Implementing and embedding cyber strategies and solutions in line with business objectives and surrounding risk landscape.

Business Outcomes

- ADVANCED PROTECTION
- RISK AND COMPLIANCE LEADERSHIP & CULTURE
Implement Strategy & Secure Environment

Nefarious actors seek to exploit vulnerabilities across every aspect of the business and IT landscape. The rise of connectivity has called for an increased focus on cybersecurity across the entire business model and organisational culture.

Businesses need to ensure that every part of their organisation is protected and that the right protection strategies are embedded across the end to end value chain. Organisations need to build digitally resilient cultures in which a culture of trust and an understanding of cybersecurity is widely appreciated by all business functions and not just technology stakeholders.

Dell Technologies cybersecurity capability covers every aspect of the value chain from infrastructure to business operations. This includes implementing cybersecurity tools, systems, procedures and precautionary measures to protect the following:

- **IT INFRASTRUCTURE**
- **GOVERNANCE, RISK & COMPLIANCE**
- **APPLICATIONS**
- **SECURITY OPERATIONS**
- **END-USER DEVICES**
The following framework outlines the scope of Dell Technologies solutions across the IT Operating Model and end to end value chain.

The Dell Technologies cyber methodology and portfolio of cybersecurity solutions are focused on equipping our clients with the right cyber capabilities, tools and insights to protect and grow their business.

Our methodology and supporting cyber solutions protect the full IT operating environment and end-to-end business model.
Dell Technologies delivers a secure, modern infrastructure which is resilient and protected from the ground up.

Companies today attribute more of their security issues to improper network segmentation than the volume of threats overall. In response, network virtualisation is becoming a key piece of the security apparatus for leaders across industries as organisations leverage the power of virtual capabilities to enable strategic security initiatives. 13.

Dell Technologies solutions help enhance cybersecurity whilst reducing the burden on the run of the business. The following solutions help organisations achieve a secure environment at the infrastructure layer.
Addressing Security Vulnerabilities with Zero Trust

Organisations are restructuring their infrastructure in a way that allows all data to be protected regardless of where it sits in the network.

The Zero Trust security model is the premise that there is no longer a trusted and untrusted network, but rather all networks are untrusted and need to be secured equally. Organisations are exploring how network virtualisation and micro-segmentation can increase the security of their network.

75% are exploring how network virtualisation can help better protect their network from security threats 13.

These three strategies deliver the following benefits:

- **Improved Security**
  Network virtualisation enables easier control and isolation of environments and assets.

- **Improved Network Visibility**
  Virtualisation technology to enhance isolation improves control within those protected network segments, empowering security teams to respond more intelligently to attacks.

- **Improved Business Continuity**
  Network virtualisation technology can enable a more adaptable recovery mechanism for leadership and is a key piece of any redundant system.

Separates day-to-day business data from sensitive enabling security and risk teams to place the proper security and access controls on sensitive data segments.

These three strategies deliver the following benefits:

- **Enhanced Control**
  Quickly identify privileges for certain data types to enable businesses to quickly respond to changing security needs.

- **Improved Visibility and Protection**
  Understand where data exists, and which users are supposed to have access to improve monitoring and agility.

- **Stop lateral Spread of Threats**
  Micro-perimeters are created around specific sets of data to inhibit the spread of threats.
Infrastructure Networking

To meet these changing demands of network security, VMware’s network and virtualisation security platform enables a software-defined approach to networking that extends across datacentres, clouds, and endpoints.

Network & Virtualisation Security Platform

VMware NSX Datacentre (NSX) delivers consistent, automatable network security to workloads. Network security policies can be defined based on application contexts and enforced on every individual workload, without the need to touch the physical network.

The NSX platform allows cybersecurity policies to be defined based on application, user, and workload contexts. Network security teams have more flexibility to design policies that are resilient in the face of ever-changing applications.

Providing insight into network traffic flow between and within applications, it automatically suggests security groups and policies for achieving micro-segmentation.

Benefits

Holistic Application Visibility
Decrease the amount of time that your network security teams spend in application security review cycles.

Consistent Enforcement of Security Controls
Stop managing separate policies for different parts of the environment. With NSX Datacentre, you can enforce network security policies that span multi-data-centre and hybrid cloud environment.

Adaptive Network Security Policies
Automatically provision security policies for each workload that will remain with the workload even as the application changes over time.
Ensuring the reliable and lasting security of sensitive information is one of the main tasks of the IT department. The implementation of the NSX platform will bring us unprecedented possibilities for micro-granulation of security settings, and hence more selective and improved protection of individual applications.”

Miroslav Prokeš
Director of ICT Development and Operations,
Prague Stock Exchange

For more information: bit.ly/2V78TK3
Buffer & Data Protection

Hardware failure, human error, natural disasters, cybercriminals – these actors pose risks to your business continuity. As consumers continue to demand 24/7/365 accessibility, businesses must employ a robust backup and disaster recovery plan to ensure minimal disruption to the business and customers.

The following solutions outline how Dell EMC helps your business define a backup architecture roadmap, choose the most appropriate backup appliance, and leverage industry-leading software to transfer data.
Infrastructure

Blueprint for Backup Architecture

Blueprint for Backup Architecture reviews current data protection operations to provide an overall assessment of the backup services provided by the IT organisation, identify gaps between the backup and archive services and the requirements to protect and manage data. It also recommends appropriate changes in people, processes or technology to improve the backup services and identify roadmap and time frames for implementing the remediation recommendations.

Backup & Recovery

Dell EMC offers a robust set of data protection solutions both software and hardware that can protect all applications wherever they live (on-premises or public cloud).

Our backup solutions offer performance of up to 68 TB per hour, significantly reduce backup and archive storage requirements by 10 to 55 times, and shrink bandwidth requirements by up to 98%. Consolidating backup, archive and disaster recovery on a single platform, our backup solutions ensure data recoverability, and seamlessly integrates directly with enterprise applications or primary storage.

Flexible Investment Options

Dell EMC offer flexible options to invest and consume data protection solutions, options include:

- **Build**
  - Leverage software to transfer data to a purpose built target offering flexibility to scale software independent of hardware.

- **As-a-Service**
  - Leverage all the advanced capabilities and benefits of our solution through a service provider who can fully host backup environment for private cloud capabilities.

- **Buy**
  - An integrated approach combining software, hardware, compute, networking and storage in a single appliance for simple, easy and scalable protection.

- **Cloud**
  - All solutions can be deployed in the public cloud.

- **Software Defined**
  - Software only option available across all solutions can be procured and deployed on commodity hardware.
Dell EMC’s data protection solutions are cloud-enabled with the ability to natively tier deduped data to the public, private or hybrid cloud.

Our cloud backup and recovery solutions have been created in partnership with leading cloud providers like Amazon AWS, Microsoft Azure & Google Cloud Platform, so businesses can deploy and scale the right-sized cloud data protection no matter where data lives.

**Dell EMC’s Data Protection software enables business to:**

- Move workloads to the cloud
- Protect workload in the cloud
- Backup and recover in the cloud
- Achieve cloud disaster recovery

**Product Solutions**

**On Premise**

**Backup to Cloud**

**Protect in Cloud**

The Data Protection Suite spans across on-premise, direct to cloud and workloads within the cloud.
Applications

As applications are increasingly more accessible over the network, cybersecurity continues to be a prevalent concern during the development cycle.

A sound application security strategy will ease the process of patch management, and minimise the risk of malicious code being deployed.
There are three principles of cloud-native security:

**Repair**
Repair vulnerable software as soon as updates are available. Organisations can repair vulnerable operating systems and application stacks consistently within hours of patch availability. Pivotal refers to this as a "stemcell," and we update the stemcell with the latest OS patches for Pivotal Cloud Foundry customers.

**Repave**
Repave servers and applications from a known good state. With Pivotal Operations Manager, enterprises can repave every virtual machine in their datacentre from a known good state every few hours without application downtime. They can deploy applications from a continuous integration tool such as Concourse, and application containers will also be repaved every few hours.

**Rotate**
Rotate user credentials frequently, so they are only useful for short periods of time. In order to easily rotate system credentials every few minutes or hours, Pivotal customers can use identity management systems with multi-factor authentication to help safeguard systems as we work on automated credential management.

Prior to implementing Pivotal Cloud Foundry, we had many manual processes as part of our security procedures for deploying new applications. We used to have developers spending roughly four weeks to get all of the security elements they needed done by various security teams and infrastructure teams for their project. Today, they can get everything they need in a few seconds.”

Michael Ehrman
Information Security Manager,
Kroger Company

For more information: bit.ly/2Brem5d
VMware AppDefense is a datacentre endpoint security product that protects applications running in virtualised environments. AppDefense understands an application's intended state and behaviour, then monitors for changes that indicate a threat. When a threat is detected, AppDefense automatically responds.

AppDefense generates authoritative alerts coupled with automated response capabilities which allow the Security Operations Centre to focus on catching and eradicating threats from their environment, rather than sifting through noisy data and investigating threats that aren’t there.

To ensure security are aligned with modern applications, AppDefense creates a common source of truth between application teams and the security teams, streamlining the security review and readiness process.

AppDefense complements our other security solutions very nicely by filling a gap that we didn’t have covered before. Ransomware attacks against hospitals do happen, and you can lose thousands of computers in minutes. With AppDefense and NSX Datacentre bolstering our Sphere foundation, we can mitigate risk by extending a zero-trust model across the network, all the way to the endpoints. It’s a powerful combination.”

Christopher Frenz
Assistant Vice President of IT Infrastructure
Interfaith Medical Centre

For more information: bit.ly/2EFkw58
An increase in remote working, the gig economy, and bring-your-own-device programmes, has required a stronger focus on how organisations manage devices, applications, and access permissions. The solutions on the following page focus on easing end-user security.
VMware Workspace ONE is an intelligence-driven digital workspace platform powered by VMware AirWatch Technology. The platform enables organisations to simply and securely deliver and manage any app on any device with an integrated digital workspace platform.

Workspace ONE integrates access control, application management and multi-platform endpoint management and is available as a cloud service or for on-premises deployment. The comprehensive and predictive security feature Workspace ONE Trust Network provides a comprehensive and modern approach to enterprise security for your employees, apps, endpoints and networks.

With capabilities to protect, detect and remediate modern-day threats, Workspace ONE Trust Network combines access, device and app management, and analytics with an ecosystem of integrated partner solutions based on a framework of trust.

With Workspace ONE, we can have a laptop ready with all security policies in less than half a day. It can be shipped off to an employee, who can start using it as early as the next day. That capability will be even more valuable as we continue to globalise our workforce and continue to refine a true out-of-the-box service delivery model. As a security company, we take endpoint security and compliance very seriously, and AirWatch technology helps us keep our laptops healthy and compliant.”

Mark Zigadlo
Vice President of IT, Cofense

For more information: bit.ly/2ShCT41
Adopting a Risk-Based Mindset

Dell Technologies works in partnership with leading advisory firms to instil a risk-based mindset and enable your organisation to take the right steps towards securing your digital future.

Ensuring that business leaders and executives build a culture and environment where people understand how to behave securely and do the right thing is paramount to the success of our cybersecurity solutions. Any solution, no matter how prescient, is only as good as its execution.

We believe cybersecurity and compliance need support at board level and are not to be outsourced solely to a technology team. They require strategy and governance to get this right. Digital relationships with customers, suppliers and others expose businesses to new areas of risk that need to be managed.

We support senior management and boards to shape a strategic response to risk as well as provide detailed technical expertise.

The following section outlines Dell Technologies’ cyber solutions on governance, risk and compliance.
RSA’s Risk Framework is designed to help organisations tackle some of the most complex and fastest-moving risks emerging from digital business practices. This service encompasses two offerings:

- In-depth assessments of your risk business’ management maturity
- A detailed roadmap for maturing practices across the domains outlines on the right.

The four key areas are detailed below:

**Cyber Incident Risk Management**
Improve maturity in defending against attacks, detecting breaches and applying remediation, with action aligned to organisational risk objectives.

**Data Privacy Risk Management**
Infuse business context into compliance processes and technology, with monitoring capabilities to alert stakeholders to regulatory changes.

**Third Party Risk Management**
Develop a strategy to pro-actively manage third-party risk around loss events, opportunity cost and potential impacts to achieving objectives.

**Digital Business Resiliency Risk Management**
Integrate information governance into corporate infrastructure and business processes so compliance becomes routine.
Our Clients say...

We have all of the elements of the RSA Archer Suite. The Governance, Risk and Compliance module has very expansive capabilities and is critical in enabling us to drive the risk culture ME bank needs. It gives us the ability to push clear accountability into our front-line management concerning the risks and controls that they own. We’ve been able to significantly reduce the time it takes for them to accurately report to the governance committees.”

Joe McDavitt
Risk Assurance Manager,
ME Bank

For more information: bit.ly/2QHvTkj
Integrated Risk Management

Once a business determines the level of risk posed, a detailed roadmap can be developed to drive increased security maturity using the RSA Risk Framework. RSA delivers a robust Integrated Risk Management platform to help implement security measures and reduce enterprise risk for our clients.

RSA’s Archer Suite, a leader in the 2018 Gartner Magic Quadrant for integrated risk management, empowers you to manage multiple dimensions of risk on one configurable, integrated software platform. With RSA Archer, a business can implement risk management processes based on industry standards and best practices. This delivers improved levels of risk management maturity, more informed decision-making and enhanced business performance.

RSA Archer has six elements to provide an integrated approach:

**RSA Archer Audit Management**
Transform your internal audit function from reactive and compliance focused to become a proactive and strategic enabler of the business.

**RSA Archer Business Resiliency**
Automate business continuity and disaster recovery planning and execution to protect your organisation from crisis events.

**RSA Archer Enterprise & Operational Risk Management**
Gain a clear, consolidated view of risk across your business by aggregating disparate risk information in one central solution.

**RSA Archer IT & Security Risk Management**
Compile a complete picture of technology and security-related risks and understand their financial impact to improve decision-making.

**RSA Archer Regulatory & Corporate Compliance Management**
Establish a sustainable, repeatable and auditble regulatory compliance program by consolidating information from multiple regulatory bodies.

**RSA Archer Third Party Governance**
Get an accurate picture of third-party risk while managing and monitoring the performance of third-party relationships and engagements.
Our Clients say...

RSA Archer has helped us evolve from an organisation that was constantly chasing data and information... Now we have a source of record where employees can more quickly access and consume data and make decisions based on it.”

Reid Stephan
Director of IT Security, St. Luke’s Health System

For more information: bit.ly/2EL1B97
Fraud Prevention

RSA Fraud & Risk Intelligence Suite brings together fraud protection, adaptive authentication, web threat detection and fraud intelligence services to protect your business and consumers from online and mobile fraud, phishing, account takeover and data breaches.

This offering improves organisations’ fraud detection and prevention capabilities, enhances their fraud intelligence, and provides secure consumer access, 3D secure authentication, behavioural analytics, and mobile transaction protection.

"We needed to change our way of doing online banking. After talking to advisories to understand how we should address our customers in the future, we found that the best way to do that would be to go with a reliable partner like RSA, that is well known through the audit and security community. They have partnered with us to help us, and enable us to do better online banking."

Hakon Akerlund
IT Security Manager,
Landsbankinn

For more information: bit.ly/2Qv8fSO
Governance, Risk & Compliance

Identity & Access Management

RSA SecurID Suite goes beyond traditional identity and access management, using identity insights, threat intelligence and business context to provide secure access to all users, across all applications, from the ground to the cloud.

It brings together multi-factor authentication, risk-based access management, identity governance and user lifecycle management in one powerful suite of solutions.

"It used to take over 600-hours for the team just to execute one recertification campaign. With the consolidation and automation from the RSA Identity Governance & Lifecycle deployment we’ve been able to slash this time by 50%.”

Ritesh Mohan
Identity and Access Management, Dell

For more information: bit.ly/2CqZYW7
Cybersecurity Operations | ADVANCED PROTECTION

Managed Detection & Response (MDR)

Accelerate security with an all-encompassing, flexible solution.

The MDR solution provides businesses with advanced protection, detection and response capabilities throughout your environment, on-premise and cloud, from endpoints to servers and network devices.

The holistic solution, which features several key Secureworks services, includes threat intelligence, security monitoring capabilities, server monitoring, Intrusion Prevention System capabilities (IPS), Endpoint Detection and Response, Cloud Security Monitoring, and Emergency Incident management.

Outlined over the next two pages are four of the Secureworks Managed Services solutions.
Managed Detection & Response (MDR) continued

1. Advanced Threat Services

Secureworks expert security Counter Threat Unit™ (see section 5) use advanced tools and techniques to thoroughly dissect malware to determine its functionality, purpose, composition and source.

The intelligence from our CTU informs our Managed Security, Incident Response (IR), and Threat Intelligence services to help you close the gap between your defences and the latest cyber threats. Findings from an IR engagement, calls into our Security Operations Centres (SOCs), and results from endpoint scans are quickly applied to security device signatures and policies, attacker black lists, event correlation, threat analysis and response procedures.

2. Security Management & Orchestration

Our Intrusion Prevention System technology removes the burden of device or signature management while helping clients eliminate malicious inbound and outbound traffic.

Provided on a 24x7 basis, this fully managed solution helps enable clients to comply with regulations to protect against the latest threats and vulnerabilities, and demonstrate the effectiveness of security controls through comprehensive reporting. As a fully managed service, Secureworks augments your existing security team, eliminating the need to increase in-house headcount.

The cost of just maintaining our previous intrusion detection and prevention system was more expensive than the overall cost of Secureworks. We saved $60,000 in the first year, and we avoided having to hire a full-time security expert.”

Kevin Pilgrim
Executive Vice President and Chief Information Officer,
Lone Star National Bank

For more information: bit.ly/2EEIbU9
3. Vulnerability Management

Secureworks Vulnerability Management performs internal and external scan audits across network devices, servers, web applications, databases, and other assets in on-premise and cloud environments.

Perform scan audits across internal and external environments, both on and off-premises. Reduce recovery time and enrich your approach by leveraging deep security expertise from resources in our Security Centre of Excellence (SCoE) serve as extension of your security team.

4. Security Monitoring

We provide you with real-time monitoring, correlation and expert analysis of activity occurring in your environment. Powered by the CTU, we help unify and simplify your security operations with a powerful combination of artificial and human intelligence.

Built upon billions of event data points, daily monitoring across 4,400 clients worldwide, and global threat visibility driven by the CTU, this solution allows you to see more, know more and respond faster. We staff our SOCs with an elite team of researchers, analysts, engineers and consultants, who provide our clients with continuous investigation of real threats.

350,000
remediated up to 350,000 vulnerabilities monthly

400%
improvement in remediation of urgent vulnerabilities

For more information: bit.ly/2GClIZt
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
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

Fraud Prevention

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.

Incident Response

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
Detect & Respond

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
Dectects 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.
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. 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.

3. **Rapid insight**
   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.

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. 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.

5. **Efficient Response**
   The most effective way to turn insights into action is to orchestrate and automate response.
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

(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

**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
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.

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.

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.

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.

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.

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

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

Identify
- Business Context
- Risk Assessment
- Business Impact

Protect
- Recovery planning
- Incident Response

Recover
- Crisis Management
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.
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

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