4:

RESPOND & RECOVER

Equipping our clients with leading cyber solutions and a proven methodology to build operational resilience in the event of an attack.

Business Outcomes

OPERATIONAL RESILIENCE

Respond & Recover

Implementing precautionary measures to take a proactive approach to security is the best way to keep ahead of threats.

However, as the threat landscape is constantly changing and attacks continue to grow more sophisticated, Dell Technologies recommends our clients always have a response and recover strategy in place, so that in the event an attack does occur, the business can function as normal.

Taking this approach will equip the business with worst case scenario remediation plans to ensure the business can continue to operate as normal. The following solutions outline Dell Technologies Response & Recovery cybersecurity solutions.

Respond | OPERATIONAL RESILIENCE

Fraud Prevention

PRODUCT SOLUTIONS

The RSA NetWitness Platform, a leader in Gartner's 2018 Magic Quadrant for Security Information and Event Management, applies the most advanced technology to enable security teams to work more efficiently and effectively.

It uses behavioral analysis, data science techniques and threat intelligence to help analysts detect and resolve both known and unknown attacks before they disrupt your business.

The platform uses machine learning to automate and orchestrate the entire incident response lifecycle. This allows security teams to collapse disparate security tools and the data they generate into a single, powerful, and fast user interface.

> RSA NetWitness® Platform enables the experts in our cyber defence centre to understand the true nature, scope and impact of an incident and empowers them to take immediate, targeted action."
>
> **K Lakshmi Narayanan**
> AVP and Head of Cybersecurity
> Technology and Operations,
> Infosys
>
> **For more information:** bit.ly/2BAMrjr

Incident Response

MANAGED SERVICE SOLUTIONS

Secureworks accredited cyber incident response team backed with proprietary Secureworks Threat Intelligence and purpose-built response technologies helps you resolve complex cyber incidents at scale.

Our services help you reduce response time and incident impact by leveraging Secureworks seasoned incident responders.

Using purpose-built response technologies enriched with years of cyberattack and threat group data to help you respond to and mitigate cyber incidents efficiently and effectively.

Recover – Dell EMC Cyber Recovery Solution | OPERATIONAL RESILIENCE

PRODUCT SOLUTIONS

Operational Resilience in the Event of an Attack

Datacentres are a fundamental part of business infrastructure. An attack on this infrastructure can not only devastate a business commercially but can have a much wider impact on society as a whole as it disrupts core services to customers.

This threat to society has meant that there is an increased focus on protecting backup systems and enhancing disaster recovery capabilities so that in the event of an attack, businesses can continue to function as normal.

BUSINESS CHALLENGE

Whilst proactive solutions can help to protect businesses from cyberattacks, ***insider threats*** still pose a huge risk to the business and are much harder to detect and defend against. Whether it is a rogue employee or an intruder has taken over access of your systems, ***businesses must protect their ability to recover*** in order to minimise disruption to the running of the business and impact on customers.

THE SOLUTION

Dell EMC's Cyber Recovery solution ***protects your business' most critical data*** by leveraging an ***air gapped cyber recovery vault*** and limiting access to authorised personnel only. This sophisticated, secure backup solution ensures critical data is physically and virtually separate from production systems. The vault is only accessible to the network when it is transferring data – it then disconnects leaving the vault in true isolation.

> One of the most poignant things I've heard a client say about this solution is that:
>
> "This solution is the difference between business continuance and business existence. In the absence of this capability we might cease to exist after a successful cyberattack.""
>
> **Todd Lieb**
> Cyber Recovery Lead,
> Dell EMC

Recover | OPERATIONAL RESILIENCE

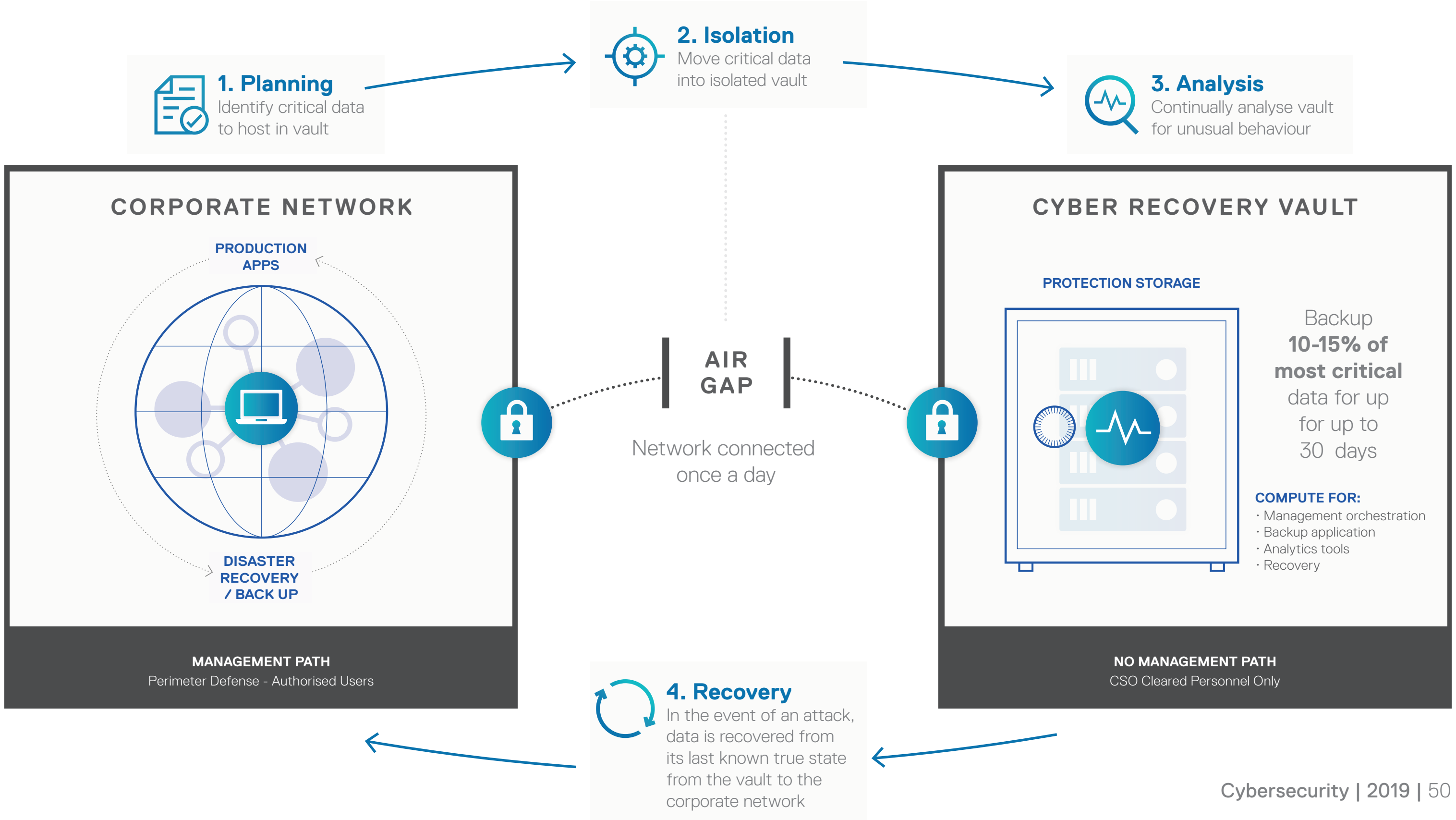
Dell EMC Cyber Recovery Solution

PRODUCT SOLUTIONS

This solution works best in addition to disaster recovery and backup systems.

Dell EMC recommends to only backup 10-15% of your most critical data in the vault, updating once per day and storing data for up to 30 days.

In the event of an attack, this solution enables you to recover data in its last known true state to be moved back into the corporate network to enable your business to operate as normal.



1. Planning
Identify critical data to host in vault

2. Isolation
Move critical data into isolated vault

3. Analysis
Continually analyse vault for unusual behaviour

CORPORATE NETWORK

PRODUCTION APPS

DISASTER RECOVERY / BACK UP

MANAGEMENT PATH
Perimeter Defense - Authorised Users

AIR GAP

Network connected once a day

CYBER RECOVERY VAULT

PROTECTION STORAGE

Backup **10-15% of most critical** data for up for up to 30 days

COMPUTE FOR:
- Management orchestration
- Backup application
- Analytics tools
- Recovery

NO MANAGEMENT PATH
CSO Cleared Personnel Only

4. Recovery
In the event of an attack, data is recovered from its last known true state from the vault to the corporate network

Recover | OPERATIONAL RESILIENCE

Dell EMC Cyber Recovery Solution

PRODUCT SOLUTIONS

This robust business resilience solution is made up of four components:

1. Planning

Assess business critical systems to protect and create dependency maps for associated applications and services, as well as the infrastructure needed to recover them.

The service generates recovery requirements and design alternatives, identifies the technologies to analyse, host and protect data, along with providing a business case and implementation timeline.

2. Isolation

The centrepiece of the solution is the cyber recovery vault, an isolated and protected part of the datacentre. The vault hosts critical data on Dell EMC technology used for recovery and security analytics.

The goal of the vault is to move data away from the attack surface, so that in the event of a malicious cyberattack, organisations can quickly resort to a good, clean copy of data to recover critical business systems. Using vault protections around the isolated data also protects it from insider attacks.

Dell EMC Cyber Recovery automates the synchronisation of data between production systems and the vault, and creates immutable data copies.

3. Analysis

Cyber Recovery's automated workflow includes the ability to create sandbox copies that organisations can use for security analytics. Analytics can automatically be performed on a scheduled basis.

CyberSense applies over 40 heuristics to determine indicators of compromise and alert the user.

Cyber Recovery stays ahead of the bad actor by enabling tools such as CyberSense which incorporate Artificial Intelligence and Machine Learning analytics methods to the vault.

4. Recovery

Automate recovery workflows to perform recovery and remediation after an incident and bring business resiliency to a higher level.

Cyber Recovery allows customers to leverage dynamic restore / recovery procedures using existing disaster recovery procedures that bring business critical systems back online.

Dell EMC and its ecosystem partners provide a comprehensive methodology for protecting data, as well as performing damage assessments and forensics to either recover your systems or remediate and remove the offending malware.

Our Clients say...

Financial institutions are among the most targeted organisations for cyberattacks and our responsibility is to ensure the highest levels of security for our members and the financial assets they entrust us with.

All it takes is for one successful intrusion or ransomware attack to seriously disrupt any business and if the bad guys are smart enough to know where your backups are, you're left with no protection.

Dell EMC Cyber Recovery helps my team isolate all of our critical data off-network, giving us confidence in our business resilience in the event of a worst-case cyberattack scenario."

Bob Bender
Chief Technology Officer,
Founders Federal Credit Union

For more information: bit.ly/2eYyAcn

Industry Analysts say...

The most effective plans for cyber threat resilience must include provisions to protect and isolate the data protection infrastructure.

By design, data protection systems are architected on the same networks as production systems and are therefore part of the potential attack surface.

Dell EMC offers a smart solution that employs an air-gapped Cyber Recovery Vault, along with automated software that helps isolate, analyse and recover an organisation's critical data so business can resume in the event of a cyber intrusion or ransomware attack."

Christophe Bertrand
Senior Analyst,
ESG

For more information: bit.ly/2IZEtnn

Contact Details

www.DellTechnologies.com

@DellTech

Dayne Turbitt
Senior Vice President UKI

Dayne.Turbitt@Dell.com

bit.ly/2xGgo0p

Margarete McGrath
Chief Digital Officer UKI

Margarete.Mcgrath@Dell.com

bit.ly/2NGJdUq

Chris Miller
RSA Regional Director, UKI

Chris.Miller2@RSA.com

bit.ly/2V9TI82

Simon Godfrey
Secureworks Regional Director, UKI

SGodfrey@Secureworks.com

bit.ly/2V5J3pD