-first of all, lets define what is net sec,At a foundational level, network security Is the operation of protecting data,applications,devices and systems that are connected to the network,but let me clarify one thing,that there is an overlapping btween network security and cybersecurity in many ways,network security is most often defined as a subset of cybersec

-so to better understand what is net sec using a perimeter-based security approach-in which the org is like a casle and the data stored within the castle is the crown jewels -network security is most concerned with the security within the castle walls.

- In this perimeter-based scenario, the area within the castle walls can represent the IT infrastructure of an enterprise, including its networking components, hardware, operating systems, software, and data storage.

network-security-threats-and-vulnerabilities:

Thousands of data breaches happen every year – approximately 1,767 publicly reported breaches in the first six months of 2021, which exposed a total of 18.8 billion records.

**Common Network Security Threats and Vulnerabilities**

### **Insider Threats**

Insider breaches typically occur as a result of actions from employees, former employees, or contractors. Although some of these breaches can occur from malicious attacks by employees, approximately [64% of insider threats are a result of employee negligent behavior](https://www.darkreading.com/threat-intelligence/human-negligence-to-blame-for-the-majority-of-insider-threats-/d/d-id/1333937) or human error.

In order to block potential security threats within small businesses, business owners must establish a strong culture of security awareness in their organization. This includes creating employee cybersecurity policies, security threat training, and the implementation of additional security software to ensure that threats are identified and stopped before a potential breach occurs.

### **Phishing attacks**

Phishing is one of the most common network security threats where a cyber-threat gains access to your sensitive information through a social engineering scheme, and is often disguised as a fake email from a recognizable source. By clicking on it, you may inadvertently share your credentials and other critical data.

Occasionally, the attackers may send Ransomware or a worm through these emails, linking to a website that has the ability to harvest sensitive or encrypted information. A weak email security structure is the most significant vulnerability exploited by phishing scammers.

### **DOS and DDOS attack**

A denial-of-service DDoS attack happens when a threat overwhelms your network resources with traffic, preventing users from accessing crucial applications.

**Buffer overflow attacks:**  The concept is to send more traffic to a network address than the programmers have built the system to handle

**ICMP flood** : sending spoofed packets that ping every computer on the targeted network

**SYN flood:** sends a request to connect to a server, but never completes the [**handshake**](https://www.paloaltonetworks.com/documentation/glossary/what-is-a-port-scan)

### **Man-in-the-middle attacks**

This is a vulnerability that allows attackers to spy on or alter the communication between devices in your network. A man-in-the-middle attack could lead to the installation of viruses, warms, or Ransomware.  Cybercriminals can carry out MITM through:

* IP spoofing
* DNS spoofing
* HTTPS spoofing
* SSL hijacking
* Wi-Fi hacking

**MALWARE**:

short for “malicious software,” refers to any intrusive software developed by cybercriminals to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware.

### **Neglecting Regular Patching and Updates**

One extra network security threat that is both common sense and unhappily commonplace: neglecting regular patching and updates. Having to constantly apply new patches and install updates can be tedious. However, failing to do so leaves your business vulnerable to flaws that have been fixed by your hardware and software vendors

PREVENTION MECHANISMS

Many professionals are looking at the statistics and wondering what they can do to protect their organizations, as well as their employee base, from potential network security threats & vulnerabilities.

- Next-generation firewalls (fortinet, paloalto)

Security information and event management (SIEM) is a solution for advanced behavioral analytics and monitoring of real-time security events. Based on data produced by IDPS, EDR, and more,

- Security information and event management(splunk,IBM)

Security information and event management (SIEM) is a solution for advanced behavioral analytics and monitoring of real-time security events. Based on data produced by IDPS, EDR, and more, l

-WAF(akamai,impreva)

protects web servers and hosted web applications from application-layer HTTPS attacks, By inspecting hypertext transfer protocol (HTTP), WAFs can identify and defend your organization from attacks like [SQL](https://www.esecurityplanet.com/threats/what-is-sql-injection) injections, [cross-site scripting](https://www.esecurityplanet.com/endpoint/how-to-prevent-cross-site-scripting-xss-attacks/) (XSS), and [distributed denial-of-service](https://www.esecurityplanet.com/networks/s/how-to-stop-ddos-attacks-tips-for-fighting-ddos-attacks/) (DDoS).

-Network access control(cisco ISE,forescout modern NAC)

Network access control, also called network admission control, is a method to bolster the security, [visibility](https://techtarget.com/searchnetworking/definition/network-visibility) and [access management](https://searchsecurity.techtarget.com/definition/identity-access-management-IAM-system)  of a proprietary [network](https://techtarget.com/searchnetworking/definition/network). It restricts the availability of network resources to endpoint devices and users that comply with a defined [security policy](https://searchsecurity.techtarget.com/definition/security-policy).

- Identity and access management(okta,microsoft):

An Identity and Access Management (IAM) system defines and manages user identities and access permissions. Users of IAM include customers (customer identity management) and employees (employee identity management). With IAM technologies, IT managers can ensure that users are who they say they are (authentication) and that users access the applications and resources they have permission to use (authorization).

- Intrusion detection and prevention system(cisco,trend micro)

Intrusion detection and prevention systems (IDPS) monitor systems by signature or anomaly-based intrusion behavior. IDPS has threat detection, smart alerting, and automatic blocking capabilities.

Breach and attack simulation:BAS(XM cyber, cymulate)  
Security information and event management (SIEM) is a solution for advanced behavioral analytics and monitoring of real-time security events. Based on data produced by IDPS, EDR, and more, l.

Cloud access security broker :CASB(McAfee,microsoft)

Cloud access security brokers (CASB) are secure cloud gateways for monitoring and managing cloud-connected networks.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Perimeter-based security: to secure systems and ward off(prevent) threats as they enter a network, Perimeter security is comprised of systems like firewalls and browser isolation systems.