There are several common external threats to networks:

* ****Viruses, worms, and Trojan horses**** - These contain malicious software or code running on a user device.
* ****Spyware and adware**** - These are types of software which are installed on a user’s device. The software then secretly collects information about the user.
* ****Zero-day attacks**** - Also called zero-hour attacks, these occur on the first day that a vulnerability becomes known.
* ****Threat actor attacks**** - A malicious person attacks user devices or network resources.
* ****Denial of service attacks**** - These attacks slow or crash applications and processes on a network device.
* ****Data interception and theft**** - This attack captures private information from an organization’s network.
* ****Identity theft**** - This attack steals the login credentials of a user in order to access private data.  
  It is equally important to consider internal threats. There have been many studies that show that the most common data breaches happen because of internal users of the network. This can be attributed to lost or stolen devices, accidental misuse by employees, and in the business environment, even malicious employees. With the evolving BYOD strategies, corporate data is much more vulnerable. Therefore, when developing a security policy, it is important to address both external and internal security threats, as shown in the figure.

**BYOD (Bring Your Own Device)** refers to the practice where employees, students, or individuals bring their personal devices (such as smartphones, tablets, and laptops) to their workplace, school, or organization and use them to access the organization's systems, networks, or data.

### Key Benefits of BYOD:

* **Cost Savings**: Organizations save on hardware costs because employees use their own devices.
* **Increased Productivity**: Employees may feel more comfortable and work more efficiently on devices they are familiar with.
* **Flexibility and Mobility**: Users can work from anywhere using their personal devices, offering greater flexibility.

### Challenges of BYOD:

* **Security Risks**: Personal devices may introduce vulnerabilities like malware or data breaches into the organization's network.
* **Data Management**: Organizations may struggle with how to protect and manage sensitive data on personal devices.
* **Compliance**: It can be difficult to ensure compliance with industry regulations and data protection laws.

### Common BYOD Strategies:

**Device Security Policies**:

* + Enforcing encryption, strong passwords, and device locks.
  + Requiring anti-virus and security updates.

**Network Access Control (NAC)**:

* + Limiting access to certain parts of the network based on device type, security status, or role of the user.

**Mobile Device Management (MDM)**:

* + Implementing MDM software that allows IT administrators to monitor, manage, and secure personal devices.
  + Remote wiping of data in case a device is lost or stolen.

**Virtual Private Network (VPN)**:

* + Requiring users to connect to the organization's network through a secure VPN to protect data in transit.

**Containerization**:

* + Separating personal data from corporate data on the same device to ensure company data remains secure and private data remains untouched.

**Data Encryption**:

* + Enforcing encryption of sensitive data, both at rest (on the device) and in transit (over networks).

**Acceptable Use Policies (AUP)**:

* + Clear guidelines for how personal devices can be used to access company resources, outlining security expectations and responsibilities.

**Employee Education**:

* + Educating employees on safe practices for using personal devices at work, such as recognizing phishing attacks, avoiding unsafe applications, and managing their own device security.

In conclusion, network security requires a layered approach to protect against diverse threats. Home networks typically use basic measures like antivirus and firewalls, while corporate networks implement more advanced solutions such as dedicated firewalls, ACLs, IPS, and VPNs. Both environments need adaptable security strategies to ensure data protection and service quality. A solid understanding of network infrastructure is key to implementing effective security measures.