



Transforming Data Protection to Data Resilience

Michael Berg

Advisory System Engineer – Data Protection Division

DELLTechnologies

It's not IF....

but When

Events once seen as extreme and unusual are now commonplace.

Cyber Resilient Data Protection Leadership

2600+
Cyber Recovery
customers¹

35 EB+
Data protected
in the cloud²

¹ Based on Dell Technologies internal analysis, February 2025

² Based on Dell Technologies internal analysis, January 2025

>35K
Service & Support
Professionals

241M+
Assets supported

94%
Technical Support
CSAT rating

10,000+
Transformation
projects completed



80%

REDUCTION IN HOURS SPENT ON RECOVERY



75%

REDUCTION IN DOWNTIME

*Based on research by Forrester Consulting commissioned by Dell Technologies, "The Total Economic Impact™ of Dell PowerProtect Cyber Recovery," August 2023.

“

Every day that we're not open, we are losing revenue. If we're not providing services to the public, we could lose millions of dollars.

CISO, local government

”

Cyber Resilience

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 business withstand a cyber attack?

Cyber requirements from the Industry

Building **maturity** to ensure **confidence** in resilience processes and technology through reliable optimised **testing and reporting**

1. Supply Chain Inspection
2. Separation of Duty
3. Data Isolation (offline)
4. Observability
5. Run Book Creation
6. Ability to Test Recoveries
7. Timely Recovery in the event of an attack.

Separation of Duty

NIST:


“that no user should be given enough privileges to misuse the system on their own”

NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

Definition(s):

 refers to the principle that no user should be given enough privileges to misuse the system on their own. For example, the person authorizing a paycheck should not also be the one who can prepare them. Separation of duties can be enforced either statically (by defining conflicting roles, i.e., roles which cannot be executed by the same user) or dynamically (by enforcing the control at access time). An example of dynamic separation of duty is the two-person rule. The first user to execute a two-person operation can be any authorized user, whereas the second user can be any authorized user different from the first [R.S. Sandhu., and P Samarati, “Access Control: Principles and Practice,” IEEE Communications Magazine 32(9), September 1994, pp. 40-48.]. There are various types of SOD, an important one is history-based SOD that regulate for example, the same subject (role) cannot access the same object for variable number of times.

Source(s):

[NIST SP 800-192](#)

- Separation of Duty is a key security principle.
- Simple to implement with well designed architecture
- Regulations define the Three-line defence model

Threat funnel to Advance Cybersecurity & Resilience



Reduce The
Attack Surface

Minimize the vulnerabilities and entry points that can be exploited to compromise the environment.



Detect & Respond
To Cyber Threats

Actively identify and address potential security incidents and malicious activities.

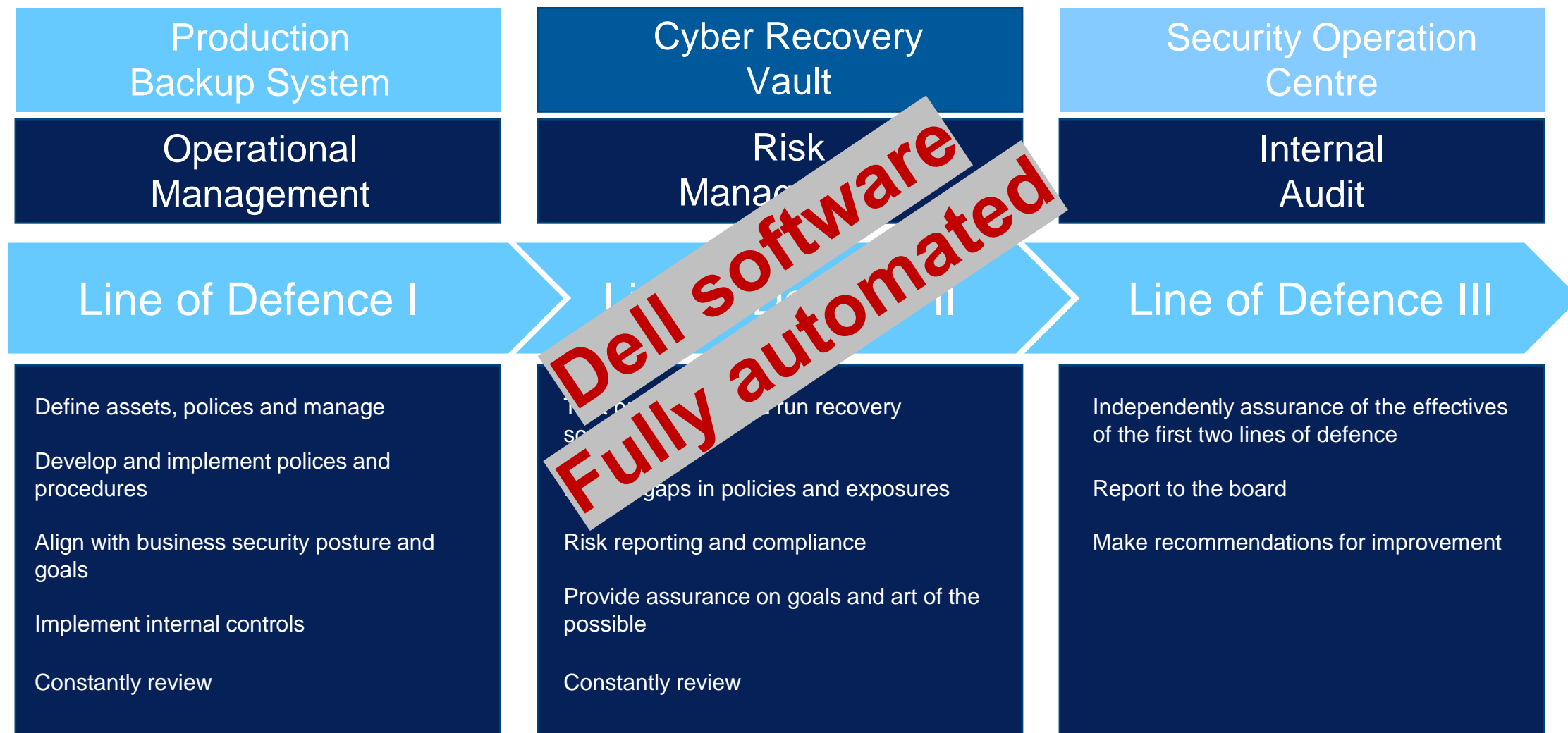


Recover From
A Cyberattack

Restore the organization as quickly as possible while minimizing disruption.



Three lines of defence model



The Time for Resilience is Now!

The Gartner logo is displayed in a large, bold, dark blue font on a white rectangular background. The logo consists of the word "Gartner" followed by a registered trademark symbol (®).

"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."

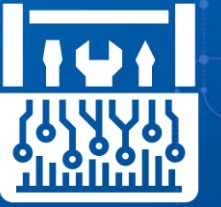
Gartner, *You Will Be Hacked, So Embrace the Breach!*

"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*

Tools for Your Resilience Journey

Your Data Protection Toolbox



Backup



Continuous
Data
Protection



Immutable
Primary
Storage



Immutability
for backups
(2-copy resilience)



Clean Rooms
& Mature
Recovery



Replication
to DR



Snapshots



Immutable
Snapshots



Isolated Vault
for Critical
Rebuild



Vault for Key
Applications
(3rd copy)

Dell DPS Means Resilience



The Resilience Foundation

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 DD

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 – DD FS

- 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

Efficiency Now Matters More Than Ever

Deduplication enhances security

Production Data

Front-end TB
in production



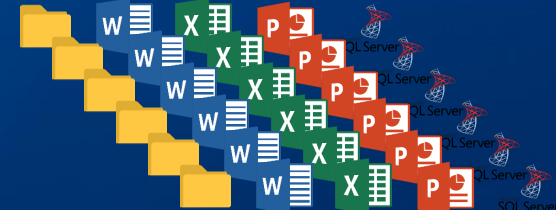
Dell

Others

Dedupe 50 -1

Dedupe 5 -1

Production Backup



DR



Isolated Vault



- ✓ Fewer components =
 - Less network traffic
 - Less to secure
 - Less to monitor
- ✓ Save data center space
- ✓ Save data center cooling
- ✓ Fewer FTE

Anomaly Alerting



Alert for anomalous behavior as soon as it happens via alerts



Monitor selected appliance and systems with suitable set of rules



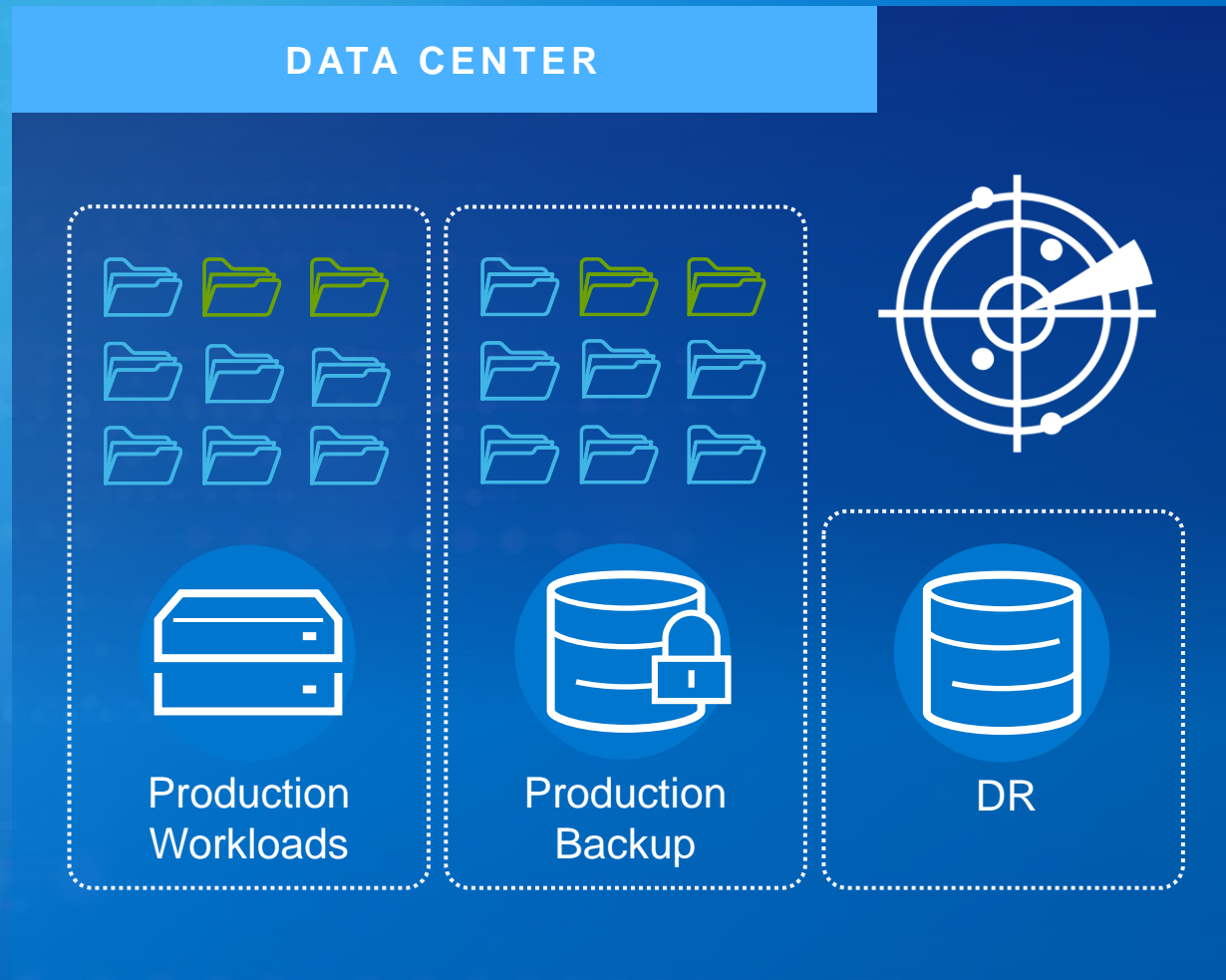
Analysis Engine is stateful with continuous monitoring



Easy to configure and setup default and new rules

Data Resilience – Production Environment

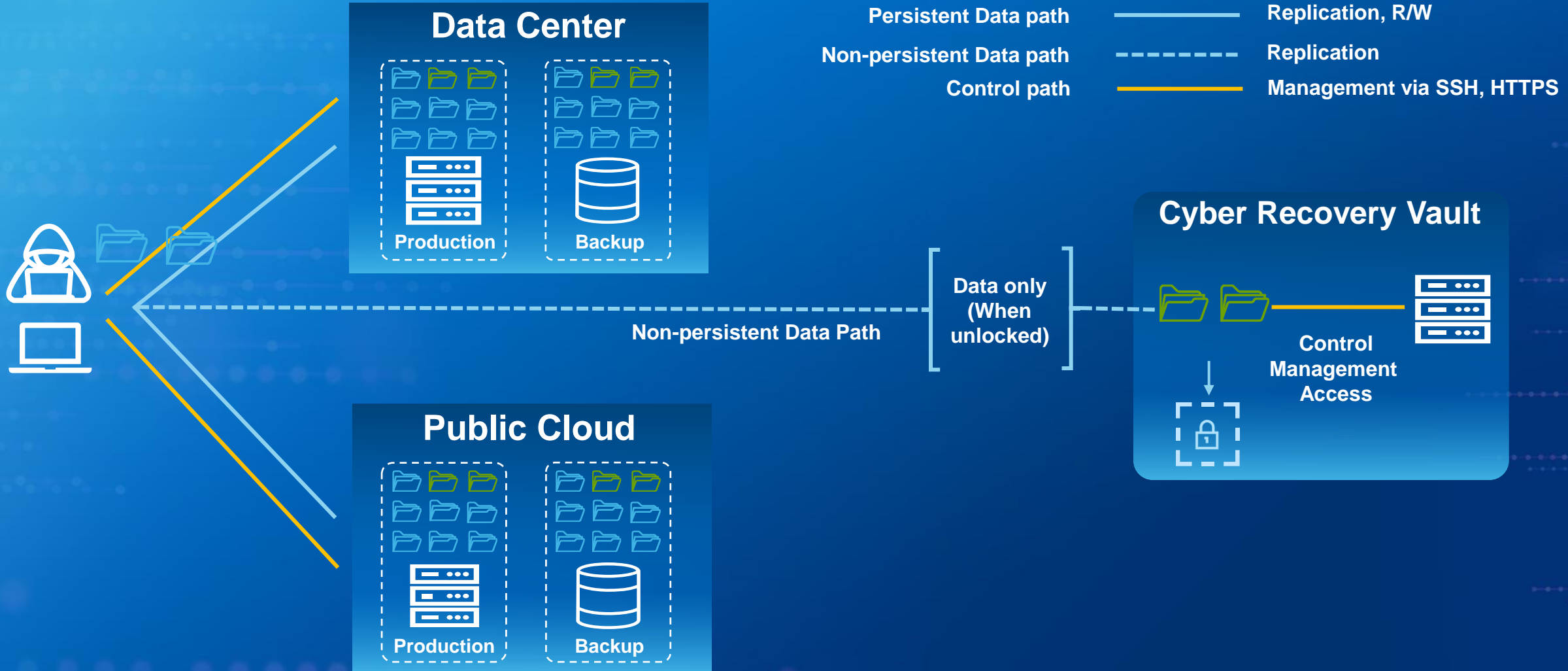
The Most Secure 2-copy Resilience Solution



- Zero Trust Alignment
- Role Based Access Control (RBAC)
- Immutability
- Pervasive Encryption
- Hardened Appliance
- Dual Role Authorization
- Multi-Factor Authentication
- Data Deduplication
- Efficient Consumption
- Key Management (KMIP)
- Data Invulnerability Architecture (DIA)
- Integrated Lights Out Mgt Hardening (iDRAC)
- No exposed CIFS/NFS
- *Anomaly Alerting and Reporting*

The Importance of Isolation

Improve On Immutability By Denying Access

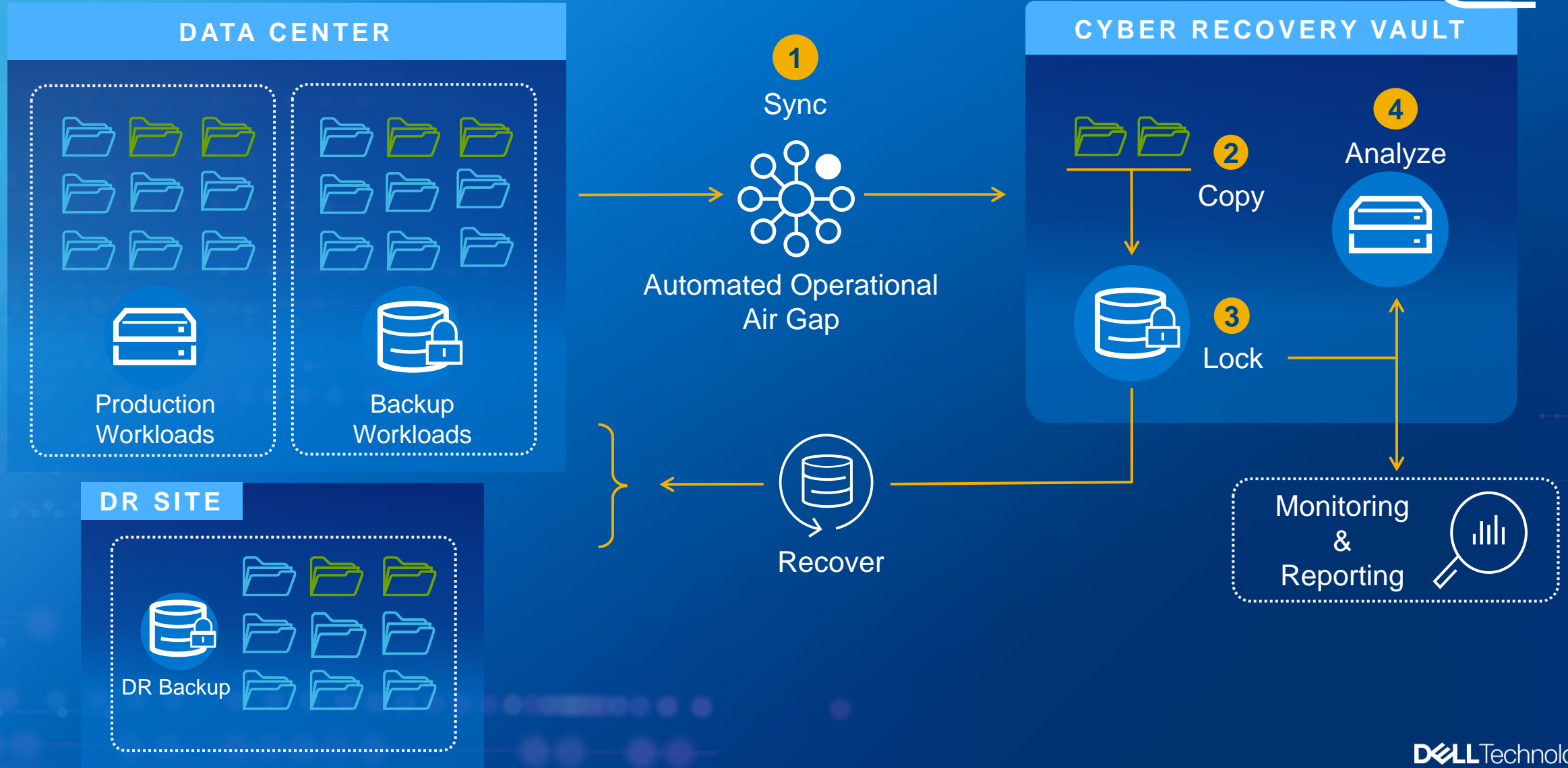


Primary Purpose of the Vault

““Reduce the attack surface and maintain control of critical materials in the event of a cyber attack.”

Dell PowerProtect Cyber Recovery

Ensuring Recovery After A Cyber Disruption



Dell Differentiators

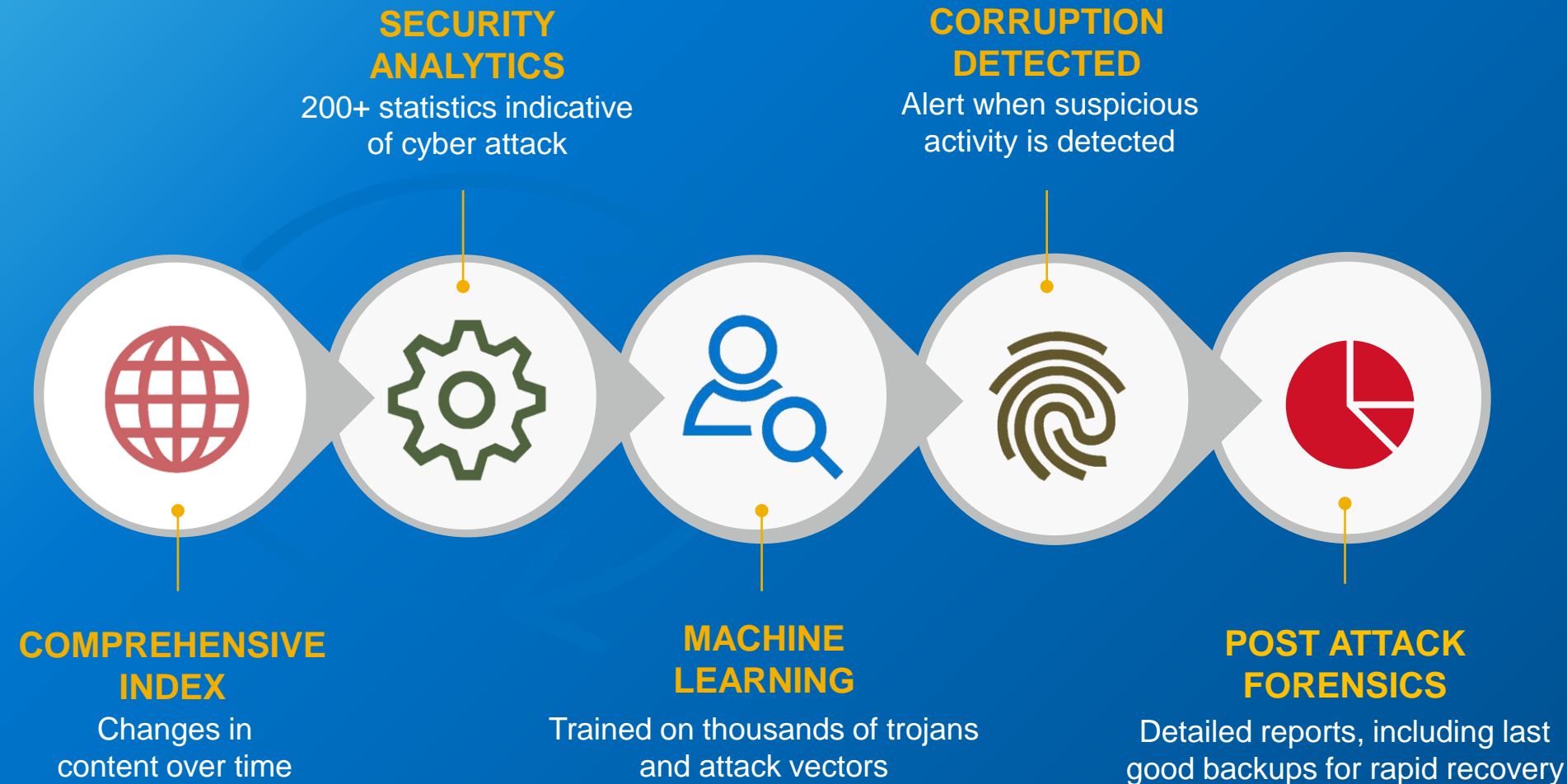


Isolating Data in the Cyber Recovery Vault

1. Industry's Smallest attack surface
2. No direct exposure to the vault from the production network
3. Not vulnerable to credential theft
4. Control and Management plane inside of the vault
5. Independent capability: test restores and recovery

Integrity Validation with CyberSense

Intelligence = Analytics, Machine Learning and Forensic Tools to Detect & Recover from Cyber Attacks



CyberSense Provides

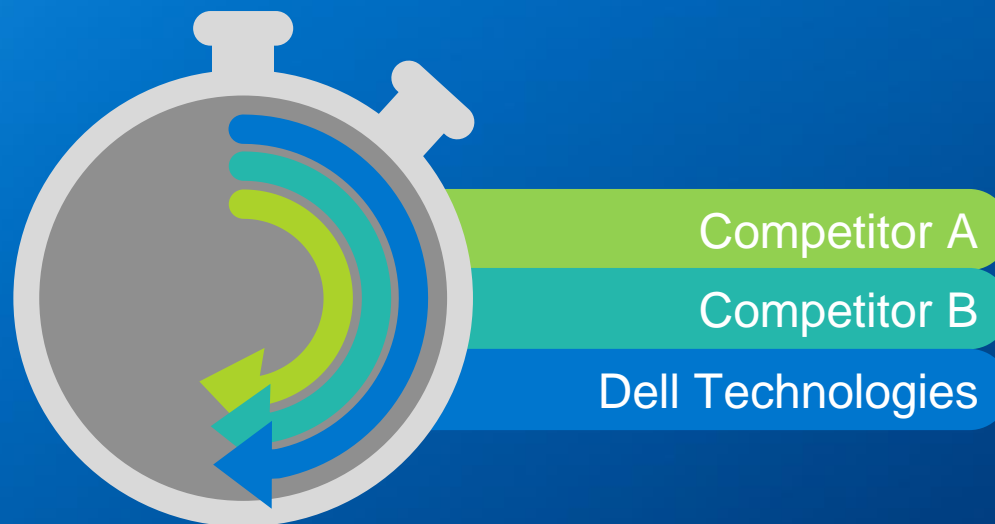
- Attack type notification
- Ransomware detection
- Corrupted file details
- Data changes / deletions
- Breached user accounts
- Breached executables
- Last good backup copy

Anomaly Alerting or Integrity Validation?

Use Both For Better Outcomes

Anomaly Alerting

- Identifies and alerts on abnormal activities
- Can help determine if threat actors are targeting the backup environment



Integrity Validation

- Validates the integrity of the data to use in recovery operations
- "Last known good copy"

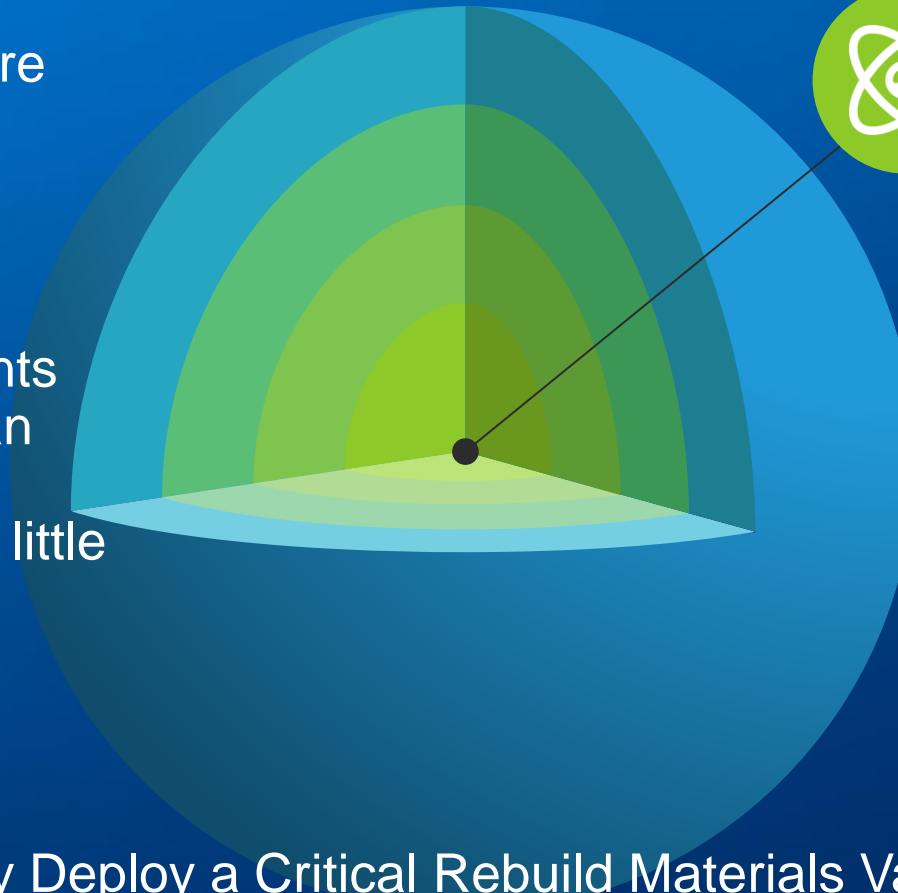


Critical Rebuilds Start at the Core

Deploy A Vault with Basic Recovery Building Blocks



- Critical Rebuild Materials are **"Tier 0"** infrastructure needed before business applications can run.
- Protecting Tier 0 components such as Active Directory can substantially speed and improve recovery with very little complexity or overhead requirements.



Tier 0

Protect the critical data needed to begin the rebuild of your environment first. Some examples are:

- Active Directory / LDAP
- DNS
- Switch / router / IP configurations
- Firewall rules
- Gold copy images / binaries
- Configurations and settings

Why Deploy a Critical Rebuild Materials Vault?

- Fast deployment and low complexity
- Enhanced resilience
- Provide a foundation for future vault contents such as databases and business applications

Continue Your Data Recovery Journey

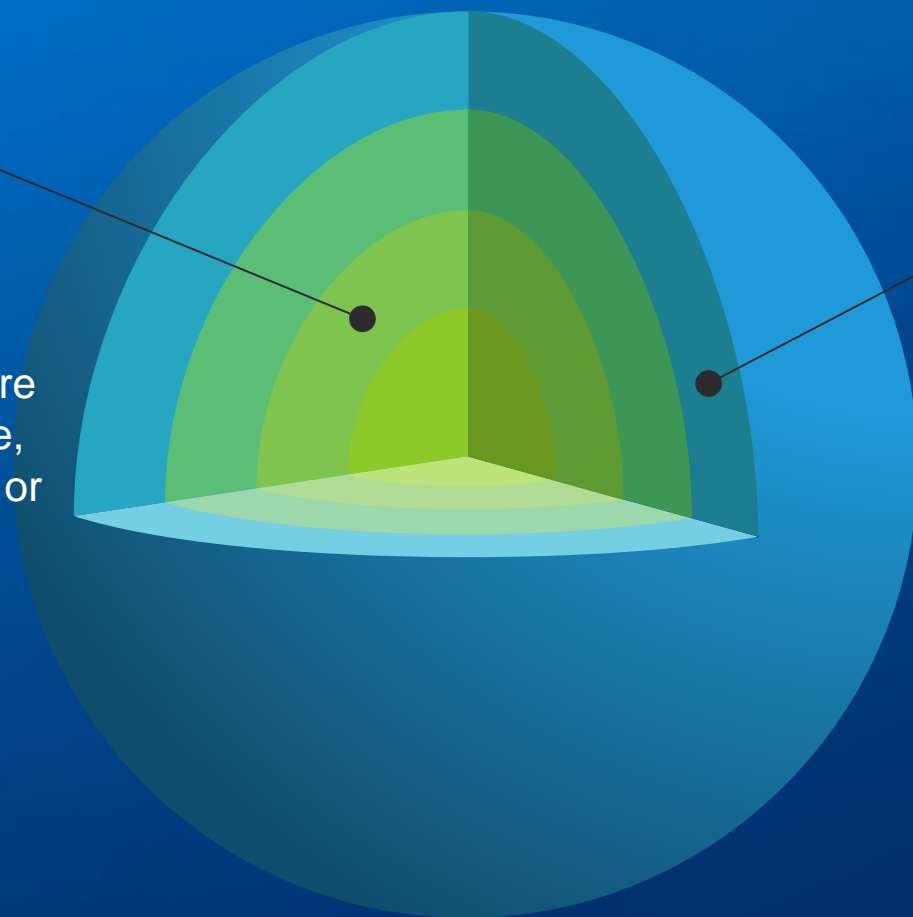


Understand the data in your environment and how it impacts the business



Tier 1 Applications

Progress to the top 2 or 3 applications that are most important to keeping the business running. These are typically aligned to revenue, reputation, systematic risk or safety.



Tier 2 Applications

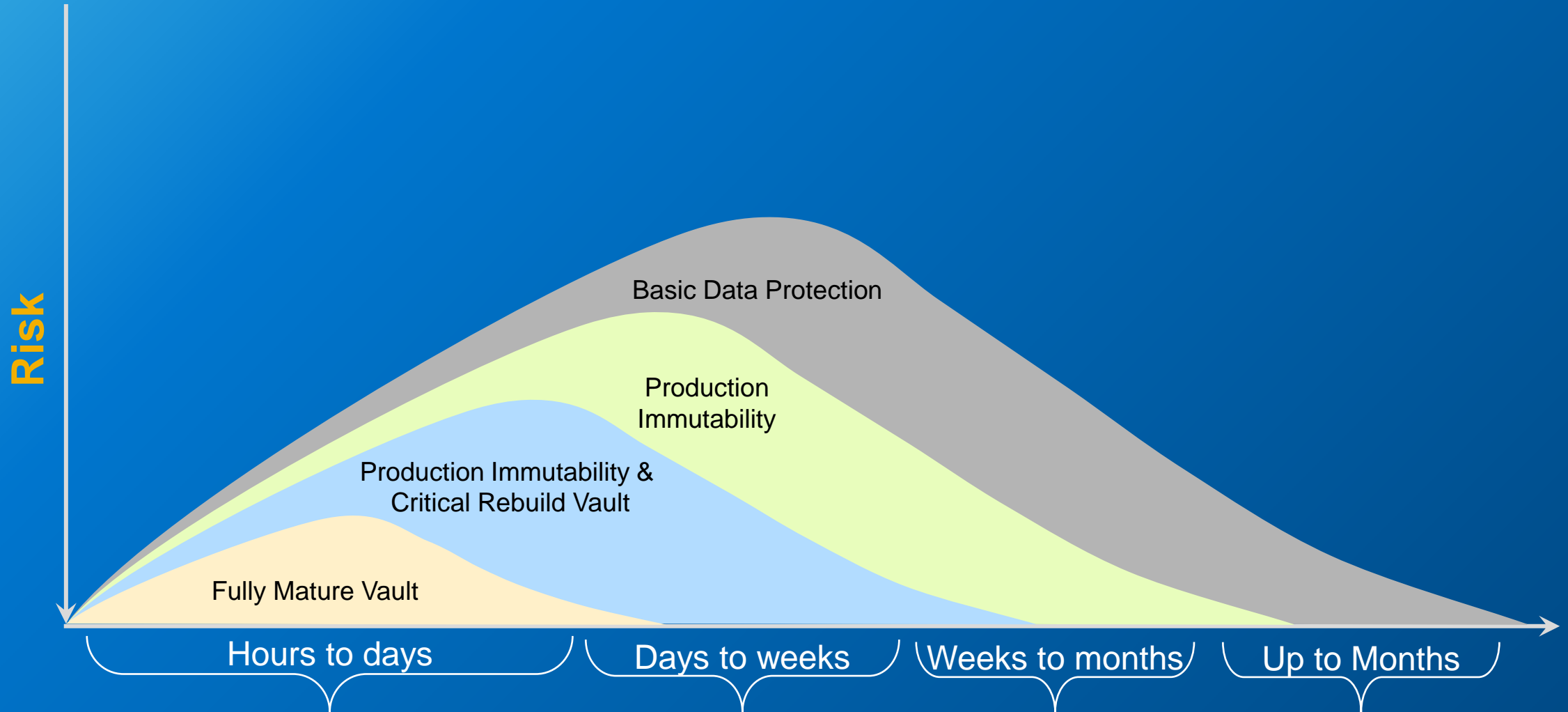
Protect additional applications and data that are important to the business. This will enable more of the business to be quickly recovered. Grow, as needed, over time.

Recovery Maturity

Consider advanced capabilities such as clean rooms and landing zones to speed and further enhance the recovery process.

Stronger Resilience. Better Outcomes.

Reduce Risk, Speed Recovery, and Lower Costs



Full Time to Recover

Extensive Dell Security & 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



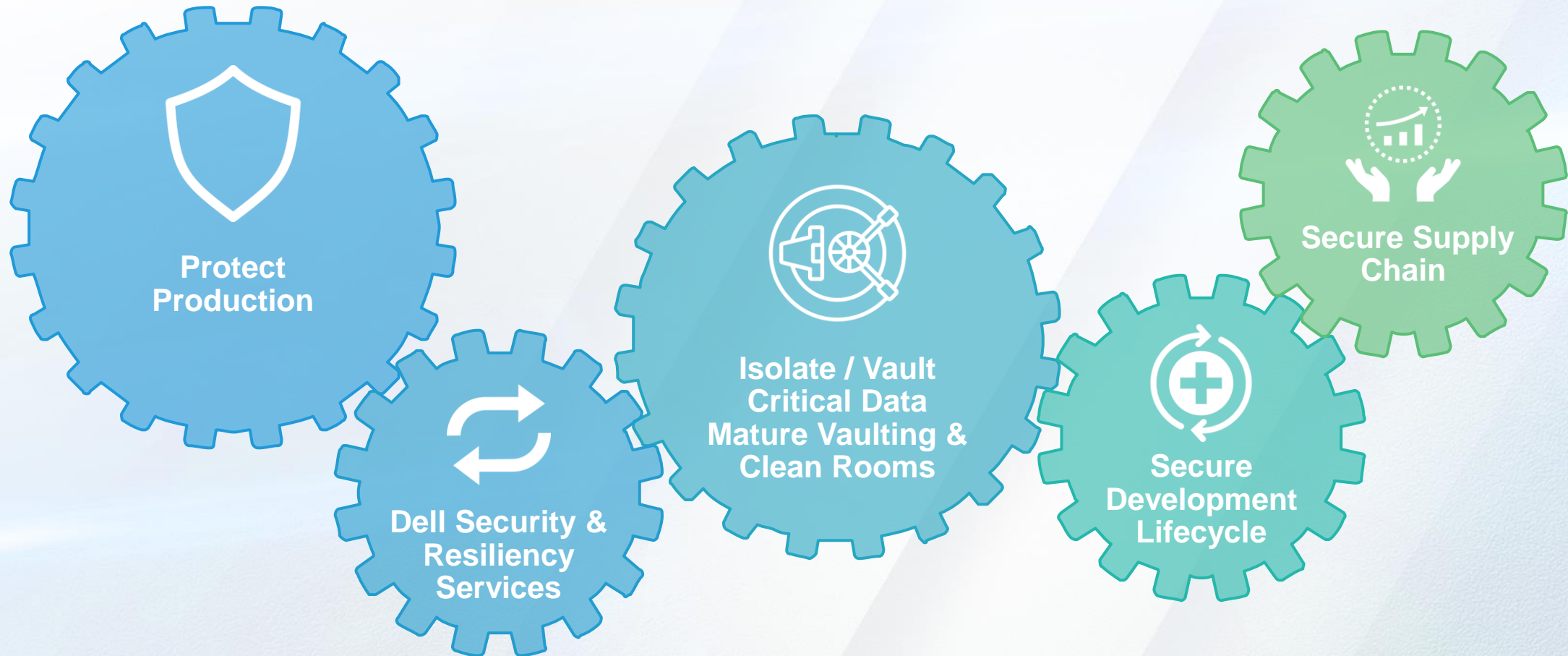
>35K
Service & Support Professionals

**Certified Cyber
Security Experts**

20+ years of
resiliency services innovation

Dell DPS Summary

Protect Your Business with the Right Tools



The logo for Dell Technologies, featuring the word "DELL" in a bold, sans-serif font, followed by "Technologies" in a lighter, sans-serif font. The "E" in "DELL" is stylized with three diagonal lines extending from its right side.