What Is Data Encryption?

Data encryption is a security method that translates data into an unreadable format so that it's protected. Only users with the correct decryption keys or passwords can convert the secure text back into readable data, called plaintext.

Data encryption is used to protect sensitive information, such as personal data, financial records, and intellectual property. It's also used to secure communications over the internet and protect data stored on devices like smartphones and laptops. However, there's more to data encryption than simply scrambling data: Encryption also allows enterprises to authenticate the source of data requests, verify permissions, and ensure data integrity.

Why Use Data Encryption?

The goal of data encryption has been the same: to prevent important information from falling into the wrong hands and ensure the authenticity of received data. In decades past, encryption might have referred mostly to methods for protecting vital national security data—data that typically stayed in one place and wasn't mobile. Today, data is constantly in motion and continually being shared, adding to the challenges of safeguarding it.

Encryption doesn't just encode data: It also adds metadata that allows the decryption step to verify the source of the data and creates a hash value based on the data that can be used by the recipient to detect whether the data has been altered or substituted. A hash value is a unique string of characters algorithmically derived from the data at encryption. After receipt of the data, the same hash function can be used to create a new hash value, and if the values match, data integrity has been maintained.

Where Can You Use Data Encryption?

Encryption can be applied virtually anywhere in the data lifecycle—for example, as files are created and databases updated by software and applications; as data is sent over a public or private network, at rest in storage on premises or in the cloud; and at the individual file level or on entire disks or partitions. Email applications have their own encryption protocols. End-to-end encryption (E2EE) assures protection even as data is moved through various servers and sent from one point to another. This is the encryption used by Apple and other messaging providers for messaging that's billed as "100% secure."

Types of Data Encryption

Data encryption typically falls into these categories:

Symmetric encryption algorithms encrypt and decrypt through the use of a single key possessed by both sender and receiver. This is a straightforward method of encryption that's typically used for large amounts of data at rest or when the data will only be shared within a closed system.

Asymmetric encryption uses separate public or private keys—allowing anyone to use the public key to encrypt data while requiring the private key to decrypt. Asymmetric encryption is used for safe transmission of data over public systems and is the encryption method underneath online transactions, secure email, and cloud-based data sharing. Public key infrastructure (PKI) is the widely used system for creating, distributing, authenticating, and securing public and private key sets. Asymmetric encryption can result in larger file sizes, adding another important variable to data management.

Homomorphic encryption allows computations, scanning, and analysis of encrypted data without making it fully accessible through decryption. It has become more important recently as a way of solving the data management challenges of extracting value from data and allowing AI models to ingest encrypted data without privacy concerns.

Where Is Data Encryption Headed?

Encryption algorithms continue to evolve as computing power grows and the needs of modern cybersecurity progress. Today's encryption algorithms are primarily math-based. But on the horizon is quantum encryption, which secures data with quantum mechanics instead of mathematics. Quantum encryption has the potential to create cryptographic keys that are theoretically impervious to brute force attacks. (Quantum computing may also have the power to break encryption—stay tuned.)

AI is also being used to improve encryption and has tremendous potential to revolutionize data security. AI-based encryption systems can learn to become more secure by incorporating the latest threat intelligence. The systems can also optimize storage by setting encryption algorithms dynamically based on network traffic, storage availability, or predicted activity.

Data Encryption Vulnerabilities

While data encryption is a powerful security method, it does have some vulnerabilities.

Attackers use encryption too. The same qualities that make encryption a powerful tool for securing data also make it an ideal technique for cybercriminals, especially those deploying ransomware. Data does not need to be stolen to force a ransom payment, but rather, simply encrypted. When victims pay the ransom, the threat actors provide the decryption keys, a very efficient process for those launching ransom attacks en masse. A smart ransomer will provide a hash value so that the victim can be convinced that data is complete and unaltered.

Quantum computing offers stronger encryption and more ways to break encryption. As mentioned above, quantum computing offers great potential for more secure encryption. But criminals love to adopt cutting-edge technology, which means traditionally encrypted data could become vulnerable if hackers gain access to quantum technology first.

Poor key management endangers data. Encryption could provide a false sense of security if decryption keys are not well-secured too. Smart cybercriminals might focus on stealing the keys rather than simply stealing data. For this reason, it’s essential to have a system, preferably dedicated software, for creating, managing, and disposing of keys.

Side-channel attacks can ferret out keys. Side-channel attacks are exploits created through illicit observation of system metadata, along with timing and other contextual information, to infer the contents of encrypted material or help gain access to cryptographic keys.

Brute force attacks can break encryption. In a brute force attack, perpetrators break encryption by systematically entering possible encryption keys until they discover the correct one. While modern, strong encryption is generally capable of repelling such attacks, advances in computing power and the rise of new technologies such as AI and quantum computing could put older encryption methods at risk.

Data Encryption and Privacy: How Much Encryption Is Too Much?

One of the thorniest issues facing the technology industry is how to maintain privacy through encryption while providing law enforcement access to data of suspected criminals. In the 2021 case of the San Bernardino shooting, law enforcement officials sought access to a suspect's iPhone to aid in their investigation. Apple refused to break the phone user's data encryption, so law enforcement used a private contractor to help gain access to the phone's data.

In February 2025, the British government announced that it would require Apple to provide access to cloud data for all of its users worldwide. Sources say that Apple is likely to stop offering encrypted storage in the U.K. Homomorphic encryption has been discussed as a possible solution to allow selective scanning of encrypted data. The privacy versus security dilemma is likely to continue as a flashpoint among law enforcement, governments, and technology users.

In today's landscape, robust encryption is no longer optional—it's the foundation of trust and compliance. Pure Storage exemplifies this principle by integrating enterprise-grade security with operational efficiency. Pure Storage solutions feature always-on AES-256 data-at-rest encryption that requires zero configuration, FIPS 140-2 compliance, and seamless integration with host-level encryption tools like Thales Vormetric Transparent Encryption—all while preserving storage efficiency through innovations like EncryptReduce™. By automating key management with multi-layered, self-rotating keys and maintaining certifications, Pure Storage eliminates the traditional trade-offs between security and performance. Whether safeguarding healthcare records or financial data, Pure Storage ensures encryption isn't just a checkbox but a frictionless layer of cyber resilience, empowering organizations to focus on innovation rather than infrastructure complexity.

Learn what steps enterprise CISOs are taking to stay ahead of evolving cyber threats. Read "Perfecting Cyber Resilience: The CISO Blueprint for Success."