

4:

DEFEND & 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

Detect & Respond

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 that our clients always have a strategy to ensure appropriate detection and response systems are in place.

Resilient businesses are able to operate while under persistent threat and active compromise. In the event an attack does occur, the business can rapidly identify, mitigate and remove the threat from the infrastructure.

Defenses need to be robust whilst at the same time ensuring that the organisation continues to operate effectively under attack without disruption to business systems and operations.

This section presents a number of comprehensive solutions from Dell EMC, RSA and Secureworks that are focussed on detecting, responding and helping our clients recover when an attack occurs.



Detect & 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.

Detect & Respond | OPERATIONAL RESILIENCE

RSA NetWitness Platform

PRODUCT SOLUTIONS

The RSA NetWitness Platform evolved SIEM accelerates threat detection and response by providing unparalleled visibility to see threats anywhere – on endpoints, across the network, in the cloud and virtual environments. In addition, it combines essential business context with automation and machine learning capabilities to help pinpoint and respond definitively to the threats that matter most.

Visibility, Analytics, Action

The RSA NetWitness Platform provides pervasive visibility across a modern IT infrastructure, enabling better and faster detection of security incidents, with full automation and orchestration capabilities to investigate and respond efficiently. RSA NetWitness Platform takes security “beyond SIEM,” extending the traditional log-centric, compliance-focused approach to security to include state-of-the-art threat analytics, including user and entity behaviour analytics (UEBA), and visibility into cloud, network and endpoints.

Advanced Analytics

Detects and identifies threats using sophisticated rules, threat intelligence and malware analysis, as well as behavior analytics. Sophisticated threat detection algorithms operate across disparate data types and sources, for fast identification and correlation of indicators of compromise (IOCs) and real-time prioritisation of true threats.

True UEBA

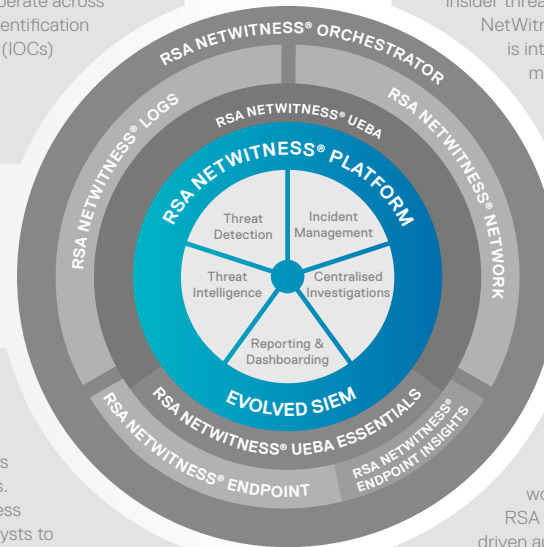
User and Entity Behaviour Analytics (UEBA) detects anomalies in behaviour patterns, highlighting potential exploits or insider threats. Fully automated and “zero touch,” RSA NetWitness UEBA is RSA proprietary technology that is integrated into the platform’s common data model and analyst toolset.

Broad Visibility

Provides unsurpassed visibility across logs, packets, endpoints and NetFlow data, across on-premises, virtual and cloud environments. A common data model, enriched with business context and threat intelligence, enables analysts to correlate anomalies wherever they occur, providing fast insight into the full scope of an attack.

Automation & Orchestration

Automates security tasks and analyst workflows to increase SOC efficiency and speed. RSA NetWitness Orchestrator features playbook-driven automated response actions, and machine-learning insights that integrate your entire security arsenal.



Detect & Respond | OPERATIONAL RESILIENCE

RSA NetWitness Platform

PRODUCT SOLUTIONS

A robust cyber defense solution is made up of five pillars:



1. Full visibility

Security and fraud teams must be able to proactively see what's happening within the enterprise and across all consumer-facing channels at all times – including processes, networks, devices, people and transactions.

Only with this 360-degree ability can teams identify risks across the environment – before they become real problems.



2. Risk awareness

Organisational leaders and operational personnel should establish a foundation of infrastructure, data and fraud risk that they apply across the enterprise, assuring proper focus on high-risk assets.



3. Rapid insight

Faster “time to insight,” through better analytics and detection capabilities, is paramount in today’s environment of external partners, cloud computing, personal devices and the like.

Time to insight for security teams is collapsing to zero; the more time you need to interpret an event, the greater your risk. This means heavier reliance on scalable systems that employ machine learning and less reliance on manual policies and adjustments that cannot scale.



4. Operational Context

The security team can't rely only on seeing what is happening on its network and among its internal and external users; team members must also be able to interpret those events quickly, while understanding the criticality of affected systems and processes.

Such contextual intelligence facilitates faster and better decisions. Understanding operational context (such as the criticality of account data or the importance of a particular financial transaction) can also help analysts determine how urgently to escalate incidents.



5. Efficient Response

Today, many security teams take the findings from their security tools and remediate in a highly manual way that doesn't scale.

The most effective way to turn insights into action is to orchestrate and automate response.

Spot a user acting suspiciously or a potentially fraudulent transaction, and the control plane of identity goes into action, stepping up authentication to ensure that this user is legitimate. Expedited – and, where possible, automated – case management is paramount.

Our Clients say...



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/2eYyAcn

Industry Analysts say...



(RSA) has the ability to support enterprise buyers focused on advanced threat detection and looking for a single vendor that integrates capabilities including core SIEM, network monitoring and analysis, EDR, and UEBA.

The combination of RSA NetWitness Network and NetWitness Endpoint provides strong coverage of the five styles of advanced threat defense: real-time network and endpoint monitoring, and forensic network and endpoint investigation.

RSA NWP provides strong OT monitoring capability due to its ability to deploy RSA NetWitness Network to capture data in ICS/SCADA environments, and then process it using native support for common protocols.”

Gartner Magic Quadrant for Security Information and Event Management 2018

Recover

With the complexity of business processes, critical IT, infrastructure and third party relationships growing rapidly, digital transformation increases organisations risk of significant business disruption.

Achieving operational resiliency starts with understanding the systemic risk to the continuity of your organisation, creating processes that naturally adapt to adverse conditions and mitigate the impacts of a disruption.

Dell Technologies also recommended that provisions are made to recover when a cyber attack targets or impacts all online systems including production and backup infrastructure, as can be the case with ransomware or other destructive malware.



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 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.

Recover |  OPERATIONAL RESILIENCE

RSA Archer Business Resiliency

 PRODUCT SOLUTIONS

RSA Archer helps organisations transform from recovery to resiliency with solutions that address and mitigate resiliency risk to your organisation.

RSA Archer helps organisations transform from recovery to resiliency with solutions that address and mitigate resiliency risk to your organisation.

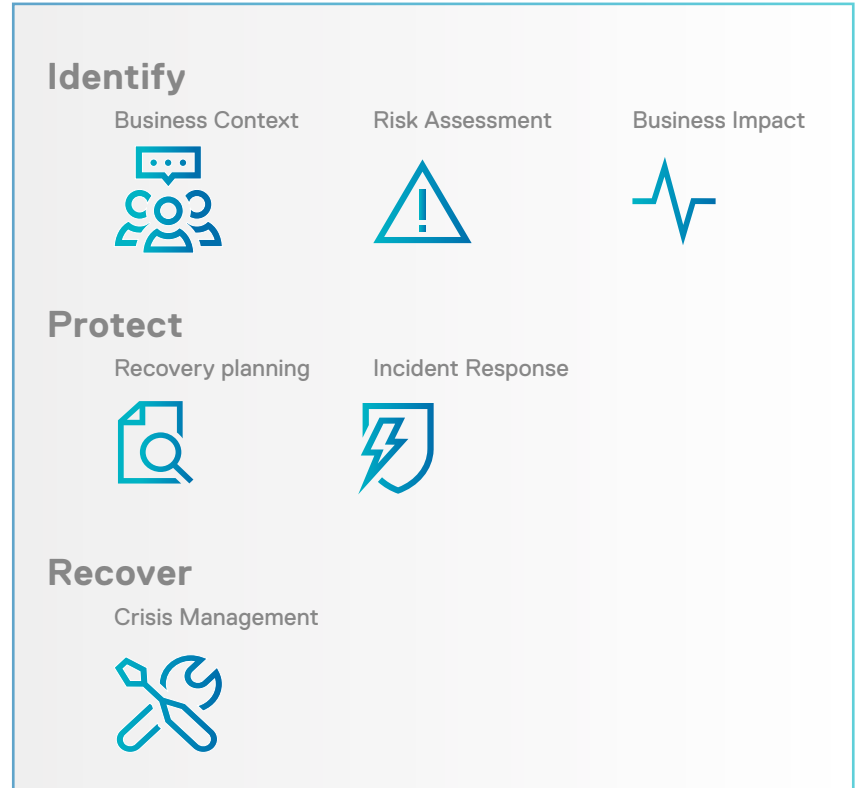
corporate network to enable your business to operate as normal.

Step 1:
Determine Business Context & Priorities

Step 2:
Coordinate Business Continuity & IT Disaster Recovery Planning

Step 3:
Coordinate Incident & Crisis Response

Step 4:
Adapt your Resiliency Programme



Recover |  OPERATIONAL RESILIENCE

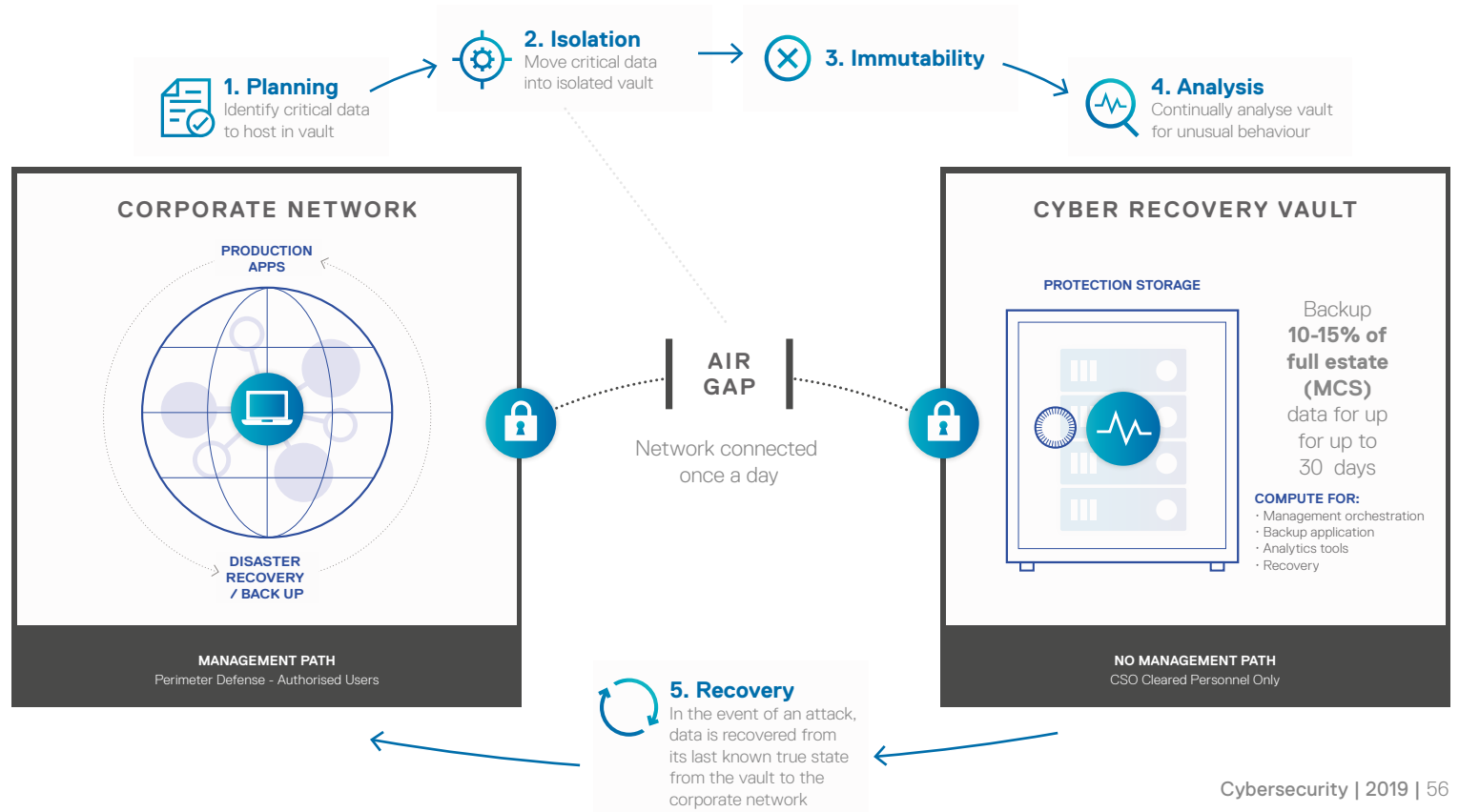
Dell EMC Cyber Recovery Solution

 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.



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/2IZEttn


Contact Details

 www.DellTechnologies.com

 [@DellTech](https://twitter.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

The Dell Technologies logo is centered on a dark gray background. It features the word "DELL" in a bold, white, sans-serif font, with a stylized "E" that consists of three horizontal bars. To the right of "DELL" is the word "Technologies" in a lighter, white, sans-serif font. The background is decorated with a network of thin white lines connecting various sized gray circular nodes, creating a complex web-like pattern that extends across the entire frame.

DELLTechnologies