Position Paper

OpenText Enterprise Backup and Recovery Data Protector Security

Table of Contents

page

Malware should not have a chance of sneaking into your back solution and all data should be moveable or stored in an encrypted way.

Data Protector as Part of Your Security Strategy

You may wonder why data protection (Backup & Recovery) is considered part of a security strategy.

First of all, you want your backup data to be safe and invulnerable. Malware should not have a chance of sneaking into your back solution and all data should be moveable or stored in an encrypted way. Depending on the strategy in use (3-2-1, etc.) you want backup copies in different locations and on different media types. All of that should be driven from a central console making sure reporting, auditing, and monitoring are automatic and easy.

Secondly, DP is your last line of defence if information has already been lost or corrupted. Getting your important data back with a press of a button makes sure infected data is replaced or missing data is restored. This could have been a security system like a firewall server or a network proxy or a digital rights management solution.

This position paper will introduce you to the individual concepts and features Data Protector uses as part of a larger security strategy.

Security Model

Security is the baseline for everything!

The way we handle backup data must be secure from the beginning. If attackers can sneak into commands or data stored in the backend or on the move the whole concept is questionable. This is why we have introduced various security features supporting the overall procedures.

A very simple first step to improved security may be using a hardened Linux platform with main DP components since Linux seems less vulnerable to Malware attacks. The fact that DP uses an internal Database makes it even harder to intrude.

These security features are corner stones for getting certified for Common Criteria.
Main topics for the following paragraphs here are encryption, networking, architecture and storage.

Common Criteria Certification

The Common Criteria for Information Technology Security Evaluation (referred to as **Common Criteria** or **CC**) is an international standard (ISO/IEC 15408) for computer security certification. It is currently in version 3.1 revision 5.

Common Criteria is a framework in which computer system users can *specify* their security *functional* and *assurance* requirements (SFRs and SARs respectively) in a Security Target (ST), and may be taken from Protection Profiles (PPs). Vendors can then *implement* or make claims about the security attributes of their products, and testing laboratories can *evaluate* the products to determine if they actually meet the claims. In other words, Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.

Body Text is styled with Calibri font size 11 and black font color. Good communication happens when the message is received and understood in exactly the way it was intended. Looking for pre-written, signed-off material? Check out Brand Central.

Data Protector relies on proven and certified Malware and Ransomware protection solutions

Enterprise Class Scalability and Security

DATA PROTECTOR SECURITY MODEL

- Centralized command and control
- Secure client communication via TLS
- Configurable Data encryption
- AES/TLS data encryption per client
- User authentication and LDAP integration
- Network Port Consolidation—only one major port for DP operations

Ransomware Recovery Strategy

A successful Ransomware recovery strategy must support a number of steps:

- Retention time that goes beyond what Ransomware expects (at least 6 months). Snapshots are not providing long-term retention since they fill up your storage systems too fast, slow down overall storage performance and they are not independent from the source volume. **A snapshot is not an independent 1:1 copy of your data!**
- Being able restoring to another (non-infected) system
- Test your backup sets with a verification process, test restore procedures
- Being independent of platforms and backup devices used with multiple copies
- Support 3-2-1, 3-2-1-1-0 or 4-3-2 backup strategies
- Have clear RTO/RPO set up and verify regularly with reports
- Scanning/detection taking place on Workstations and Servers since they are the main entry-point

Data Protector stores backup object information from the internal Database (IDB) on each medium at the end of each backup session. This allows for migration of backup data from one CM to another CM by “shipping” media.

Malware Protection Building Blocks

This particular section is showing the recovery strategy and the combined solutions OpenText has on offer.

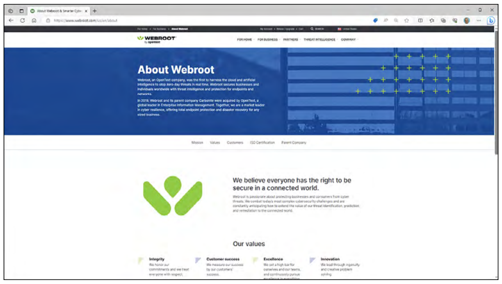
Type of Activity	Data Protector
Offline Backup	✓
True Air Gap Backup	✓
Immutable Backup	✓
WORM Media	✓
Backup Verification	✓
Enhanced Automatic DR	✓

Backup Method	Data Protector
Backup to Cloud	Data Protector supports private and public cloud as backup target.
Backup to Tape	Data Protector supports an exhausting list of Tape Drives and Tape Libraries
Backup to Disk	Data Protector makes use of deduplication Appliance Features. Data-at-Rest Encryption, Data Immutability, Data Replication, Cloud Upload
Backup Replication	Data Protector provides the option to configure a second cell in remote (DR) location.
Secure Backup Transport	Data Protector provides encrypted command and data communication

Malware Protection as a Solution

Data Protector relies on proven and certified Malware and Ransomware protection solutions. These are permanently updated, have proven their effectivity many times, and they are accepted by industry-leaders. It is important finding infections before they are part of a backup set, therefore scanning of data should take place in the backup client to not slow down backup and restore performance too much. This would force a redesign of RPO/RTO.

DP can be offered partnering with OpenText WebRoot or BitDefender, but isn’t limited to these two.



About Webroot

Webroot, an OpenText company, was the first to harness the cloud and artificial intelligence to stop zero-day threats in real time. Webroot secures businesses and individuals worldwide with threat intelligence and protection for endpoints and networks.

In 2019, Webroot and its parent company Carbonite were acquired by OpenText, a global leader in Enterprise Information Management. Together, we are a market leader in cyber resilience, offering total endpoint protection and disaster recovery for any sized business.

We believe everyone has the right to be secure in a connected world.

Webroot is passionate about protecting businesses and consumers from cyber threats. We combat today's most complex cybersecurity challenges and are constantly anticipating how to extend the value of our threat identification, prediction and remediation to the connected world.

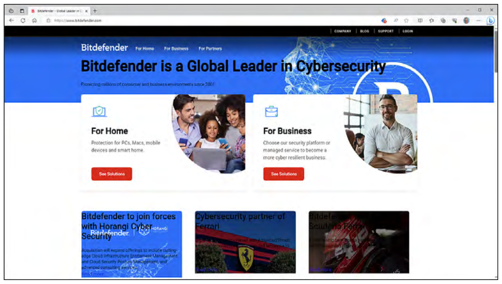
Our values

Integrity: We honor our commitments and we treat everyone with respect.

Customer success: We measure our success by our customers' success.

Excellence: We set a high bar for ourselves and our teams, and continuously pursue

Innovation: We lead through ingenuity and creative problem solving.



Bitdefender is a Global Leader in Cybersecurity

Protecting millions of consumer and business environments since 2001

For Home: Protection for PCs, Macs, mobile devices and smart home.

For Business: Choose our security platform or managed service to become a more cyber resilient business.

Bitdefender to join forces with Horangi Cyber Security

Acquisition will expand offerings to include cutting-edge Cloud Infrastructure Entitlement Management and Cloud Security Posture Management, and advanced consulting services.

Cybersecurity partner of Ferrari

Ransomware/Malware Recovery Option: EADR

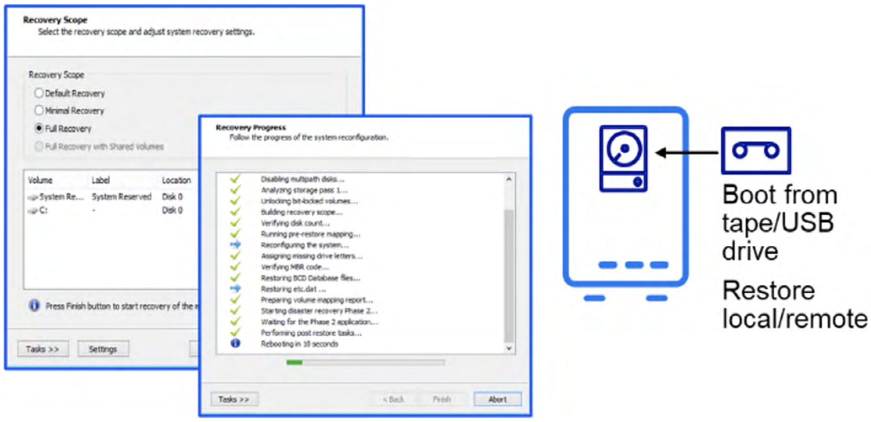
Sometimes it might be too dangerous overwriting all or part of an infected system while it is still online. In that case you can wipe out the system and recover it using the DP Enhanced Automatic Disaster Recovery (EADR) procedure. The process is partially offline and starts with setting up partitions and file systems cleaning out any remains of previous malware. The process works for physical and virtual servers.

Bare Metal Disaster Recovery:

- Enhanced Automated Disaster Recovery (EADR)
- Manual DR
- DR to different system
- DR to Virtual Machine (P2V)

Note: For medium/large scale migrations we offer PleateSpin as preferred solution

Immutability makes sure backup data cannot be changed or deleted from those backup targets until the defined timeframe has run out.



Recovery Scope
Select the recovery scope and adjust system recovery settings.

Recovery Scope
○ Default Recovery
○ Minimal Recovery
● Full Recovery
○ Full Recovery with Shared Volumes

Volume	Label	Location
System Re...	System Reserved	Disk 0
C:	-	Disk 0

Press Finish button to start recovery of the r

Recovery Progress
Follow the progress of the system reconfiguration.

```
✓ Disabling multpath disks...
✓ Analyzing storage pass 1...
✓ Unlocking bit-locked volumes...
✓ Building recovery scope...
✓ Verifying disk count...
✓ Running pre-restore mapping...
➡ Reconfiguring the system...
✓ Assigning missing drive letters...
✓ Verifying MBR code...
✓ Restoring BCD Database files...
➡ Restoring etc.dat ...
✓ Preparing volume mapping report...
✓ Starting disaster recovery Phase 2...
✓ Waiting for the Phase 2 application...
✓ Performing post restore tasks...
ⓘ Rebooting in 10 seconds
```

What If the Cell Manager Is Lost?

Let's assume the Cell Manager (CM) got lost in a Malware attack, restore of the CM is not working for some reason…

Data Protector stores backup object information from the internal Database (IDB) on each medium at the end of each backup session. This allows for migration of backup data from one CM to another CM by "shipping" media. On the other hand, it also allows a CM IDB being recreated by importing all needed media.

Media is always disconnected from the CM. Whatever happens to a CM cannot reach into backup media. Also, DP ships with an internal Database which is not exposed to the outside world like a normal Database would be.

- Infection being identified on a system backed up by DP (done by Malware scanner, infection could not be cleaned by the tool)
- Information sent to DP Cell Manager and schedules get paused/disabled for this client (this part needs manual integration today)
- DP shows restores from a timeframe before the infection (last known good)
- DP to offer restore/overwrite of client data or restore to a safe location first for further checks
- Malware scanner to confirm the client is clean and can be put back into production

Data Protector supports this approach with its universal approach to backup device management. Data Management is done using the DP Object Copy feature which lets you copy/ migrate backup data to any other device at any time.

Malware Recovery Workflow

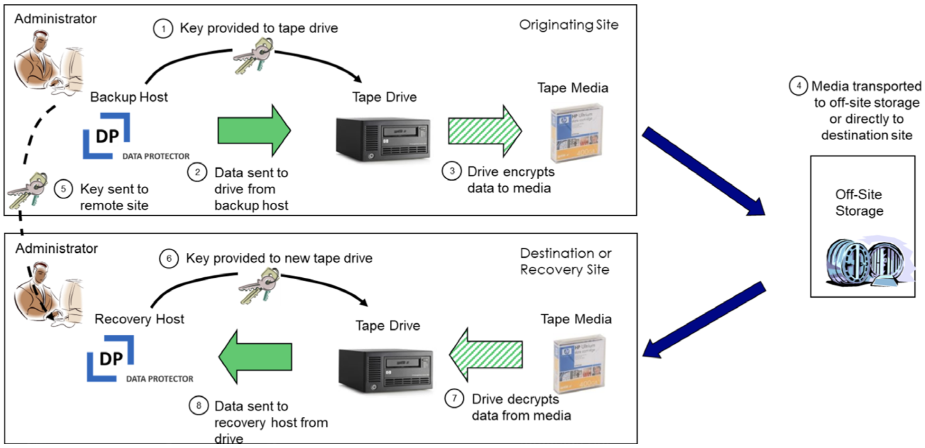
- Infection being identified on a system backed up by DP (done by Malware scanner, infection could not be cleaned by the tool)
- Information sent to DP Cell Manager and schedules get paused/disabled for this client (this part needs manual integration today)
- DP shows restores from a timeframe before the infection (last known good)
- DP to offer restore/overwrite of client data or restore to a safe location first for further checks
- Malware scanner to confirm the client is clean and can be put back into production

Tape Drive Encryption

Tape drives and media are the ultimate air-gap approach in a security solution addressing protection against Malware like Ransomware or Viruses.

- First of all, tape media is never directly accessible by Malware, since they don't provide file-system-like access. Data is usually interleaved, encrypted and only readable by the owning backup application.
- Secondly you can export tape media from a drive or library and store it in a secure place. This would also address fire, flooding, earthquakes and other disasters.
- Tape media can be shipped to another location preventing data from moving over potentially unsecure WAN connections. They can also move a huge amount of data in one go.
- DP supports vaulting of media by setting location information. You don't want to lose media, right?
- Last but not least data on tape media can be encrypted and used in WORM (Write-Once, Read Many) format preventing any changes from happening on a physical layer.

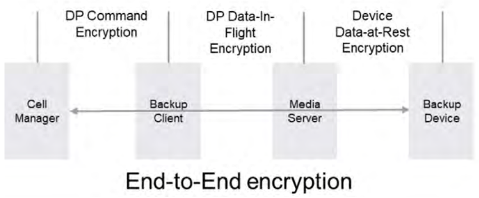
Tape Drive Encryption Workflow


Administrator
1 Key provided to tape drive
Originating Site
Backup Host
Tape Drive
Tape Media
DP DATA PROTECTOR
2 Data sent to drive from backup host
3 Drive encrypts data to media
5 Key sent to remote site
4 Media transported to off-site storage or directly to destination site
Off-Site Storage
Administrator
6 Key provided to new tape drive
Destination or Recovery Site
Recovery Host
Tape Drive
Tape Media
DP DATA PROTECTOR
8 Data sent to recovery host from drive
7 Drive decrypts data from media

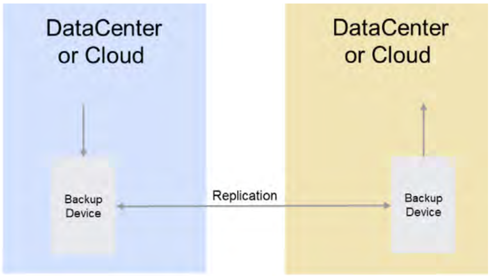
Deduplication Software and Appliance Encryption

When working with deduplication appliances the following features are most important:

- Encryption
- Replication
- Immutability



End-to-End encryption



Immutability

Data Protector supports backup target immutability with:

- DP Deduplication (software-based dedupe target)
- HPE StoreOnce (appliance-based dedupe target)
- Dell/EMC DataDomain (appliance-based dedupe target)

Immutability makes sure backup data cannot be changed or deleted from those backup targets until the defined timeframe has run out. This protects against the backup manager system being infected or otherwise unusable or against a mistake in media management by an administrator. Backup data can be re-imported into the backup manager system anytime during the immutability timeframe.

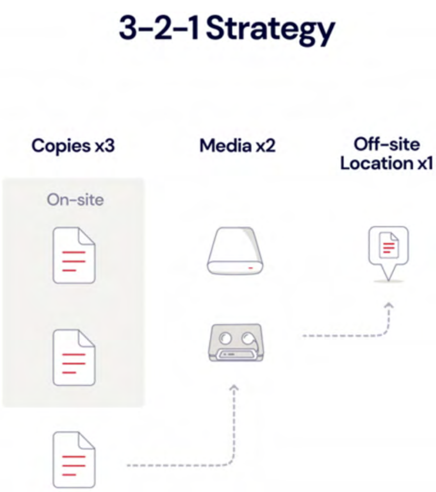
Backup Strategies

Data Protector supports many backup strategies including:

- 3-2-1 Backup Strategy
- 3-2-1-1-0 Backup Strategy
- 4-3-2 Backup Strategy

You can also cross-combine or come up with your own customized version of a strategy. It is most important that a strategy exists, and regular tests are a must-have and part of your business continuity plan.

3-2-1 Strategy

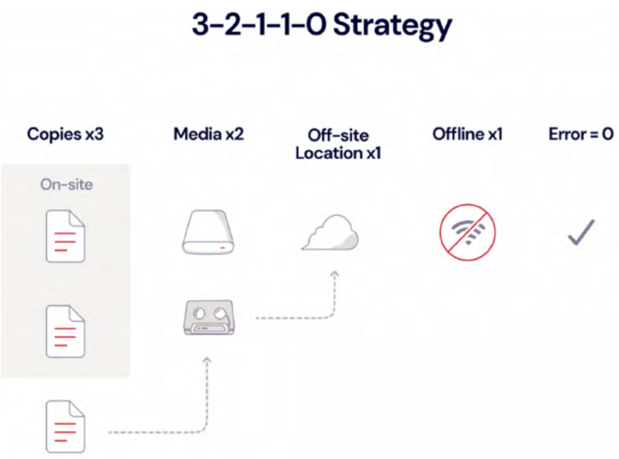


The 3-2-1 rule advises keeping three copies of your data (e.g., one primary copy and two backups) on two different media (e.g., the primary copy on an internal hard disk, a backup copy on tape, and an additional backup copy on an external HDD or tape) with one copy off-site (likely the tape backup).

Data Protector supports this approach with its universal approach to backup device management. Data Management is done using the DP Object Copy feature which lets you copy/migrate backup data to any other device at any time. Copies are automatically used if the primary backup is not available for any reason.

Some customers prefer data migration directly after a backup was done. Others prefer a consolidated approach to move a larger portion of data in a dedicated time window.

3-2-1-1-0 Strategy



A 3-2-1-1-0 strategy recommends that you:

- Maintain at least three copies of business data.
- Store data on at least two different types of storage media.
- Keep one copy of the backups in an off-site location.
- Keep one copy of the media offline or air gapped.
- Ensure all recoverability solutions have zero errors.

This approach uses the same feature-set as 3-2-1 but on top of that you make use of DP Object Verification to check for errors not any of the shown media levels. This gives assurance about the quality of your backups, and it’s properly reported.

4-3-2 Strategy

Your backup strategy may be subscribing to the 4-3-2 rule:

- Four copies of your data.
- Data in three locations (on-prem with you, on-prem with an MSP and stored with a cloud provider).
- Two locations for your data are off-site.

OpenText Trademark Information

Company Details

Company name: OpenText
Place of registration: England and Wales
Registered number: 5134647
Registered address: The Lawn, 22-30 Old Bath Road, Berkshire, RG14 1Q

Learn more at
www.microfocus.com/en-us/products/data-protector-backup-recovery-software/overview

Connect with Us

opentext™