Fortify your data: Complete air gap protection with OpenText Data Protector

Four layers of defense: Physical, logical, data isolation, and network segmentation. Plus, seamless compliance with GDPR, HIPAA, and beyond.

Benefits

- Comprehensive air gap coverage
- Advanced security features
- Regulatory compliance made simple
- Seamless integration and scalability

Introduction to air gaps

An air gap is a fundamental component of data security strategies, characterized by the physical or logical separation between systems containing sensitive information and other connected networks or environments. This separation acts as a barrier to unauthorized access, safeguarding critical data from potential threats.

Comprehensive air gap coverage

Supports physical, logical, data isolation, and network segmentation for multi-layered protection. There are four primary types of air gaps, each serving a specific purpose in data protection:

1. **Physical air gapping:** Creates tangible barriers that physically isolate systems, ensuring no direct connection exists between sensitive systems and external networks. OpenText™ Data Protector achieves physical separation by ensuring backup environments are isolated from production systems through unified storage solutions and advanced network segmentation tools. This physical separation minimizes the risk of data leaks and unauthorized access.
2. **Logical air gapping:** Uses encryption, access controls, and authentication mechanisms to isolate data within a system, preventing unauthorized internal or external access. OpenText Data Protector provides robust logical isolation via encryption for data at rest and in transit, coupled with granular access controls and multi-factor authentication (MFA).
3. **Data isolation air gap:** Focuses on segregating highly sensitive datasets through secure repositories and advanced data classification features, ensuring only authorized personnel can access critical information. OpenText Data Protector offers secure repositories designed for highly sensitive datasets.
4. **Network segmentation air gap:** Divides networks into smaller, controlled segments with specific access rights, reducing the attack surface and limiting potential threats. OpenText Data Protector includes comprehensive network segmentation capabilities through role-based permissions and monitoring tools.

Advanced security features

OpenText Data Protector ensures strong logical separation by encrypting data both at rest and in transit, while implementing fine-grained access controls and multi-factor authentication to defend against internal and external threats. OpenText Data Protector delivers robust network segmentation through role-based access controls and real-time monitoring, ensuring data flows only within authorized zones to strengthen security and minimize exposure to threats.

Resources

Learn more about OpenText Data Protector ›

Explore the complete OpenText Enterprise Data Backup and Recovery 360 solution ›

Gain insights about the OpenText Device and Data Protection business unit ›

Regulatory compliance made simple

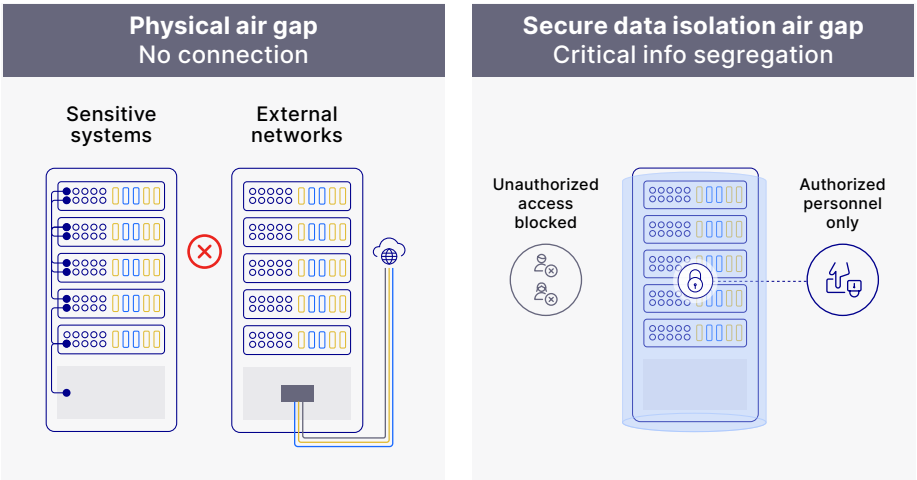
OpenText Data Protector secures highly sensitive data with dedicated repositories and intelligent classification tools, ensuring critical information is protected and regulatory standards like GDPR and HIPAA are consistently met.

Seamless integration and scalability

OpenText Data Protector distinguishes itself by delivering a holistic approach that encompasses all types of air gaps, seamlessly integrating with existing IT infrastructure to provide cost-effective, enterprise-grade security, including robust network segmentation and data classification tools.

Comprehensive solution for various air gap types

OpenText Data Protector's support for physical, logical, data isolation, and network segmentation air gaps, combined with seamless integration and advanced security features, positions it as an all-in-one platform for robust data protection.



Copyright © 2025 Open Text • 11.25 | 260-000420-001

opentext™