The science behind the report:

Improve cyber resiliency and protect data from cyber ransomware threats by using an isolated vault, AI-based ML analytics software, and more

A Principled Technologies report: Hands-on testing. Real-world results.

Improve cyber resiliency and protect data from cyber ransomware threats by using an isolated vault, AI-based ML analytics software, and more

With Dell Technologies PowerProtect Cyber Recovery with CyberSense

As the frequency of cyber threats continuously grows and attack methods evolve, data protection plans must take an approach that secures and analyzes all IT components, from the most superficial to the deepest reaches. Dell PowerProtect Cyber Recovery can help protect the most critical and sensitive data while also helping ensure proper recovery in the face of a cyberattack or another disruptive event.

Dell PowerProtect Cyber Recovery is a data management, protection, and recovery solution that helps organizations protect their data and applications against ransomware, destructive cyberattacks, and unexpected events. The solution uses a multi-copy approach, meaning that after creating backups, it copies those backups to isolated storage for safeguarding and analysis. PowerProtect Cyber Recovery comprises many components, including one or more storage vaults, located either potentially on-premises in a PowerProtect DD (formerly known as Data Domain) appliance or in the cloud via software-defined Dell APEX Protection Storage for Public Cloud (formerly known as DD Virtual Edition). In both cases, the vault is operationally air-gapped, i.e., isolated from the production environment--potentially physically air-gapped in the case of the on-premises environment, and logically air-gapped in the case of the APEX environment. This makes it extremely difficult for bad actors or unauthorized users to log in and compromise backup copies.

PowerProtect Cyber Recovery also includes CyberSense, a fully automated and integrated intelligent security analytics engine that automatically scans data, files, databases, and images in the vault for signs of corruption from a ransomware attack. CyberSense provides full content analysis; takes observations from files to use as inputs for its artificial intelligence (AI)-based machine learning (ML) model; and detects malicious activity that includes mass deletions, encyption, and other suspicious changes in core infrastructure (including Active Directory and DNS), user files, and critical production databases that might indicate ransomware or a destructive attack. When CyberSense detects patterns of corruption, it generates an alert in the PowerProtect Cyber Recovery dashboard that gives additional information on the scale and impact of the attack.[1]

PowerProtect Cyber Recovery helps organizations mitigate cyberattacks, enhance data resilience with multiple copies of data backups from separate locations, reduce downtime, and maintain business continuity. This report uses publicly available data to highlight key data protection features and functionality and presents our findings from a competitive analysis of CyberSense.

Protect sensitive data

Encrypt immutable data in flight during backup replication to physically and logically isolated vaults

Detect SQL Server page corruption

CyberSense found an infection where a competing solution could not

Identify uncorrupted backup copies

CyberSense identified the most recent uninfected backup copy for recovery

Improve cyber resiliency and protect data from cyber ransomware threats by using an isolated vault, AI-based ML analytics software, and more

July 2024

This document describes what we tested, how we tested, and what we found. To learn how these facts translate into real-world benefits, read the report Improve cyber resiliency and protect data from cyber ransomware threats by using an isolated vault, AI-based ML analytics software, and more.

We concluded our hands-on testing on July 13, 2023. During testing, we determined the appropriate hardware and software configurations and applied updates as they became available. The results in this report reflect configurations that we finalized on May 23, 2023 or earlier. Unavoidably, these configurations may not represent the latest versions available when this report appears.

Our results

To learn more about how we have calculated the wins in this report, go to http://facts.pt/calculating-and-highlighting-wins. Unless we state otherwise, we have followed the rules and principles we outline in that document.

Table 1: Summary of the time (in hh:mm:ss) it took to complete backup and restore tasks using the two solutions. Source: Principled Technologies.

	CyberSense for Dell PowerProtect Cyber Recovery	Vendor X data protection analytics software
Detected encrypted files with obscured file names	Yes	Yes
Detected encrypted files with original file names	Yes	Yes
Detected SQL Server page corruption	Yes	No
Number of *incremental* backups required to create a baseline for scanning	0	14
Total number of backups required to create a baseline for scanning	1	15

System configuration information

Table 2: Detailed information on the server from our testbed.

System component information	Dell PowerEdge R750
BIOS name and version	Dell 1.8.2
Operating system name and version/build number	VMware® ESXi™, 7.0.3, 20328353
Processor	
Number of processors	2
Vendor and model	Intel® Xeon® Gold 5318Y
Core count (per processor)	24
Core frequency (GHz)	2.10
Memory	
Total memory in system (GB)	256
Network adapter	
Vendor and model	Mellanox® MT2894
Number and type of ports	4x 10GbE

Table 3: Software information for the Dell data protection solution.

Backup solution software	Version
PowerProtect Cyber Recovery	19.13.0.2-16
PowerProtect Data Manager	19.13.0-20

Table 4: Information on the VMs we used in testing.

Backup clients	OS version
2x Linux clients (test scenarios 1 and 2)	CentOS Linux® 8.5.2111
2x Windows clients (test scenarios 1 and 2)	Microsoft Windows Server 2019 DataCenter Server Core 10.0.17763.3887
SQL Server (test scenario 3)	Microsoft SQL Server 2019 15.0.2000.5

How we tested

Testing overview

From our lab at PT, we connected to a Microsoft Windows VM jumpbox running in a remote lab. From the jumpbox, we could access, verify, and control the lab environment, including VMware vCenter, VMs, and backup solutions under test. For these efforts, we used either web-based GUI or SSH connections, or both.

For the solution deployment phase of our testing, we observed lab personnel performing the installations of each solution. The process for each solution followed the same three basic sets of steps: install the solution software, configure or customize each product for use in the lab's environment, and create and start an initial backup of the same test VM. The lab personnel conducted the software installation phase via either a Windows 'setup' executable or through the deployment of an OVA. After deployment and when the solution presented the opportunity to log into its UI, lab personnel moved onto the next step, which included customizing the appliance for use in this lab environment. This customization included steps such as setting up user accounts, configuring networking addresses, and accepting any license agreements and other infrastructure requirements. Finally, lab personnel created policies that included a test VM and executed these policies to test the applications.

We tested three scenarios:

1. Encrypt all files and obfuscate file names

In this test case, we simulated a malicious event where the encryption obfuscates the file names. We ran an encryption script on two Linux client VMs (one VM backup type and one Filesystem backup type) and two Windows client VMs (one VM backup type and one Filesystem backup type). In the PowerProtect environment, we took one full backup before the encryption started and an incremental backup after the encryption completed. We then ran a Secure Copy Analyze from Cyber Recovery. In the Vendor X environment, we took one full backup and then at least 14 incremental backups before we ran the encryption script.

2. Encrypt all files and keep original file names

In this test case, we simulated a malicious event where the encryption keeps all original file names. We ran an encryption script on two Linux client VMs (one VM backup type and one Filesystem backup type) and two Windows client VMs (one VM backup type and one Filesystem backup type). In the PowerProtect environment, we took one full backup before the encryption started and an incremental backup after the encryption completed. We then ran a Secure Copy Analyze from Cyber Recovery. In the Vendor X environment, we took one full backup and then at least 14 incremental backups before we ran the encryption script.

3. Infect a SQL Server page

In this test case, we simulated a malicious event where infection corrupts a SQL database table. We simulated the event on a SQL database VM by running an infection query on a database table from the SQL Server Management Studio. In the PowerProtect environment, we took one full backup before the infection started and an incremental backup after the infection completed. We then ran a Secure Copy Analyze from Cyber Recovery. In the Vendor X environment, we took one full backup and then at least 14 incremental backups before we ran the infection script.

The following sections describe the steps we took to run the test cases.

Backing up files and VMs on Cyber Recovery

1. Log into the Power Protect Data Manager GUI.
2. Under the Protection menu, select Protection Policies. Click the checkbox next to the policy to be backed up, and click Protect Now.
3. Select All Assets.
4. Set the backup type to Full for the first backup (and Synthetic Full for the subsequent incremental backups). Click Next.
5. Complete steps 2 through 4 for all Protection Policies.
6. Log into the Cyber Recovery server, and wait until all backups complete.
7. From the Policies screen, select each policy, click Actions, and from the pull-down menu, select Secure Copy Analyze.
8. In the Secure Copy Analyze screen, select the CyberSense server from the Application Host pull-down menu.
9. To enable Advanced Options, click the slider.
10. In the Content Format pull-down menu, select the correct content for the backup type for the selected policy. For filesystem policies, select the Filesystem option. For VM backups, select the Backup option. For SQL database, select the Databases option.
11. To start Secure Copy Analyze job, click Apply.
12. Under the Jobs menu on the left panel, select Protection Jobs to monitor the progress.
13. When all the protection jobs complete, click Dashboard, and verify that the solution found no anomalies.

Performing an app-direct backup of the SQL database

1. Log into the SQL Server via remote desktop.
2. Open the SQL Server Management Studio.
3. To pull up the application direct window, click Agent.
4. In the Microsoft app agent for Application Direct screen, enter a name and description for the backup.
5. Click the ellipse next to the PowerProtect DD system.
6. In the PowerProtect DD System List & Lockbox Settings window, select the target DD system for the backup, and click OK.
7. In the Microsoft app agent for Application Direct screen, select the databases you will back up, and select Full in the Backup type pull-down menu.
8. To execute the backup, click Run.
9. When the backup completes, click OK to close the application Agent window.

Encrypting all files and obfuscate file names

1. Log into the Linux VMs via ssh.
2. Run the following commands to encrypt all files and obfuscate file names:

```
SAVEIFS="$IFS"; IFS=$'\n'; echo "Encrypting…"; for file in 'find /fs1 -type f'; do echo -n $file,;
openssh aes-256-cbc -salt -in $file -out 'dirname $file'/'tr -dc A-Za-z0-9 </dev/urandom | head -c 13'
-k Password123; rm -f $file; done; echo -e "\nDone."; IFS="$SAVEIFS"
```

3. Log into the Windows VM consoles from vCenter.
4. Run the following commands to encrypt all files and obfuscate file names:

```
$testfolder = "x:\"; $files = Get-ChildItem -Path $testfolder -Recurse -File | Select-Object
-ExpandProperty FullName; Write-Host "Encrypting…"; foreach ($f in $files){; Write-Host "$f,"
-NoNewLine; $randomalphanum = -join ((48..57)+(65..90)+(97..122)|Get-Random -Count 13|%
{[char]$_}); $path = Split-Path "$f"; c:\encrypt\openssl.exe aes-256-cbc -salt -in "$f" -out
"$path\$randomalphanum" -k Password123 2>&null; Remove-Item "$f"; }; Write-Host; Write-Host "Done."
```

Encrypting all files and keep original file names

1. Log into the Linux VMs via ssh.
2. Run the following commands to encrypt all files and keep original file names:

```
SAVEIFS="$IFS"; IFS=$'\n'; echo "Encrypting…"; for file in 'find /fs1 -type f'; do echo -n $file,;
openssh aes-256-cbc -salt -in $file -out $file.enc -k Password123; rm -f $file; mv $file.enc $file; done;
echo -e "\nDone."; IFS="$SAVEIFS"
```

3. Log into the Windows VM consoles from vCenter.
4. Run the following commands to encrypt all files and keep original file names:

```
$testfolder = "x:\"; $files = Get-ChildItem -Path $testfolder -Recurse -File | Select-Object
-ExpandProperty FullName; Write-Host "Encrypting…"; foreach ($f in $files){; Write-Host "$f,"
-NoNewLine; c:\encrypt\openssl.exe aes-256-cbc -salt -in "$f" -out "$f.enc" -k Password123 2>&null;
Remove-Item "$f"; Rename-Item "$f.enc" "$f"; }; Write-Host; Write-Host "Done."
```

Infecting a SQL Server page

1. Connect to the SQL Server VM via remote desktop.
2. Open SQL Server Management Studio.
3. Expand the databases tree.
4. Right click the targeted database, and select New Query.
5. Type the following text in the blank query window:

```
ALTER DATABASE virt01sql01
SET PAGE_VERIFY CHECKSUML
DROP TABLE IF EXISTS #table_pages;
DECLARE @dbid int = DB_ID(n'virt01sql01');
SELECT dpa.allocated_page_file_id, dpa.allocated_page_page_id
INTO #table_pages
FROM virt01sql01.sys.schemas s
         INNER JOIN virt01sql01.sys.objects o ON 0.schema_id = s.schema_id
CROSS APPLY sys.dm_db_database_page_allocations(@dbid, o.objects_id, NULL, NULL, 'DELETED') dpa
WHERE o.name = N'Table_001'
         AND s.name = N'dbo'
         AND dpa.page_type_desc = N'DATA_PAGE';

USE master;
ALTER DATABASE virt01sql01 SET SINGLE_USER WITH ROLLBACK IMMEDIATE;
GO
DECLARE @dbid int = DB_ID(N'virt01sql01');
DECALRE @fileid int;
DECALRE @pageid int;
DECALRE @offset int;
DECLARE @value varbinary(1);
DECALRE cur CURSOR LOCAL FORWARD_ONLY STATIC READ_ONLY
FOR
SELECT dpa.allocated_page_file_id, dpa.allocated_page_page_id
FROM #table_pages dpa
OPEN cur;
FETCH NEXT FROM cur INTO @fileid, @pageid;
WHILE @@FETCH_STATUS = 0
BEGIN
      SET @offset = CONVERT(int, CRYPT_GEN_RANDOM(2)) % 8192;
      SET @value = CRYPT_GEN_RANDOM(1);
      DBCC WRITEPAGE (@dbid, @fileid, @pageid, @offset, 1, @value, 1) WITH NO_INFOMSGS;
      FETCH NEXT FROM cur INTO @fileid, @pageid;
END
CLOSE cur;
DEALLOCATE cur;
GO
ALTER DATABASE virt01sql01 SET MULTI_USER;
GO
```

6. On the menu, click Execute to run the corruption query.

Performing Secure Copy Analyze from Cyber Recovery after encryption

1. Connect to the Cyber Recovery UI, and log in.
2. From the left panel, click Policies.
3. From the Policies screen, select each policy, click Actions, and select Secure Copy Analyze from the pull-down menu.
4. In the Secure Copy Analyze screen, select the CyberSense server from the Application Host pull-down menu.
5. Click the slider to enable Advanced Options.
6. In the Content Format pull-down menu, select the correct content for the backup type for the selected policy. For filesystem policies, select the Filesystem option. For VM backups, select the Backup option. For SQL database, select the Databases option.
7. To start Secure Copy Analyze job, click Apply.
8. Under the Jobs menu on the left panel, select Protection Jobs to monitor the progress.
9. Once the Protection Jobs complete, return to the dashboard.
10. Verify that Cyber Recovery found all five Critical Alerts (two filesystem backup objects, two VM backup objects, and one SQL database object).

Read the report ▶

This project was commissioned by Dell Technologies.

Principled Technologies®

Facts matter.®

DISCLAIMER OF WARRANTIES; LIMITATION OF LIABILITY:
Principled Technologies, Inc. has made reasonable efforts to ensure the accuracy and validity of its testing, however, Principled Technologies, Inc. specifically disclaims any warranty, expressed or implied, relating to the test results and analysis, their accuracy, completeness or quality, including any implied warranty of fitness for any particular purpose. All persons or entities relying on the results of any testing do so at their own risk, and agree that Principled Technologies, Inc., its employees and its subcontractors shall have no liability whatsoever from any claim of loss or damage on account of any alleged error or defect in any testing procedure or result.

In no event shall Principled Technologies, Inc. be liable for indirect, special, incidental, or consequential damages in connection with its testing, even if advised of the possibility of such damages. In no event shall Principled Technologies, Inc.'s liability, including for direct damages, exceed the amounts paid in connection with Principled Technologies, Inc.'s testing. Customer's sole and exclusive remedies are as set forth herein.