

# Know About Latest Infrastructure Security Tools and frameworks

A discussion on Infra security

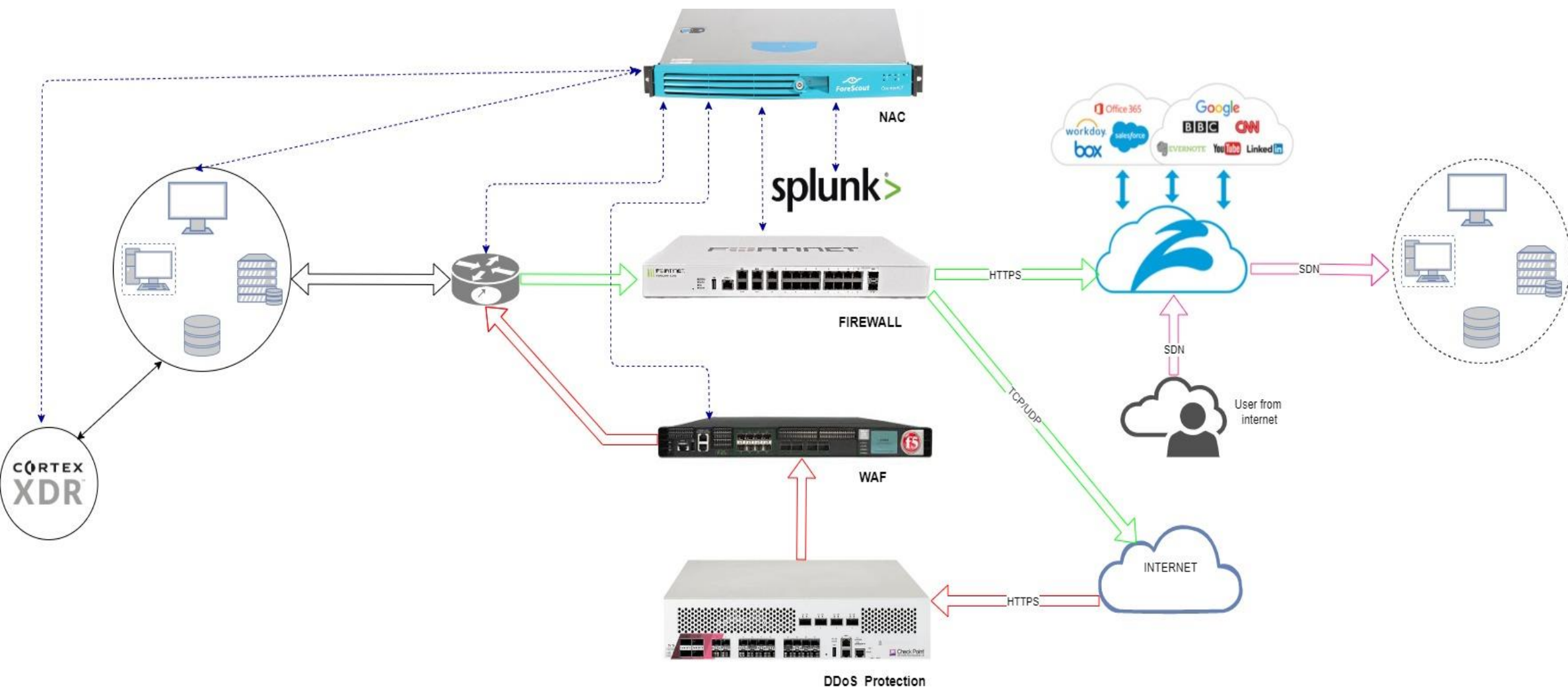





<https://www.linkedin.com/in/anandraj-amaran>



0518d58c1927b65e97eba0a095f0059282fd70d6649f0c48e3f9d30394f2297d20





**INBOUND**   
**OUTBOUND**   
**BI-DIRECT** 

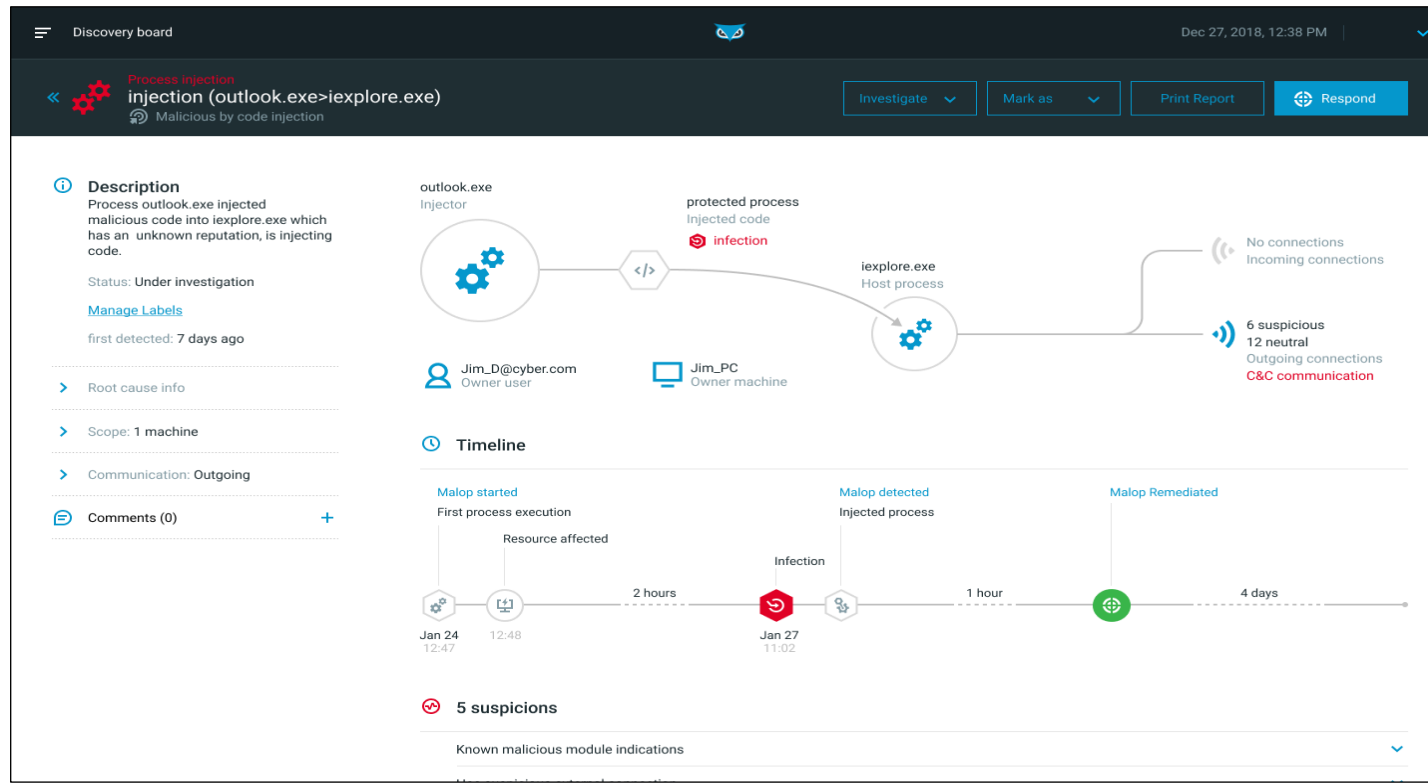
# BYOD VS CYOD VS COPE VS COBO

## Comparison Chart

BYOD	CYOD	COBO	COPE
BYOD stands for "Bring Your Own Device."	CYOD stands for "Choose Your Own Device."	COBO is short for "Company-Owned, Business-Only."	COPE stands for "Company-Owned, Personally-Enabled."
Employees are granted permission to use their personal mobile devices.	Greater control by the company on end-user devices.	Full control by the company on the end-user devices.	Near total control by the company on the end-user devices.
Data security risk is higher.	Risk of mixing personal and work data.	Most secured of all with least chance of data leak.	Risk of data leak as personal use is allowed with limited access.

# ENDPOINT DETECTION AND RESPONSE (EDR)

- Ultimate visibility on Endpoint
- Threat Intelligence
- ML-Powered Detection and Correlation of Malicious Behaviors
- Threat Hunting / IOC /Malware Analysis
- Live Monitoring
- Extended Logs



# NEXT GENERATION FIREWALL (NGFW)

A stateful firewall is a network security device that filters incoming and outgoing network traffic based upon Internet Protocol (IP) port and IP addresses. By intelligently inspecting the payload of some packets, new connection requests can be associated with existing legitimate connections. A next generation firewall adds additional features such as application control, integrated intrusion prevention (IPS) and often more advanced threat prevention capabilities like sandboxing.

Anti-Virus

Application Control

DNS Security

DLP

Dmain & IP Reputation

IPS

Email Security

Web Filter

Load Balance

SSL Inspection

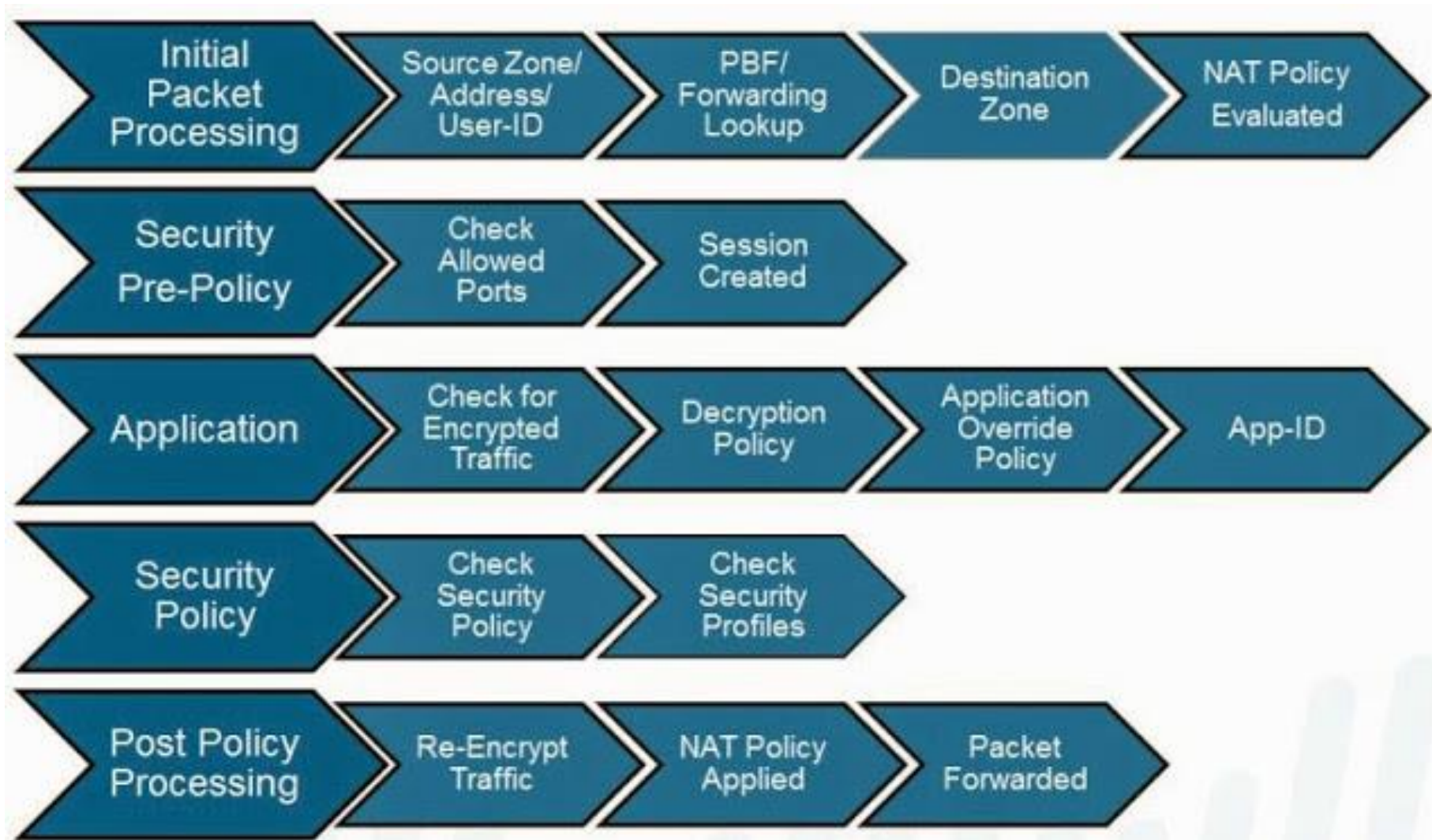
WAF

Vulnerability Check

SandBoxing

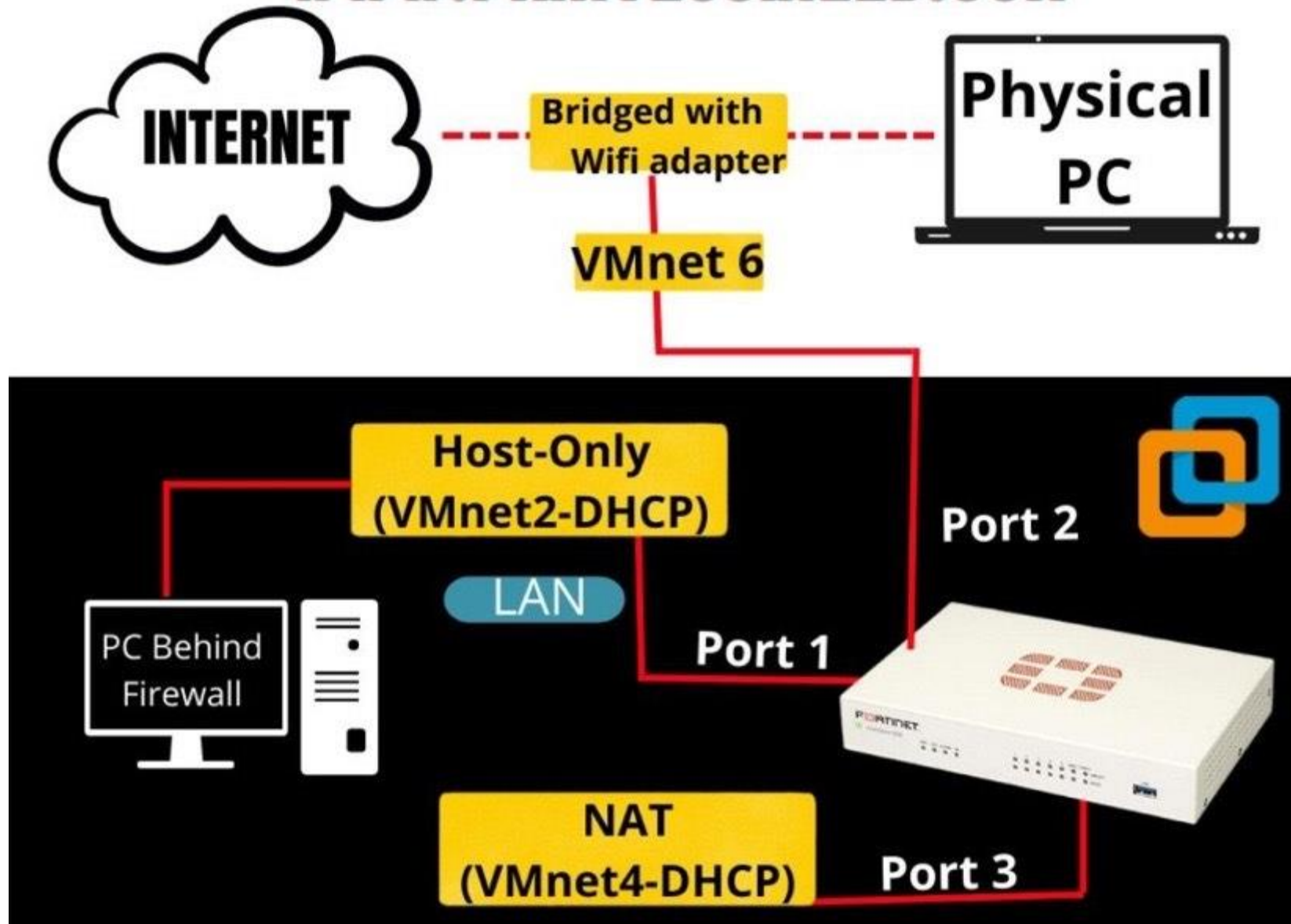


## FLOW LOGIC OF THE NEXT-GENERATION FIREWALL



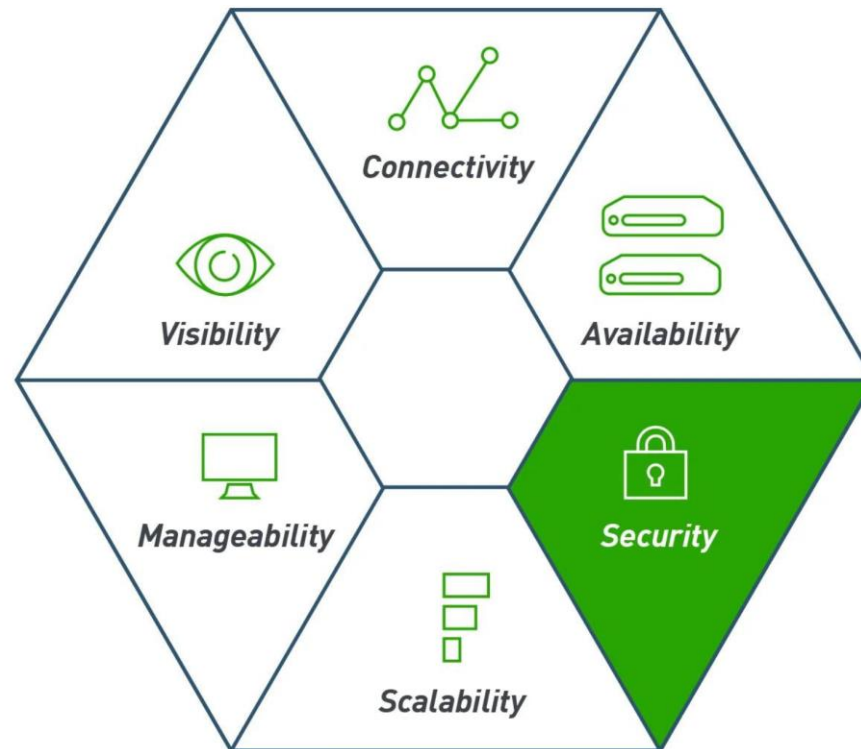
# Setup FortiVM in VMware-Workstation

[WWW.PIRATESSHIELD.COM](http://WWW.PIRATESSHIELD.COM)



# WEB-SECURITY (FORWARD-PROXY)

- Improve security
- Secure employees' internet activity from people trying to snoop on them
- Balance internet traffic to prevent crashes
- Control the websites employees and staff access in the office
- Save bandwidth by caching files or compressing incoming traffic

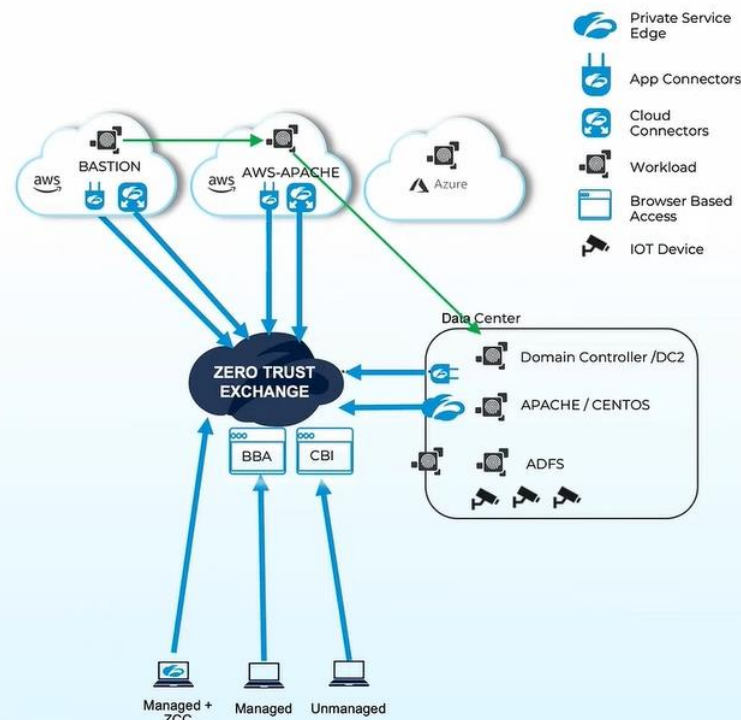




# ZSCALER PRIVATE ACCESS

The Zscaler Private Access (ZPA) service enables organizations to provide access to internal applications and services while ensuring the security of their networks. ZPA is an easier to deploy, more cost-effective, and more secure alternative to VPNs. Unlike VPNs, which require users to connect to your network to access your enterprise applications, ZPA allows you to give users policy-based secure access only to the internal apps they need to get their work done. With ZPA, application access does not require network access

## Zscaler Private Access: Secure and fast private app access



Devices/Users Authenticate to SAML IDP  
Managed Devices perform Device Auth  
Managed Device with ZCC  
Managed Device without ZCC  
Unmanaged Device without ZCC

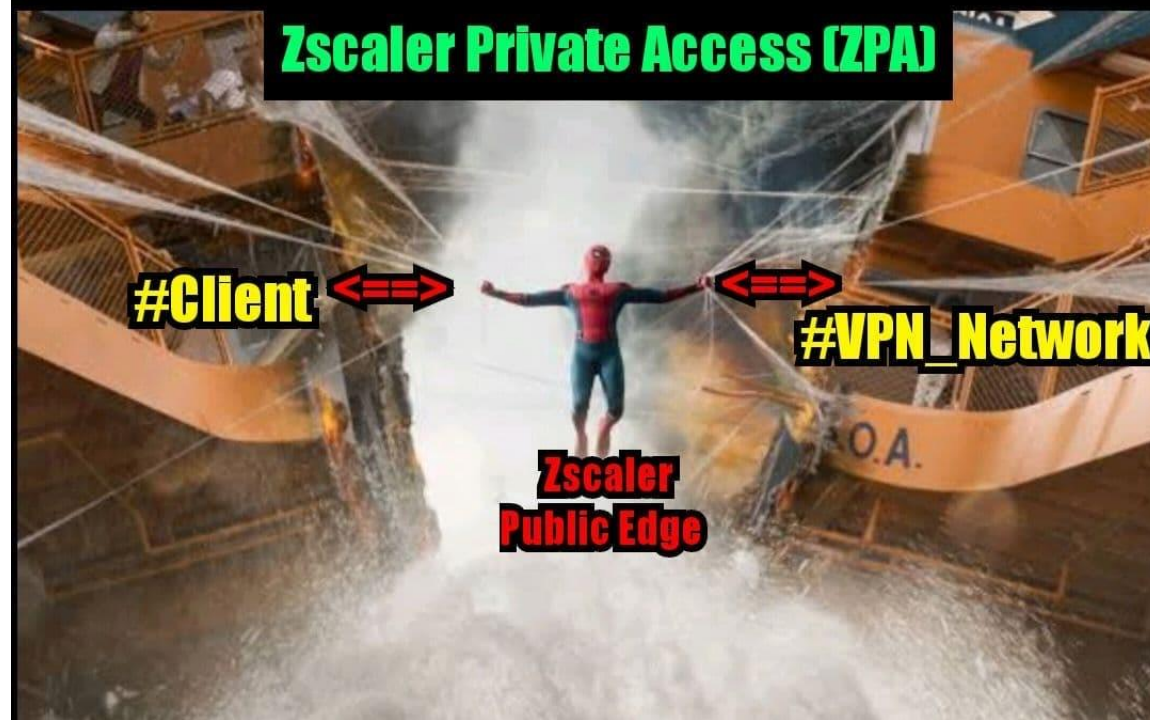
Zscaler Client Connector – Partner Web Page  
Browser Based Access – Partner Web Page  
Cloud Browser Isolation – Partner Web Page

Inspection Policy – ZCC, Browser Based, CBI

Cloud Connector – Bastion Host in AWS to DataCenter  
Update Webpage

Privileged Remote Access  
SSH to CentOS Server – Update Webpage  
RDP to Domain Controller  
Support Access – Client to Client

Deception – Swift/SAP/SSH

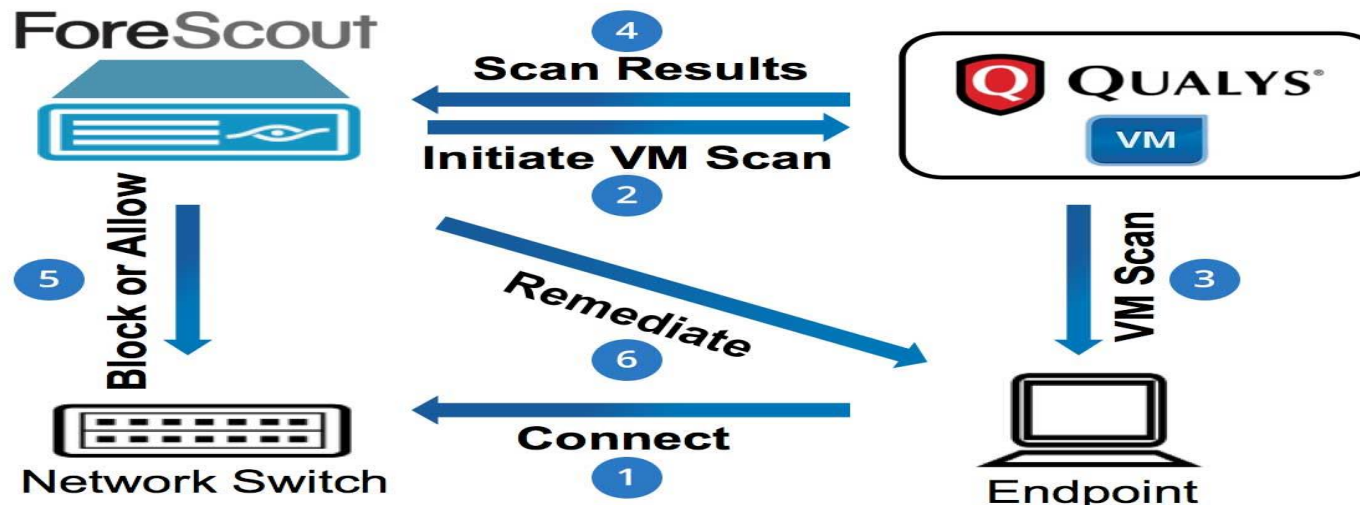


# WEB APPLICATION FIREWALL (WAF)

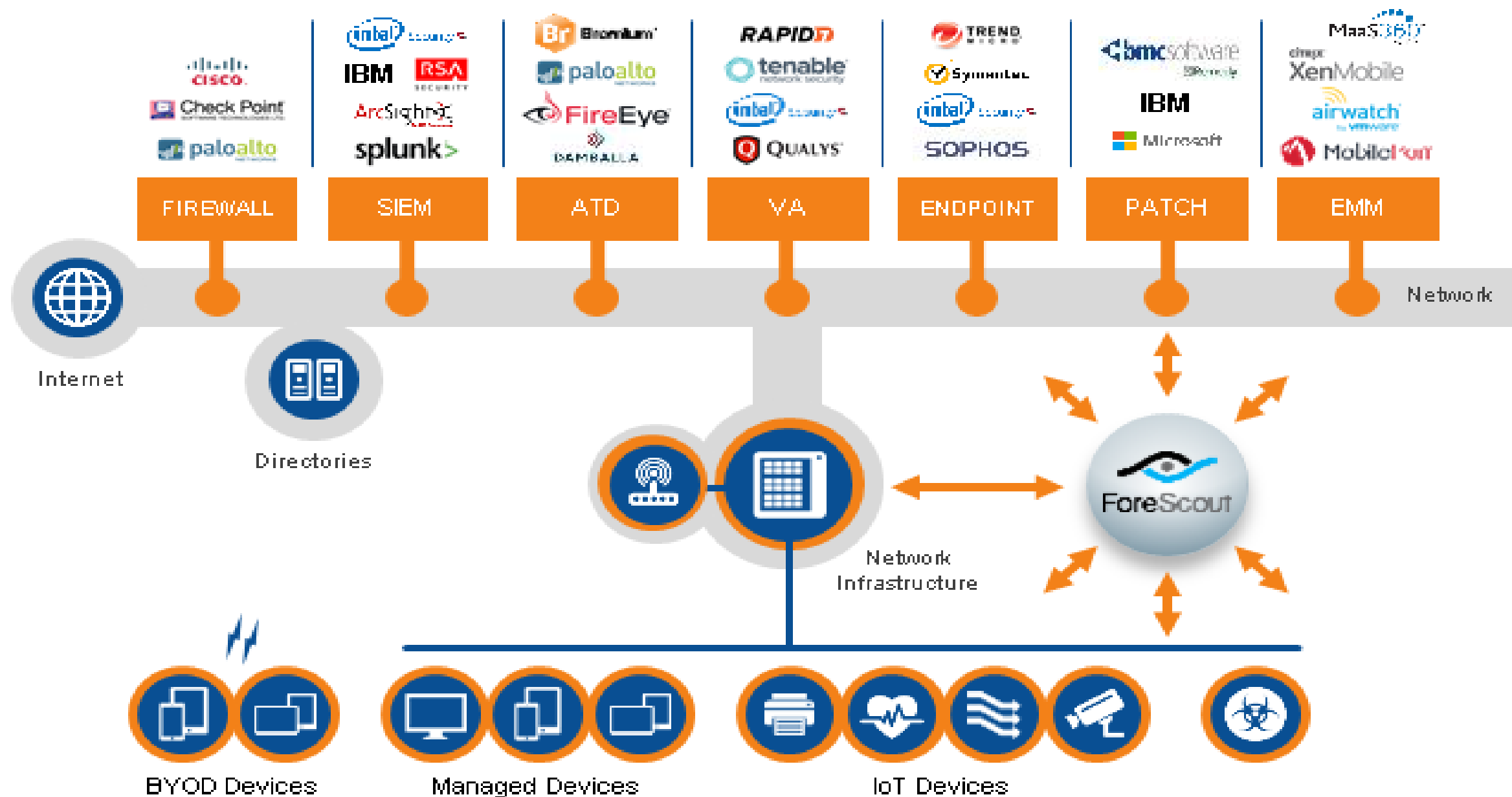
- Use as 'Reverse-Proxy' to hide original server IP
- Block Known OWASP attacks
- Control the rate of Sessions and IP / Geo based access
- Protect Sensitive information
- Avoid Zero day Attacks
- Traffic Load Balance
- Act as Cache & CDN server
- API Security
- BOT /Spam traffic protection
- DDOS Protection

# NETWORK ACCESS CONTROLLER (NAC)

- With organizations now having to account for exponential growth of mobile devices accessing their networks and the security risks they bring, it is critical to have the tools that provide the visibility, access control, and compliance capabilities that are required to strengthen your network security infrastructure.
- A NAC system can deny network access to noncompliant devices, place them in a quarantined area, or give them only restricted access to computing resources, thus keeping insecure nodes from infecting the network.

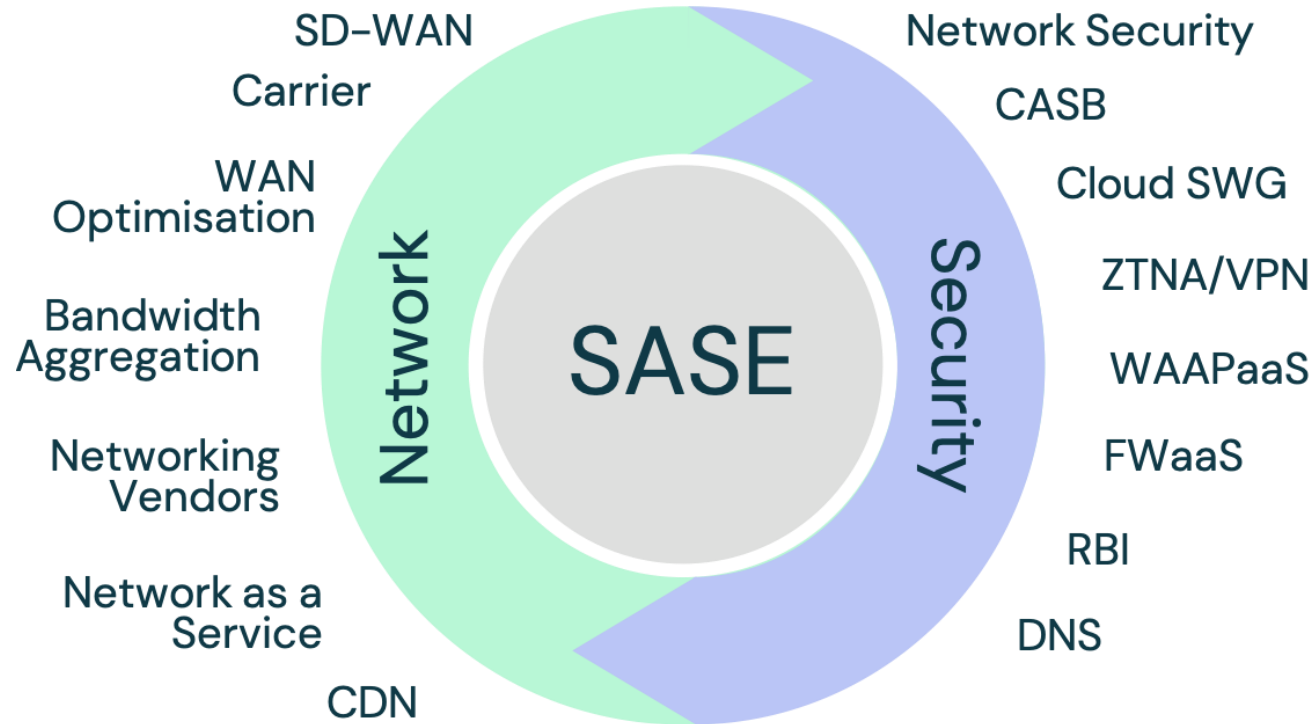


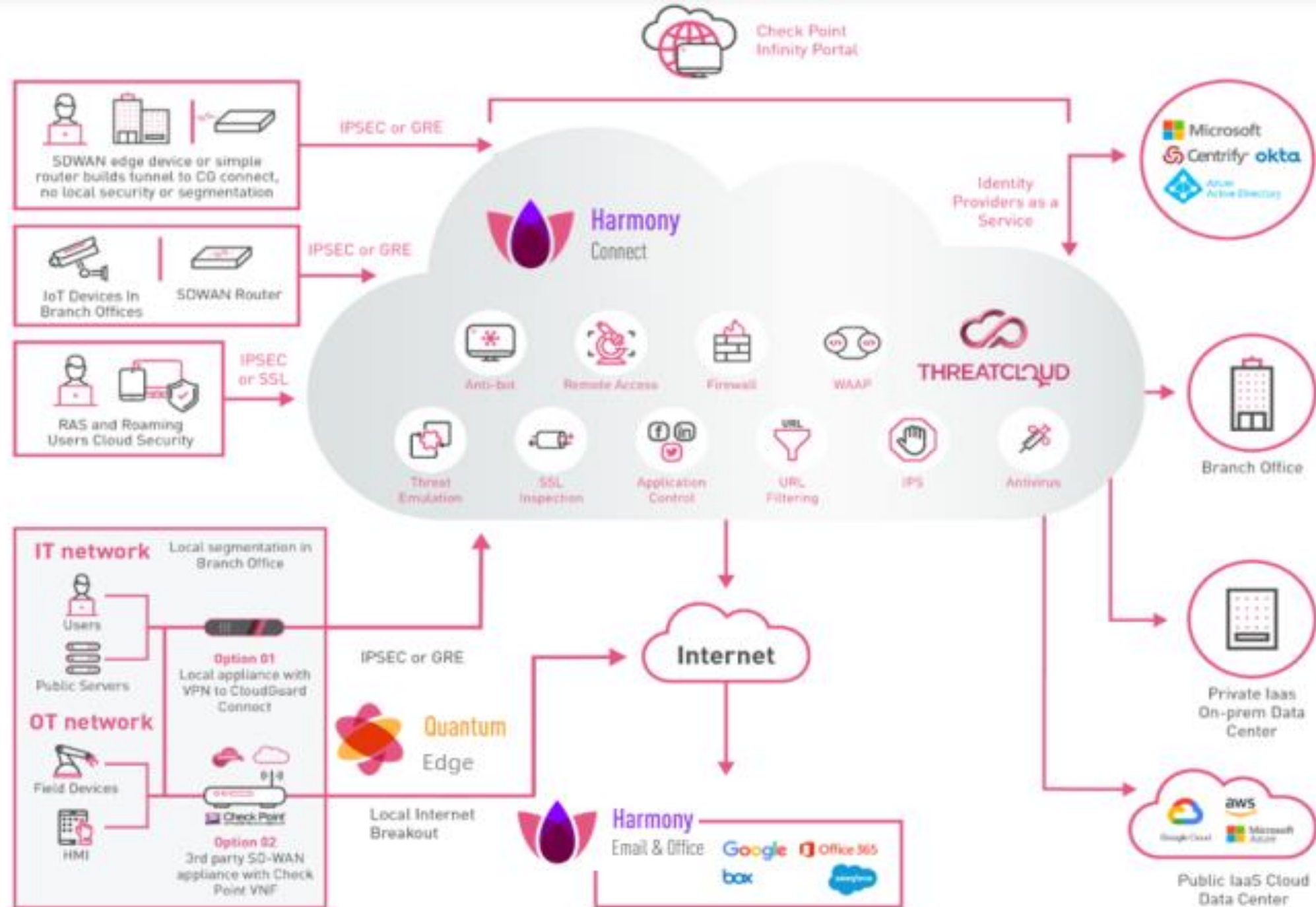




# Secure Access Service Edge (SASE)

Secure access service edge (SASE) is a cloud-based enterprise security framework designed to address the network and security challenges caused by digital business transformation. The move to cloud coupled with increasingly mobile workforces places users, devices, applications, and data outside of the enterprise data center and network, creating an “access pattern inversion.” Introduced by Gartner, the SASE model responds to this inversion delivering networking and network security controls at the edge — as close to users as possible.





# PRIVACY BY DESIGN

UK : 

## **GDPR** **General Data Protection Regulation**

India : 

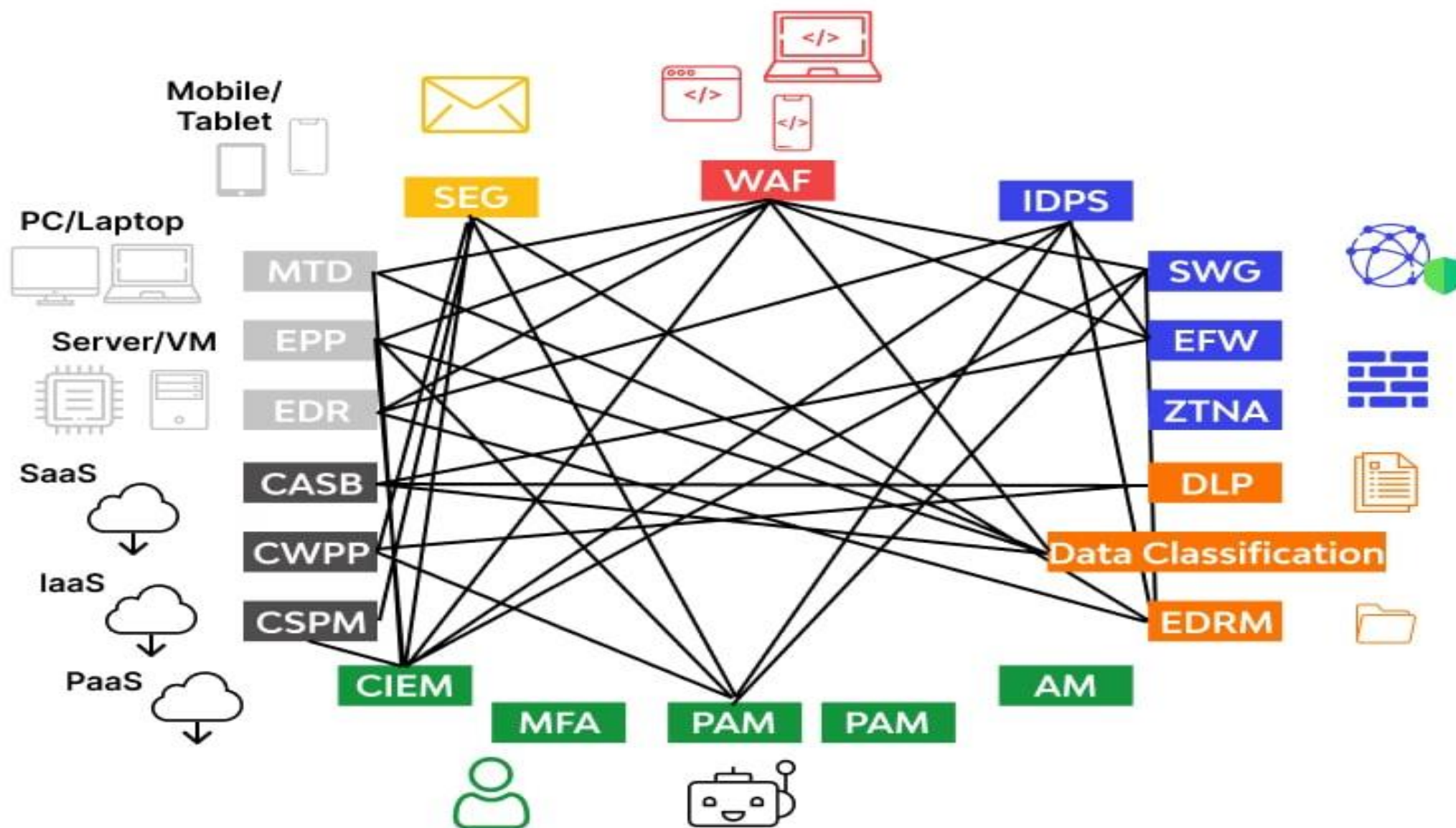




# Zero trust security model

- Zero trust network access (ZTNA), also known as the software-defined perimeter (SDP), is a set of technologies and functionalities that enable secure access to internal applications for remote users. It operates on an adaptive trust model, where trust is never implicit, and access is granted on a need-to-know, least-privileged basis defined by granular policies. ZTNA gives remote users seamless, secure connectivity to private applications without ever placing them on the network or exposing apps to the internet.
- Zero trust security is a big buzzword these days. While many organizations have shifted their priorities to adopt zero trust, zero trust network access (ZTNA) is the strategy behind achieving an effective zero trust model.

# Gartner Cybersecurity mesh architecture



# FOSS

- NAC
- Firewall
- VPN / Proxy Based Intranet connection

<https://www.packetfence.org/about.html>

<https://www.pfsense.org/>

<https://tailscale.com/> <https://boringproxy.io/>

- Threat Intel.

<https://otx.alienvault.com/>

- DNS Security

<https://pi-hole.net/>

- Manage Linux servers Like Pro

[https://www.freeipa.org/page/Main\\_Page](https://www.freeipa.org/page/Main_Page)

**Thank For Listening!!!**

**Any Questions???**

