How to Successfully Strengthen Data Security

Over the past few years, the cost of data loss due to inadequate protection and more advanced hacking has grown to a more serious level. Small businesses are dealing with several risks associated with securing data: from hacking and other malicious attempts to mounting compliance concerns to address privacy mandated by internal policy and GDPR. It has become even more crucial for businesses to guard their data on top of customer data and intellectual property (IP).

But how do you secure your data in a manner that is less intrusive and more transparent? The key elements of an effective data protection strategy include the hard drives in your data center, inside servers and dedicated storage. Without proper protection, the storage in these devices can be physically removed and forcefully hacked using many of the available data retrieval methods. Proper security methods require an intentional approach to building a data security strategy (also called data-at-rest) for businesses.

Creating an Effective Data-at-Rest Security Approach

To develop a successful data-at-rest security strategy, you'll first want to answer some essential questions:

1. Where is the data located?
2. What is the data's level of sensitivity?
3. What is the best method to keep it secure?
4. How does the data move within the organization, across multiple networks, remote sites or even into the cloud?

The creation of key management systems has helped lessen many of the concerns linked to data-at-rest protection while meeting the need to secure data across the business.

These systems reduce the risks of servers and hard drives potentially walking out of a secure or non-secure location and then being unencrypted by a third-party if keys are in the device being stolen. A central key manager helps you create and manage keys in a secure way while encrypting your business hardware. Key managers leverage and follow a variety of cryptography standards, including FIPS and KMIP. Enterprise Key Managers store keys on a separate, highly available system to avoid keys being taken with devices, such as servers.

More Ways to Protect Data Fast and Scale

If you're looking for another tool to help with transparent, near real-time encryption, consider using self-encrypting drives, also known as SEDs, for your servers. Deploying SED drives makes securing your data quick, thanks to their built-in encryption feature. And SED drives with a key management system helps encryption and decryption become more transparent and faster. Scale your data protection as you scale storage capacity across your data center with enterprise key management.

We offer security capabilities to address data-at-rest protection requirements for businesses. The Dell EMC OpenManage Secure Enterprise Key Manager is embedded in Dell EMC PowerEdge servers and works in combination with leading Key Management Servers. Businesses can scale up to meet demanding data growth while effectively maintaining secure keys for encryption across the enterprise. Our solution is a primary component of Dell EMC OpenManage FlexSelect, providing integrated security features that enable cyber-resiliency across your server infrastructure.

Now you can easily scale up from one drive to many with a dedicated key management solution and meet global compliance security and privacy standards. We're here to support your business with key tools so that you can be sure your customer data stays safe from anywhere in the world.

We Are Ready To Help

Our Dell Technologies Advisors are ready to help you with tailored product solutions designed to keep your business productive.

SPEAK WITH AN ADVISOR TODAY

1800-880-855

DELL Technologies