Introduction Cyber-attacks, Vulnerabilities, Defense Strategies and

Techniques, Authentication Methods- Password, Token and

Biometric, Access Control Policies and Models (DAC, MAC,

RBAC, ABAC, BIBA, Bell La Padula)

Software Security Memory and Address Protection, File Protection Mechanism,

User Authentication, Database Security Requirements,

Reliability and Integrity, Sensitive Data, Inference Attacks,

Multilevel Database Security

Wireless Security Mobile Device Security- Security Threats, Device Security,

IEEE 802.11xWireless LAN Security, VPN Security,

Wireless Intrusion Detection System (WIDS)

Cloud Security Risks and Countermeasures, Data Protection in Cloud,

Cloud Application Security, Cloud Identity and Access Management,

Cloud Security as a Service.

Web Security Considerations, User Authentication and Session

Management, SSL, SSH, Privacy on Web, Web Browser Attacks, Account

Harvesting, Web Bugs, Clickjacking, Session Hijacking and Management,

Phishing and Pharming Techniques, DNS Attacks, Web Service Security,

Secure Electronic Transaction, Email Attacks, Web Server Security as per

OWASP, Firewalls.

Security Policies, Business Continuity Plan, Risk Analysis, Incident

Management, Legal System and Cybercrime, Ethical Issues in

Management Security Management.

## **Infrastructure security TLDR**

Infrastructure security is all about securing your organization's infrastructure. That infrastructure certainly can include permanent assets like real estate, but "infrastructure security" is most commonly used to refer to technology assets, including:

* Computers and endpoints/devices
* Networking systems
* Cloud resources — both hardware and software

The concept of infrastructure security includes not only protection from a [traditional cyberattack](https://www.splunk.com/en_us/blog/learn/cybersecurity-attacks.html) but also protection [from natural disasters](https://www.splunk.com/en_us/blog/learn/disaster-recovery-planning.html) and other calamities. It concerns [the topic of resilience](https://www.splunk.com/en_us/blog/learn/business-continuity-vs-business-resilience.html), which considers how an enterprise recovers from an attack or other disruption. The ultimate goal of infrastructure security is to:

* Boost security measures and your overall posture.
* Minimize the amount of downtime and associated customer attrition, loss of brand and reputation, and compliance costs that businesses face.

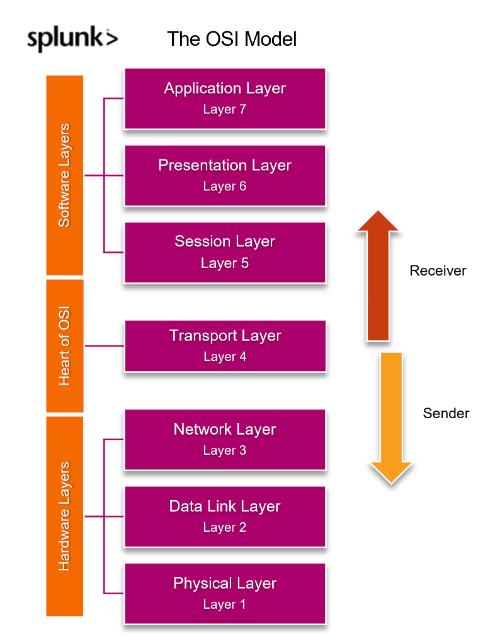
Fundamentally, infrastructure security describes a high-level way of thinking about the protection of the entirety of the organization’s technology perimeter. More tactical security plans — how to protect the data on our workers’ laptops — may be developed as subsets beneath that overarching strategy.

In this blog post, we will discuss the various components of infrastructure and infrastructure security, the most common threats, and ways to protect against them.

## **Levels of infrastructure security**

There is no universal definition of the various levels or categories of infrastructure security, but in the enterprise, one common way to look at security includes securing the following four levels:

* Physical Level: Infrastructure needs physical protection in the form of locked doors, fences, backup generators, security cameras, and the like. Failover plans that locate backup equipment in another part of the world are also part of a physical security strategy.
* Network Level: At its core, network security protects data as it travels into, out of, and across the network. This includes traffic encryption, whether it is on-premises or in the cloud, proper firewall management, and the use of authentication and authorization systems.
* Application Level: Security also needs to be considered at the application level. This includes protection of databases against attacks such as SQL injections as well as the hardening of other applications against unauthorized use or malicious exploits.
* Data Level: At the lowest level of infrastructure security, data protection must be considered, no matter where or how it is stored. This includes data encryption, backups, and anonymization tactics where they are appropriate.



## **Common threats to your infrastructure**

OK, now that we know what infrastructure security is, what exactly is the threat to your infrastructure? Some of the most common infrastructure threats in the market today include:

### **Phishing**

[Phishing](https://www.splunk.com/en_us/blog/learn/phishing-scams-attacks.html) remains one of the most pervasive and damaging threats to individuals and enterprises alike, growing in both quantity and complexity while no longer easy to detect. The goal of phishing attacks, however, remains the same: to separate users from their login credentials, which [attackers](https://www.splunk.com/en_us/blog/learn/threat-actors.html) then use to:

* Access corporate resources.
* Steal funds or intellectual property.
* Wreak havoc on the enterprise.

Phishing attacks skyrocketed throughout the pandemic, ranging from [COVID-19 relief scams](https://www.kagstv.com/article/news/local/scam-alert-direct-deposit-covid-19-money-text-message-link/499-b12afa0f-f1ef-4b3c-a282-f511bce3c12c) and [impersonating the CDC](https://www.techrepublic.com/article/hackers-imitating-cdc-who-with-coronavirus-phishing-emails/), to the lure of [small business loans](https://www.sba.gov/document/report-20-16-serious-concerns-potential-fraud-eidl-program-pertaining-response-covid-19) and [tax extensions.](https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-potential-charity-fraud-associated-with-the-covid-19-pandemic)

### **Ransomware**

[This type of attack involves](https://www.splunk.com/en_us/blog/learn/ransomware-attack-types.html) the threat actor [installing malware](https://www.splunk.com/en_us/blog/learn/malware.html) on the corporate network, which then encrypts targeted data. The threat actor thenholds that data for ransom, waiting for you, the victim, to pay up. If the ransom is not paid, attackers will prevent the victim from accessing their files. Even if the ransom is paid, there is no guarantee that system functionality will be restored.

Ransomware attacks are becoming more common and widespread: in [June 2021 a ransomware attack crippled the networks of hundreds of businesses](https://www.npr.org/2021/07/03/1012849198/ransomware-cyber-attack-revil-attack-huntress-labs) by targeting a software supplier and using it as a conduit to spread through cloud-service providers.

### **Botnets**

Botnets have historically been used to launch distributed denial of service (DDoS) attacks. In more recent years, botnets have been used for surreptitiously mining cryptocurrencies and [targeting IoT infrastructure](https://securityintelligence.com/posts/internet-of-threats-iot-botnets-network-attacks/). Enterprises that have fallen victim to this type of attack are often unaware that their resources are being exploited, sometimes for years. Cloud-based resources are particularly vulnerable to botnet attacks.

### **Physical theft**

It doesn’t matter how secure your infrastructure is from cyber threats if it is not effectively protected by physical barriers such as locked doors, fences, alarm systems and security guards. To that end, a stolen laptop belonging to a medical facility exposed and potentially compromised the personal information and health data of [650,000 patients](https://healthitsecurity.com/news/computer-theft-exposes-personal-health-data-of-654k-oregon-patients).

**TYPES OF AUTHENTICATIONS**

**Password Authentication**

This type of authentication requires the supplicant to recall what he knows. There are two parts to this method. First, the supplicant enters the username, and second, the password. The password is the secret combination of words and numbers that the supplicant knows.

**Strength of Password Authentication**

One of the strengths is that a longer password is very difficult to break. At the point when utilizing passwords, it's imperative to

utilize solid passwords. A solid secret key has a blend of

capitalized, lowercase, numbers, and unique characters. Now

security administrators recommend 12 characters passwords.

A 12 characters password with 94 cardinality and 78.7 bits

entropy will take 55 days to crack using super computers. And

using PC it will take 3018 years to crack. Online site such as

PasswordStrengthCalculator.org can be used to test the

strength of a password [4].

2.1.2 Password Authentication Vulnerabilities

Password sniffing is the biggest problem since when the user

enters the password (Fig.1). An attacker can sniff the

password at different stages of communication. Even if the

password is strong, it can easily be known to the attacker [3].

A key problem with user name and password, the human

actor [2]:

. passwords are easy to guess or search if easy to

remember

. passwords are easily stolen if written down

. users may share passwords

· passwords can be forgotten if difficult to remember