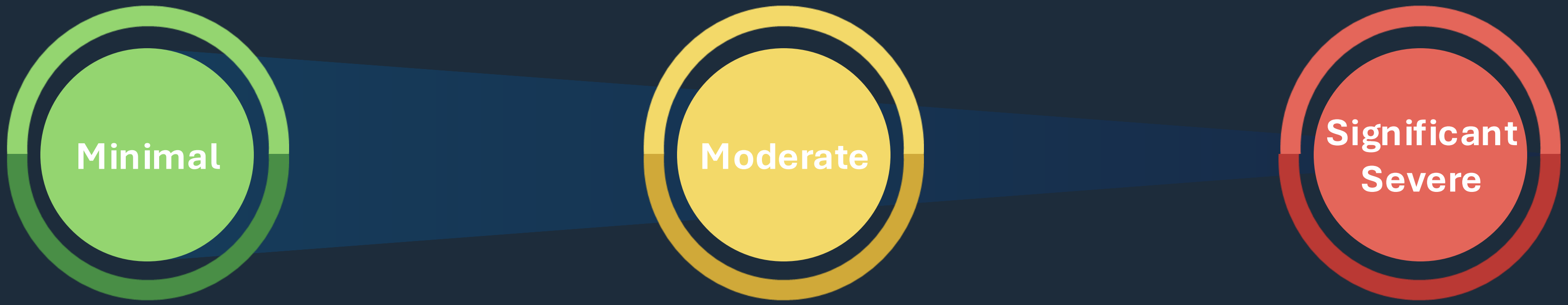
Stealth Data
Tampering

Operational Impact
Reputational Damage

Integrity

Recovery Based On Impact Level

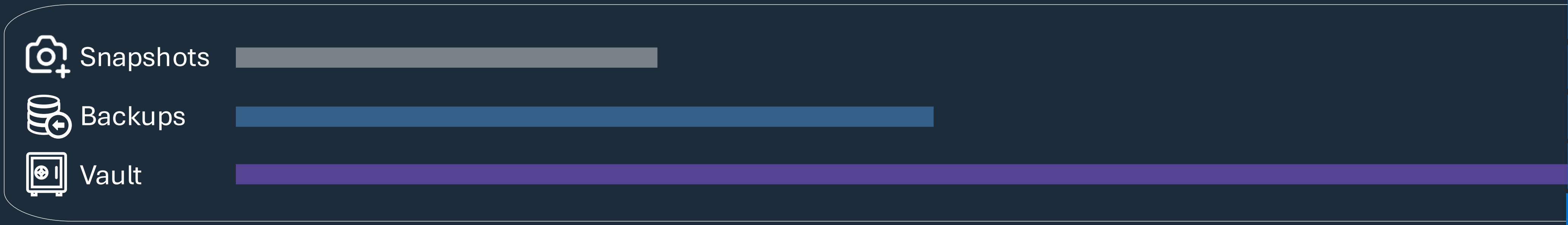
Level of Impact Categorized by Forensics



Defining Characteristics

Minimal	Moderate	Significant Severe
Incident is **notable** and **contained**	Incident is **widespread** but **largely contained**	Incident is **pervasive** and **uncontained**
Production network and most infrastructure resources remain trusted	Some production network and infrastructure resources may be untrusted	All production network and infrastructure resources are likely untrusted

Viable Recovery Options



PowerStore

PowerMax

PowerScale

PowerFlex

ObjectScale

PowerProtect

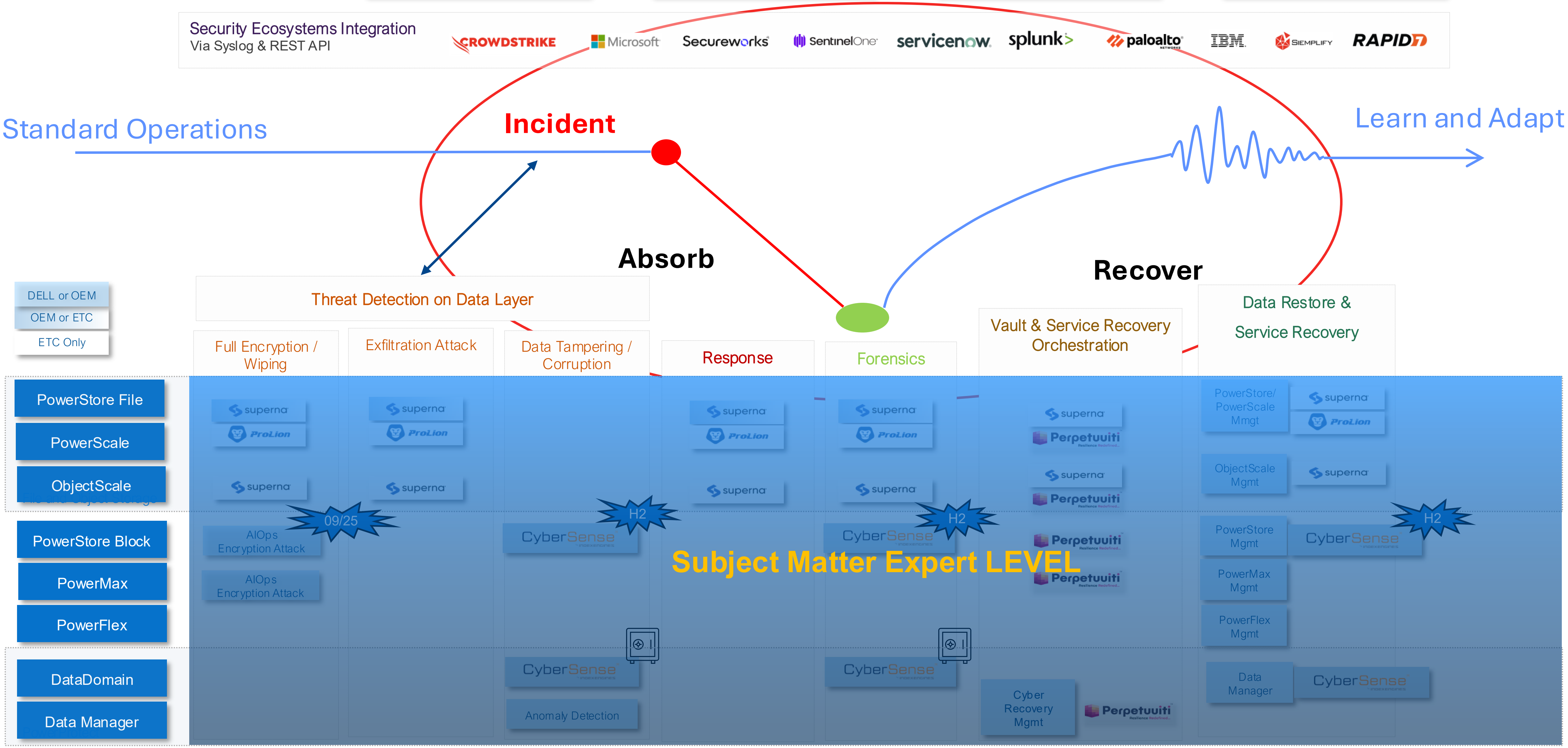
Recovery options become progressively more constrained

Storage Cyber Resilience: Today’s Portfolio View. Better together with Partners

Dell Services: Advisory and Design Services | Proactive Resilience Services | Managed Detection and Response (MDR) | Incident Response and Recovery + Retainer Service

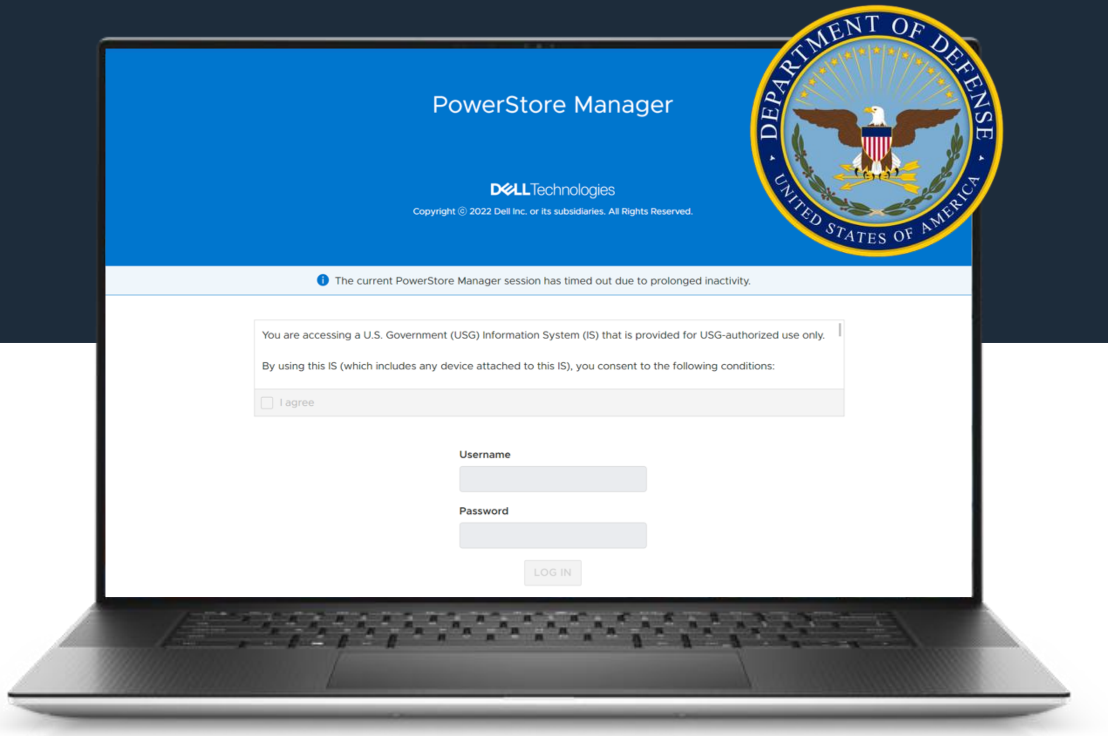
Security Ecosystems Integration
Via Syslog & REST API

CROWDSTRIKE · Microsoft · Secureworks · SentinelOne · servicenow · splunk> · paloalto · IBM · SIEMPLIFY · RAPID7



STIG Compliance

PowerStore is certified to accommodate the security requirements of the US Federal Government



PowerStore Manager

DELL Technologies

Copyright © 2022 Dell Inc. or its subsidiaries. All Rights Reserved.

The current PowerStore Manager session has timed out due to prolonged inactivity.

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

□ I agree

Username

Password

DoD IT security compliance configurations

- ✓ Custom DoD login banner
- ✓ Password complexity requirements and rules
- ✓ Periodic intrusion detections and alerts
- ✓ User lockout policies

Federal Approved Product List (APL) certification is acquired!

STIG Compliance

Standards-based hardening

Access Control

Use role-based access control (RBAC) to manage user permissions effectively

Data Encryption

Ensure that data at rest and data in transit are encrypted using strong encryption algorithms

Patch Management

Regularly update and patch the storage system's firmware and software to address security vulnerabilities.
Ensure that security patches are tested and applied promptly

Network Security

Implement network segmentation to isolate storage systems from other parts of the network

Audit and Logging

Enable audit logging to track and monitor activities on the storage system.
Maintain log files and regularly review them for suspicious activities

Secure Configuration

Guidelines for secure configuration of Dell storage systems, including disabling unnecessary services and features

Account Management

Enforce strong password policies and regularly review and update user accounts.
Ensure that default and unused accounts are disabled or removed

Vulnerability Assessment

Regularly conduct vulnerability assessments and security scans to identify and remediate vulnerabilities in the storage system

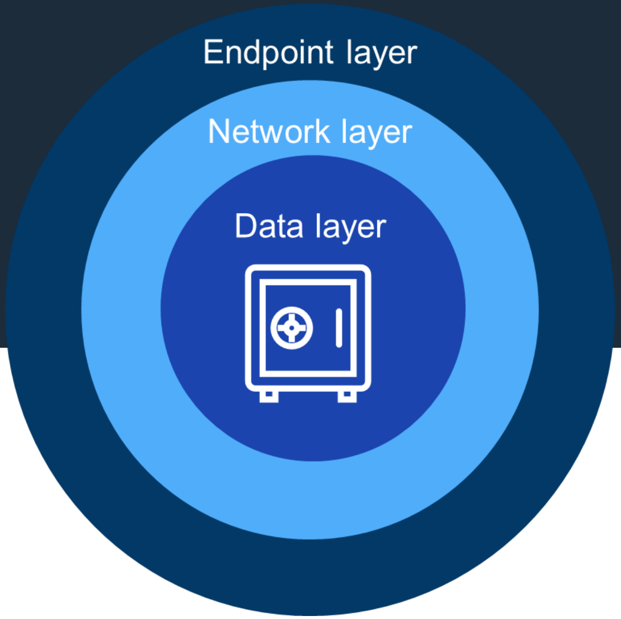
Physical Security

Secure the physical environment of the storage systems to prevent unauthorized access to the hardware

DELL Technologies

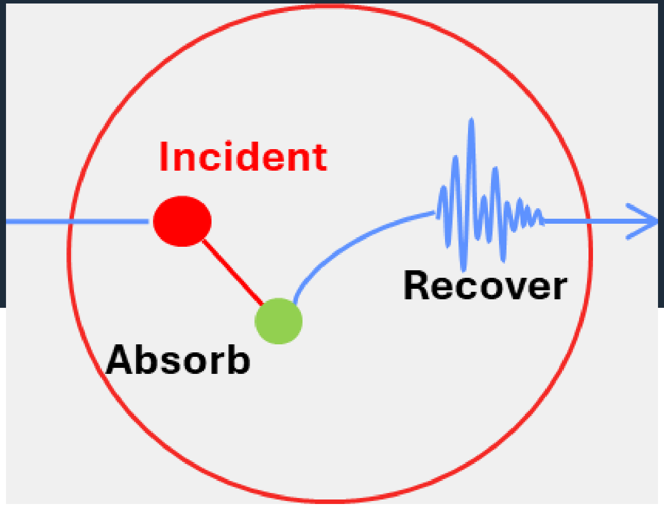
CALL TO ACTION

Have a discussion within your organization about the primary risk : CYBER INCIDENTS.



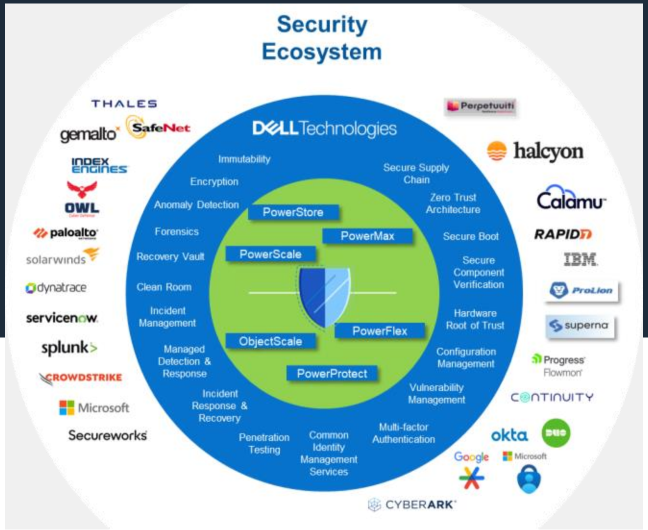
The data layer is the focus of many attacks.

Dell's storage solutions make your data not only secure, but also resilient



Prepare for when it happens.
Reduce the circle or the v-shape.
= People, Processes & technology

Cyber resilient businesses can reduce downtime up to 75%



Security is a team sport!
Dell integrates with leading Cybersecurity vendors

Call with subject matter experts

Thank You