DELL EMC CYBER RECOVERY

DATA PROTECTION AND RECOVERY WHEN YOU NEED IT MOST.

GET STARTED
DELL EMC CYBER RECOVERY
DATA PROTECTION AND RECOVERY WHEN YOU NEED IT MOST.

INDUSTRY SNAPSHOT
COMMON VULNERABILITIES
THE SOLUTION
ADDITIONAL RESOURCES

CLICK A BOX TO NAVIGATE
INDUSTRY SNAPSHOT

39% of detected malware is ransomware*

92% of organizations can’t detect cyberattacks quickly†

67% of organizations had incidents with a negative impact in past 12 months‡

Sources
* 2018 Verizon Data Breach
† Gartner Research, Shift in Cybersecurity Investment to Detection, January 2016
‡ RSA Cybersecurity Poverty Index
TRUE COST OF RANSOMWARE

Lost Revenue: $2,500,000
Incident Response: $75,000
Legal Advice: $70,000
Lost Productivity: $250,000
Forensics: $75,000
Recovery & Re-Imaging: $60,000
Data Validation: $25,000
Brand Damage: $500,000
Litigation: $200,000

Total Cost of Attack:
$3,785,000

Ransom: $30,000
RELIABLE DATA PROTECTION, DELIVERED WHERE YOU NEED IT MOST.

Protecting your organization from the inevitability of cyberattacks – especially ransomware – requires a multi-layered approach. You’ve got to prevent attacks (of course), but you’ve also got to be prepared for the worst.

Dell EMC Cyber Recovery protects your organization’s most critical data within an isolated secure vault. Through an innovative REST API-based automation approach, your data is removed from the attack surface. Additionally, Cyber Recovery brings flexibility in automating robust analytics by integrating custom or well-known industry tools into your workflow. This facilitates a robust and proactive workflow to help increase cyber resilience throughout your organization.
COMMON VULNERABILITIES
COMMON VULNERABILITIES
COMMON VULNERABILITIES

RISK PROFILE SUMMARY

TECHNICAL
- All data is currently susceptible to a cyberattack
- Primary storage replication can replicate corruption
- Backup catalog not replicated
- Recovery of backup catalog from tape is slow and failure-prone
- Backup copies not isolated from network

PEOPLE & PROCESS
- IT Engineering and Ops have access to most if not all Backup Assets
- Security teams not assigned to assets. Bad actors inside the firewall can create havoc.
- Franchise critical and non-critical data are not segregated
- Backup images can be expired without authorization

These risks are consistent with traditional disaster recovery models. This is a different challenge and requires a different architecture.
## DISASTER RECOVERY VS. CYBER RECOVERY

Traditional disaster recovery solutions are ill-equipped to recover from a cyberattack.

<table>
<thead>
<tr>
<th></th>
<th>DR</th>
<th>CR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recovery Time</strong></td>
<td>Close to Instant</td>
<td>Reliable &amp; Fast</td>
</tr>
<tr>
<td><strong>Recovery Point</strong></td>
<td>Ideally Continuous</td>
<td>1 Day Average</td>
</tr>
<tr>
<td><strong>Nature of Disaster</strong></td>
<td>Flood, Power Outage, Weather</td>
<td>Cyberattack, Targeted</td>
</tr>
<tr>
<td><strong>Impact of Disaster</strong></td>
<td>Regional; typically contained</td>
<td>Global; spreads quickly</td>
</tr>
<tr>
<td><strong>Topology</strong></td>
<td>Connected, multiple targets</td>
<td>Isolated, in addition to DR</td>
</tr>
<tr>
<td><strong>Data Volume</strong></td>
<td>Comprehensive, All Data</td>
<td>Selective, Includes Foundation SVCs</td>
</tr>
<tr>
<td><strong>Recovery</strong></td>
<td>Standard DR (e.g., failback)</td>
<td>Iterative, selective recovery; part of IR</td>
</tr>
</tbody>
</table>
THE SOLUTION

CYBER RECOVERY SOFTWARE

• End-to-end workflow automation
• Runs only in CR Vault
• Creates isolated gold copies
• Robust REST API framework enables analytics with AI/ML for malware (incl. ransomware)
• Modern UI / UX experience
• Easy to deploy and maintain

PRODUCTION

1. Synchronize Air Gap

CR VAULT

2. Immutable Copies
3. Sandbox Copies
**PROACTIVE ANALYTICS IN THE CR VAULT**

**Why Analytics in the Vault?**
- Increase effectiveness of Prevent/Detect cybersecurity when performed in protected environment.
- Diagnosis of attack vectors can take place within an isolated workbench.
- App restart activities can detect attacks that only occur when application is initially brought up.

**Categories of Data**
- Transactional Data – dynamic/large (log variances, sentinel records, etc.)
- Intellectual Property – static/large (checksums, file entropy)
- Executables / Config. Files – static/small (checksums, malware scans)
THE SOLUTION

ADDITIONAL CYBER RECOVERY SERVICES

DEPLOYMENT
New deployment services from Dell EMC Services accelerate the value of Data Domain based Cyber Recovery Solution. These implementation services are available in two sizes to fit your needs based on number of MTrees and data subsets.

WORKSHOP
Dell EMC Consulting leads a facilitated Business Resiliency workshop with key stakeholders to share Dell EMC best practices for resiliency, including IT Continuity and data protection, with an emphasis on cyber recovery.

ADVISORY SERVICES
Dell EMC Consulting Advisory services include the workshop and provide you with a deeper understanding of the solution, specific data to contain in the vault, and advises on roadmap and custom solution design. These offers scale based on your specific needs.

PREV  ADDITIONAL RESOURCES →
ADDITIONAL RESOURCES

Case Study: Founder's Federal Credit Union
WATCH VIDEO

Business Cyber Risk Bulletin
DOWNLOAD PDF

Learn more about our Cyber Recovery Solution
WATCH VIDEO

Cyber Recovery Solution Overview
DOWNLOAD PDF
ADDITIONAL RESOURCES

Analyst Report: Cyber Recovery

DOWNLOAD PDF

ESG Video: Cyber Recovery

WATCH VIDEO

PREV  ○  ○