Dell EMC Cyber Recovery protected our test data from a cyber attack

A Dell EMC Cyber Recovery solution with CyberSense can ensure your organization has a path to recovery from destructive cyber attacks

Modern companies can't function without their data. While most organizations realize the importance of backing up critical data in case of hardware failure or natural disaster, many lack adequate protection against attacks from cybercriminals that can similarly threaten financial ruin. The interconnection between company servers, end-user devices, and the rest of the internet at large leaves business-critical data open to attack from malicious entities that take sensitive data hostage, ruining consumer confidence and threatening revenues.

Dell EMC™ Cyber Recovery is a management and automation software solution that exists to protect organizations from these potentially devastating attacks. In the Principled Technologies data center, we set up servers and storage in a Dell EMC Cyber Recovery Vault and launched an attack on our test data. We found that when we infected production files and synced them to the copy in the vault, Index Engines™ CyberSense was able to detect the cyber attack, provide an alert, and report its findings.

With a Dell EMC Cyber Recovery solution, your organization is armed with immutable clean backups waiting in your vault even if cybercriminals manage to infiltrate your production or backup data. This gives you one more line of defense against data and revenue loss while also minimizing costly downtime that could occur without a cyber recovery solution in place.

What is Cyber Recovery?

Don't confuse cyber recovery with disaster recovery (DR)—they protect data in different ways, from different kinds of threats. Disaster recovery involves planning for events that render an organization's primary data center unusable, such as flooding or power grid failure. DR plans involve keeping backups of all data and services in a separate location that's far away enough to avoid the primary site disaster, but close enough to quickly replicate backups, either in a company-owned DR site or in the cloud.

The Dell EMC Cyber Recovery Vault protects critical infrastructure and data with an isolated, immutable copy of data for critical applications, which is protected from cybercriminals that infiltrate an organization and destroy or hold hostage its data. An organization that loses access to and control of their sensitive data may find it difficult or impossible to continue with their mission for multiple reasons, and paying an exorbitant ransom may be the only way to regain access. Day-to-day operations may cease as their infrastructure grinds to a halt, costing untold revenue loss.

Cyber recovery solutions exist to enhance an organization by making backup copies more resilient, allowing recovery after more sophisticated attacks.

How do attackers get in?

If there's a way in, cybercriminals can find it. That's why a comprehensive, proactive cyber recovery plan is an organization's best defense against both external and internal threats. Here are some common methods of attacks that criminals use:

Taking control of your backup server

Cybercriminals know that you have a DR plan in place that involves keeping backups, so it's not enough to target your production environment. By targeting your backup servers, criminals take away your ability to recover by ensuring you don't have a place to start over if they attack your production environment.

Destroying or encrypting your data protection storage

Enlisting data protection storage using Dell EMC Data Domain™ can enable you to restore reliably and to complete backups faster via inline deduplication of data, but it also provides another point of attack for criminals. In these types of attacks, the criminal may gain access to your backup environment by stealing credentials or employing tactics, which could result in the loss of your data protection storage. Or, they may encrypt your backup data—which means it's no longer of use to you unless you have the encryption key.

Compromising the management network for storage and servers

Cybercriminals can also attack the management network for your infrastructure, and even if your backups are protected by data governance, cybercriminals can use a low-level attack destroying the storage RAID group. By luring unsuspecting end-users connected to your network with phony links and downloads, attackers plant malware or ransomware that gives them control of data unless you pay to give it back.

Insider attack

It's not just an urban legend—sometimes the criminal is already inside the house. Disgruntled employees can map out an entire organization and gain access to critical systems credentials, or attach small devices to the network that seek out critical information to later gain access to the system. Once they obtain the right information, it's only a matter of time before a serious attack can happen.

Levels of data protection

As threats continue to emerge, so do protection options for your critical data. Below, we outline a good-better-best approach that lets you review your current data protection strategy and find ways to improve.

Good

Data backups: Backing up data to another location offsite or in the cloud.

Disaster recovery plan: A DR plan is the documented process you have in place that directs your team how to recover in the event of a disaster. DR plans include a recovery time objective (RTO), which is a time target for restoring business processes, and a recovery point objective (RPO), which is the age of the files/data you will start from after a disaster.

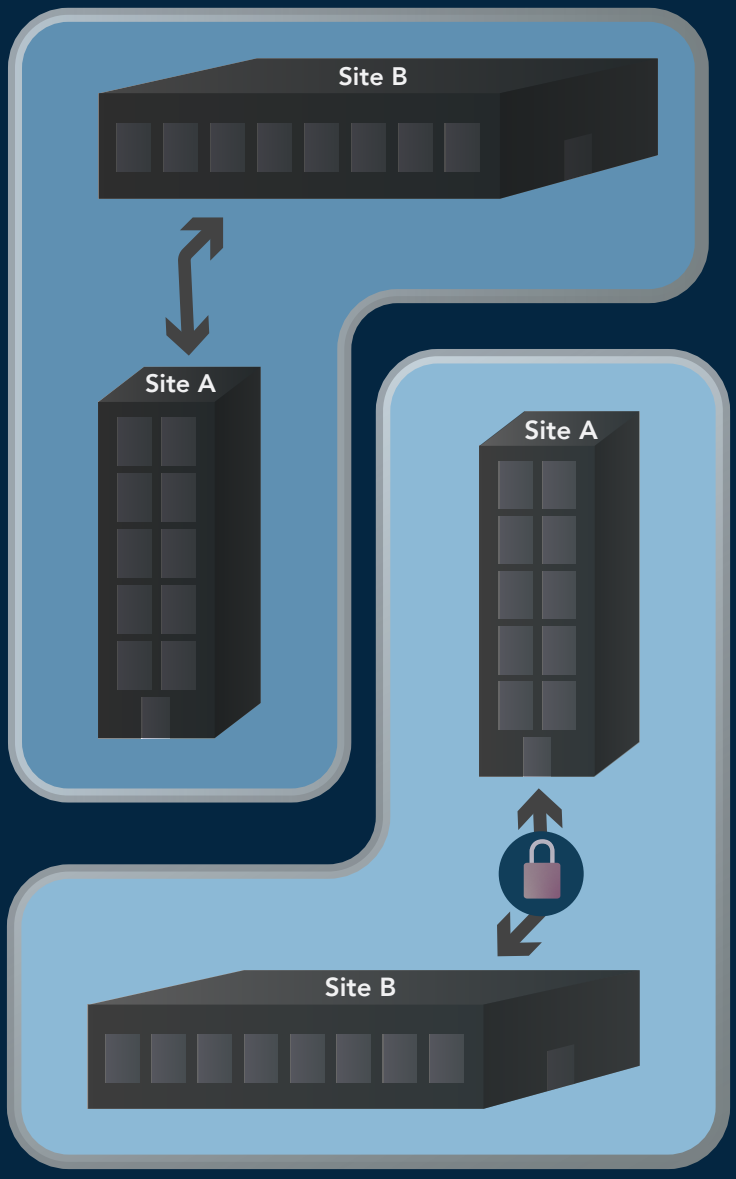
Warm or hot replication sites for DR: Replicating data to warm or hot sites reduces your business downtime. Warm site failover should be ready to restore business process with hours of downtime; hot site failover is for zero-downtime targets for the most critical data.

Better

Encryption at rest: Data protection that makes stored (or at-rest) data unreadable to unauthorized users. Users must have an encryption key to access this data.

Retention lock: Dell EMC Data Domain Retention Lock software offers immutable file locking and flexible retention policies.

Product-hardening best practices: Reduce the surface of vulnerability by reducing the number of functions a system performs.

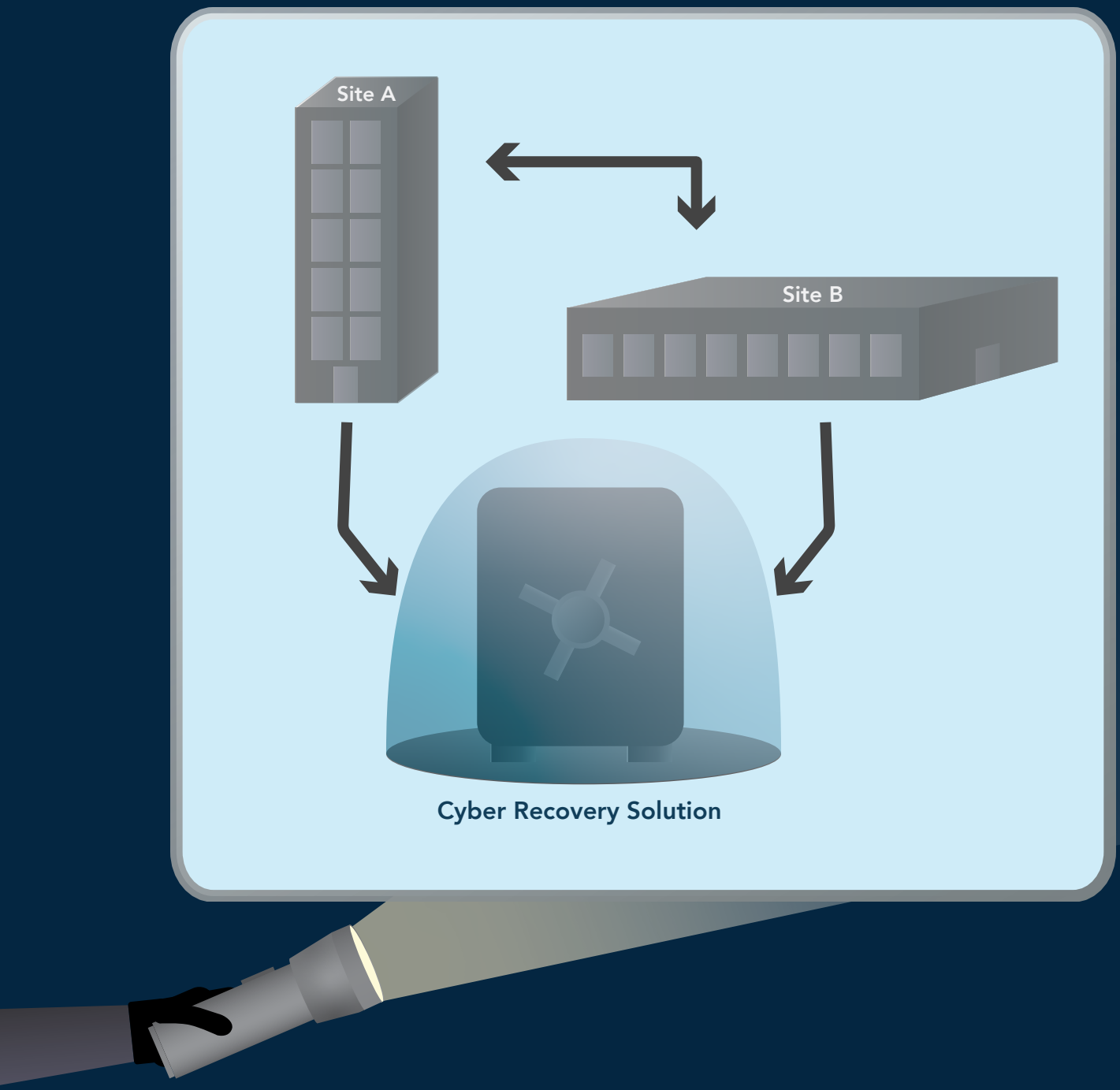


Best

Cyber recovery solution: Provides a physically- and network-isolated copy of data that protects against ransomware, insider attacks, and more.

Professional services: Professional services can help you assess your organization's needs and advise on the best plan to keep your data safe.

Security analytics: In the event something does go wrong, analytics looks for indicators of compromised data and can help you discover the who, how, and the why, so you can recover quickly from attack.

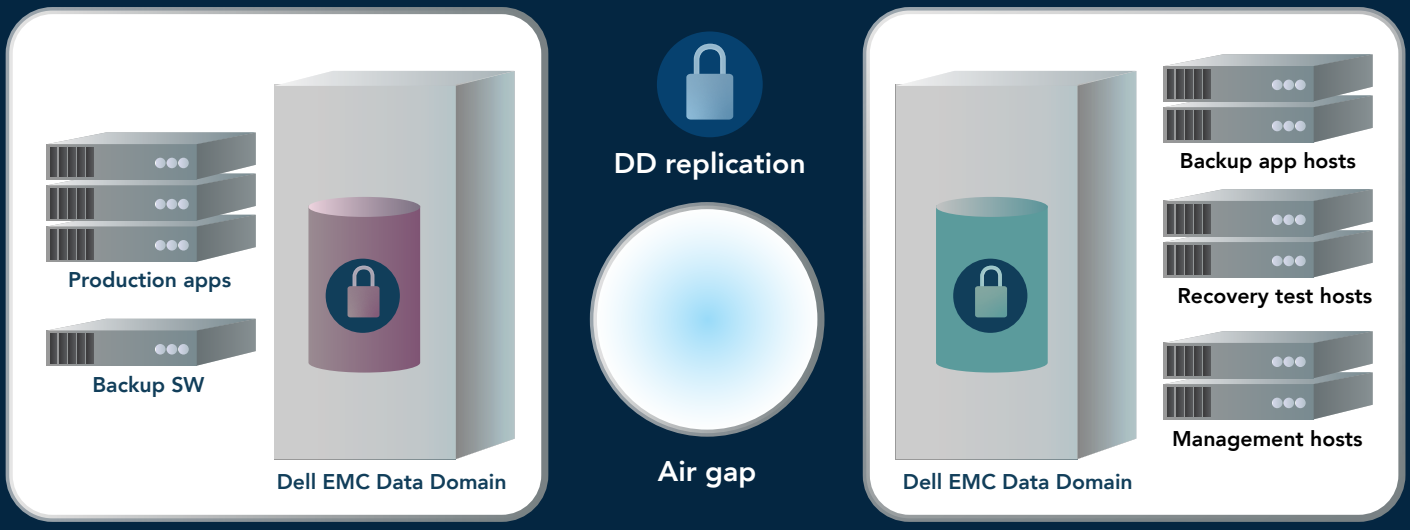


How the Dell EMC Cyber Recovery Vault works to help you recover from attacks

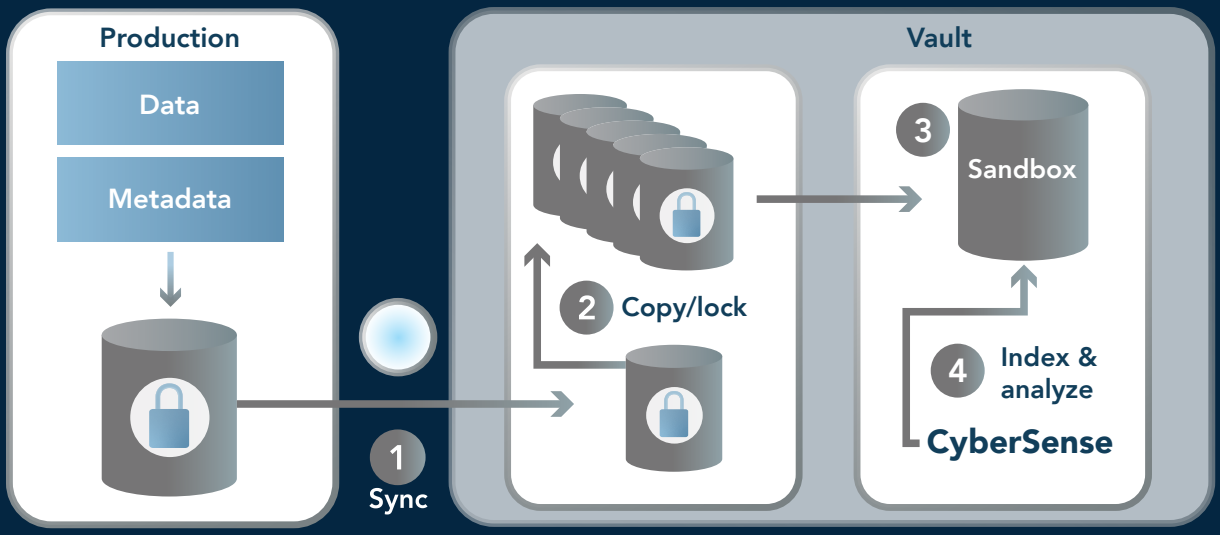
Dell EMC Cyber Recovery is a complete, isolated recovery solution that helps you minimize downtime, expense, and lost revenue by providing a resilient backup to critical data and a path to recovery from a cyber attack. To start, Dell EMC offers professional services that help you assess, plan, implement, and validate your cyber recovery solution.

Production environments are vulnerable to attack. Dell EMC Cyber Recovery keeps your data in a vault, where it is physically and logically isolated from other systems and locations. Physically, the Cyber Recovery Vault resides in a restricted room or area in your facility accessible only by authorized physical access, which limits the ability of in-house saboteurs and those that wish to hold your data for ransom to complete their objectives.

Logically, Dell EMC Cyber Recovery disables the replication NIC, effectively creating an air gap between the production network and the Cyber Recovery Vault to ensure that the data inside is isolated from other networks. Command and control of the vault comes from within Dell EMC Cyber Recovery software. The software orchestrates connecting the network interface to the production Data Domain appliance, replicating the data into the vault, and disabling the network interface to secure the vault when replication is complete. Data Domain replicator software can encrypt data in flight for further security. The CR Vault is not vulnerable during replication, offering no access to the management plane.



The image below shows how Dell EMC Cyber Recovery and CyberSense work to protect, analyze, and secure your critical data.



Breaking into the vault: Our hands-on tests

Does a Dell EMC Cyber Recovery solution work? When we set up our own infrastructure and tested it out, we found that we were able to successfully set up the solution and that Dell EMC Cyber Recovery offered protection against the simulated cyber attack we introduced.

In the PT data center, to simulate an enterprise solution with real applications running, we installed and configured a four-node Dell EMC VxRail™ V470F cluster, deploying Microsoft® SQL Server®, clients, and infrastructure VMs. We racked and configured two Data Domain appliances, deployed Networker, and set up backup policies so that the SQL Server databases would back up to a storage pool managed by the first Data Domain appliance.

In this testbed, we deployed Cyber Recovery and set up replication between both Data Domains; the first we used as our production backup appliance, and the second we used as the Cyber Recovery Vault storage. We created a new Cyber Recovery policy to synchronize between the Data Domains, and initialized a copy from production to the Vault. We were able to verify that during synchronization between the production and vault environments, only the replication port—which is data only and provides no management capabilities—was accessible from the production environment. When the sync ended, the replication port once again became inaccessible because the interface was disabled. The CR solution also offers the ability for the CR administrator to manually secure the vault, and no new data can replicate into the vault until the admin removes the secure lock. Our team also tested a recovery scenario from the vault by creating a duplicate copy of the target data inside the vault, and then exporting that duplicate copy to an application server outside the vault environment. We found that the recovery process worked as intended, and could offer a predictable recovery experience should an organization need to start fresh from their locked down backup.

Dell EMC Cyber Recovery with CyberSense analytics detected an attack

First, we deployed Index Engines software on a Linux host, added it as an Application Asset in Cyber Recovery, and synced and created a clean backup copy from our production server to our storage in the vault. We ran an Analyze job using CyberSense and found no evidence of attack.

When we added files infected with malware to the production server and replicated this data to the vault, CyberSense correctly ascertained that an attack had taken place and raised an alert to CR when it detected the suspicious copy.

Conclusion

Failing to consider the possibility of malicious actors controlling or holding hostage your organization's data is a potentially expensive gamble. While planning for natural disaster or hardware failure with a DR plan is the first step to keeping your data safe, your critical data is still vulnerable without a comprehensive recovery plan that guards against cyber attacks. In our labs, we found that Dell EMC Cyber Recovery offered an isolated recovery solution that provides an isolated, immutable copy of critical data, and enables analysis of that data so organizations can quickly recover critical infrastructure and data assets.

Read the science behind this report at http://facts.pt/a2jur2w ►

Principled Technologies®

Facts matter.®

This project was commissioned by Dell EMC.