Enterprise Strategy Group | **Getting to the bigger truth.™**

White Paper

Cyber Resiliency with the Dell EMC Cyber Recovery Solution

Dell EMC Cyber Recovery and Its Data Isolation Architecture Provide Technologies and Services to Protect Data Assets Effectively

By Christophe Bertrand, ESG Senior Analyst
Doug Cahill, ESG Group Director and Senior Analyst
and Monya Keane, ESG Senior Research Analyst

November 2018

This ESG White Paper was commissioned by Dell EMC
and is distributed under license from ESG.

Contents

Executive Summary

Cybercrime, including ransomware, is rampant and is creating a significant data protection and recovery challenge for many organizations. Traditional backup and recovery approaches have proven insufficient to fend off the evolving threats—they cannot do enough to minimize production network exposures and avoid the resulting negative business impacts. Dell EMC's Cyber Recovery Solution and its Data Isolation Architecture provide services and technology to effectively protect organizations' data assets.

Introduction

Cybercrime, ransomware attacks, hacking—not a day passes without technology crimes making the news. They wreck corporate reputations and hurt customer and employee confidence. Ransomware in particular is widespread, and its frequency is actually accelerating. Additionally, there seems to be no limit to the creativity of the cybercriminals launching these attacks.

A combined 35% of organizations surveyed by ESG report experiencing ransomware attacks at least monthly. A combined 62% experienced at least one attempted attack at some point during the previous 12 months.[1] Considering those findings, it should come as no surprise that senior executives at many organizations are concerned about the technical and business risks that go hand in hand with ransomware attacks. A combined 81% of respondents surveyed by ESG said their companies' leadership teams are either concerned (47%) or highly concerned (34%) about ransomware.[2]

It's not an easy job for most organizations to address, either; 69% of the respondents agreed that the relationship between IT security and business risk can be difficult to coordinate.[3]

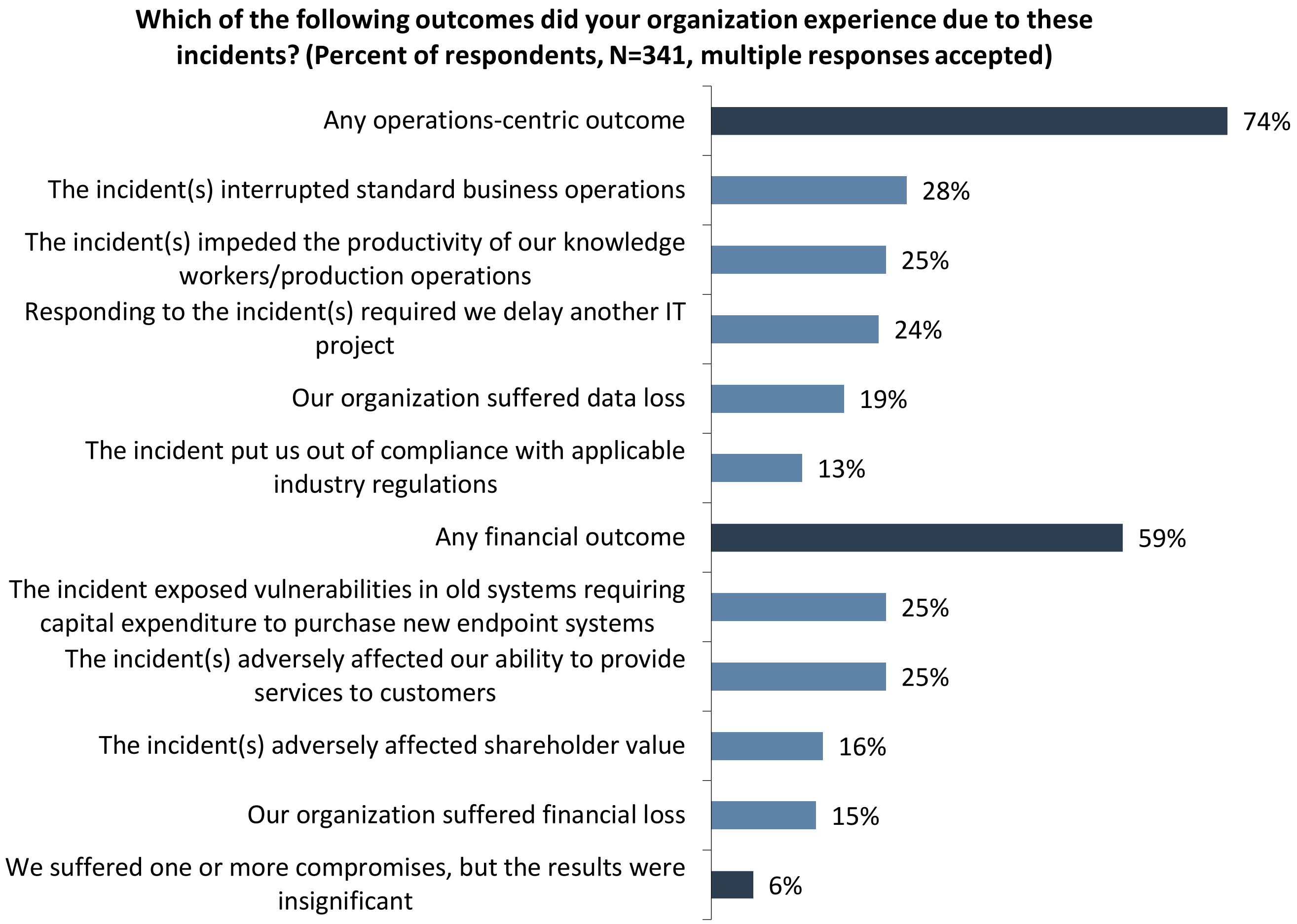
Still, they have been trying to take meaningful action. For 2018, cybersecurity topped the list of IT spending priorities among organizations surveyed by ESG.[4] It is also important to note that 39% of respondents surveyed say their organizations' board of directors is actively involved in establishing cybersecurity priorities and strategies. In addition, 54% of respondents say their organizations' chief information security officer (CISO) is actively involved in defining requirements for data recovery. [5] Although sentiments are split regarding whether cybersecurity is a business or technology issue, fending off ransomware and its consequences is clearly imperative.

One reason—more than just employees' endpoints are affected. Ransomware attack chains move beyond the initial desktop/laptop infection vector, extending laterally across the IT infrastructure. In the process, they target endpoint-resident data, structured data, and unstructured production data—exacerbating the risks and worsening the adverse business impacts. Some ransomware deletes the production data; it has been observed in attacks on MongoDB databases. And recent new strains and variants, such as the new strain of SamSam ransomware, showcase the high level of sophistication now present in ransomware and offer evidence of how committed cybercriminals are to this type of attack.

Separate data-protection-specific research conducted by ESG for Dell EMC revealed that 74% of companies that experienced some type of cybersecurity incident last year subsequently dealt with one or more operational impacts. That means they most likely lost some money. Attacks affect business operations in bad ways. They impact knowledge workers' productivity, they cause IT project delays, they result in data losses, and they impact compliance (see Figure 1).

[1] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.
[2] ibid.
[3] ESG Custom Research Conducted for RSA Security, June 2018.
[4] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.
[5] Source: ESG Custom Research for Dell EMC, *Understanding Organizations' Isolated Recovery Requirements and Capabilities*, February 2018. All ESG research references and charts in this white paper have been taken from this custom research, unless otherwise noted.

Figure 1. Outcomes of Cybersecurity Incidents



Source: Enterprise Strategy Group

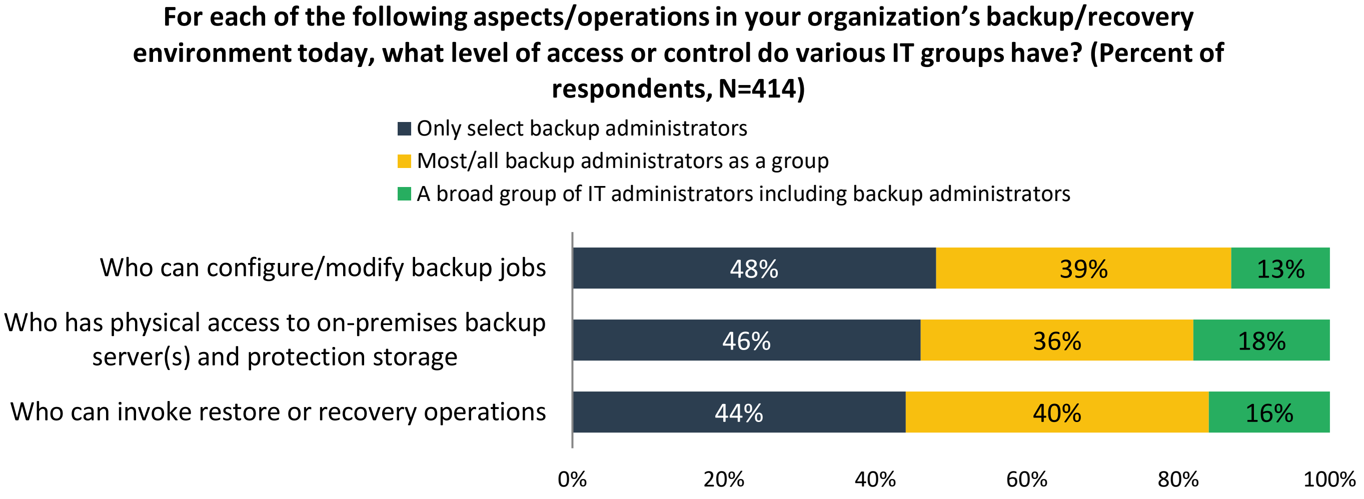
Incident response has thus become a serious strategic priority and an area of intense focus for IT and operations teams. They have work to do—36% of organizations surveyed by ESG still don't have formal incident response plans in place, although 12% of them do use informal guidelines, 15% are developing their formal plan, and 8% are interested in creating one. Making the effort more complicated is a serious shortage of qualified IT staff—51% of organizations surveyed by ESG say they have problematic skill shortages related to cybersecurity.[6]

Recovering from an attack that results in data loss will require leveraging pristine preserved copies. Notably, 49% of surveyed IT managers reported their organization uses some form of "traditional" backup/recovery as their primary means of ransomware remediation. However, they think that on average, only 60% of their business-critical apps can be restored to service from isolated protection storage. Even worse, three-fourths of respondents (76%) are somewhat concerned (48%) or very concerned (28%) that their backups could also become corrupted as part of a ransomware attack.

Companies are also concerned about insider attacks. Among organizations surveyed by ESG, it appears many general IT and backup administrators have been given the ability to access and modify backup copies (see Figure 2).

[6] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

Figure 2. Level of Access/Control Various IT Groups Have over the Backup/Recovery Environment



Source: Enterprise Strategy Group

Air-gapped Recovery Is Gaining Momentum

Clearly, when it comes to ransomware, traditional backup and recovery is not enough. Additional capabilities are needed. Using tape on-premises alone, for example, isn't really an adequate solution. Tape comes with shortcomings such as elongated RPOs, risk of media loss, and a lack of analytics. Tapes also are not indexed and don't have search capabilities.

So, to complement their traditional BC/DR processes in this fight, organizations are adopting a strategy centering on a **Data Isolation** approach. This is a modern approach that involves (1) keeping a copy of critical data off of the network ("air-gapping" it to leave no direct/constant network connections), and (2) creating multiple recovery points to ensure an uncompromised gold copy is available for recovery. Nine out of ten surveyed organizations regard offline recovery as a preventative measure with merit. Unfortunately, less than half of them have deployed such a solution.

Recovery from destructive ransomware or other type of cyberattack presents specific challenges. They aren't like meteorological disasters or power outages because they can take place simultaneously in multiple national/international locations, and that adds complexity to the recovery process. Isolating and segregating the infrastructure and its data is therefore going to be vital to shortening incident response time and optimizing effectiveness.

Technology Requirements

As mentioned, copies of business-critical data should be air-gapped to avoid tampering, corruption, or outright destruction. To ensure maximum security, the IT organization must ensure there is no direct/indirect constant connection between the server and storage and any private, public, or Internet network.

A Data Isolation Architecture relies on a "hardened" repository for critical data, which ensures the data will always be available to ensure business continuity. That repository is designed to operate without constant/active network links. To create fresh copies, only intermittent connections to the rest of the infrastructure—to synchronize data volumes, get the latest file versions, etc.—are allowed. Also, even when connected, the isolated network is not "routable," and no management controls are exposed. It is not vulnerable. In this way, it is assured that one or more copies of mission-critical data will not be infected, corrupted, or destroyed if an attack occurs. The copies also can be locked with WORM (write once, read many) solutions to further guarantee they can't be tampered with.

Should a recovery become necessary, IT can quickly connect the hardened repository to the network, recover the good data, and enable business to resume.

Given the frequency of ransomware attacks, a well-designed Data Isolation Architecture maintains multiple recovery points (point-in-time copies) to ensure recoverability, and it runs integrity checks on incoming data. If it detects an issue, it uses alerting mechanisms to protect the system and ensure data remains uncorrupted.

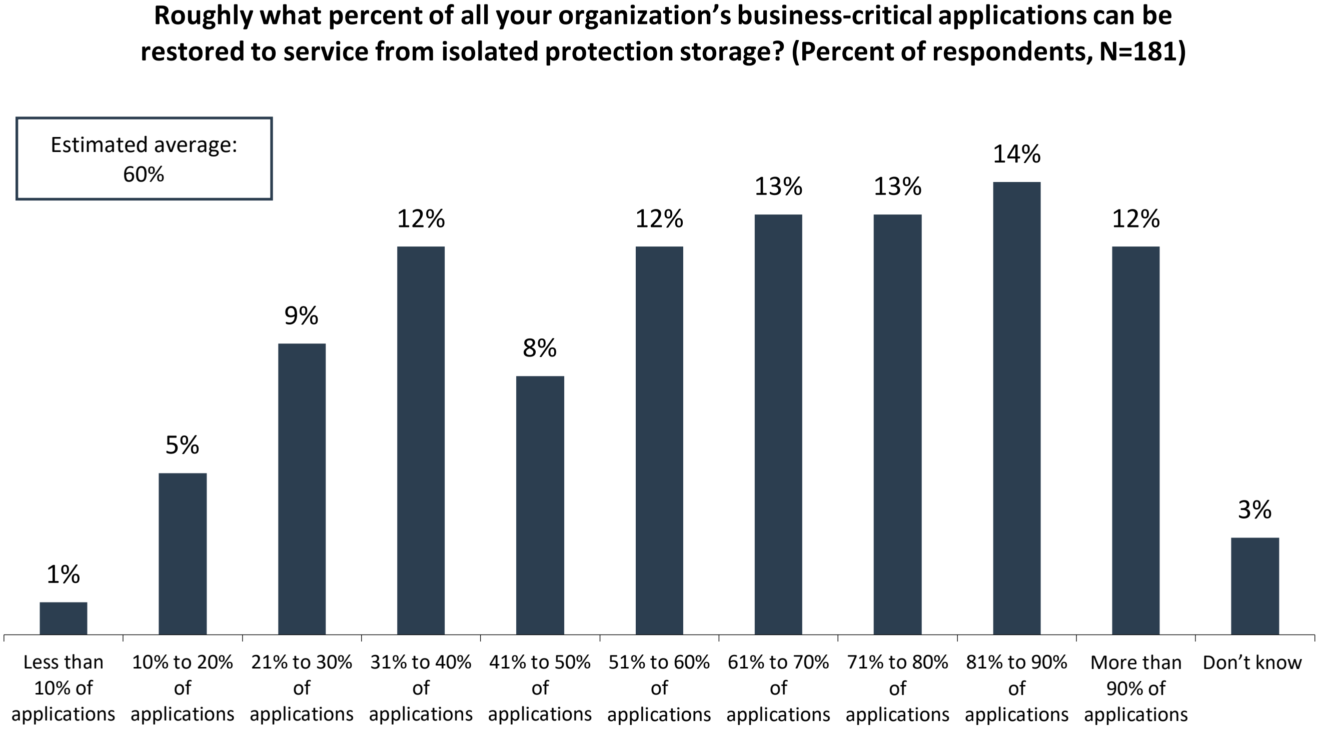
Automation and policy management capabilities are additional potential requirements to consider, as protection and recovery workflows can be complex and susceptible to error when dependent on manual intervention.

Lastly, having access to a secure "sandbox" test environment is a plus (see Architecture section). It can assist not only in performing recoveries, but also in running analytics. And that capability can help with the diagnosis and detection of threats in a protected environment.

The Market

ESG has researched current market trends and end-user affinity levels for offline protection topologies. The approach is not only gaining in popularity; for some organizations, it appears to have become a business-critical strategy to protect key applications and assets. As mentioned earlier in this paper, organizations surveyed by ESG that use offline protection storage believe that on average, they can recover 60% of their business-critical applications in that way (see Figure 3). While there is still plenty of room for growth in adoption, the approach is clearly maturing.

Figure 3. Percentage of Business-critical Applications that Can Be Restored to Service from Offline Protection Storage



Source: Enterprise Strategy Group

Cyber Recovery with the Dell EMC Cyber Recovery Vault

It should be no surprise that Dell EMC, a market-leading IT vendor and strong proponent of IT Transformation, has been setting the tone in the marketplace with a powerful, feature-rich offline recovery solution.

From Dell EMC's perspective, and ESG wholeheartedly agrees, ***recovery is everything***. Organizations will significantly mitigate consequences of attacks from inside or outside their corporate network if they isolate their recovery environment from their production network.

Offering a way to ensure business-critical data can withstand cyberattacks and be recoverable fast is central to the design of the Dell EMC Cyber Recovery Solution and its centerpiece, the Cyber Recovery Vault (CR Vault). Dell EMC developed an architecture that not only isolates critical data—the gold copies—but also includes a robust process/methodology to support Dell EMC customers in the design and implementation of their overall recovery strategies.

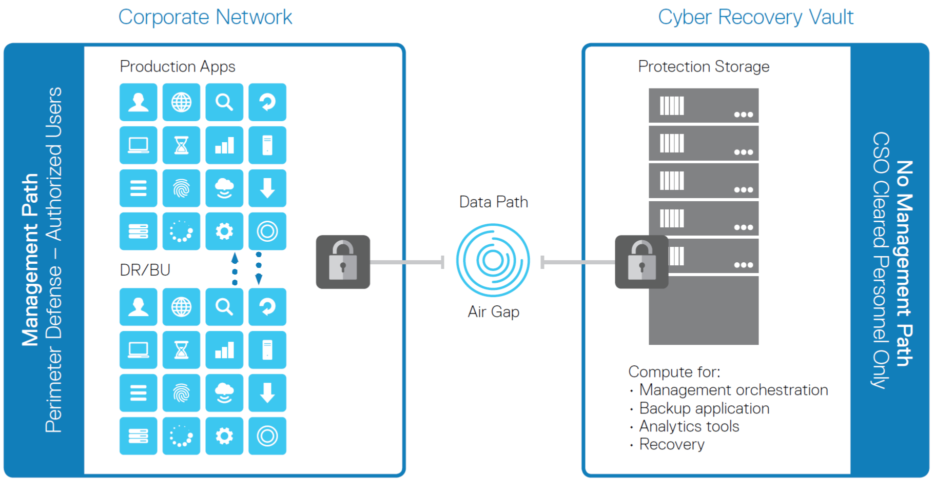
Architecture and Key Components

The Dell EMC Cyber Recovery solution and the CR Vault create a protected section of a data center:

- The vault hosts organizations' critical data on Dell EMC technology.
- The CR Vault is offline from the network (air-gapped, and removed from the surface of attack). It is only accessible to users who have proper clearance.
- The solution includes management tools that "operationalize" a data recovery, starting with the creation and automation of recovery restore points.
- Restore points can be leveraged not just for recovery, but also for integrity checking and security-related analytics through the creation of sandbox copies. Analyses would take place on data-at-rest and cause no impact to the production environment. The sandbox copies could be the perfect way to perform offline malware/ransomware detection testing, such as looking for indicators of compromise or integrity attacks.
- Recovery is everything, as outlined above, and this solution allows organizations to bring critical systems and data assets back online fast and securely.
- Organizations can leverage the expertise of the Dell EMC services team, who offer proven methodologies for data protection, damage assessment, forensics, recovery, and remediation.

Figure 4 depicts the CR Vault architecture. Central to its design are the data path air-gap and resulting segregation and isolation of the protection storage.

Figure 4. The Dell EMC Cyber Recovery Vault



Source: Dell EMC

Compute capabilities and resources are still needed inside the CR Vault to support system-management tasks, infrastructure services, the backup application, on-demand security analytics, and recovery testing. The required levels of compute capabilities in the CR Vault will vary based on the frequency and type of operations that end-users want to perform.

CR Vault sizes also vary according to the type and amount of data to be analyzed, the particular analytics tools being used, and the frequency of validation and testing. Dell EMC offers a number of options, starting with simple deployments such as a small ESX cluster or one hyper-converged appliance.

Beyond isolation/air-gapping, another major capability of this solution is its automation of workflows. The Dell EMC Cyber Recovery solution automates the workflow that is needed to create the restore points required for data recovery or analytics. This capability would not only simplify operations, but also minimize the risk of manual errors. It would also help the IT organization's efforts to adhere to already-established backup frequency service levels and recovery point objectives.

A Focus on Analytics

Cybersecurity processes and tools should always be used on endpoint devices, networks, and servers/hosts. It is notable that the Dell EMC Cyber Recovery solution enables some interesting additional ways to help organizations perform cybersecurity analyses and mitigation tasks in a protected environment. In this context, one benefit of isolation is to allow specialist security teams to run malware scans or look for indicators of compromise while avoiding masking routines, diagnose attack vectors, and identify risks associated with future application restarts. A number of tools are available:

- **System-level validation tools** to assist with restore point creation, system health monitoring, and recovery management.
- **Anomaly detection tools** to uncover unusual patterns (such as the unusually high change rates that are typical in certain ransomware attacks), and then trigger alarms that prompt further analysis. A number of user-defined options are available to determine thresholds, zoom in on new files in sensitive execution paths, and perform related entropy checks.
- **Malware detection tools** to identify the actual malware/ransomware. The solution employs several detection technologies to provide a comprehensive, adaptive solution. The technologies include signature-based tools, behavioral analysis tools, artificial intelligence-based tools, and application-level analysis tools leveraging Dell and third-party analytics engines for offline detection.

The Bigger Truth

Cyber attacks are a serious concern of business leaders. They represent a risk that just can't be ignored because the consequences of data and systems unavailability are so costly. But protecting business-critical data against cybercrime is not just a business imperative, it is an exercise fraught with complexity.

On the technical side, the limitations of traditional backup and recovery approaches created a need for another line of defense, and it is a defense that is now being widely adopted as a component of a complete approach to cyber recovery—an air-gapped topology with advanced protection, recovery, and proactive cyber-analysis capabilities.

Recovery is everything. And Dell EMC has done a good job of supporting its customers with this set of Cyber Recovery solutions and services—these are tools that will protect the "digital heartbeat" of an organization and significantly augment its disaster recovery and cyber-crime prevention capabilities.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.

www.esg-global.com contact@esg-global.com P. 508.482.0188