**What is security**

Security, in information technology ([IT](https://searchdatacenter.techtarget.com/definition/IT)), is the defense of digital information and IT assets against internal and external, malicious and accidental threats. This defense includes detection, prevention and response to threats through the use of security policies, software tools and IT services.

Security is critical for enterprises and organizations of all sizes and in all industries. Weak security can result in compromised systems or data, either by a malicious threat actor or an unintentional internal threat. Not meeting security standards that are regulated by a separate organization or law, such as PCI DSS 3.0 or HIPAA (**Health Insurance Portability and Accountability Act of 1996** )compliance, can also result in financial penalties.

**Physical security**

Physical security is the protection of personnel, hardware, software, networks and data from physical actions, intrusions and other events that could damage an organization. This includes natural disasters, fire, theft and terrorism, among others. Physical security for enterprises often includes employee access control to the office buildings as well as specific locations, such as data centers. An example of a common physical security threat is an attacker gaining entry to an organization and using a USB storage drive to either copy and remove sensitive data or physically deliver malware directly to systems. Threats to physical security may require less technical savvy on the part of the attacker, but physical security is just as important as information security.

**Information security**

Information security, also called [infosec](https://searchsecurity.techtarget.com/definition/information-security-infosec), encompasses a broad set of strategies for managing the process, tools and policies that aim to prevent, detect and respond to threats to both digital and nondigital [information assets](https://whatis.techtarget.com/definition/information-assets). Infosec includes several specialized categories, including:

**Application security** - the protection of applications from threats that seek to manipulate application and access, steal, modify or delete data. These protections use software, hardware and policies, and are sometimes called countermeasures. Common countermeasures include [application firewalls](https://searchsoftwarequality.techtarget.com/definition/application-firewall), encryption programs, [patch management](https://searchenterprisedesktop.techtarget.com/definition/patch-management) and [biometric authentication](https://searchsecurity.techtarget.com/definition/biometric-authentication) systems.**rmation security update 2015 with David Sherry** 0%

[**Learn from the past: Ensure a secure future of information security**](https://searchsecurity.techtarget.com/video/Learn-from-the-past-Ensure-a-secure-future-of-information-security)

[**Cloud security**](https://searchcompliance.techtarget.com/definition/cloud-computing-security) - the set of policies and technologies designed to protect data and infrastructure involved in a [cloud computing](https://searchcloudcomputing.techtarget.com/definition/cloud-computing) environment. The top concerns that cloud security looks to address are [identity and access management](https://searchsecurity.techtarget.com/definition/identity-access-management-IAM-system), and [data privacy](https://searchcio.techtarget.com/definition/data-privacy-information-privacy).

[**Endpoint security**](https://searchsecurity.techtarget.com/definition/endpoint-security-management) - the part of network security that requires [network devices nodes](https://searchnetworking.techtarget.com/definition/node) to meet certain security standards before they can connect to a secure network. Nodes devices include PCs, laptops, smartphones and tablets. Endpoint security also extends to equipment like point-of-sale ([POS](https://whatis.techtarget.com/definition/point-of-sale-terminal-POS-terminal)) terminals, [bar code readers](https://whatis.techtarget.com/definition/barcode-reader-POS-scanner-bar-code-reader-price-scanner) and [IoT devices](https://internetofthingsagenda.techtarget.com/definition/IoT-device).

**Internet security**-the protection of software applications, [web browsers](https://searchwindevelopment.techtarget.com/definition/browser) and virtual private networks ([VPNs](https://searchnetworking.techtarget.com/definition/virtual-private-network)) that use the internet. Using techniques such as [encryption](https://searchsecurity.techtarget.com/definition/encryption) and internet security aim to defend the transfer of data from attacks like malware and [phishing](https://searchsecurity.techtarget.com/definition/phishing) as well as denial-of-service ([DoS](https://searchsecurity.techtarget.com/definition/denial-of-service)) attacks.

[**Mobile security**](https://whatis.techtarget.com/definition/mobile-security) - the protection of portable devices, such as smartphones, tablets and laptops. Mobile security, also known as wireless security, secures the devices and the networks they connect to in order to prevent theft, [data leakage](https://searchsecurity.techtarget.com/definition/extrusion-prevention) and malware attacks.

**Network security** - the protection of a network [infrastructure](https://searchdatacenter.techtarget.com/definition/infrastructure) and the devices connected to it through technologies, policies and practices. Network security defends against threats such as unauthorized access, and malicious use and modifications.