RECOVERING FROM A DESTRUCTIVE CYBER-ATTACK

Leveraging Dell EMC Cyber Recovery to Recover the Lifeline of Your Business

ABSTRACT

Cyber-attacks have become a common occurrence – and they are growing more sophisticated and devastating every day. In 2019, cyber-attacks on businesses cost as much as $600 billion a year globally . Ransomware attacks like WannaCry and Petya/NotPetya have cost organizations tens of millions of dollars in lost revenue per day. They also inflict damage to reputation and negatively impact stock prices. The cyber threat is expected to increase as the world economy continues to digitize operations, supply chains, business transactions, and employee and customer services.

Most organizations have strong detection capabilities in place. But could your organization recover if an attacker gets through the perimeter and encrypts or wipes your data? Organizations need to consider recovery as a vital part of their overall cyber-security and risk management strategy. This white paper highlights how Dell EMC Cyber Recovery, leveraging Dell technologies and services, can augment your overall cyber-security posture and provide a way to recover from a destructive cyber-attack.

March 2020

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Cyber-attacks like WannaCry and Petya/NotPetya have had devastating consequences on organizations worldwide. The impact of the recent NotPetya attack on a global retail company alone was estimated to be in the range of $15 million per day in forgone revenue. It took the company almost 5 days to recover. When also factoring in brand damage, impact on stock price, and the cost to recover, it is clear that the true cost of ransomware can be significant.

The attack also highlighted other recurring themes and patterns:

- The velocity with which the malware spreads throughout an environment can be extremely rapid. In this case, NotPetya spread in seconds after the initial infection.
- The impact on a highly connected business can be significant. Hundreds of critical servers, desktops, and phones were rendered useless. Over 10,000 employees were impacted.
- The supply chain impact can be substantial. The production of more than 15 factories was brought to a halt. This included real-time inventory management systems, where the downtime of these systems directly impacted the overall supply chain, impacting final assembly of goods.
- The malware exploited known vulnerabilities in operating systems and found their way into third party software consumed by the organization. The malware was inserted into a patch of this software.
- Rather than pay the ransom, the organization decided to focus on recovery. Paying ransom is not recommended and would have not been effective in this case. Hackers promised a decryption key upon ransom payment, but forensic analysis of the malware determined that a decryption key would not have allowed the data to be recovered.
- Good detection and prevention strategies were in place, but did not stop the event from occurring. A good recovery strategy was a critical element in getting this company back on track. Recovery from tape was ruled out, because it would have taken over 4 weeks.
- There was wide-spread agreement that a better cyber recovery strategy was needed so that the organization could more quickly and effectively respond in the future.

Organizations are not worried only about ransomware, even though it is the fastest growing cybercrime activity. Most Chief Information Security Officers (CISOs) worry about all types of attacks including slow-moving and sophisticated varieties that target industrial systems and other areas that can put people at risk of harm. In the case of a prominent media and entertainment company, an organized group is believed to have attacked data centers in a sophisticated manner. The hackers strategically destroyed server, storage, and backup assets. It was the first documented instance of destroying backup infrastructure.

Destroying backup infrastructure is an emerging trend, because hackers think that neutering the backup system increases the likelihood of payment. The trend of deleting backups was recently seen in the attack on a municipal rail system in November of 2016 and the April 2017 destruction of backups at a regional medical center in upstate New York. Any system that is connected to the network is a potential target, including the backup system.

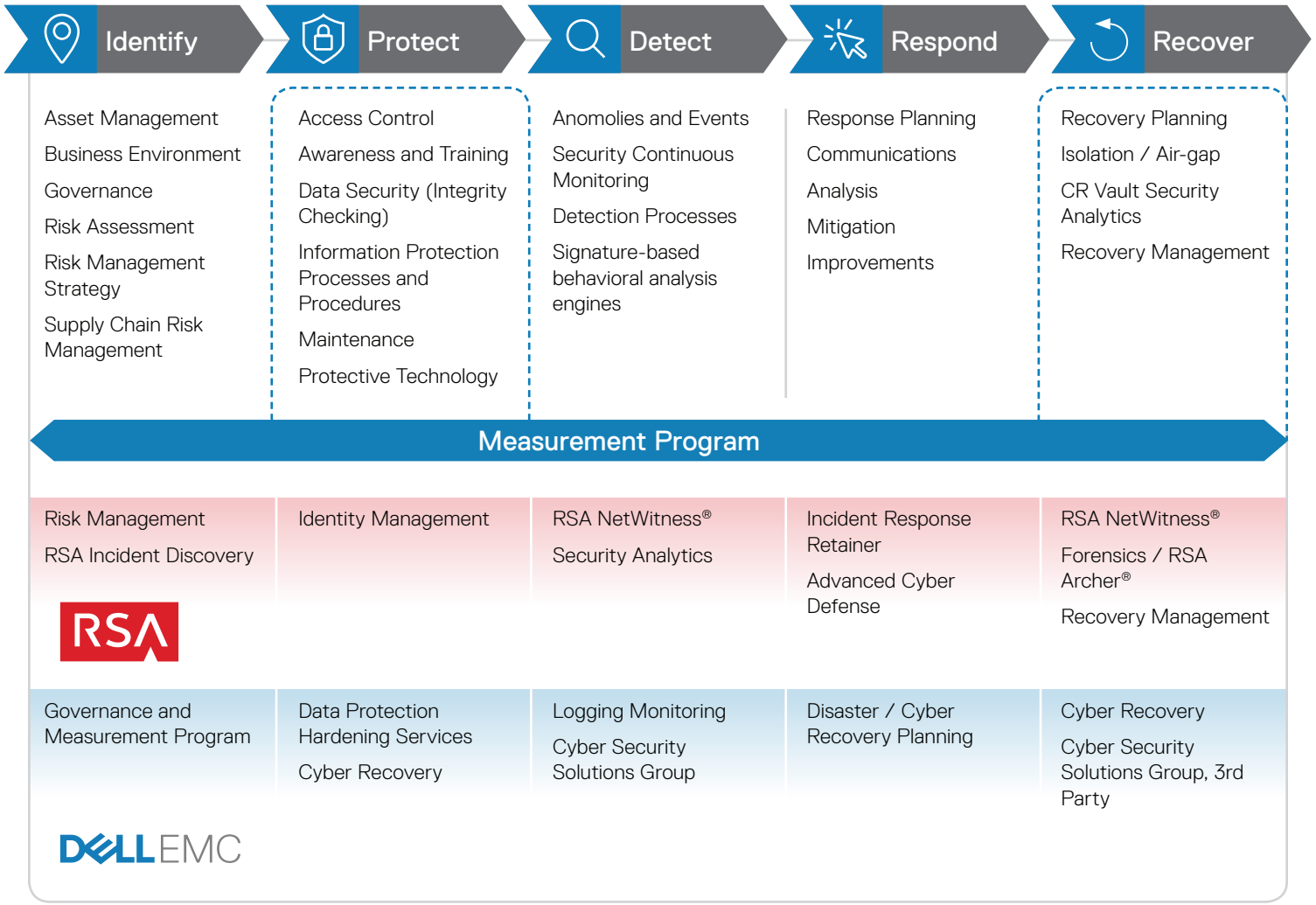
Because cyber-attacks are becoming more sophisticated and devastating, organizations are considering new recovery strategies that represent the “last line of defense” for the lifeline of the organization. Many are considering isolated environments that host business critical data that is sequestered from the production network. In fact, recent regulatory guidance and government warnings (including FBI) emphasize that backup and recovery are key components of a good cyber security strategy, preferably with

a backup or recovery infrastructure that is segregated from other systems. While tape backups can provide this level of isolation, recovery takes too long and involves too much risk when the daily revenue or mission critical applications are at stake.

Dell EMC Cyber Recovery provides a solution that combines the benefits of isolation and business continuity. It minimizes the impact of a cyber-attack and provides a faster and higher likelihood of success in the recovery of mission critical systems. This technology provides innovative automation and workflow tools to ensure gold copies of critical data are available so business processes can be resumed in the event of a destructive cyber-attack.

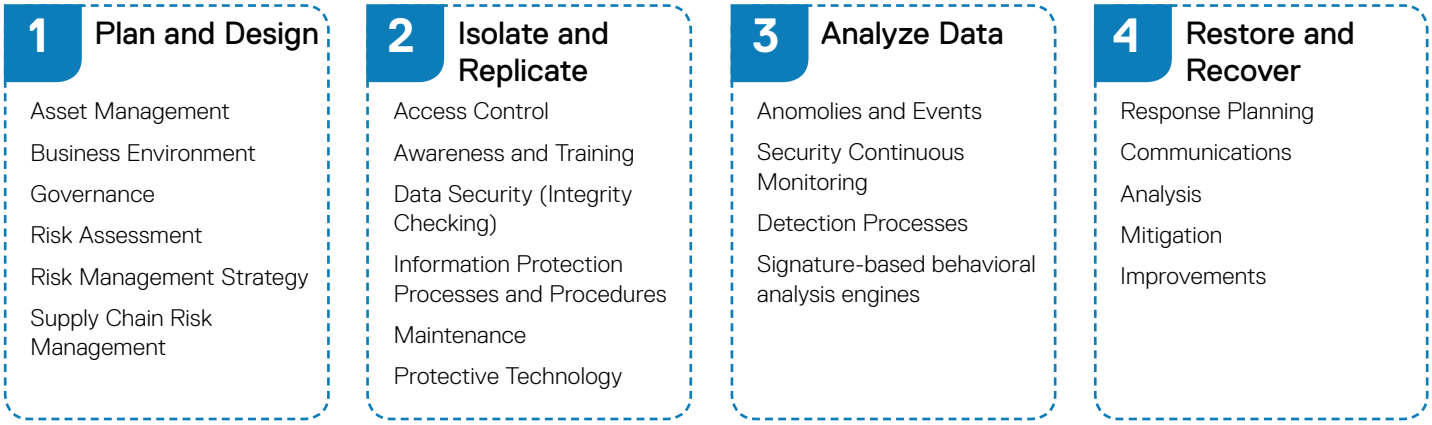
DELL EMC CYBER RECOVERY OVERVIEW

A robust and comprehensive cyber security strategy should leverage frameworks like the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), which can help outline an end-to-end cyber-attack defense continuum. Dell Technologies has strong capabilities in each category. It leverages technology and services from RSA, SecureWorks, VMware, Dell EMC Information Systems Group, Dell EMC Cyber Solutions Group, and Dell EMC Services.



Dell EMC Cyber Recovery focuses on the protection and recovery pillars of the cyber security continuum and leverages a combination of professional services and technology that provide the following four key elements:

1. **Planning and Design** – Assess mission critical systems and applications, current infrastructure, cyber-attack recovery time and recovery objectives in order to tailor a solution deployment. Dell EMC Advisory Services can help organizations determine their business critical systems and create dependency mappings with associated foundation services, metadata, and other components needed to bring them back online. Today, our consulting services experts work with organizations to determine their recovery objectives and design solutions with matching technologies to economically meet organizational requirements.
2. **Isolation and Replication** – Based on the outcome of the Planning and Design phase, a custom implementation of Dell EMC replication technologies will be completed. These technologies synchronize data between the production environment and the air-gapped Cyber Recovery Vault (CR Vault). Within the CR Vault, the created immutable restore points can be leveraged for recovery and analytics.
3. **Analytics** – CR Vault offers distinct advantages for analytics in an offline and controlled environment but it is also not intended to be a substitute for good end-point and cyber security tools. Organizations have the ability to leverage a variety of existing, Dell Technologies, and third-party tools for analytics in the CR Vault.
4. **Restore and Recovery** – Recovery procedures mostly follow standard processes, but special considerations apply across a variety of different scenarios. The steps usually follow invoking a cyber incident response plan, performing forensics and damage assessment, preparing the recovery, cleaning out the malware or rebuilding systems from gold-copy images of application and OS binaries, and then recovering the data back into the production environment.



Dell EMC Cyber Recovery provides an effective strategy against destructive cyber-attacks, but it is not designed to be equally effective across all of them. The table below highlights some common attacks, the likelihood of their occurrence, and the effectiveness of Dell EMC Cyber Recovery.

Attack Vector	Examples	Probability	IR Effectiveness	Notes
Persistence / Dormant Malware	Ransomware: WannaCry, Petya/NotPetya	HIGH	HIGH	• Consider leveraging a clean room to route binaries and OS images to the CR Vault prior to distribution.
Data Wiping / Data Destruction	Shamoon Worm Variants, Petya/NotPetya	HIGH	HIGH	• Spread of wiper software is contained within production environment. • Data in CR Vault is stored in raw backup format.
Data Locking	Ransomware: WannaCry, CryptoLocker	HIGH	HIGH	• Spread of encrypting malware is contained within the production environment. • Restore points are available in CR Vault.
Insider Attack	Known Attacks: Media, Government; Sensitive Data Exposed	MODERATE / HIGH	HIGH	• CR Vault stores restore points that are not accessible from the production network. • CR Vault is accessible only to CSO assigned admins.
Backups Compromised	Known Attacks: Media, Healthcare; Ransomware / Sensitive Data Exposed	MODERATE / INCREASING	HIGH	• CR Vault stores restore points that are not accessible from the production network. • CR Vault is accessible only to CSO assigned admins.
Air Gap Bypass	Stuxnet	LOW	MODERATE	• Secure / immutable copies cannot be deleted. • Risk of physical destruction remains.
Data Theft	Credit Card Skimmers, Data Breaches: Stolen Identities and Personally Identifiable Information	HIGH	LOW	• Intellectual Property and sensitive data stored only in CR Vault reduces data theft risk. • Original data that is maintained in production is not protected from theft.

Often, the above mentioned attack vectors occur in combination. In the following sections, some of the more prominent attacks are described across three use cases.

USE CASE 1:

LARGE MEDIA AND ENTERTAINMENT COMPANY

Attack Vector: A large Media and Entertainment Company was attacked and lost data throughout their environment. This a good example of a slow-moving, multi-stage attack conducted for a variety of motives. Sensitive data was exposed and while the attackers demanded ransom, they did not provide an effective means to collect. The attackers also pursued an ideological agenda. It is generally believed that the hackers were inside the victim's production network for as long as 6 to 18 months leveraging dormant malware before the attack was triggered. The malware exploited unpatched SMB (CIFS) vulnerabilities and persisted by attaching the malware to a boot time loaded binary. Aspects of attack are believed to have been facilitated by insiders, and logon credentials were compromised. The attackers logged onto the backup infrastructure and deleted backup images and destroyed associated backup storage. The attackers also destroyed primary storage targets with a high degree of sophistication and preparation. Malware wiped data from more than 3,000 of close to 7,000 PCs and in excess of 800 of more than 1,500 servers.

How Dell EMC Cyber Recovery Can Help: Dell EMC Cyber Recovery would have provided a recovery environment that the hackers would find difficult to compromise or even discover due to its segregation from the production network. This dramatically reduces the risk of compromising or destroying backups. By replicating clean room copies of vendor-provided OS images and binaries into the CR Vault before distributing them, IR can provide a path to store clean OS images and binaries before malware persistence occurs. To recover from data that is wiped from production systems, the CR Vault stores prior copies of data that can be used in the recovery process. Since only CSO-appointed administrators have access to recovery assets in the CR Vault, the chance of an insider attack is dramatically reduced.

USE CASE 2:

LOCAL HEALTH CARE PROVIDER

Attack Vector: More than 6,000 computer disk drives were encrypted and subject to data locking. The cyber criminals demanded $44,000 in ransom, payable in bitcoin. They breached an improperly configured and externally facing webserver and used a JBoss middleware exploit. They then leveraged a SamSam malware variant to compromise the JBoss Management Console. The attackers performed reconnaissance for weeks looking for important data and staking out critical infrastructure before unleashing the ransomware attack. The attackers also compromised the backup infrastructure by encrypting the backup catalog and metadata. The health care provider did not pay the ransom and was able to recover most of their critical systems in six weeks.

How Dell EMC Cyber Recovery Can Help: With Dell EMC Cyber Recovery, the Ransomware attack would have likely exploited the webserver and the encryption malware might have been copied into the CR Vault. But would have not been activated in its raw data format. Depending on tools used to perform analytics within the CR Vault, the malware variant could have been detected in the contained environment. While the encrypted backup catalog would have been replicated, tools are available to detect this encryption. The previous copy of the backup catalog and associated data could have been used to recover business critical systems. Removal of the recovery infrastructure from the production management network makes it unlikely that cyber-attackers can compromise the recovery infrastructure in the CR Vault. Without a network connection, an attacker cannot access and delete immutable copies located in the CR Vault.

USE CASE 3:

GLOBAL RETAIL AND MANUFACTURING CORPORATION

Attack Vector: The organization was one of multiple firms in several countries that was impacted by the Petya/NotPetya malware, a Ransomware / Data Destruction attack. It is believed that the company wasn't even the primary target of the attack. Both WannaCry and Petya/NotPetya exploited known vulnerabilities. The hackers persisted the malware as part of a patch into a bookkeeping software. Petya/NotPetya spread and locked systems within seconds of infection locking servers, desktops, and phones. The attack stopped more than 15 of the company's manufacturing plants and real-time inventory management systems. Initial estimates of sales loss was $15 million dollars a day. Additional costs included damaged reputation, negative stock price impact, and the cost of recovery.

Analysis of the NotPetya strain of malware determined that even if the ransom was paid, it may not have been possible to decrypt the data. In the attack, the NotPetya malware destroyed the company's backup server. The company had offline copies of backups on tape, but internal testing revealed that recovering the entire environment from tape would have taken over 4 weeks. To expedite the recovery, the company

restored the backup tapes onto a Dell EMC Data Domain Protection Storage System, rebuilt the backup catalog, and recovered their mission critical systems in approximately 5 days limiting their total financial loss for the quarter.

How Dell EMC Cyber Recovery Can Help: Dell EMC Cyber Recovery provides faster restore times when compared to tape. In this case, evidence suggests that the attackers did not target this company and therefore did not plan to destroy or compromise the backup infrastructure. Had this been the case, the recovery time would have been dramatically increased. In either scenario, recovery from the CR Vault would have been faster, because the CR Vault has immutable copies of data and the backup catalog. The addition of pre-rehearsed CR Recovery Runbooks would have further expedited the recovery.

CYBER RECOVERY IS NOT TRADITIONAL DISASTER RECOVERY (DR)

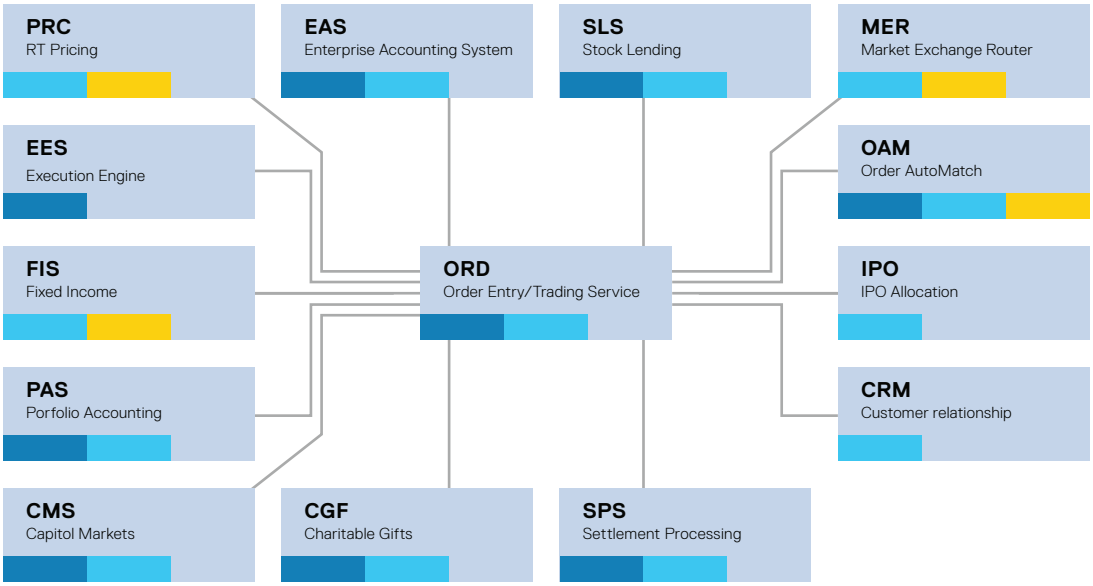
Organizations need to consider that their definition of disaster recovery may not help them to recover from a destructive or ransomware cyber-attack. The table below lists some key differences.

Category	Traditional DR	Cyber Recovery (CR)	Notes
Recovery Time	As Short As Possible	Reliable and Fast Recovery	· Reliable recovery is critical to address data corruption and malware.
Recovery Point	Ideally Continuous	One Day on Average	· Longer recovery points allow time for analytics, recovery drills, etc. · Business critical environments, such as mainframe systems, often require near continuous recovery points.
Nature of Disaster	Broad / Data Center / Regional	Selective / Individual Machines / Apps / Data Stores	· Cyber-attacks typically exploit specific weaknesses at some layer of the stack. · Traditional disasters range from complete machine outages to rare regional disasters.
Impact of Disaster	Data Center / Regional / Typically Contained	Global / Often Spreads	· Traditional Disasters tend to be locally contained. · Cyber-attacks can spread globally in a very short amount of time.
Geographic Diversity	Important for the Regional DR Scenario	Less Important	· Cyber-attacks are not region-specific, so regional diversity has limited effectiveness.
Logical Separation	Only Important During Testing	Very Important	· Segregation of IT resources that limits the spread of the destructive cyber-attack can save the business.
Data Volume	Comprehensive / All Data	Selective / 10-15% of Data on Average	· Implementing an Cyber Recovery Environment recommends a selective approach for maximum effectiveness in large environments. · In smaller environments or organizations where data inter-dependency is suspect, consider isolating a copy of all production data.
Recovery Process	Standard DR Processes	Augmented DR Processes with Dynamic Recovery / Added Security Analytics	· Forensics, damage assessment, recovery of pre-distribution unaffected binaries, and recovery of affected systems. · Organizations can leverage standard disaster recovery tools for application recovery. · Additional consideration needs to be paid for security analytics as part of the recovery process.

Recovery from a destructive cyber-attack can be very different from other types of disasters, such as power outages, fires, or floods. Since cyber-attacks are typically not limited to a specific location, their impact can often be felt globally, even with traditional disaster recovery solutions in place. For this reason, a logical segregation of infrastructure that limits the spread of malware and reduces the surface of attack is more effective than maintaining regionally-dispersed data centers. Recovery procedures can be more involved due to additional forensics and security analytics.

WHAT DATA TO PROTECT?

Since cyber-attacks are often targeted, it is more important to identify business critical systems than protect entire data centers. However, even if the typical volume of data protected by Dell EMC Cyber Recovery represents around 10-15% of the traditional disaster recovery envelope, it is critical to understand the dependencies of this business critical data across databases, applications, and foundation services. Dell EMC Advisory Services can help organizations understand the dependencies of their business critical applications. A sample dependency map for an organization's trading service is illustrated below .



Type	Dependent services
	ACH processing
	Swift
	Audit
	Fax processing
	FileNet
	Mobile and web trading interface
	Money laundering
	Multi-currency exchange calculator
	Telephone trading interface
	Application logging
	Authentication, authorization, and audit
	AV endpoint protection
	Bare metal provisioning
	Certificate services
	Cluster / pool balancing
	Consumption reporting
	Custom infrastructure "shim" services
	DB clustering services
	Domain name services
	Email management
	Event correlation
	HP LILO / IBM RSA
	IPv4 management
	IPv6 management
	Messaging services
	Middleware services
	Patch level monitoring
	Performance monitoring
	Power monitoring
	RSS/NNTP newsfeed services
	Trace and log collection services

Organizations typically have a very good idea of what constitutes the lifeline of their business. Some examples of data that is currently protected by Dell EMC Cyber Recovery include:

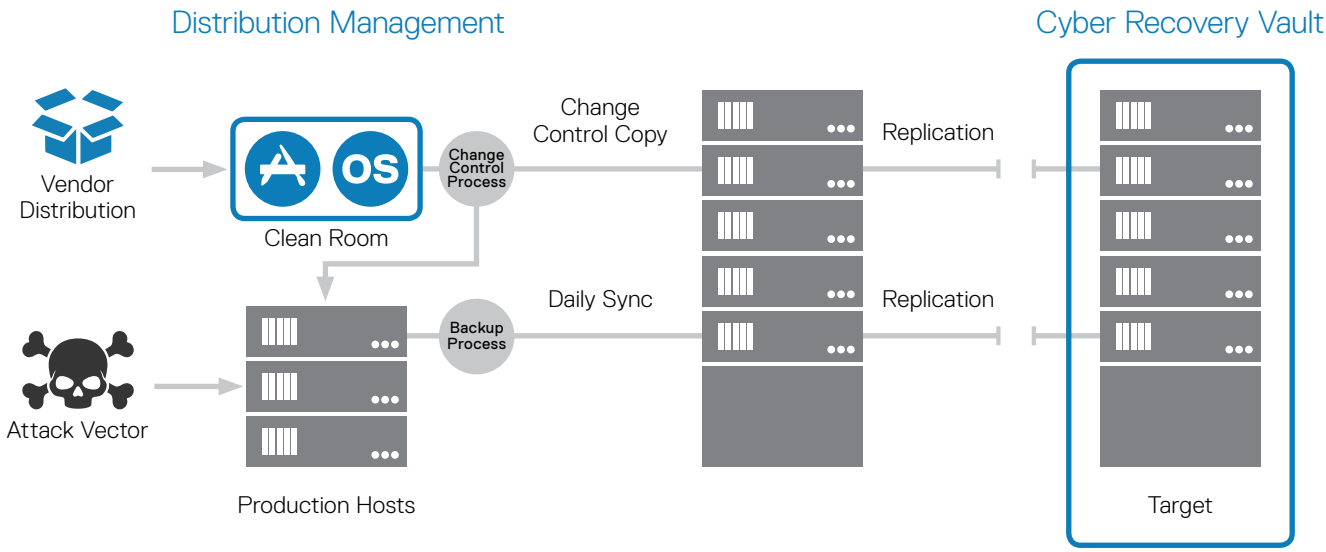
Mission- and Business-Critical Databases with Associated Applications – Often supporting transaction processing systems. An attack on these systems has a direct negative impact on top line revenue.

Mainframe Environments – Similar to the above, these systems are often tied to business processes. Logical corruption can have a devastating impact. As a result, organizations often look for more granular recovery times, because every transaction can represent significant revenue.

Intellectual Property and Sensitive Data – Retailers, manufacturers, and similar firms that rely on their intellectual property to maintain a competitive edge often store critical data in an isolated environment, thereby making it difficult for insiders and hackers to access and steal the data. This can also include code as part of the organization's software development lifecycle.

Foundation Services – Organizations sometimes overlook the importance of foundation services for their business continuance, such as active directory and domain name services. Customers are increasingly considering Dell EMC Cyber Recovery for these services as they often impact every aspect of an organization.

Clean Room OS Images / Binaries – Organizations should consider routing vendor OS / Binary distributions through a clean room prior to distribution. This allows them to copy this data into the CR Vault to establish restore points in case OS images / binaries are compromised.



TECHNOLOGY SELECTION

Based on recovery objectives, the type and amount of data that organizations want to protect, and budget, Dell EMC offers different technology options to implement Cyber Recovery infrastructure. The table below outlines some considerations. A backup-based approach leverages data protection storage and a backup application. A storage-based approach leverages primary storage and built-in replication mechanisms, generally without leveraging a backup application.

Category	Backup-Based	Storage-Based
Business Critical Systems	Span Across Different Systems	Are Supported By Dell EMC Storage
Protect Backup Catalog	Built-In	Not In Scope
Retention Period	45 Days to 1 Year	Less Than 45 Days, Many Copies / Day
Recovery Point	4 Hours to 1 Day	Minutes to Hourly
Recovery Time	Hours to Days	Minutes to Hours
Level of Investment	Moderate	Moderate to High

NOTE: The numbers above are for illustration purposes only. Exact figures are dependent on sizing. Retention periods and recovery points are interdependent and the granularity of recovery points will impact retention periods.

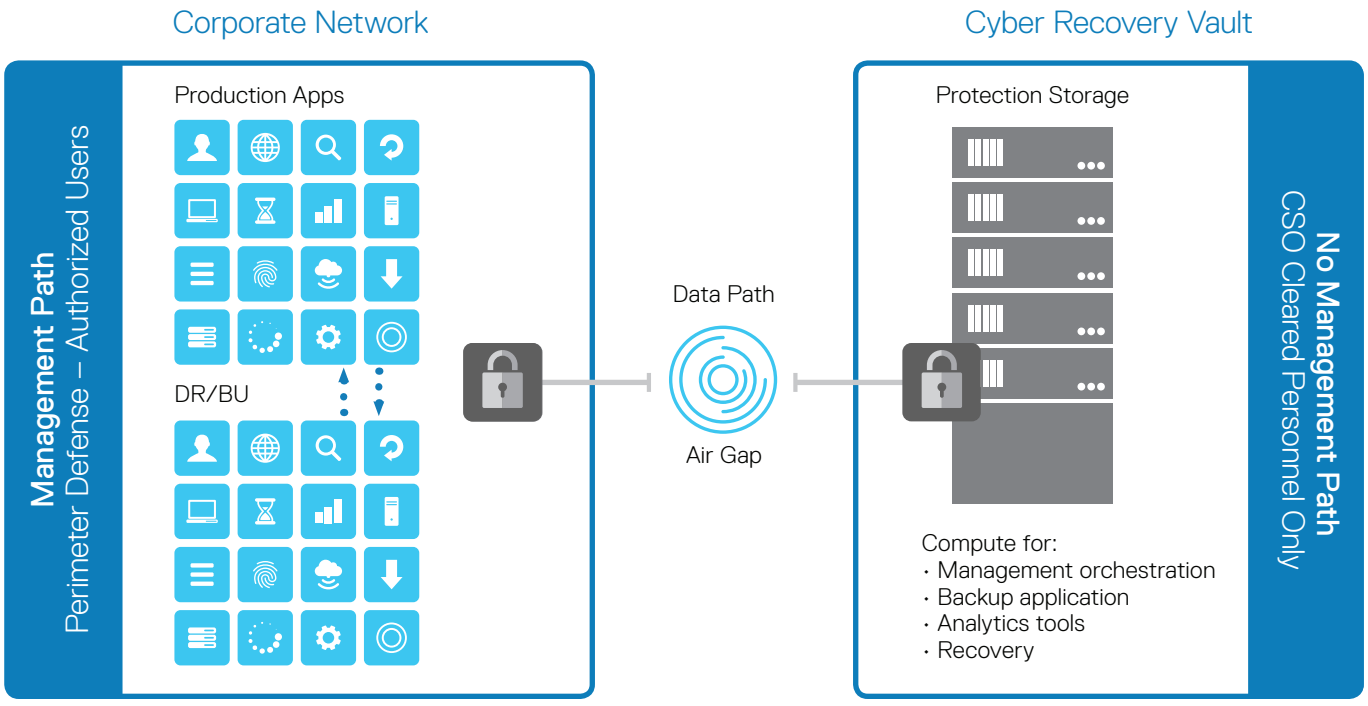
Larger deployments of Dell EMC Cyber Recovery can span across storage-based and backup-based approaches. The storage option typically covers tier 1 data for business critical systems that require granular and fast recovery. The backup-option provides an effective way to cover tier 2 data of business critical systems and ensure economical longer-term retention of clean room binaries and OS images.

DELL EMC CYBER RECOVERY DETAILS

Dell EMC Cyber Recovery provides management tools and the technology that performs the actual data recovery. It automates the creation of the restore points that are leveraged for recovery or security analytics. Dell Implementation Services are required for CR Vault design and implementation. Dell Advisory Services are recommended for designing an effective recovery strategy.

TECHNOLOGY COMPONENTS

Organizations can dramatically reduce their surface of attack from inside and outside threats by removing the cyber-attack recovery environment from the production network. The only required connection is a data path for periodically synchronizing the data. To further reduce the surface of attack, this data link is only brought online for data synchronization. This logical air gap provides another layer of defense by reducing the surface of attack.



Dell EMC Cyber Recovery eliminates the ability to access the Cyber Recovery infrastructure from the production network. Compute is needed inside the CR Vault to perform system management, infrastructure services, backup application, on-demand security analytics, and recovery testing. The required level of compute depends on the level of recovery testing an organization wants to achieve inside the CR Vault. A hyper-converged appliance or a small ESX cluster with virtual SAN can be an effective and economical strategy for maintaining an environment within the CR Vault. The management host is required because it runs the tools to orchestrate the workflow as described in the next section. Additional compute for periodic analytics and data validation is recommended. Sizing is driven by the data to be analyzed, the analytics tools used, and frequency of validation and testing.

AUTOMATED WORKFLOW

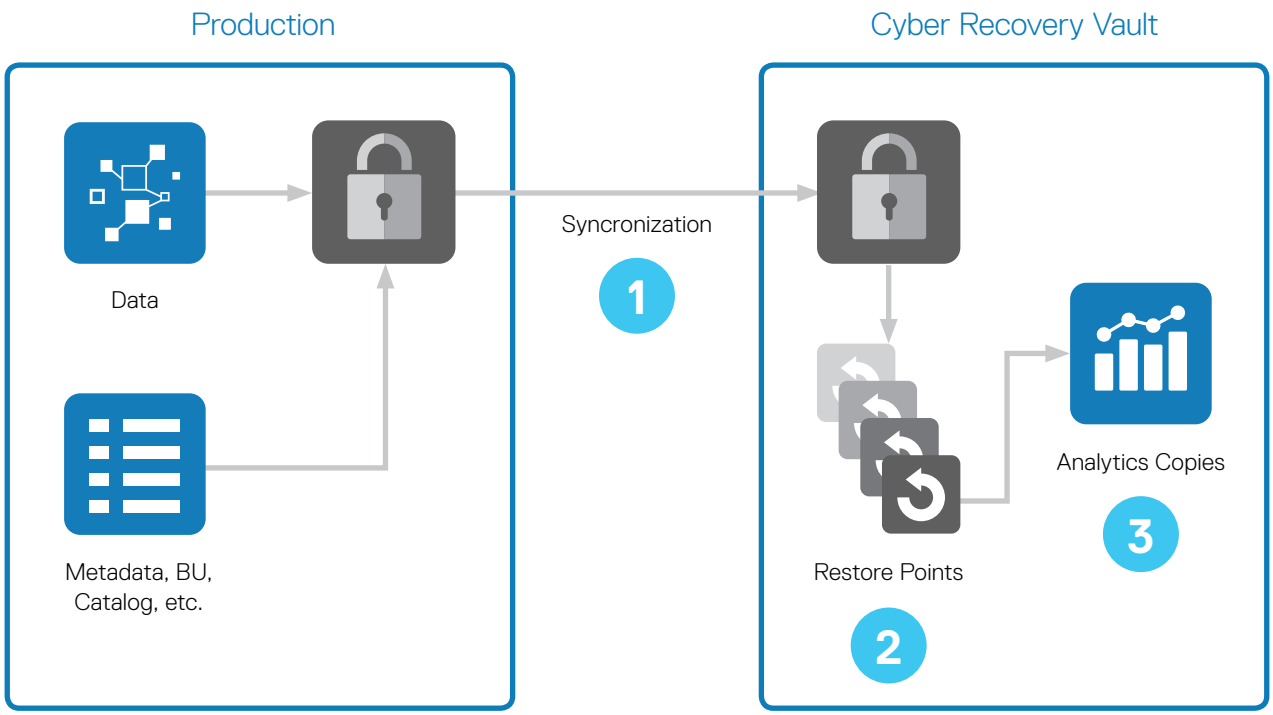
Moving infrastructure into the CR Vault removes it from potential access by bad actors. Isolation also introduces additional management challenges to approved administrators which is why automation is critical. Dell EMC Cyber Recovery automates the workflow associated with creating restore points needed for recovery or analytics. Three core benefits are:

Ease of Use – The time it takes to create a restore point is much faster than a manual management process. This also reduces the window of potential (but limited) exposure.

Automation – Instead of relying on manual creation of each restore point, administrators can schedule policies to create restore points at specific times and recurrence frequency—and then automatically delete the data when the retention period expires.

Reliability –Manual operations are often prone to error. An automated and policy-based approach simplifies the underlying mechanics and reduces the risk of failed recoveries.

The illustration below outlines the steps of creating a restore point from which to recover business critical systems.



Dell EMC Cyber Recovery handles the following discrete operations:

1. **Data Synchronization** – This activity is triggered from within the CR Vault. Deployments with larger recovery points can leverage the logical air gap mechanism. The link is enabled prior to data synchronization and then disabled once the synchronization is complete. A single transport mechanism minimizes the attack surface and brings all critical data into the CR Vault in a single transfer. This can include the backup catalog and metadata for backup-based deployments. Data synchronization is transparent to applications on the production side, hence the activity is not 'advertised' in the public domain. The actual data transfer is very efficient, because only changed blocks are copied over the wire. Production-side and target-side systems establish a trusted connection to prevent a rouge system from connecting to the CR Vault Protection Storage.
2. **Creation of Immutable Restore Points** – Once the data is synchronized and the data path is disabled, the target system conducts an operation that creates a space-efficient copy of the data. To prevent deletion, this copy is made immutable by retention locking each file. Policies can set retention periods based on space requirements. It is important to note that the CR Vault is not meant to be an archive. Retention periods typically range from 7-45 days. Exceptions can be made, for example to enable recovery of executables, organization should maintain a year's worth of copies of distribution packages containing binaries and OS images.
3. **Creation of Cyber-Attack Testing and Recovery Copies** – The management software also provides the ability to create writable sandbox copies for recovery drills and tests, data validation, and analytics. Regular recovery drills are advised to ensure the data has not been compromised and that staff is prepared to perform a recovery in the event of an actual attack.

ANALYTICS IN THE VAULT

Dell EMC Cyber Recovery does not replace good security prevention and detection—it is meant to complement these security measures. At the same time, the CR Vault provides some unique advantages over the production environment:

- A protected environment increases the effectiveness of security analytics. Because the CR Vault is isolated from the network, malware scans can be run forensically and unimpeded as they are not susceptible to malware masking routines. Diagnosis of certain attack vectors are better analyzed in an isolated workbench.
- Even if caution needs to be applied, application restart activities can detect attacks that only occur when application is initially started. Application tools like DBVERIFY, that would otherwise require downtime, can also be used in the offline environment.

Analytics techniques and tools can be grouped in the following broad categories, ranging from basic to advanced algorithms.

1. **System-Level Validation** – Geared towards validating that restore points are successfully created. The goal is to ensure that the steps involved in synchronizing the data and creating immutable copies completed successfully. This gives the organization the confidence that the restore point is actually recoverable. System-level validation also involves flagging any health issues of the overall CR Vault Infrastructure and Dell EMC Cyber Recovery management software. The validation is performed by system-level tools that can provide the required level of validation and issue alerts when needed.
2. **Anomaly Detection** – Used to detect unusual patterns and trigger alarms for further analysis. This is typically achieved by a combination of system, Dell EMC, and third-party analytics tools. System level tools can examine the replicated data and identify unusual rates of change based on user-defined

thresholds. These tools compare the previous image to the latest image and raise an alarm if the rate of change exceeds a usual threshold. Other types of entropy checking for ransomware is described in a SANS ISC InfoSec Forum. Failed entropy thresholds could indicate encryption or wiping of the synchronized data or it could signal a benign change in the data replicated to the CR Vault. Both are valuable to understand. Processes can be established to look for unexpected changes or new files in sensitive execution paths. Specialized tools can find anomalies in file systems, such as a change in a file without a change in the modification time, a change in sentinel records, or a failed entropy check. An anomaly can indicate that a file was manipulated, but these tools may not identify the specific malware. When anomalies are detected, the organization should conduct further security analytics using malware scanning tools.

3. **Malware Detection** – Used to identify the actual malware that has been persisted to specific files and binaries. Many of the recent malware attacks have used a combination of old-school malware coupled with newer tools. Several methods are used for this purpose and each scanning engine has areas of specialization. Solutions like Playground (created by Dell EMC Cyber Security Solution Group) can aggregate multiple engines into a comprehensive and adaptive cyber analytics framework. Signature-based and artificial intelligence based engines typically require a connection to a network and sometimes a cloud provider. In order to protect sensitive air-gapped systems, special design consideration such as data diodes must be taken into account. Common classes of malware detection heuristics are:
    - **Signature-Based** – Signature-based technologies that track known threats are less effective for zero-day malware, but are still useful for identifying known malware distributions. When an anti-malware solution provider identifies an object as malicious, its signature is added to a database of known malware. These repositories may contain millions of signatures that identify malicious objects. This method of identifying malicious objects has been the primary technique used by malware products.
    - **Behavioral Analysis** – Behavior-based malware detection evaluates an object based on its intended actions before it actually executes. Statistical analysis and machine learning tools can determine if an object's actual or potential behavior is suspicious. Attempts to perform actions that are clearly abnormal or unauthorized indicate the object is malicious, or at least suspicious. Evaluating for malicious behavior as it executes is called dynamic analysis. Threat potential or malicious intent can also be assessed by static analysis, which looks for dangerous capabilities within the object's code and structure.
    - **Artificial intelligence** – Some believe that only artificial intelligence based approaches offer the predictive quality that can give organizations an edge on their more sophisticated and evasive adversaries.
4. **Application-Level Analysis** – Used to verify the integrity of the entire application and database stack. This level of analysis requires a complete restore of the environment. Additional caution needs to be applied in order to prevent re-hydrating malicious malware. Segregation of resources in the CR Vault can mitigate this risk. Tools and techniques are typically application-specific. For example, Oracle DBVERIFY can validate the overall integrity of the Oracle instance. Since this activity requires downtime, it is preferable to run this utility inside the static CR Vault. Other tools like inspection of sentinel records within the database files are available to indicate the integrity of the database itself.

Dell Technologies provides tools that address items 1-3 above, whereas application-level analysis is typically done using tools provided by the application vendor. Since the combination of tools and techniques is dependent on the data that organizations are trying to protect, customization is inevitable. It is recommended that you engage Dell EMC Consulting Services to determine the most effective set of tools and techniques for different types of data and application sets.

RECOVERY PROCEDURES

The ultimate goal of Dell EMC Cyber Recovery is to provide an organization with the quickest and most reliable path to recovery of business critical systems. It is therefore critical to establish a cyber-attack recovery plan as part of a formal cyber incident response plan. This typically consists of the following elements:

1. **Invoke Cyber Recovery Plan** – Involves securing the scene of the crime, invoking the air gap to shut down connection to the CR Vault, and marshalling the resources in the Cyber Recovery Plan to start the response process.
2. **Perform Forensics and Damage Assessment** – Forensics to understand the type and scope of the attack and determine if a fix or patch available can be deployed to avoid reinfection. The Damage Assessment evaluates what is working and what is not, what can be repaired, what needs to be recovered, including any dependent systems. It also identifies any unaffected DB logs that can be applied to minimize data loss and determines the best restore point.
3. **Preparation for Recovery** – Determines the most appropriate recovery technique. This involves determining whether it is more effective to restore, repair, or rebuild and then prioritizing and sequencing the recovery of specific systems. This evaluation factors in the affected parts of the production environment, time of day, and other circumstantial details. The end goal is to choose a recovery path that prevents or minimizes the damage to business critical systems.
4. **Recovery of Data, Applications and Services** – This step is usually the execution of the system and data recovery based on steps 1-3. An organization might choose to perform a reverse synchronization of data back to a cleansed or rebuilt production system and then apply patches to prevent reinfection. Or it might elect to perform recovery within the CR Vault and then connect the recovered infrastructure back to the production network.

Several recovery techniques can prove viable depending on the cyber-attack and the damage created. A few scenarios are outlined below.

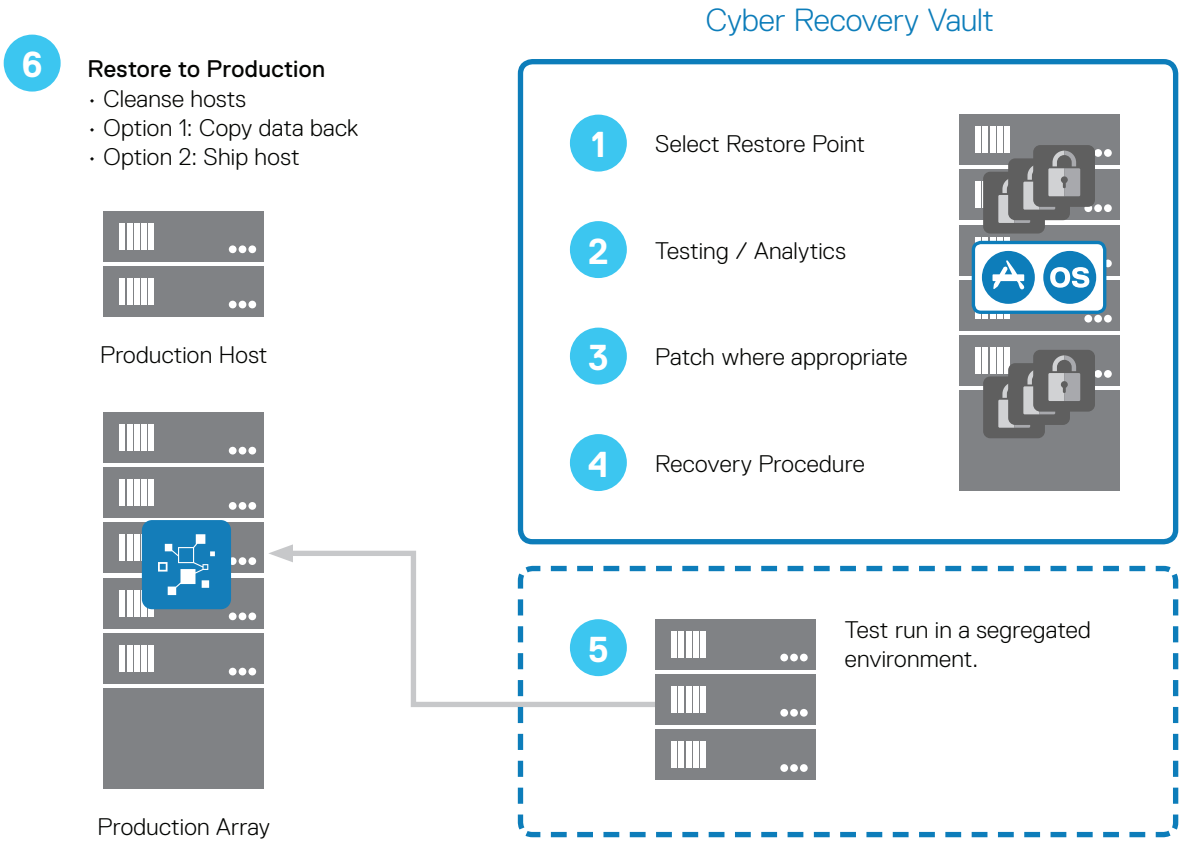
SCENARIO #1:

RESTORE DATA AND BINARIES IN THE CR VAULT

This technique provides the fastest recovery method, but does not eliminate the possibility that dormant malware is not eliminated. High level steps include:

1. Identify the restore points that were created before the attack occurred.
2. Using the forensics findings, identify the malware and where it has been persisted.
3. If binaries or OS images have been compromised, decide whether to cleanse the malware from the backup image and then restore the clean room binaries. If the confidence of cleansing is low, select a backup prior to the infection. If no clean copies of binaries exist in the generational backup images, organizations can rebuild using the clean room copies.
4. Apply security patches if possible and available.
5. Restore to data to a recovery host located within the CR Vault using the associated application's disaster recovery runbook.
6. Segment the application from the rest of the CR Vault infrastructure and bring it up. Then determine if the recovery process has eliminated the effects of the offending malware. This step is important when there is concern that the cyber-attack was based on multiple strains of malware.

7. Test run production applications using the CR Vault compute .
8. Cleanse or reimage the production environment and connect the recovery host to production [either logically or via physical shipment] and copy the application and data back to the original production servers.



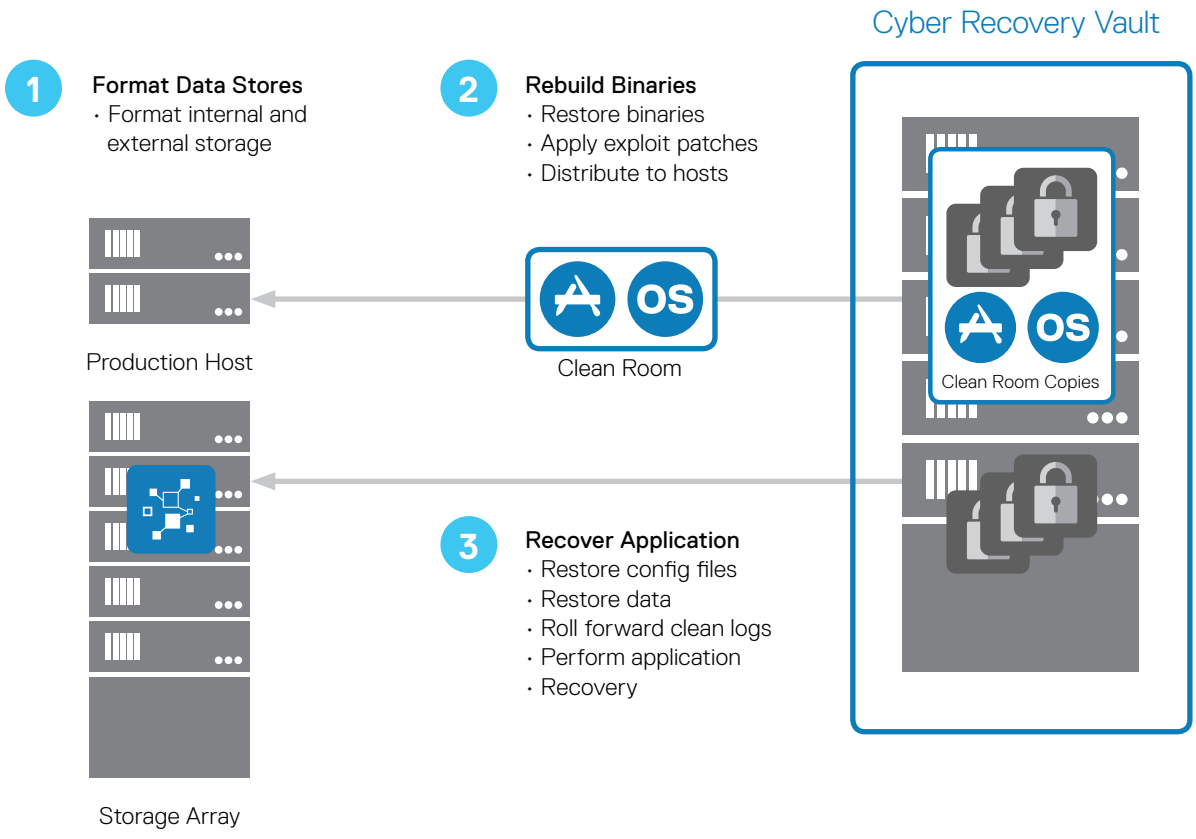
The alternative for larger and more complex environments is to reverse synchronize data from the CR Vault to the production system. This assumes that the production environment is in a state that can be used for restore.

SCENARIO #2:

COMPLETE REBUILD FROM CR VAULT

This technique is more comprehensive and conservative but it also represents a slower recovery method. This method also minimizes concerns around dormant malware. High level steps include:

1. Re-format the production systems based on the damage and forensics assessment done as part of Incident Response.
2. Rebuild binaries by restoring the appropriate clean room distro copies located in the CR Vault. This recovery process is consistent with scenario #1.
3. Apply security patches if possible and distribute to freshly formatted hosts.
4. Recover the application and data back to the original production environment by locating and restoring the appropriate copy, restoring configuration files, restoring data, and performing application recovery using the application's DR recovery runbooks.



CONCLUSION

Cyber-attacks like WannaCry and Petya/NotPetya have had devastating consequences on businesses worldwide and caused reduced revenue, loss of reputation, and millions of dollars in recovery costs. In the rapidly evolving threat landscape organizations are looking for effective recovery strategies with the knowledge that prevention and detection alone are not sufficient. Dell EMC Cyber Recovery provides a very effective recovery solution against common attack vectors, including dormant malware, data wiping and locking, data corruption, insider attacks, and destruction of backup and storage assets. It gives organizations an effective way to recover the lifeline of their business when other strategies fail.

i Graham 2017

ii https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

iii https://www.nist.gov/cyberframework

iv Does not indicate absolute probability but relative probability between types of cyber-attacks.

v https://www.us-cert.gov/ncas/alerts/TA17-181A

vi The Information has been abstracted and is for information purposes only

vii https://isc.sans.edu/forums/diary/Using+File+Entropy+to+Identify+Ransomwared+Files/21351/

viii Not all dependencies such as external feeds might be available.