Cybersecurity Basics - CS101

educative

Introduction to Cybersecurity

Cybersecurity Terminology

Cybersecurity
It is a discipline to protect data, hardware, software, and networked systems from cyber attackers and malicious users.

Threat
It's a risk that can harm a computer system or network, making it partially or completely unavailable, or compromise the confidentiality and integrity of data.

Vulnerability
It's a weakness in hardware, software, or a process that a threat can exploit.

Malicious attack
It's a deliberate action that seeks to disrupt or damage a computer system, network, or data, or tries to gain unauthorized access to them.

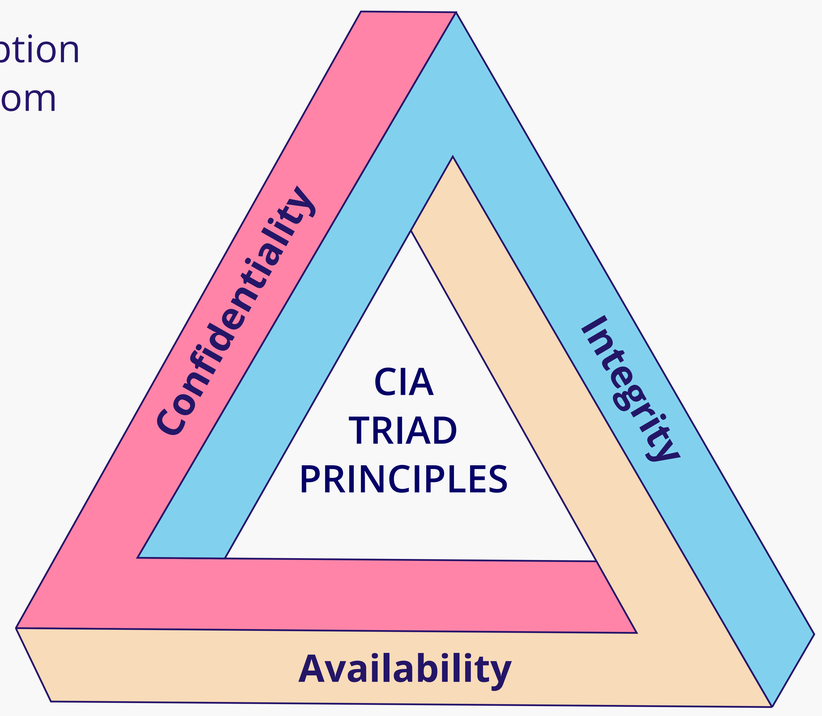
CIA Triad Principles

The CIA triad is a guiding model in information security.

Confidentiality
Only authorized parties can access sensitive information, achieved through encryption and strict access controls. This ensures that data remains private and protected from unauthorized access.
Achieved via: Encryption and access control

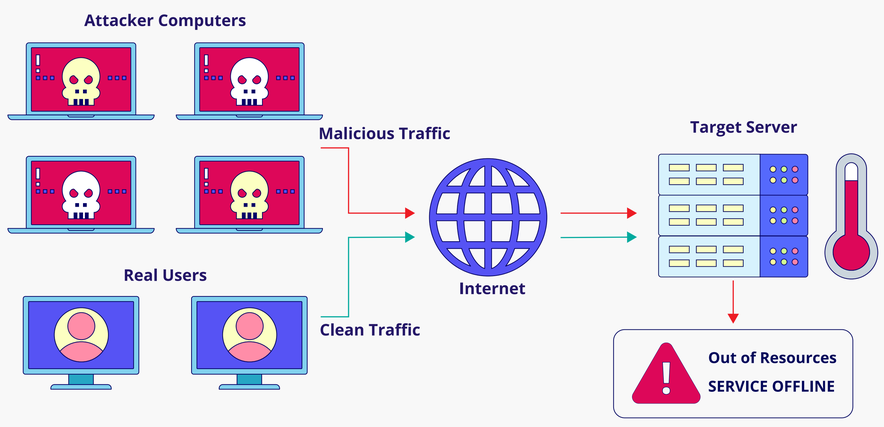
Integrity
Only authorized parties can insert, update, or delete sensitive information. Both sender and receiver should be able to verify that there has been no unauthorized tampering.
Achieved via: Digital signatures and hash digests

Availability
Outages and disruptions should be prevented—data and services should consistently be available on-demand to authorized users.
Achieved via: Backup and redundancy



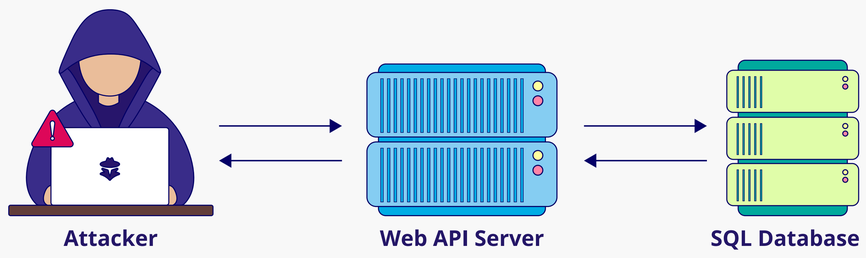
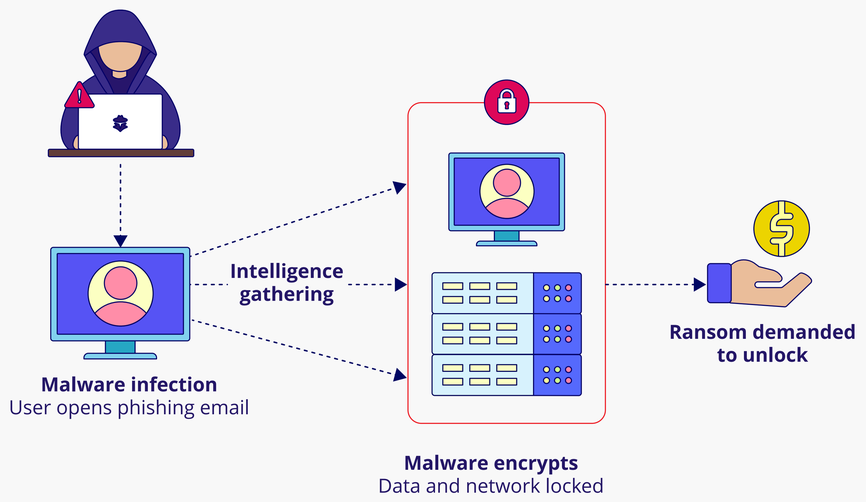
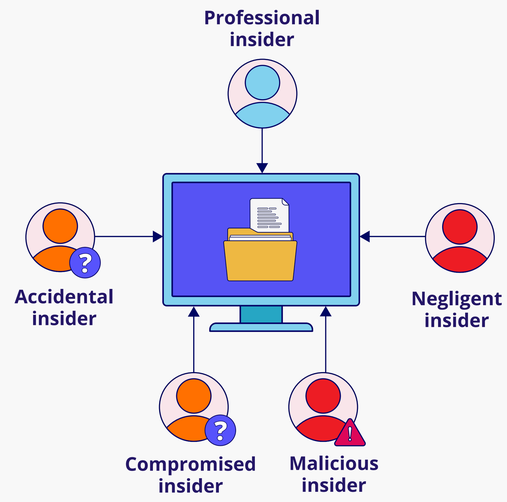
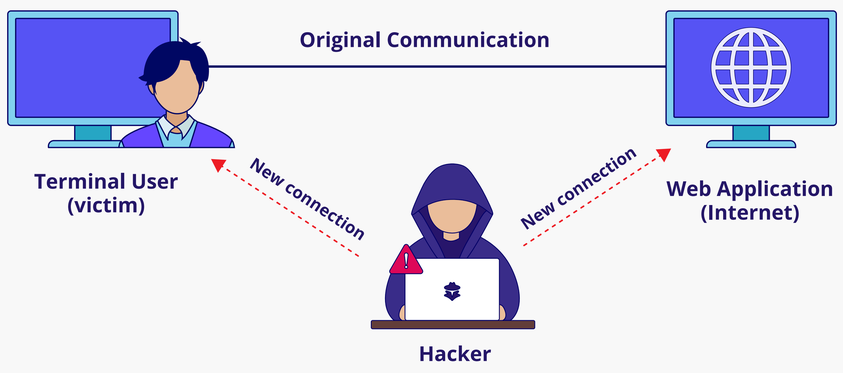
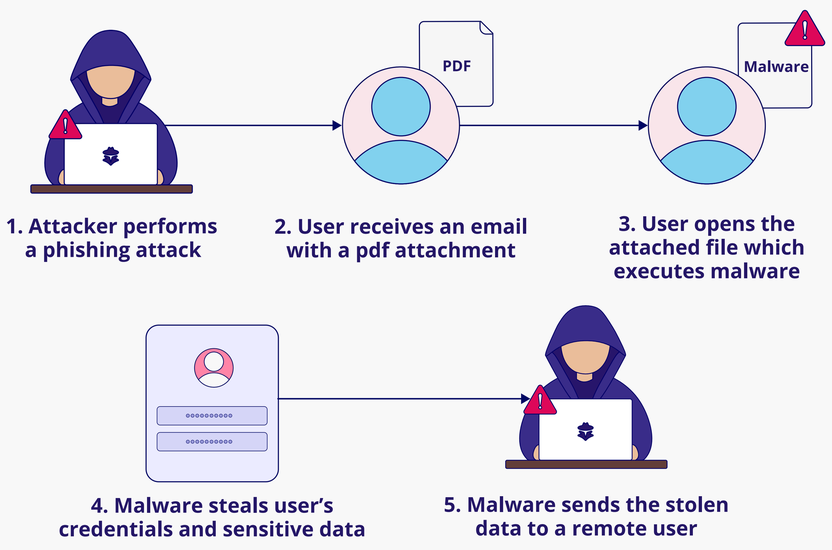
Note: Besides the CIA triad, two other critical security elements in cybersecurity are authenticity and nonrepudiation. Authenticity ensures that information originates from a trusted source and a malicious user shouldn't be able to impersonate that trusted source. It can be ensured using digital certificates and access control techniques like logins and passwords. Non-repudiation ensures that individuals or entities cannot deny their involvement in a transaction or communication. It can be achieved using digital signatures and audit logs.

Common Cyber Threats

Type of Threat	Visual Threat Depiction	Description
DDoS Attack		Involves flooding a server or a network with excessive traffic to overwhelm its capacity and crash it or prevent it from serving legitimate requests.
Malware		Involves installing software to steal or damage the data, or gain control of the system resources. The list includes viruses, spyware, worms, and more.

Cybersecurity Basics - CS101

educative

Type of Threat	Visual Threat Depiction	Description
SQL Injection		Involves inserting a malicious SQL code into a vulnerable website's input field in such a manner that it gets executed by the web server, and allows an attacker to access, modify, or delete data from its database.
Ransomware		Involves making a system unusable and data inaccessible by encrypting the files and demanding a ransom in exchange for the decryption key.
Insider Threats		Trusted individuals within an organization cause harm by misusing their access. The malicious insider tricks the negligent insider and misuses the access.
Man-in-the-Middle (MitM) Attacks		Involves secretly reading or altering communications.
Social Engineering		Involves manipulating users to gain access and control of confidential information or perform actions that compromise security. An example is phishing, where attackers disguise themselves as trustworthy entities and trick individuals into revealing sensitive information like passwords and credit card numbers.

Common Cyber Threats

User and Access Management

Password management

Strong passwords should be used to secure access to sensitive information. Here are a few tips for creating a strong password:

- **Password length:** Use a password with a minimum length of 12 characters.
- **Password complexity:** Use a mix of uppercase letters, lowercase letters, numbers, and special characters while choosing your password.
- **Avoid patterns:** Avoid predictable sequences or easily guessable patterns.
- **Unique password:** Use different passwords for different accounts.
- **Unpredictable password:** Avoid using personal information like names and birthdays or common words that could be easily guessed.
- **Change password frequently:** Change passwords periodically, especially for sensitive accounts.

Authentication

Ensures the verification of a user's identity before granting access to resources. Here are a few common examples:

- **Password-based authentication:** Verify users through usernames and passwords, which they must provide correctly to gain access.
- **Biometric authentication:** Verify users through unique biological traits such as fingerprints, voice, or facial recognition.
- **Token-based authentication:** Verify users through digital or physical tokens like smart cards or mobile devices.
- **Single Sign-On (SSO):** Enable users to authenticate once by logging into the system and getting access to multiple applications without having to reenter the passwords for each application. For example, after logging into your email, you can quickly access your calendar, online storage, and collaboration tools with just one click, without needing to enter the credentials again.

Authorization

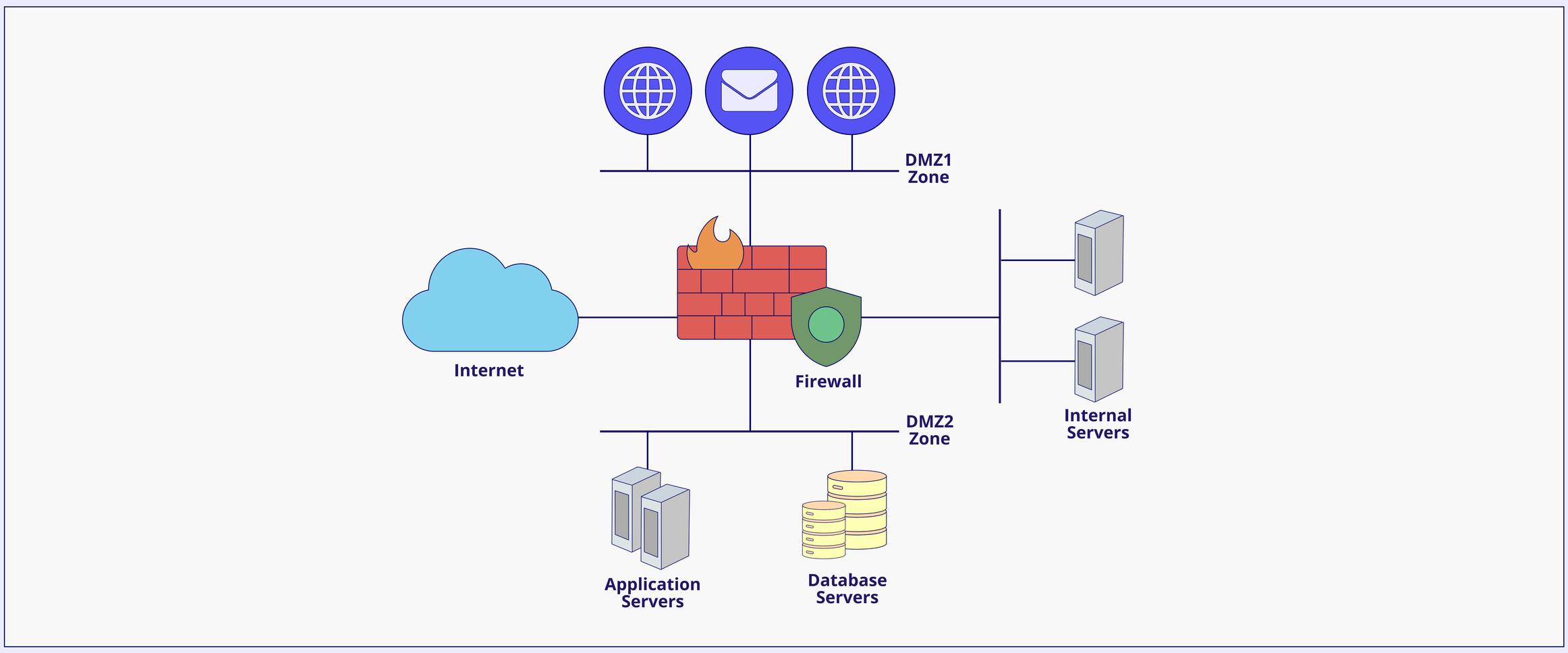
Controls the actions that the users are permitted to perform once they have been authenticated. Here are a few examples:

- **Role-based Access Control (RBAC):** Assigning permissions based on predefined roles ensures users have appropriate access based on their organizational roles. For example, admins and users will have access based on their roles.
- **Attribute-based Access Control (ABAC):** Determining access permissions dynamically by evaluating various attributes, such as user and resource attributes. For example, analysts in the finance department can access detailed financial reports only if they have the attributes Finance Department and Senior Analyst.
- **Mandatory Access Control (MAC):** Enforcing strict access controls based on security labels assigned to resources and users, typically used in high-security environments like the government. The security labels for resources can include top secret, secret, and confidential.
- **Discretionary Access Control (DAC):** Allowing resource owners to decide who can access their resources based on their own judgment and preferences. For example, a professor can decide whether students can see the teaching material and who is supposed to access it.

System and Network Security

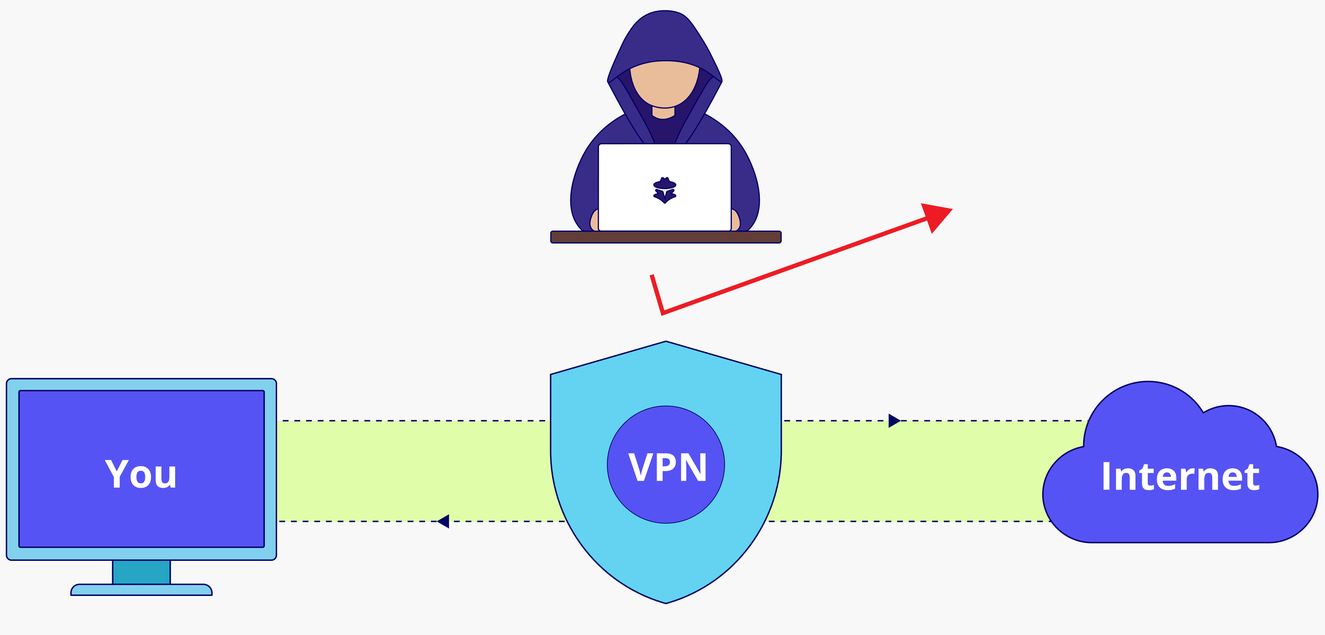
Network Segmentation

Divides networks into segments to control and secure traffic flow. This approach typically involves implementing firewalls and VLANs to enforce security policies and restrict access between different parts of the network. For example, the leadership's network might be segmented in a university setting to ensure higher security and dedicated resources, separate from networks accessible to students and outsiders.



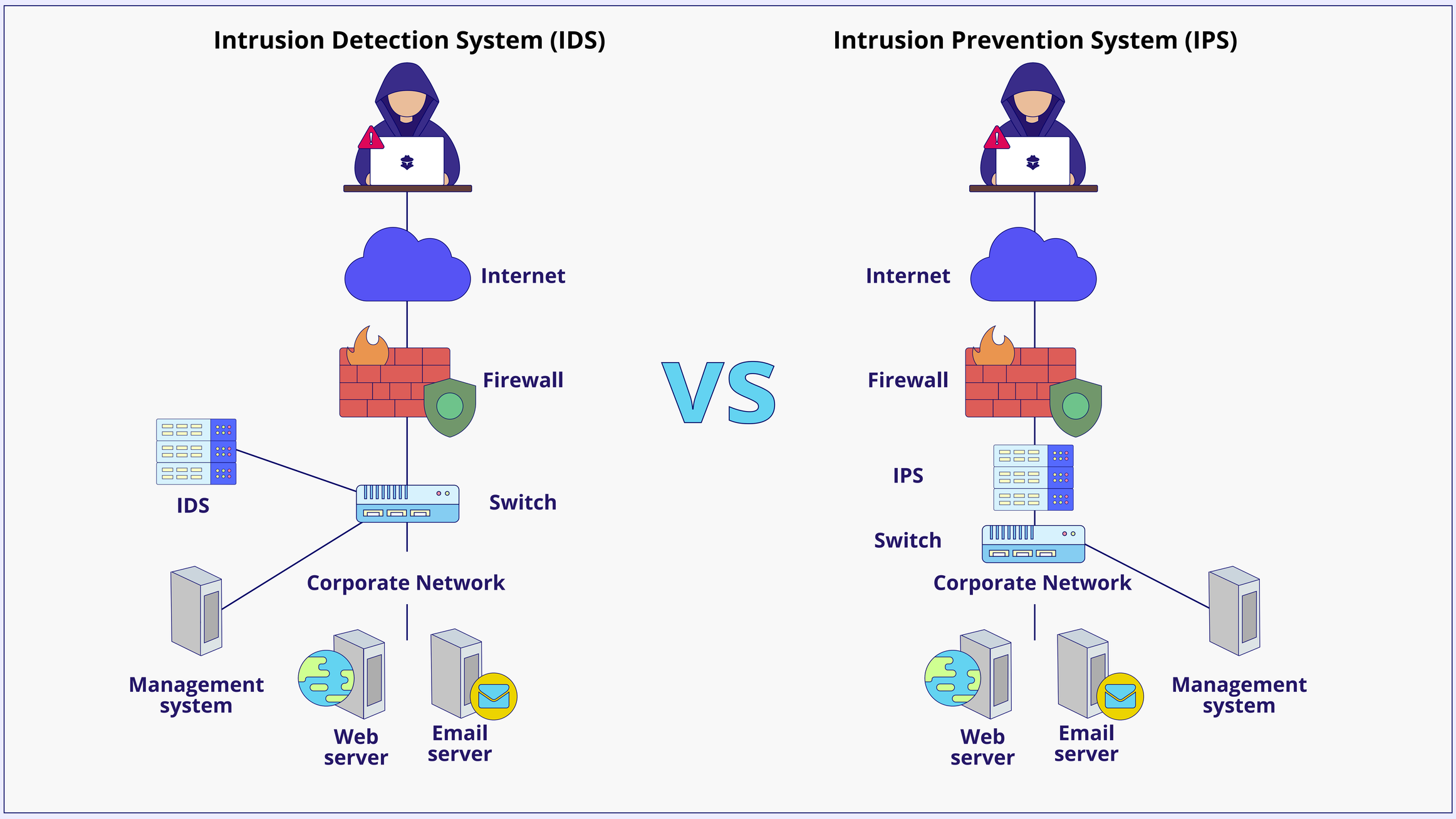
VPN (Virtual Private Network)

VPN securely connects remote users or networks over public networks. Encryption keeps the data safe, so sensitive information stays private and protected from anyone trying to listen in or intercept it.



Intrusion Detection Systems (IDS) vs. Intrusion Prevention Systems (IPS)

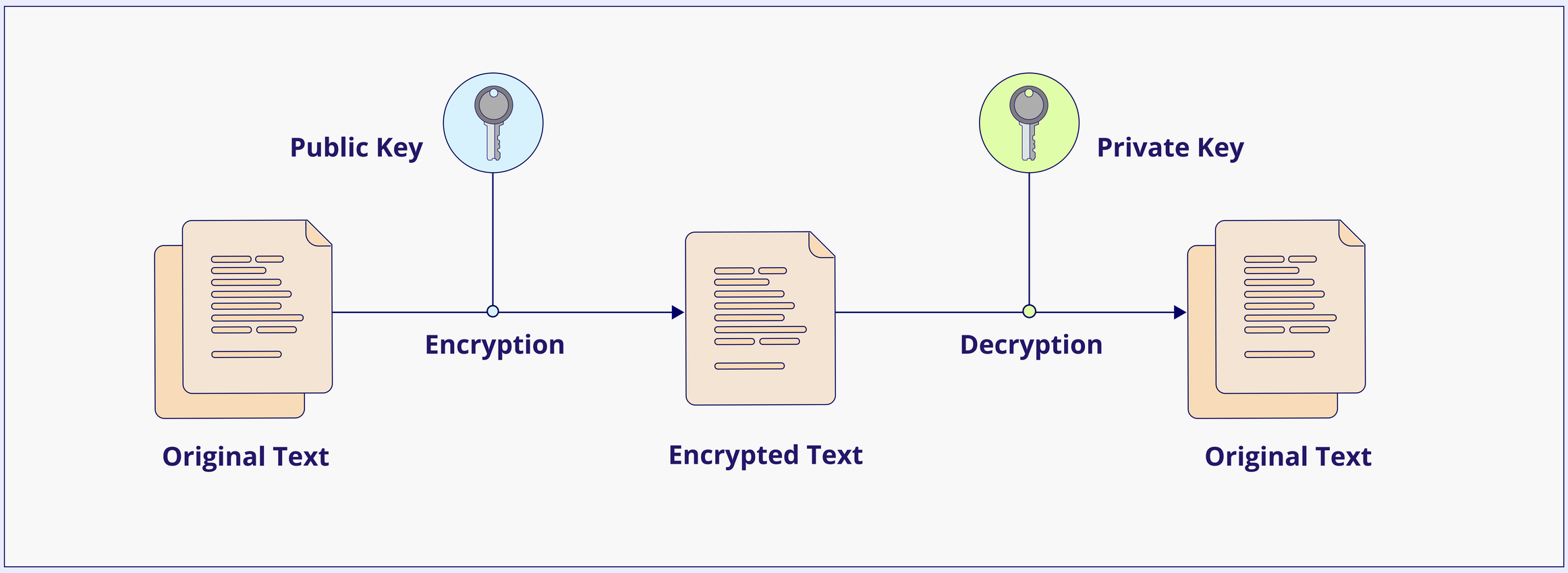
IDS monitors the network traffic for suspicious activity and sends an alert to the administrator. IPS monitors the network traffic for suspicious activity and takes action to prevent detected threats.



Data Protection

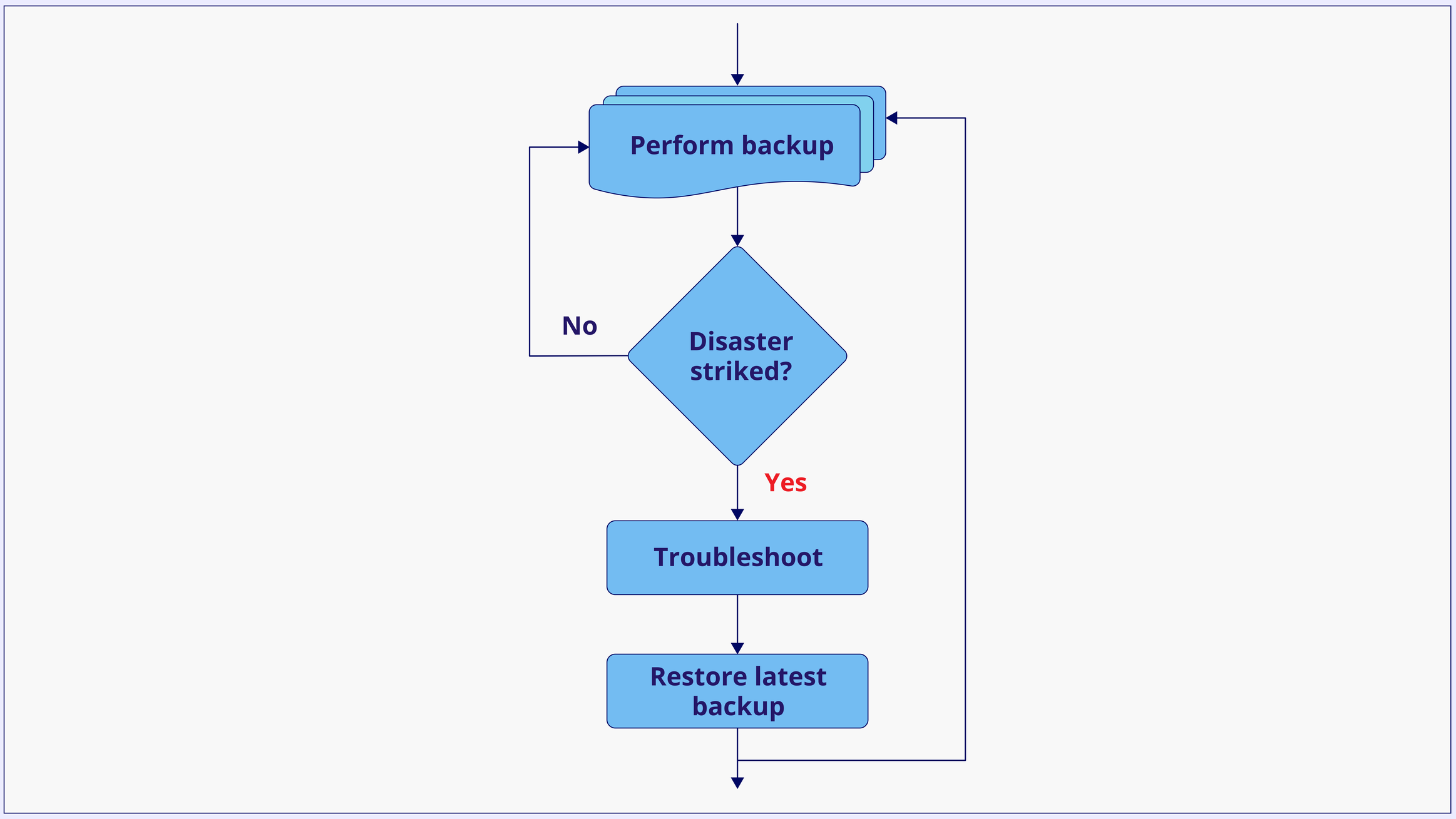
Data Encryption

Encrypts sensitive data to prevent unauthorized access, with the capability to decrypt it later using the corresponding private key. It primarily aligns with the confidentiality aspect of the CIA triad.



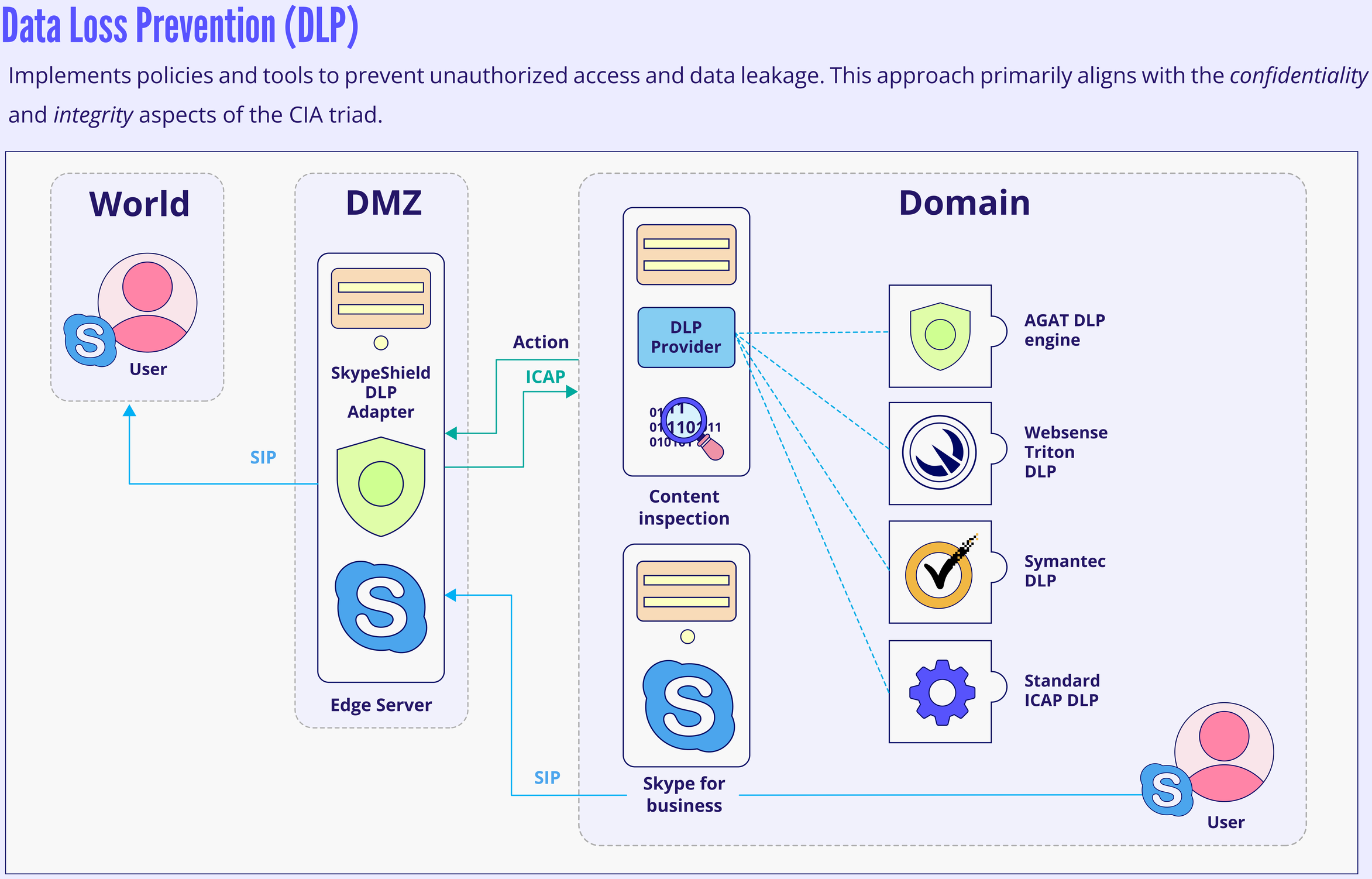
Data Backup and Recovery

Regularly backup data to secure locations and have procedures for data restoration. It primarily aligns with the availability aspect of the CIA triad.



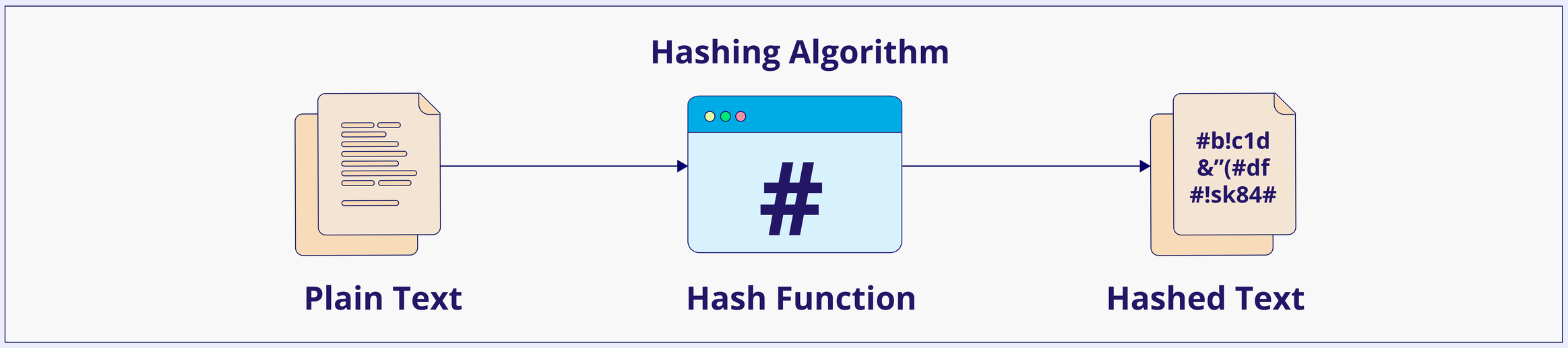
Data Loss Prevention (DLP)

Implements policies and tools to prevent unauthorized access and data leakage. This approach primarily aligns with the *confidentiality* and *integrity* aspects of the CIA triad.



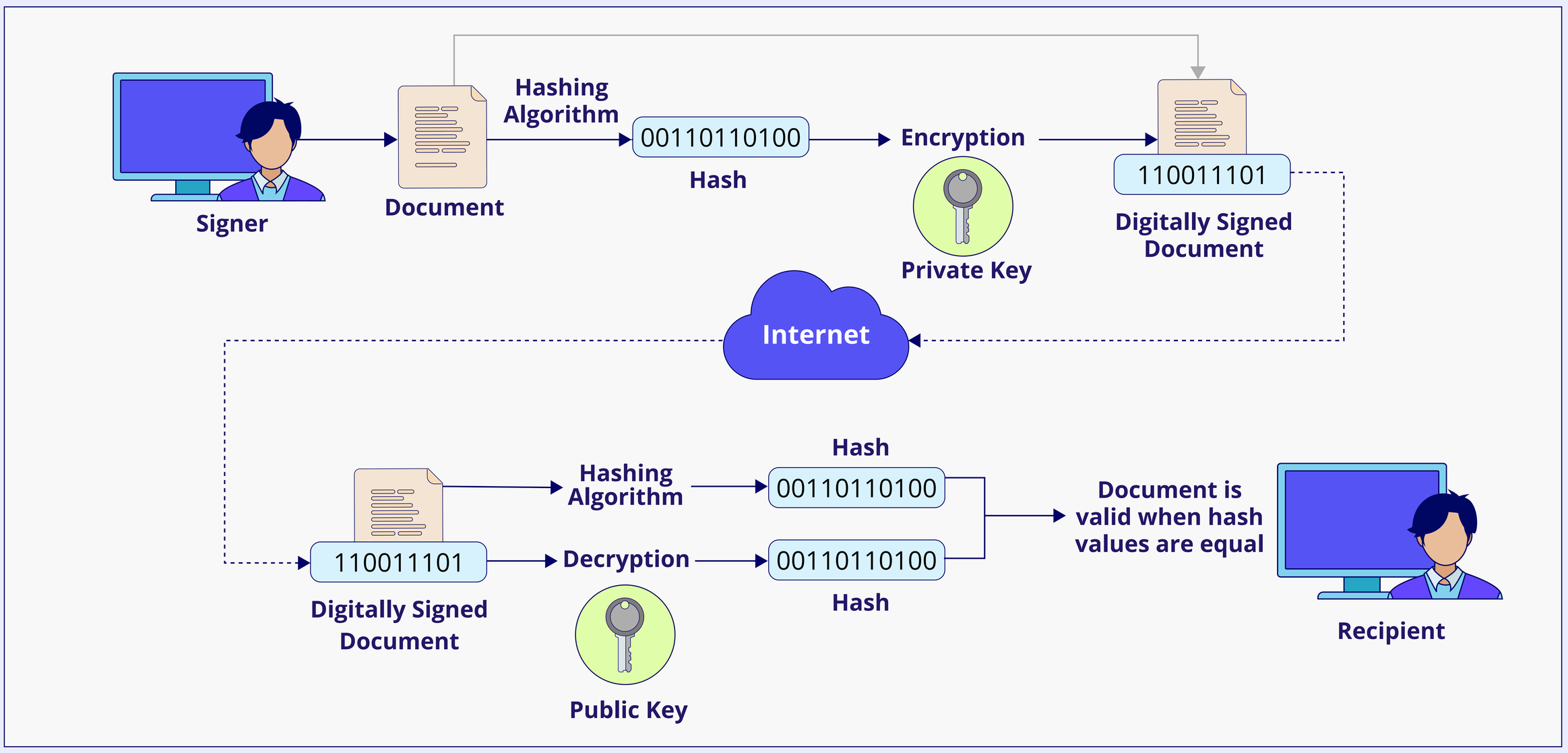
Data Hashing

Transforms a message or a document using a mathematical algorithm to a fixed-size string of characters, known as a hash value or hash code, which cannot be reversed to obtain the original data. Data can be compared with its hash code at any time to see if there has been any tampering. It primarily aligns with the integrity aspect of the CIA triad.



Data Signature

Digital signatures work with data hashing. Once, the data's hash is obtained, also known as a hash digest, it is encrypted with the sender's private key. Anyone with the sender's public key can decrypt the hash and compare it. Only the sender owns the private key, which ensures *integrity, authenticity*, and *non-repudiation* aspects of the CIA triad.



Security Tools and Technologies

Software Updates and Patch Management

Ensures software is up to date with security patches to prevent vulnerabilities. This includes fixing known bugs, addressing potential security weaknesses, and implementing new defenses against emerging threats.

Antivirus and Anti-Malware Software

Detects and removes malicious software and threats by scanning files, processes, and system memory for patterns and behaviors that match known malware signatures or suspicious activities.

Firewall Configuration

Sets up rules to monitor and control incoming and outgoing network traffic, such as allowing or blocking specific protocols, ports, IP addresses, and applications based on predefined security policies and criteria.

Secure Web Browsing

Uses secure protocols and tools to protect the users against online threats and privacy risks, such as HTTPS, which encrypts the web browsing traffic.

DDoS Protection

Implements measures to mitigate and prevent Distributed Denial of Service (DDoS) attacks, such as implementing rate limiting on incoming traffic, and employing third-party DDoS mitigation services.