Best Practices for Data Protection: Using Data Encryption

By: John Gayeski | Winning Strategies ITS

Definition of Data in Transit vs. Data at Rest

Protecting sensitive data both in transit and at rest is critical as attackers find increasingly innovative ways to compromise systems and steal data.

Data in transit, or data in motion, is data actively moving from one location to another such as across the internet or through a private network. Data protection in transit is the protection of this data while it's traveling from network to network or being transferred from a local storage device to a cloud storage device. Effective data protection measures for in transit data are critical, as data is often considered less secure while in motion.

Data at rest is data that is not actively moving from device to device or network to network, such as data stored on a hard drive, laptop, flash drive or is archived/stored in some other way. Data protection at rest aims to secure inactive data stored on any device or network. While data at rest is sometimes considered to be less vulnerable than data in transit, attackers often find data at rest a more valuable target than data in motion. The risk profile for data in transit or data at rest depends on the security measures that are in place to secure data in either state.

The Role of Encryption in Data Protection in Transit and at Rest

Data can be exposed to risks both in transit and at rest and requires protection in both states. As such, there are multiple approaches to protecting data in transit and at rest. Encryption plays a major role in data protection and is a popular tool for securing data both in transit and at rest. For protecting data in transit, organizations often choose to encrypt sensitive data prior to moving and/or use encrypted connections (HTTPS, SSL, TLS, FTPS, etc.) to protect the contents of data in transit. For protecting data at rest, enterprises can simply encrypt sensitive files prior to storing them and/or choose to encrypt the storage drive itself.

Best Practices for Data Protection in Transit and at Rest

Unprotected data, whether in transit or at rest, leaves organizations vulnerable to attack, but there are effective security measures that offer data protection across endpoints and networks to protect data in both states. As mentioned above, one of the most effective data protection methods for both data in transit and data at rest is data encryption.

In addition to encryption, best practices for robust data protection for data in transit and data at rest include the following tips:

- Implement robust network security controls to help protect data in transit. Network security solutions like firewalls and network access control will help secure the networks used to transmit data against malware attacks or intrusions.
- Don't rely on reactive security to protect your valuable data. Instead, use proactive security measures that identify at-risk data and implement effective data protection for data in transit and at rest.
- Choose data protection solutions with policies that enable user prompting, blocking or automatic encryption for sensitive data in transit, such as when files are attached to an email message or moved to cloud storage, removable drives, or transferred elsewhere.
- Create policies for systematically categorizing and classifying all company data, no matter where it resides, in order to ensure that the appropriate data protection measures are applied while data remains at rest and triggered when data classified as at-risk is accessed, used or transferred.
- Finally, if you utilize a public, private, or hybrid cloud provider for storing data or applications, carefully evaluate cloud vendors based on the security measures they offer, but don't rely on the cloud service to secure your data. Imperative questions to ask include: Who has access to your data? How is it encrypted? How often is your data backed up?

While data in transit and data at rest may have slightly different risk profiles, the inherent risk hinges primarily on the sensitivity and value of your data; attackers will attempt to gain access to valuable data whether it's in motion, at rest or actively in use, depending on which state is easiest to breach. That's why a proactive approach including classifying and categorizing data coupled with content, user and context-aware security protocols is the safest and most effective way to protect your most sensitive data in every state.

Know the Laws

Organizations of all sizes must adhere to numerous privacy-related regulations when it comes to safeguarding the personally identifiable information they manage. The top six regulations that impact institutions include: FERPA, HIPAA, HITECH, COPPA, PCI DSS and state specific data breach notifications laws.

Assess the Data

Although there is not a security rule under HIPAA that explicitly requires encryption, it does state that entities should perform a data risk assessment and implement encryption if the evaluation indicates that encryption would be a "reasonable and appropriate" safeguard. If an organization decides not to encrypt electronic protected health information (ePHI), the institution must document and justify that decision and then implement an "equivalent alternative measure."

Determine the Required or Needed Level of Encryption

The U.S. Department of Health & Human Services (HHS) turns to the National Institute of Standards and Technology (NIST) for recommended encryption level practices. HHS and NIST have both produced robust documentation for adhering to HIPAA's Security Rule. NIST Special Publication 800-111 takes a somewhat broad approach to encryption on end-user devices. In a nutshell, it states that when there's even a remote possibility of risk, encryption needs to be in place, and FIPS 140-2, which incorporates the Advanced Encryption Standard (AES) into its protocols, is an ideal choice. FIPS 140-2 helps entities ensure that PII is "rendered unusable, unreadable or indecipherable to unauthorized individuals." A device that meets FIPS 140-2 requirements possesses a cryptographic erase function that "leverages the encryption of target data by enabling sanitization of the target data's encryption key, leaving only the ciphertext remaining on the media, effectively sanitizing the data."

Be Mindful of Sensitive Data Transfers and Remote Access

Encryption must extend beyond laptops and backup drives. Communicating or sending data over the internet needs Transport Layer Security (TLS), a protocol for transmitting data over a network, and AES encryption. When an employee accesses an institution's local network, a secure VPN connection is essential when ePHI is involved. Also, before putting files on a physical external device for transfer between systems or offices, it is imperative that the device is encrypted and meets FIPS 140-2 requirements to avoid potential violations.