Solution Flyer

opentext™

Secure Backups with Data Protector

Data Protector introduces a security model that improves the security of backup data, reducing the risk of financial and reputational damage to organizations.

Data Protector at a Glance:

- **Minimizes Risk Associated with Data Breaches:**
  Uses advanced security capabilities such as secure peering and in-flight and at-rest encryption to protect backup data.
- **Increases the Security of Backup Data Sets:**
  Verifies backup software credentials and encrypts backup commands, minimizing interference by attackers.
- **Enables Rapid Recovery after a Breach:**
  Uses bare-metal recovery and point-in-time recovery features to speed up data recovery and minimize data loss.

A Missing Link in Data Security

Many organizations may be risking financial and reputational damage by failing to protect their backups from cyber attacks. While these companies have cybersecurity measures protecting their network perimeter, high-profile data breaches have shown that these defenses do not always stop attackers. If an attacker succeeds in bypassing primary security, there may be nothing stopping them from accessing backups.

However, securing backups can be difficult for companies that have a complex backup environment. The more applications, software environments, and locations they use to store backups, the greater the risk that attackers can access data.

For example, a company might have 5 petabytes of backup data distributed on snapshots that are stored on its premises and in backups stored in remote data centers, in a public cloud environment, and at other sites for disaster recovery purposes. The company might also use backup tools built into database applications and custom scripts to back up dozens of other applications running in VMware environments. Attackers could try to exploit vulnerabilities in any of these systems.

A partial solution would be to encrypt backups, making them useless to attackers. However, poorly implemented encryption could slow down mission-critical applications and the overall backup process. In addition, this strategy won't address other security vulnerabilities in backup systems either.

Streamlining Backup Security

A more secure approach to protecting backups is to use a centralized backup solution with a built-in security model. This allows administrators to implement security measures across their entire backup environment.

OpenText™ Data Protector adopts this strategy. It is an enterprise-level backup and recovery solution with several methods of protecting backup data, such as encrypting backups during storage and while they are being transferred. It also secures its own operations by encrypting commands between backup servers and clients.

With built-in advanced disaster recovery capabilities, administrators can create disaster recovery images from existing backups. This enables organizations to streamline the task of restoring the full mission-critical system (operating system, configuration files, and data) in the event of a breach or complete hardware failure, making Data Protector a key tool for protecting data from ransomware.

How Data Protector Secures Backup Data

Encrypts Backups at Rest and in Flight

IT administrators can use Data Protector to encrypt backups. The software achieves this by taking advantage of the encryption capabilities in HPE LTO Tape and StoreOnce devices and Dell EMC Data Domain backup devices.

Administrators can use this capability to stop an unauthorized person accessing information on

a lost or stolen backup drive. For example, they could use the 256-bit Advanced Encryption Standard (AES) or the U.S. Government's Federal Information Processing Standard 140-1 to encrypt backup drives located in remote offices with less physical security. That encryption could prevent a costly data breach if a contractor working at one of the remote offices misplaced a backup drive.

Companies can also use this capability to safeguard critical data while it is being transferred to and from backup devices. Data Protector does this by using the encryption capabilities within backup devices to protect the data while it is in flight. A company could use the Internet Security protocol to protect backups while they are being replicated from one HPE StoreOnce appliance to another, for example.

Protects Backup Operations

In Data Protector backup administrators have a tool that helps to increase the security of backup data sets. That is because Data Protector verifies the credentials of its installation servers, cell managers, and backup clients before they can communicate with each other. Once this secure peering process is complete, backup servers and clients use the Transport Layer Security 1.2 protocol to encrypt their communication. Additionally, only Data Protector cell managers can send commands to server clients enabling a centralized command and execution strategy.

Secure peering is particularly useful in complex and growing backup environments where administrators manage many different clients and regularly install new ones. It stops attackers successfully masquerading as a backup installation server in order to install rogue backup clients and siphon data. It also stops attackers instructing legitimate backup clients to replicate data to rogue servers.

This additional verification also stops attackers interfering with the data protection software installation and upgrade process. This includes Server Message Block Signing, which verifies that no-one has tampered with the installation files that backup installation servers send to clients running Windows. The Secure Shell protocol encrypts this data in Linux environments.

Administrators can also use the REST API to securely connect Data Protector with applications such as Microsoft SQL Server, SAP databases, Oracle databases, file systems, web portals, and virtualization and storage platforms. This enables application owners to use these third-party systems to perform data restores and some other backup operations.

Speeds Up Recovery after a Breach

Data Protector has multiple features that help administrators quickly recover systems after a security breach. For example, the no-cost bare-metal recovery feature enables centralized recovery from or to a physical or virtual system from any backup set. Integrated at the core of Data Protector, OpenText™ Enhanced Automated Disaster Recovery (EADR) provides backup of application data as well as system data including operating system files, drivers, and files required for the initial boot process. Enabled with a simple check box in the Data Protector GUI, EADR includes the necessary image information in full backups for a full system recovery. Backup administrators can also restore data from a specific point in time, rather then relying on daily backups, with the point-in-time recovery feature.

Another key feature is offsite backup to tape. It allows administrators to securely move a copy of backup data off the premises if a security breach has compromised the primary backup in the data center. Data Protector also supports Write Once, Read Many (WORM) LTO tape media, which means once written, data can't be erased. This secures the backups and helps organizations prepare for audits.

These features are particularly useful for companies with mission-critical applications that continually generate lots of data. For example, if an attacker accesses an Oracle database, administrators can instantly restore a snapshot of the database from a storage array to an uncompromised server. Using Data Protector's point-in-time recovery capability, they can choose a snapshot taken on the same day, just one hour before the breach. With this approach, they will lose less data than if they had relied on a backup created the previous evening.

By employing these safeguards, administrators can reduce the risk of losing valuable backup data due to a cyber attack.

Learn more at
www.microfocus.com/dataprotector
www.opentext.com

Connect with Us

opentext™