CRYPTO

How to: Transfer privacy-sensitive data securely to the cloud

Working in the cloud has become an essential part of modern business and personal practices. However, as convenient as cloud storage is, it also presents significant risks if not managed correctly. With cyber threats on the rise and increasingly sophisticated attacks targeting cloud services, the importance of securing sensitive information has never been greater.

Our DataDiode helps you keep privacy-sensitive information safe, by enforcing a one-way data flow. This way, data can move securely from the on-premises network to the cloud for analysis, while completely blocking any data from returning to the secure network.

The challenge

When using cloud storage, organizations must transfer data from their on-premises network to the cloud. The key challenge here is ensuring the integrity and authenticity of the data during transit. This process is vulnerable to several potential threats, such as interception, unauthorized access, and data manipulation.

To address these risks, organizations can employ strong encryption protocols and secure authentication mechanisms. However, balancing security with performance is a challenge, as encryption and other security measures can introduce latency and complexity into the data transfer process.

The solution

To address this challenge, the institution can implement a DataDiode to ensure hardware-based one-way data flow, allowing data to move securely from the on-premises network to the cloud for analysis, while completely blocking any data from returning to the secure network. This way, the integrity of sensitive data is maintained.

How it works

Step 1 DataDiode deployment:

A DataDiode is deployed at the network boundary between the on-premises network and the cloud environment. This hardware device enforces unidirectional data flow, allowing data to be sent to the cloud while preventing any data from being transmitted back to the on-premises network.

Step 2 Data transfer mechanism:

- Data to be analyzed is aggregated and formatted on-premises. It is then transferred through the DataDiode to the cloud environment using secure transmission protocols (such as, SFTP, HTTPS).
- The DataDiode ensures that the transmission path is physically and logically one-way, making it impossible for any data or commands to be sent back to the on-premises network.

Step 3 Cloud environment setup:

- The cloud environment is configured to receive data from the on-premises network for processing. Advanced analytics and ML models run in the cloud to analyze the data.
- Processed results, insights, and analytics are made available within the cloud environment but are not directly transmitted back to the on-premises network. Instead, reports or summaries are manually reviewed and securely transferred if needed.

Step 4 Security controls and monitoring:

- Comprehensive security controls are implemented in the cloud environment, including encryption, access controls, and continuous monitoring to ensure the integrity and confidentiality of data during processing.
- The on-premises network maintains strict access controls, ensuring that only authorized personnel can initiate data transfers through the DataDiode.

The benefits

- **Security at the highest level:** The DataDiode provides a robust security barrier, preventing any data or threats from the cloud environment from penetrating the secure on-premises network.
- **Regulatory compliance:** By ensuring unidirectional data flow, organizations comply with stringent regulatory requirements that mandate the protection of sensitive data.
- **Optimized analytics:** Leveraging cloud-based analytics and ML services enables organizations to process large volumes of data efficiently, gain valuable insights, and improve operational decision-making without compromising security.

Interested? Talk to an expert!

✉ internationalsales@foxcrypto.com

CRYPTO