Why is data security important?

Data security is the practice of protecting digital information from unauthorized access, corruption or theft throughout its entire lifecycle. It's a concept that encompasses every aspect of information security from the physical security of hardware and storage devices to administrative and access controls, as well as the logical security of software applications. It also includes organizational policies and procedures.

Types of data security

Encryption

Using an algorithm to transform normal text characters into an unreadable format, encryption keys scramble data so that only authorized users can read it. File and database encryption solutions serve as a final line of defense for sensitive volumes by obscuring their contents through encryption or tokenization. Most solutions also include security key management capabilities.

Data erasure

More secure than standard data wiping, data erasure uses software to completely overwrite data on any storage device. It verifies that the data is unrecoverable.

Data masking

By masking data, organizations can allow teams to develop applications or train people using real data. It masks personally identifiable information (PII) where necessary so that development can occur in environments that are compliant.

Data security strategies

Physical security of servers and user devices

Regardless of whether your data is stored on-premises, in a corporate data center, or in the public cloud, you need to ensure that facilities are secured against intruders and have adequate fire suppression measures and climate controls in place. A cloud provider will assume responsibility for these protective measures on your behalf.

Access management and controls

The principle of “least-privilege access” should be followed throughout your entire IT environment. This means granting database, network, and administrative account access to as few people as possible, and only those who absolutely need it to get their jobs done.

Application security and patching

All software should be updated to the latest version as soon as possible after patches or new versions are released.

Backups

Maintaining usable, thoroughly tested backup copies of all critical data is a core component of any robust data security strategy. In addition, all backups should be subject to the same physical and logical security controls that govern access to the primary databases and core systems.

Employee education

Training employees in the importance of good security practices and password hygiene and teaching them to recognize social engineering attacks transforms them into a “human firewall” that can play a critical role in safeguarding your data.

Network and endpoint security monitoring and controls

Implementing a comprehensive suite of threat management, detection, and response tools and platforms across your on-premises environment and cloud platforms can mitigate risks and reduce the probability of a breach.

Data security trends

AI

AI amplifies the ability of a data security system because it can process large amounts of data. Cognitive computing, a subset of AI, performs the same tasks as other AI systems but it does so by simulating human thought processes. In data security, this allows for rapid decision-making in times of critical need.

Multicloud security

The definition of data security has expanded as cloud capabilities grow. Now organizations need more complex solutions as they seek protection for not only data, but applications and proprietary business processes that run across public and private clouds.

Quantum

A revolutionary technology, quantum promises to upend many traditional technologies exponentially. Encryption algorithms will become much more faceted, increasingly complex and much more secure.

How data security and other security facets interact

Achieving enterprise-grade data security

The key to applying an effective data security strategy is adopting a risk-based approach to protecting data across the entire enterprise. Early in the strategy development process, taking business goals and regulatory requirements into account, stakeholders should identify one or two data sources containing the most sensitive information, and begin there. After establishing clear and tight policies to protect these limited sources, they can then extend these best practices across the rest of the enterprise's digital assets in a prioritized fashion. Implemented automated data monitoring and protection capabilities can make best practices far more readily scalable.

Data security and the cloud

Securing cloud-based infrastructures requires a different approach than the traditional model of situating defenses at the network's perimeter. It demands comprehensive cloud data discovery and classification tools, plus ongoing activity monitoring and risk management. Cloud monitoring tools can sit between a cloud provider's database-as-a-service (DBaaS) solution and monitor data in transit or redirect traffic to your existing security platform. This allows for policies to be applied uniformly no matter where the data resides.

Data security and BYOD

The use of personal computers, tablets, and mobile devices in enterprise computing

environments is on the rise despite security leaders' well-founded concerns about the risks that this practice can pose. One way of improving bring your own device (BYOD) security is by requiring employees who use personal devices to install security software to access corporate networks, thus enhancing centralized control over and visibility into data access and movement. Another strategy is to build an enterprise-wide, security-first mindset, encouraging employees to utilize strong passwords, multi-factor authentication, regular software updates, and device backups, along with data encryption by teaching them the value of these actions.