**TEXT**

**DATA SECURITY**

**[Data Security](https://www.imperva.com/learn/data-security/" \t "_self)** **Essentials Regulation & Compliance**

***What is Data Security?***



Data security is the process of protecting corporate data and preventing data loss through unauthorized access. This includes protecting your data from attacks that can encrypt or destroy data, such as [ransomware](https://www.imperva.com/learn/application-security/ransomware/), as well as attacks that can modify or corrupt your data. Data security also ensures data is available to anyone in the organization who has access to it.

Some industries require a high level of data security to comply with data protection regulations. For example, organizations that process payment card information must use and store payment card data securely, and healthcare organizations in the USA must secure private health information (PHI) in line with the [HIPAA](https://www.imperva.com/learn/data-security/hipaa-privacy-rule/) standard.

But even if your organization is not subject to a regulation or compliance standard, the survival of a modern business depends on data security, which can impact both the organization’s key assets and private data belonging to its customers.

***Why is Data Security Important?***



The Ponemon Institute’s Cost of Data Breach Study found that on average, the damage caused by a data breach in the USA was $8 million. 25,575 user accounts were impacted in the average data incident, which means that beyond financial losses, most incidents lead to loss of customer trust and damage to reputation.

Lawsuits, settlements, and fines related to data breaches are also on the rise, with many governments introducing more stringent regulations around data privacy. Consumers have much more extensive rights, especially in the EU, California, and Australia, with the introduction of [GDPR](https://www.imperva.com/learn/data-security/gdpr/), CCPA, APP, and CSP234.

Companies operating in regulated industries are affected by additional standards, such as HIPAA for healthcare organizations in the USA, and [PCI/DSS](https://www.imperva.com/learn/data-security/pci-dss-certification/) for organizations processing credit card data.

In the past decade, [social engineering](https://www.imperva.com/learn/application-security/social-engineering-attack/), ransomware and [advanced persistent threats](https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/) (APTs) are on the rise. These are threats that are difficult to defend against and can cause catastrophic damage to an organization’s data.

There is no simple solution to data security—just adding another security solution won’t solve the problem. IT and information security teams must actively and creatively consider their [data protection](https://www.imperva.com/learn/data-security/data-protection/) challenges and cooperate to improve their security posture. It is also critical to evaluate the cost of current security measures, their contribution to data security, and the expected return on investment from additional investments.

***Data Security Risks***



Below are several common issues faced by organizations of all sizes as they attempt to secure sensitive data.

***Accidental Exposure***



A large percentage of [data breaches](https://www.imperva.com/learn/data-security/data-breach/) are not the result of a malicious attack but are caused by negligent or accidental exposure of [sensitive data](https://www.imperva.com/learn/data-security/sensitive-data/). It is common for an organization’s employees to share, grant access to, lose, or mishandle valuable data, either by accident or because they are not aware of security policies.

This major problem can be addressed by employee training, but also by other measures, such as [data loss prevention](https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/) (DLP) technology and improved [access controls](https://www.imperva.com/learn/data-security/access-control-list-acl/).

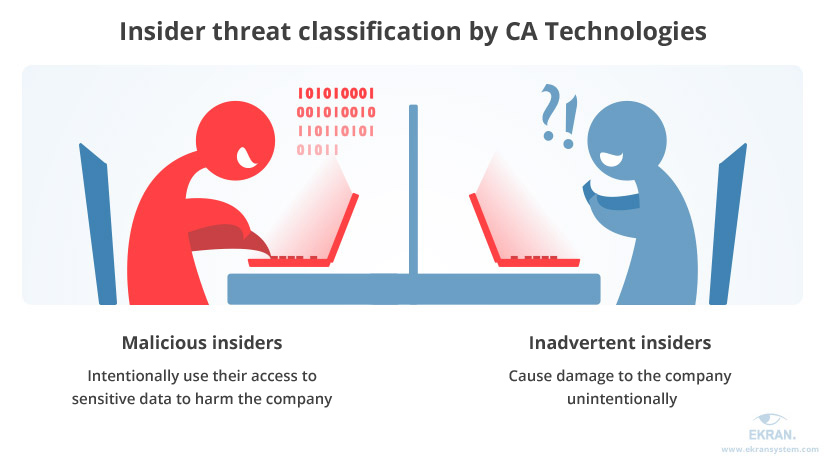
***Phishing and Other Social Engineering Attacks***



Social engineering attacks are a primary vector used by attackers to access sensitive data. They involve manipulating or tricking individuals into providing private information or access to privileged accounts.

[Phishing](https://www.imperva.com/learn/application-security/phishing-attack-scam/) is a common form of social engineering. It involves messages that appear to be from a trusted source, but in fact are sent by an attacker. When victims comply, for example by providing private information or clicking a malicious link, attackers can compromise their device or gain access to a corporate network.

***Insider Threats***



[Insider threats](https://www.imperva.com/learn/application-security/insider-threats/) are employees who inadvertently or intentionally threaten the security of an organization’s data. There are three types of insider threats:

* **Non-malicious insider**—these are users that can cause harm accidentally, via negligence, or because they are unaware of security procedures.
* **Malicious insider**—these are users who actively attempt to steal data or cause harm to the organization for personal gain.
* **Compromised insider**—these are users who are not aware that their accounts or credentials were compromised by an external attacker. The attacker can then perform malicious activity, pretending to be a legitimate user.

***Ransomware***



Ransomware is a major threat to data in companies of all sizes. Ransomware is [malware](https://www.imperva.com/learn/application-security/malware-detection-and-removal/) that infects corporate devices and encrypts data, making it useless without the decryption key. Attackers display a ransom message asking for payment to release the key, but in many cases, even paying the ransom is ineffective and the data is lost.

Many types of ransomware can spread rapidly, and infect large parts of a corporate network. If an organization does not maintain regular backups, or if the ransomware manages to infect the backup servers, there may be no way to recover.

***Data Loss in the Cloud***



Many organizations are moving data to the cloud to facilitate easier sharing and collaboration. However, when data moves to the cloud, it is more difficult to control and prevent data loss. Users access data from personal devices and over unsecured networks. It is all too easy to share a file with unauthorized parties, either accidentally or maliciously.

***Common Data Security Solutions and Techniques***



There are several technologies and practices that can improve data security. No one technique can solve the problem, but by combining several of the techniques below, organizations can significantly improve their security posture.

***Data Discovery and Classification***



Modern IT environments store data on servers, endpoints, and cloud systems. Visibility over data flows is an important first step in understanding what data is at risk of being stolen or misused. To properly protect your data, you need to know the type of data, where it is, and what it is used for. [Data discovery](https://www.imperva.com/learn/data-security/data-discovery/) and classification tools can help.

Data detection is the basis for knowing what data you have. [Data classification](https://www.imperva.com/learn/data-security/data-classification/) allows you to create scalable security solutions, by identifying which data is sensitive and needs to be secured. Data detection and classification solutions enable tagging files on endpoints, file servers, and cloud storage systems, letting you visualize data across the enterprise, to apply the appropriate security policies.

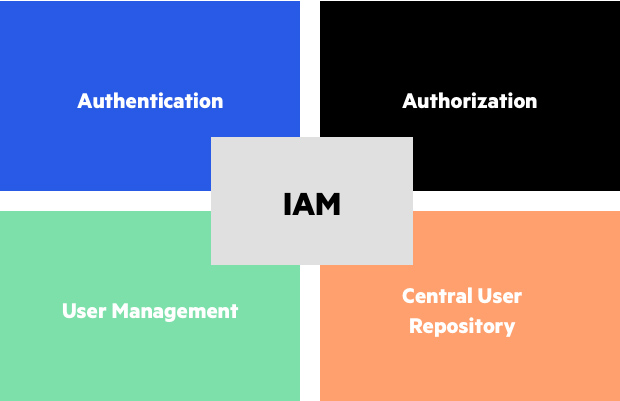
***Data Masking***



Data masking lets you create a synthetic version of your organizational data, which you can use for software testing, training, and other purposes that don’t require the real data. The goal is to protect data while providing a functional alternative when needed.

Data masking retains the data type, but changes the values. Data can be modified in a number of ways, including encryption, character shuffling, and character or word substitution. Whichever method you choose, you must change the values in a way that cannot be reverse-engineered.

***Identity Access Management***



[Identity and Access Management](https://www.imperva.com/learn/data-security/iam-identity-and-access-management/) (IAM) is a business process, strategy, and technical framework that enables organizations to manage digital identities. IAM solutions allow IT administrators to control user access to sensitive information within an organization.

Systems used for IAM include single sign-on systems, [two-factor authentication](https://www.imperva.com/learn/application-security/2fa-two-factor-authentication/), multi-factor authentication, and privileged access management. These technologies enable the organization to securely store identity and profile data, and support governance, ensuring that the appropriate access policies are applied to each part of the infrastructure.

***Data Encryption***



[Data encryption](https://www.imperva.com/learn/data-security/data-encryption/) is a method of converting data from a readable format (plaintext) to an unreadable encoded format (ciphertext). Only after decrypting the encrypted data using the decryption key, the data can be read or processed.

In public-key cryptography techniques, there is no need to share the decryption key – the sender and recipient each have their own key, which are combined to perform the encryption operation. This is inherently more secure.

Data encryption can prevent hackers from accessing sensitive information. It is essential for most security strategies and is explicitly required by many compliance standards.

***Data Loss Prevention (DLP)***



To prevent data loss, organizations can use a number of safeguards, including backing up data to another location. Physical redundancy can help protect data from natural disasters, outages, or attacks on local servers. Redundancy can be performed within a local data center, or by replicating data to a remote site or cloud environment.

Beyond basic measures like backup, DLP software solutions can help protect organizational data. DLP software automatically analyzes content to identify sensitive data, enabling central control and enforcement of data protection policies, and alerting in real-time when it detects anomalous use of sensitive data, for example, large quantities of data copied outside the corporate network.

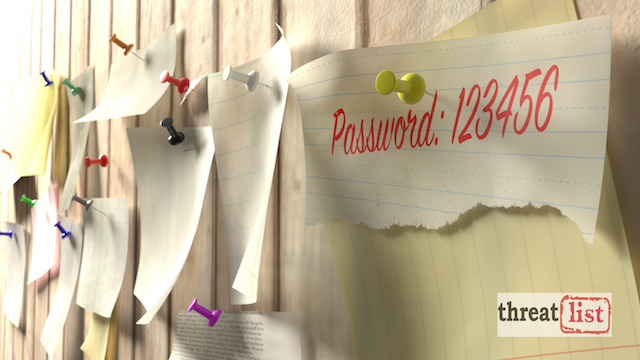
***Governance, Risk, and Compliance (GRC)***



GRC is a methodology that can help improve data security and compliance:

* **Governance** creates controls and policies enforced throughout an organization to ensure compliance and data protection.
* **Risk**involves assessing potential cybersecurity threats and ensuring the organization is prepared for them.
* **Compliance** ensures organizational practices are in line with regulatory and industry standards when processing, accessing, and using data.

***Password Hygiene***

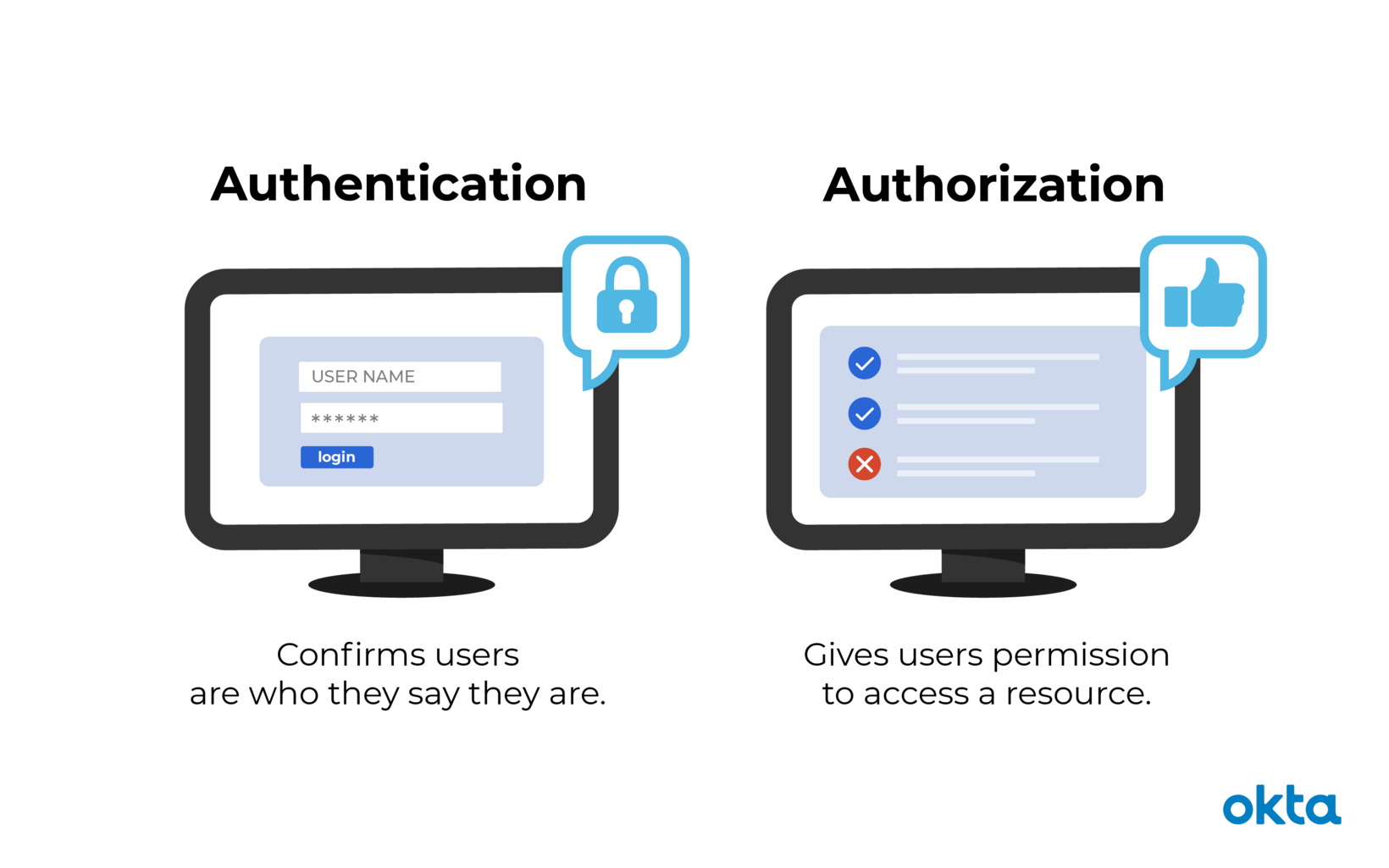


One of the simplest best practices for data security is ensuring users have unique, strong passwords. Without central management and enforcement, many users will use easily guessable passwords or use the same password for many different services. Password spraying and other [brute force attacks](https://www.imperva.com/learn/application-security/brute-force-attack/) can easily compromise accounts with weak passwords.

A simple measure is enforcing longer passwords and asking users to change passwords frequently. However, these measures are not enough, and organizations should consider multi-factor authentication (MFA) solutions that require users to identify themselves with a token or device they own, or via biometric means.

Another complementary solution is an enterprise password manager that stores employee passwords in encrypted form, reducing the burden of remembering passwords for multiple corporate systems, and making it easier to use stronger passwords. However, the password manager itself becomes a security vulnerability for the organization.

***Authentication and Authorization***



Organizations must put in place strong authentication methods, such as OAuth for web-based systems. It is highly recommended to enforce multi-factor authentication when any user, whether internal or external, requests sensitive or personal data.

In addition, organizations must have a clear authorization framework in place, which ensures that each user has exactly the access rights they need to perform a function or consume a service, and no more. Periodic reviews and automated tools should be used to clean up permissions and remove authorization for users who no longer need them.

***Data Security Audits***



The organization should perform security audits at least every few months. This identifies gaps and vulnerabilities across the organizations’ security posture. It is a good idea to perform the audit via a third-party expert, for example in a penetration testing model. However, it is also possible to perform a security audit in house. Most importantly, when the audit exposes security issues, the organization must devote time and resources to address and remediate them.

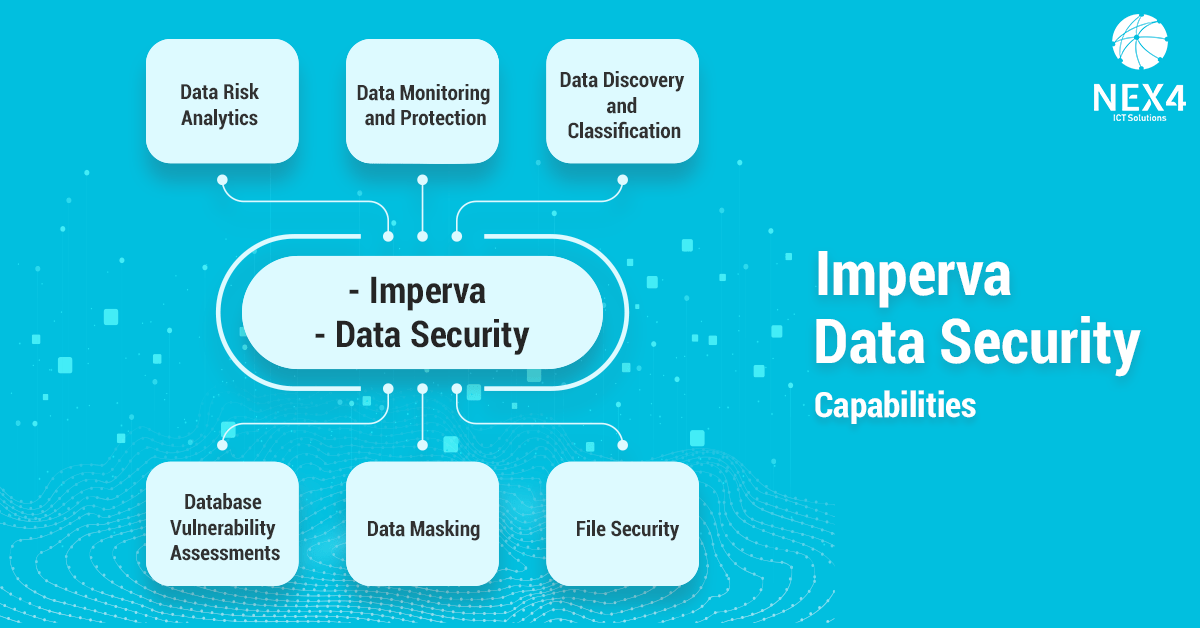
***Anti-Malware, Antivirus, and Endpoint Protection***



Malware is the most common vector of modern cyberattacks, so organizations must ensure that endpoints like employee workstations, mobile devices, servers, and cloud systems, have appropriate protection. The basic measure is antivirus software, but this is no longer enough to address new threats like file-less attacks and unknown [zero-day](https://www.imperva.com/learn/application-security/zero-day-exploit/) malware.

Endpoint protection platforms (EPP) take a more comprehensive approach to endpoint security. They combine antivirus with a machine-learning-based analysis of anomalous behavior on the device, which can help detect unknown attacks. Most platforms also provide endpoint detection and response (EDR) capabilities, which help security teams identify breaches on endpoints as they happen, investigate them, and respond by locking down and reimaging affected endpoints.

***Data Security with Imperva***



Imperva’s data security solution protects your data wherever it lives—on-premises, in the cloud, and in hybrid environments. It also provides security and IT teams with full visibility into how the data is being accessed, used, and moved around the organization.

Our comprehensive approach relies on multiple layers of protection, including:

* **Database firewall**—blocks [SQL injection](https://www.imperva.com/learn/application-security/sql-injection-sqli/) and other threats, while evaluating for known [vulnerabilities](https://www.imperva.com/learn/application-security/cve-cvss-vulnerability/).
* **[User rights management](https://www.imperva.com/learn/data-security/privileged-user-monitoring/)**—monitors data access and activities of privileged users to identify excessive, inappropriate, and unused privileges.
* **Data masking and encryption**—obfuscates sensitive data so it would be useless to the bad actor, even if somehow extracted.
* **[Data loss prevention](https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/) (DLP)**—inspects data in motion, at rest on servers, in cloud storage, or on endpoint devices.
* **[User behavior analytics](https://www.imperva.com/learn/data-security/ueba-user-and-entity-behavior-analytics/)**—establishes baselines of data access behavior, uses machine learning to detect and alert on abnormal and potentially risky activity.
* **[Data discovery and classification](https://www.imperva.com/learn/data-security/data-discovery/)**—reveals the location, volume, and context of data on-premises and in the cloud.
* **Database activity monitoring**—monitors relational databases, data warehouses, big data, and mainframes to generate real-time alerts on policy violations.
* **Alert prioritization**—Imperva uses AI and machine learning technology to look across the stream of security events and prioritize the ones that matter most.