ISACA Amman Chapter

ISACA Amman Chapter

glorythink group

AlBrza KNOWLEDGEX
Power Your Education Empire Based On Future Demands

Securig Your Enterprise Using Emerging Technologies: ZTA – CASB – SDP - SASE

glorythink group

POWERED BY AlBrza KNOWLEDGEX

Who am I ?

- ✓ Abdulrahman Al-Nimari
- ✓ Cyber Security Advisor, Architect, Consultant
- ✓ 25 Years IT & Cyber Security Experience
- ✓ Speaker : BSides, HITB, ICSC, AECT, Arab Security Conference
- ✓ Awarded Arab Cybersecurity Social Network Influencer Prize 2019, 2020
- ✓ CISSP, CISM, CCISO, PMP, GCIH, GCIA, GCUX, GREM, GSEC
- ✓ @nimari
- ✓ https://www.linkedin.com/in/alnimari/
- ✓ alnimari@gmail.com
- ✓ +966 (566) 465270

Agenda

- ✓ Traditional Network Security
- ✓ What is Zero Trust ?
- ✓ Zero Trust Building Blocks
- ✓ Steps To Zero Trust
- ✓ **SDP** – **S**oftware **D**efined **P**erimeter
- ✓ **CASB** – **C**loud **A**ccess **S**ecurity **B**roker
- ✓ **SASE** – **S**ecure **A**ccess **S**ecurity **E**dge
- ✓ Resources

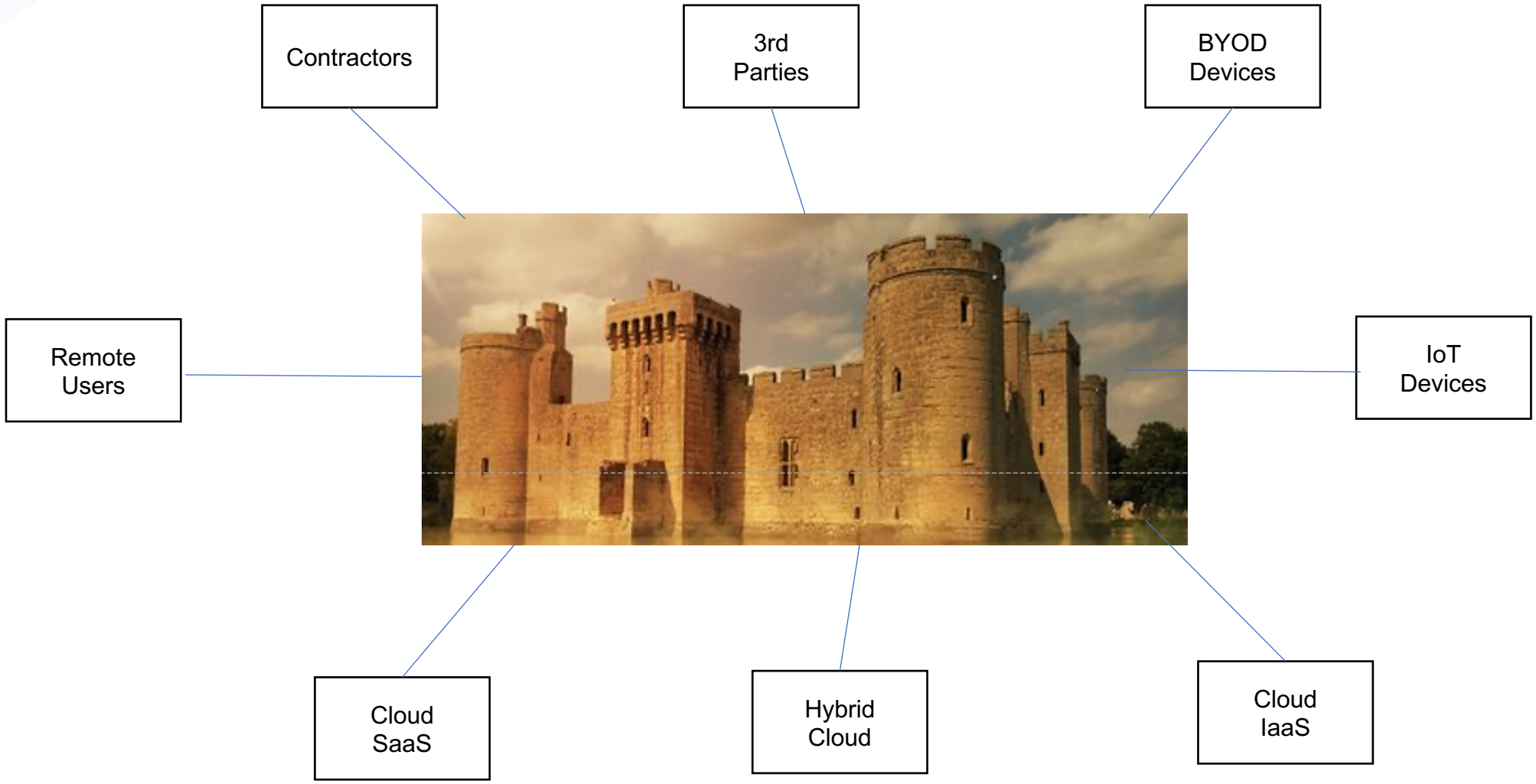
Solarwinds Attack

Who DETECTED the Solarwinds Attack in a timely manner ?

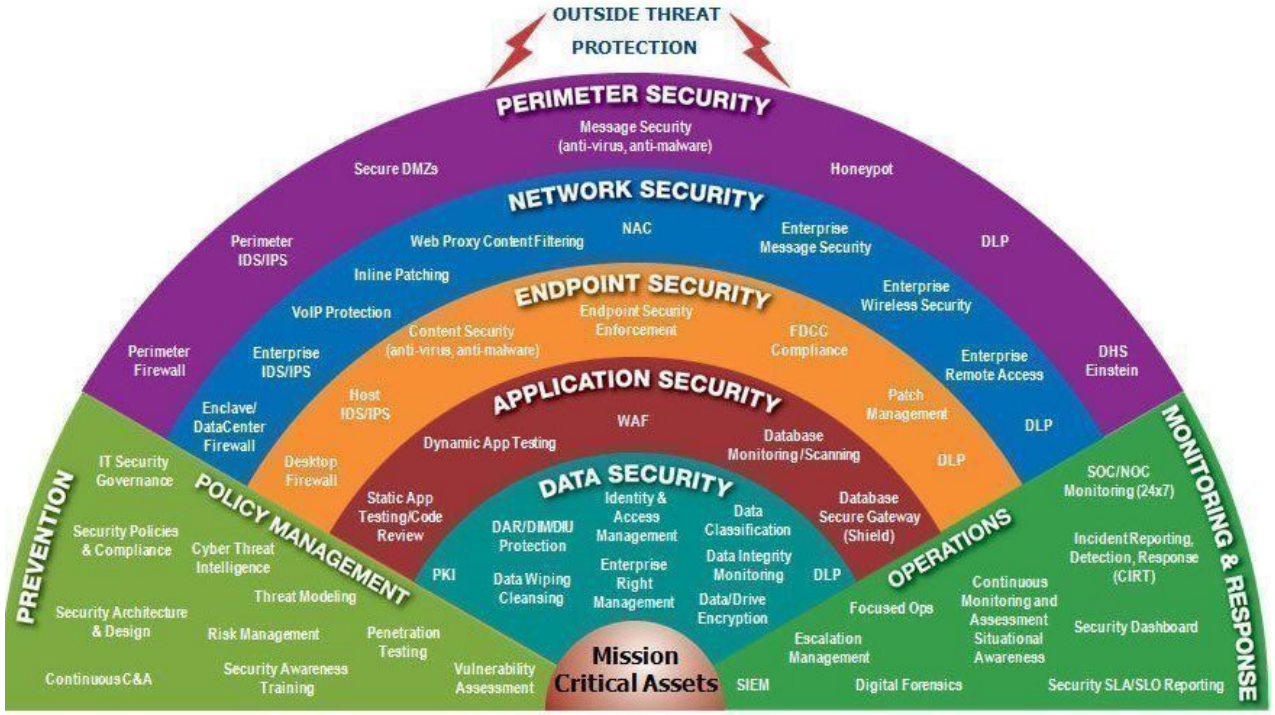
- ✓ A global impact on :
  - ✓ Many federal government agencies
  - ✓ Fortune 500 Enterprises
  - ✓ All that trusted Solarwinds Orion Software was affected

Traditional Enterprise Castle

Perimiter is Every Where

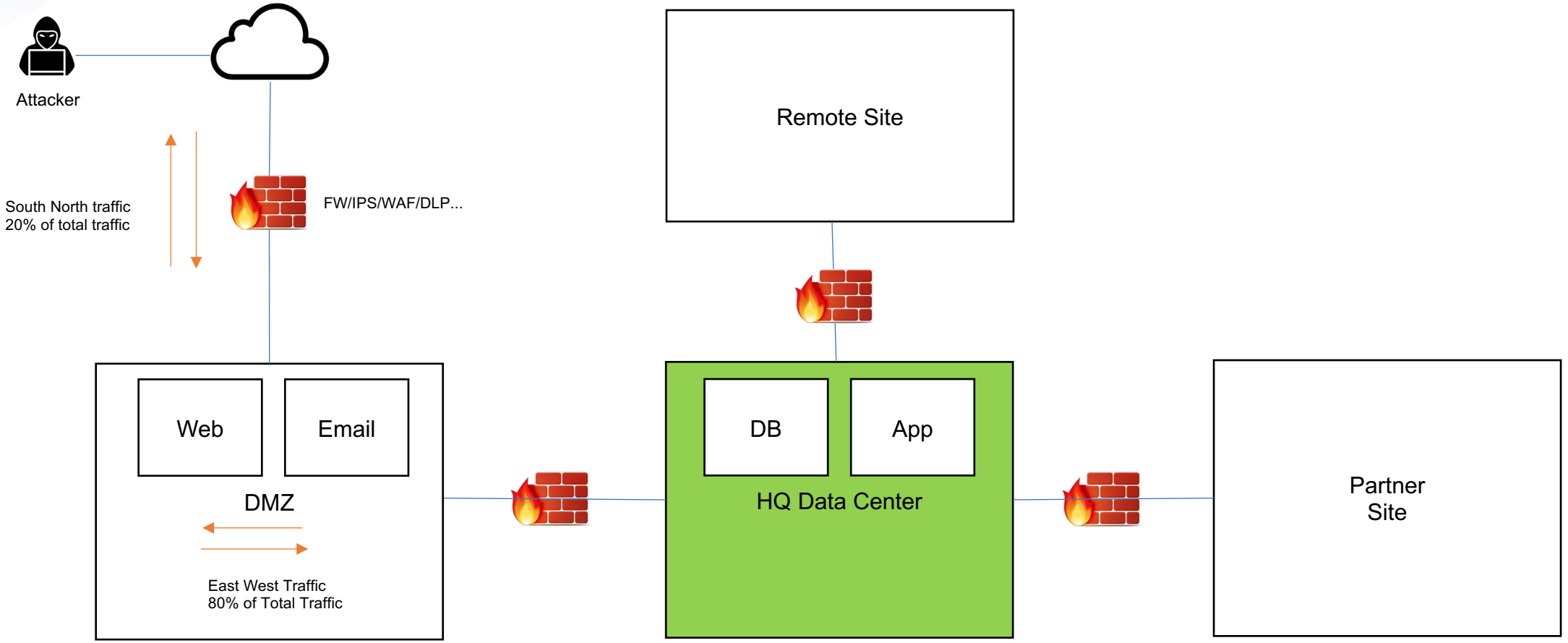


Defense in Depth

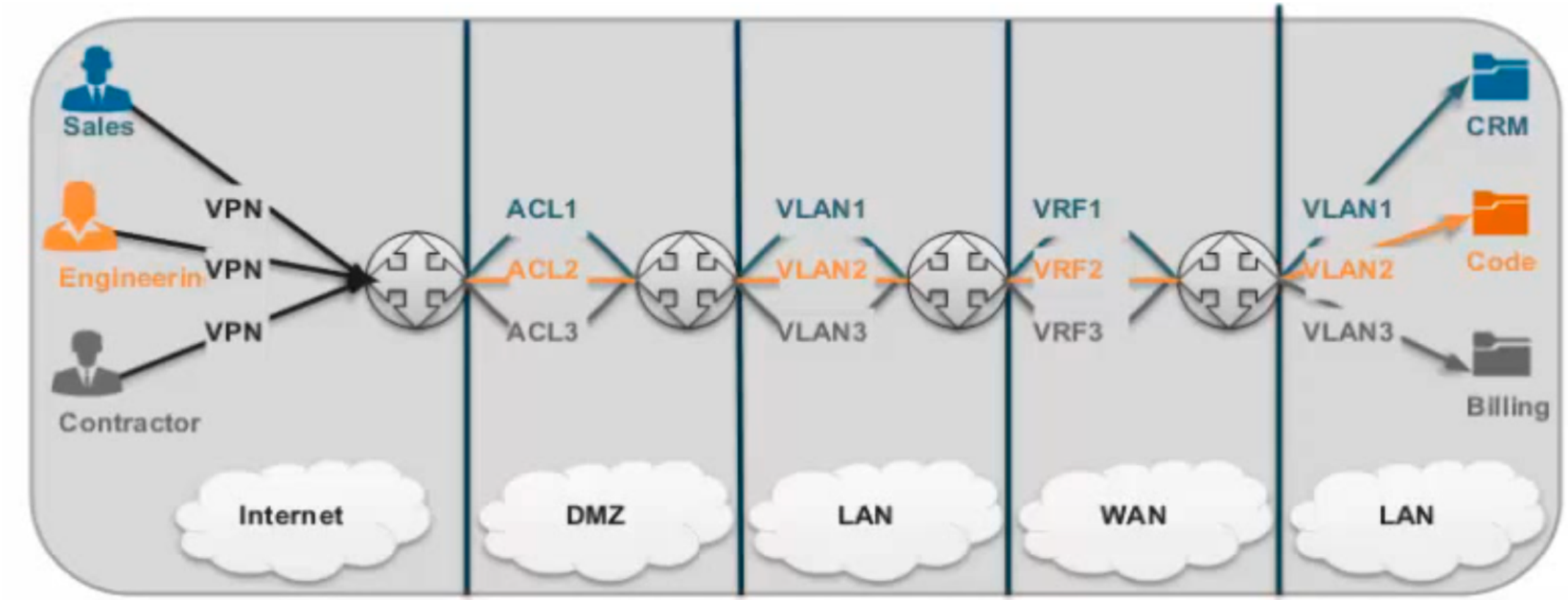


- ✓ Insider threats is not considered in ‘Defense in Depth’
- ✓ Default trust still exist

Traditional Network Security



Traditional Network Segmentation



ACLs, VLANs, VRFs were not designed with security in mind.
They are scattered every where and hard to manage.

What is bad about Traditional Approach ?

- ✓ The Big Issue : Internal Access is Trusted by Default
- ✓ Laterla Movement is Possible
- ✓ Pivoting is Possible
- ✓ Insider Threat not Considered

The Solution is to Implement Zero Trust

What is Zero Trust ?

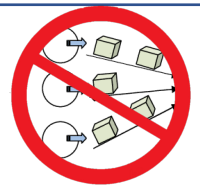
- ✓ It is a concept, NOT a technology or a device
- ✓ The concept : Do not trust anything, verify everything
- ✓ ‘Zero Trust’ term was coined by John Kindervag in 2010
- ✓ Buzzword nowadays, a game changer in Network Security
- ✓ Different Names : ZeroTrust, Perimeterless, BeyondCorp

In Zero Trust Model, Data becomes the New Perimeter

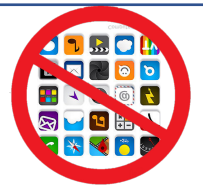
DO NOT trust anything, VERIFY EVERYTHING

Users

Devices



Packets



Apps

No Trust Assumed, Default DENY ALL Policy

Zero Trust Building Blocks

- ✓ Identity (IDAM)
  - ✓ Users
  - ✓ Devices
- ✓ Network Segmentation, microsegment as granular as needed
- ✓ Policy (Need To Know, Least Privilege)
- ✓ Data Flow – Who is talking to Who ?

Steps To Zero Trust

- ✓ Identify Critical Data, Assets, Applications and Services (Scope)
- ✓ Identify Data Flows (Who is talking to who ?)
- ✓ Create Zero Trust Policy Based on Data Flows, User Roles
  - ✓ Need to Know
  - ✓ Least Privilege
- ✓ Segment Network as granular as needed
- ✓ Architect Zero Trust Network
- ✓ Inspect, Log and Monitor Everything
- ✓ Automate and Orchestrate (Integrate tools to contain and mitigate)

Identifying Data Flows

- ✓ Flow Data Sources :
  - ✓ Log Files
  - ✓ PCAP Data (packet header to reserve space)
  - ✓ NetFlow Data

```
rwfilter --type=all --pass=stdout --proto=0-255 --daddr=192.168.1.173 --packets=4 --ack-flag=1 | rwstats --count 20 --fields=sip,dip,sport,dport,proto
```

sIP	dIP	sPort	dPort	pro
52.109.88.76	192.168.1.173	443	64635	6
52.21.178.134	192.168.1.173	80	64476	6
52.21.178.134	192.168.1.173	80	64474	6
13.227.10.5	192.168.1.173	80	64481	6
172.217.19.10	192.168.1.173	443	64436	6
216.58.208.234	192.168.1.173	443	64412	6
149.154.164.250	192.168.1.173	80	64451	6
52.21.178.134	192.168.1.173	80	64475	6
3.235.72.247	192.168.1.173	443	64602	6
149.154.167.91	192.168.1.173	80	64591	6
89.44.169.132	192.168.1.173	80	64546	6

https://tools.netsa.cert.org/silk/

Segmentation

S	Segment	Subnet	Location
1	APP-1	192.168.1.0/24	Data Center
2	Email	192.168.2.0/24	
3	APP-2	192.168.3.10/32	
4	Finance	192.168.4.0/24	
5	HTTP	192.168.5.0/24	
6	ERP	192.168.6.0/24	
7	HR-1	10.0.0.0/24	HR Dept
8	HR-2	10.0.1.0/24	
9	Sales-1	10.0.10.0/24	Sales Dept
10	Sales-2	10.0.11.0/24	
11	R&D	10.0.20.0/24	R&D
..	..	..	..

Segment as granular as needed

Segments Policy

	App1	Email	APP-2	Finance	HTTP	ERP	HR-1	HR-2	Sales-1	Sales-2	R&D
APP-1		25		22,443	80,443	675	22	3306	1433	21	
Email	25			25,22	80,443	1433	25	2525	2121	4434	
APP-2											443
Finance	80	25			80	443	80	8080	22	443	
HTTP	80	deny		25		432	22,25			1520	
ERP	443	deny		22	80		25	2525	1433	3500	
HR-1	443	25		21	443	2521		3006	5252	8082	
HR-2	443	21		3306	443	80	8081		141	25	
Sales-1	8080	25		8080	22	80	22	443		1433	
Sales-2	443	25		80	22				443		
R&D	2121	2525	443	1433							

No Access

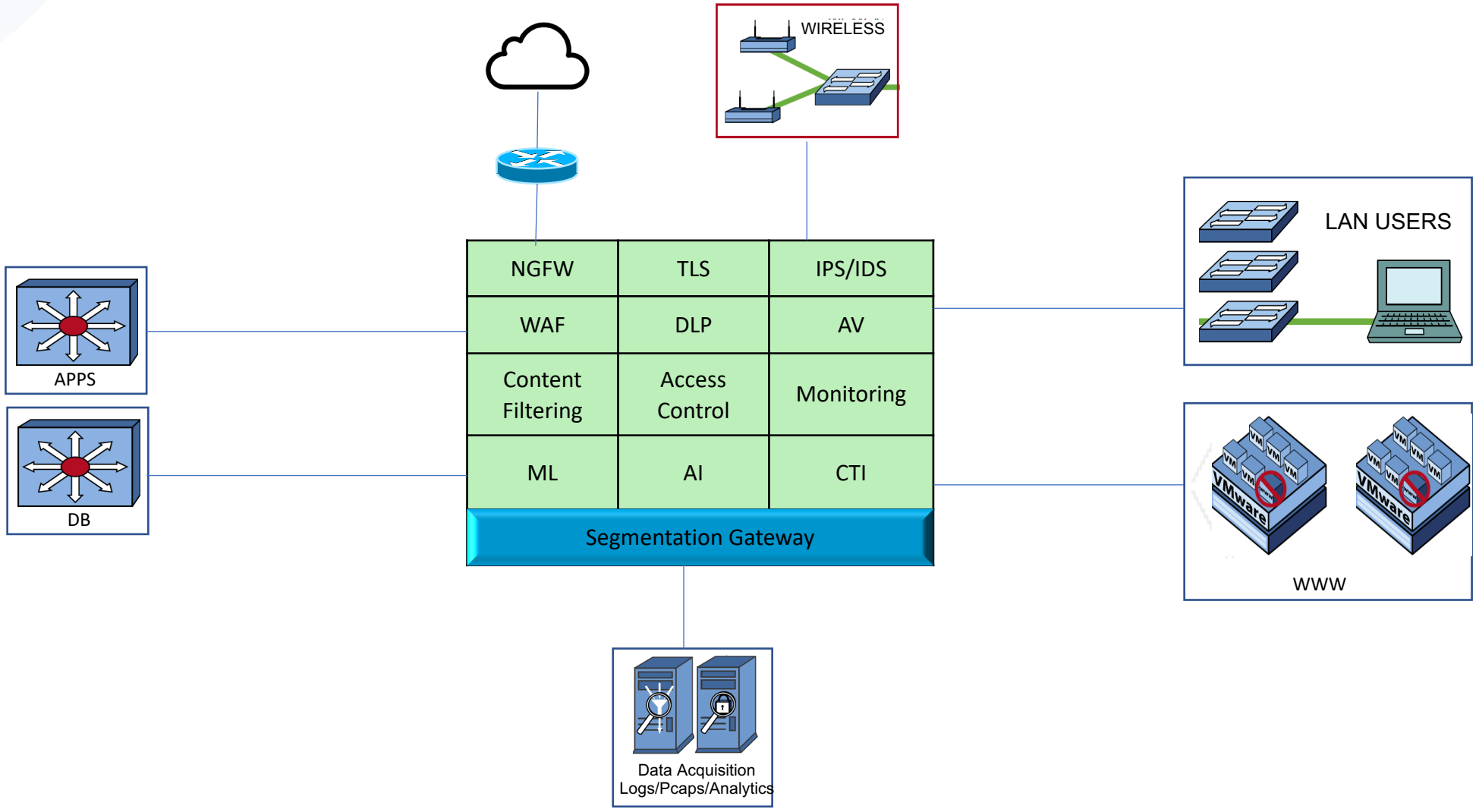
Firewall (Segmentation Gateway) Rules

Src	Dst	Service/Port	Policy	Notes
192.168.1.0/24	192.168.2.0/24	25	Allow	
192.168.3.10	10.0.20.0/24	443	Allow	
192.168.4.0/24	192.168.1.0/24	80	Allow	
…	…	…	…	
Any	Any	Any	Log	

Allow Business Traffic -> LOG Other Traffic -> Revise Logs -> Update Rules

Keep on LOGGING and REVISING logged traffic untill you are ready to DENY

Zero Trust Network Architecture



Adaptive Authorization

USER
LAN, Internet,
Partner, Contractor ..

Password, MFA

Time
Working hours, Dawn ..

GeoLocation

Device Type :
Compliant, Uncompliant
Manged, Unmanged

Connection Type :
WIFI, Internet, LAN ..

Anomaly Detection :
Failed logins,
Unusual time, location

Grant Access based on role and policy

Limit Access

Deny Access

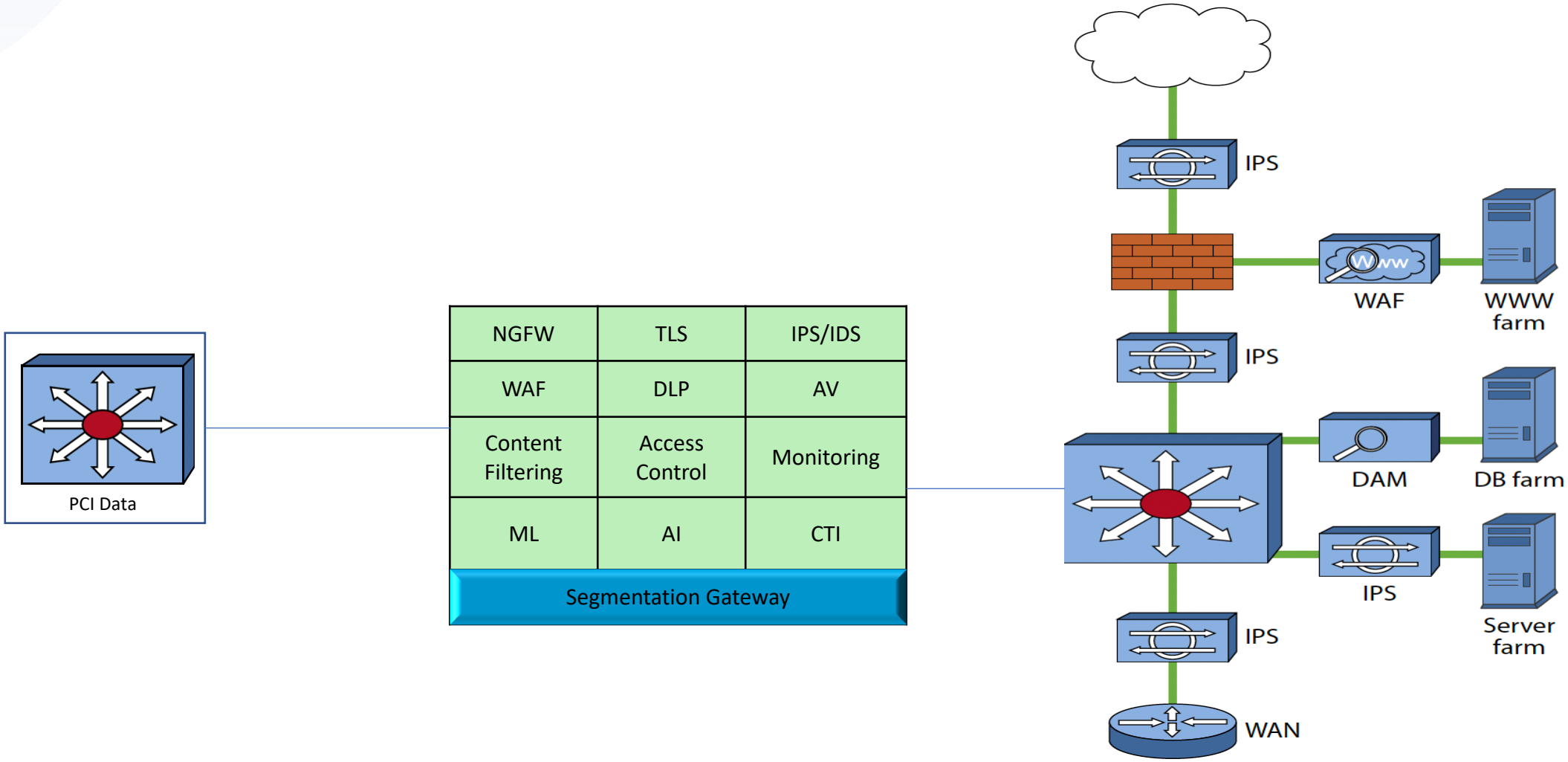
Request Password Reset

Request MFA

Remediate (Patch, AV ...)

Authentication happen at the session level, not the connection

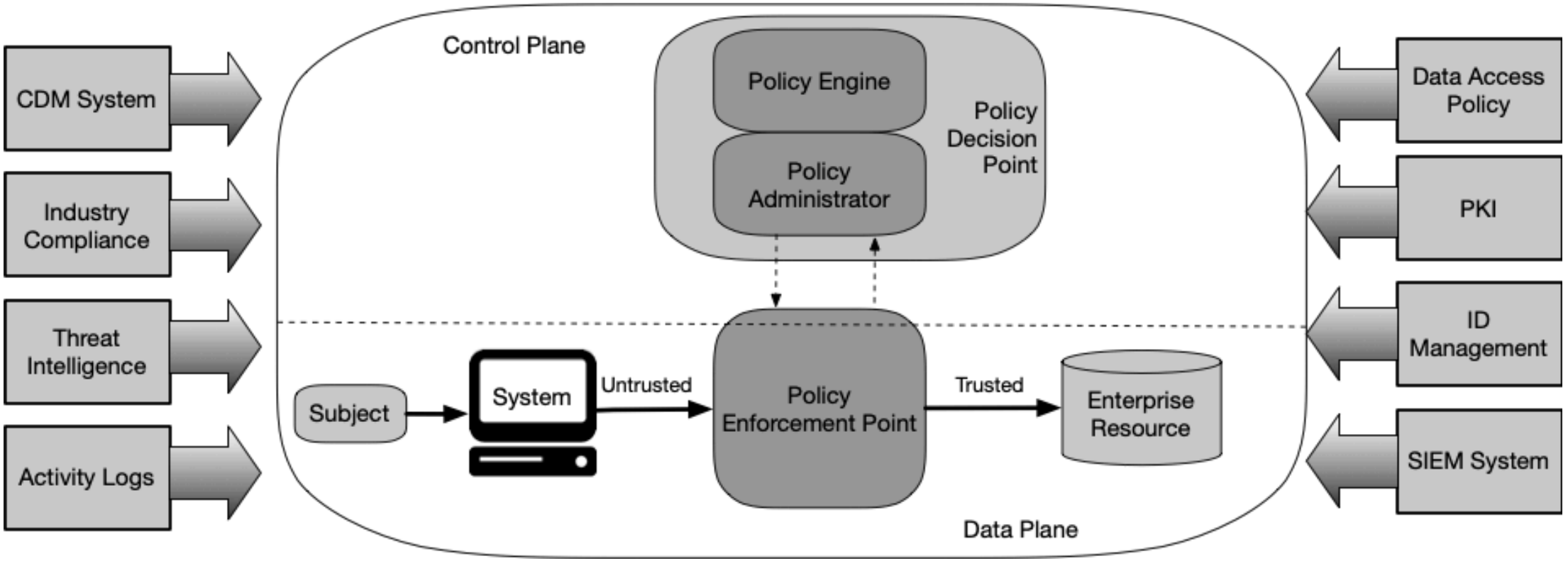
Plugging Zero Trust in Your Network



Technologies to Implement Zero Trust

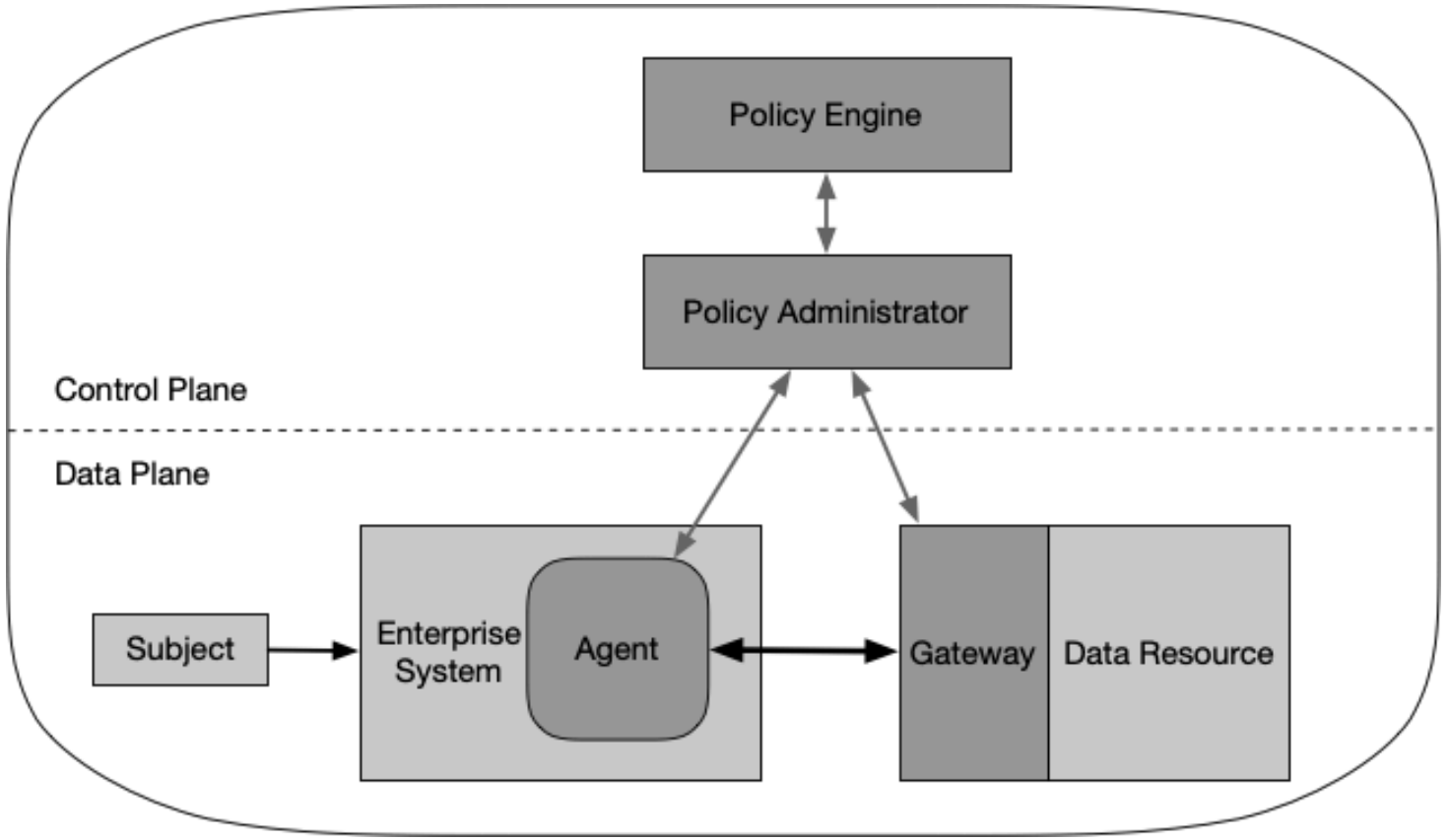
- ✓ NIST SP 800-207 - Zero Trust Architecture
- ✓ Firewalls – NGFW
- ✓ **SDP** – **S**oftware **D**efined **P**erimiter
- ✓ **CASB** - **C**loud **A**ccess **S**ecurity **B**roker
- ✓ **SASE** – **S**ecure **A**ccess **S**ecurity **E**dge

Core Zero Trust Logical Components (NIST)



From NIST SP 800-207

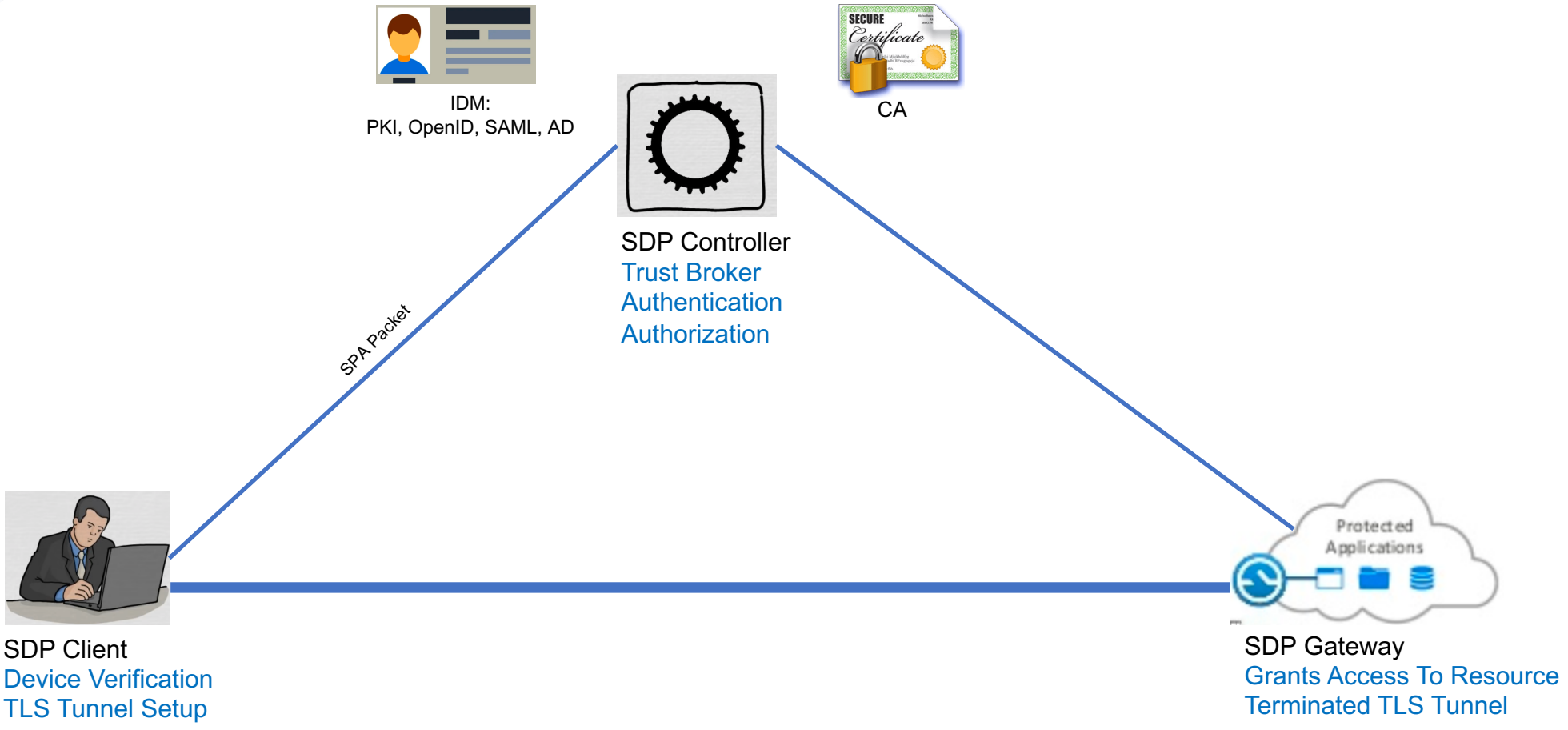
Deployed Variations of the Abstract Architecture



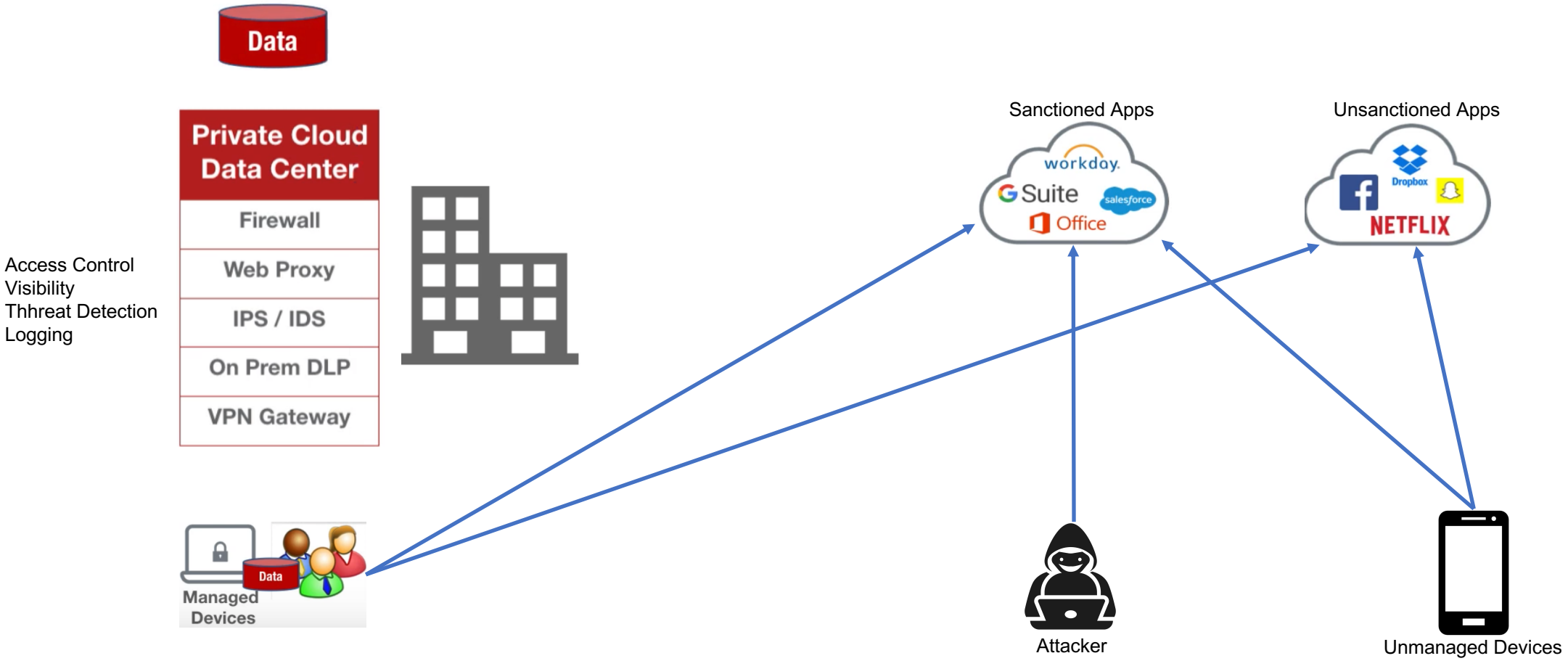
Device Agent/Gateway Model

From NIST SP 800-207

SDP – Software Defined Perimiter (Black Cloud)

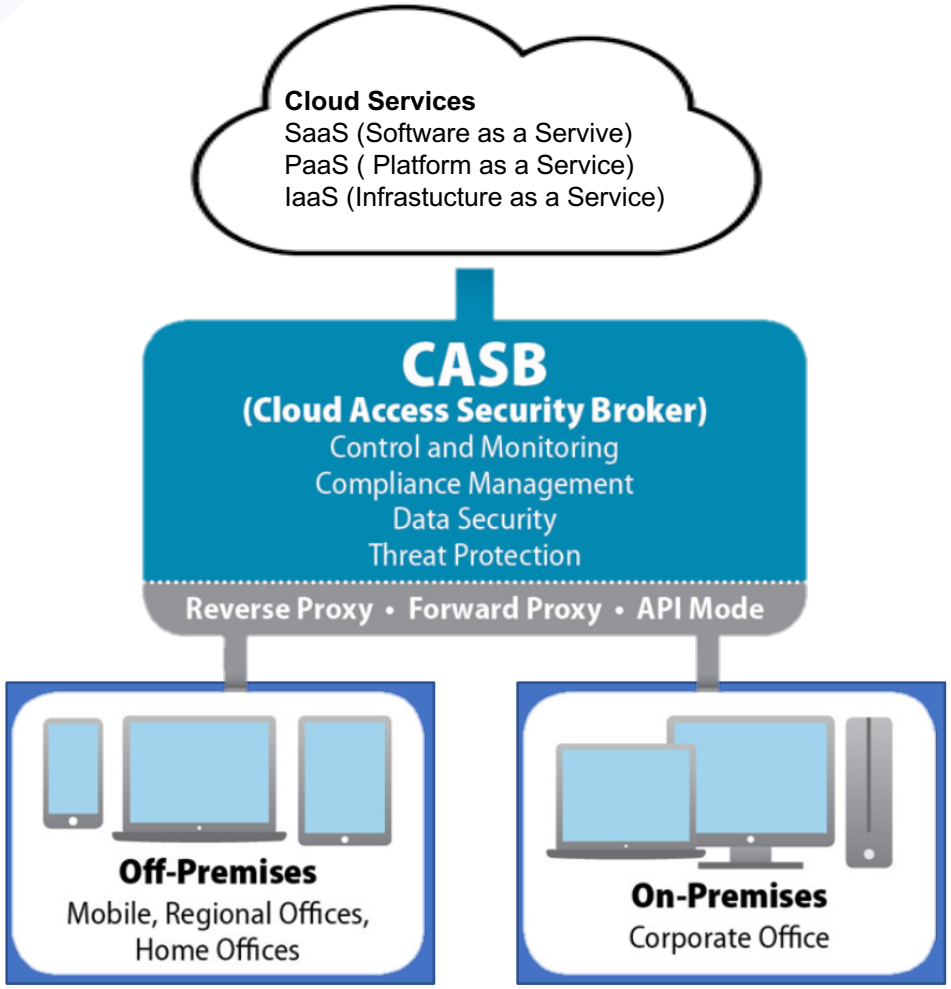


CASB – Cloud Access Security Broker



Source: Bitglass Youtube Channel

CASB Deployment



CASB can:

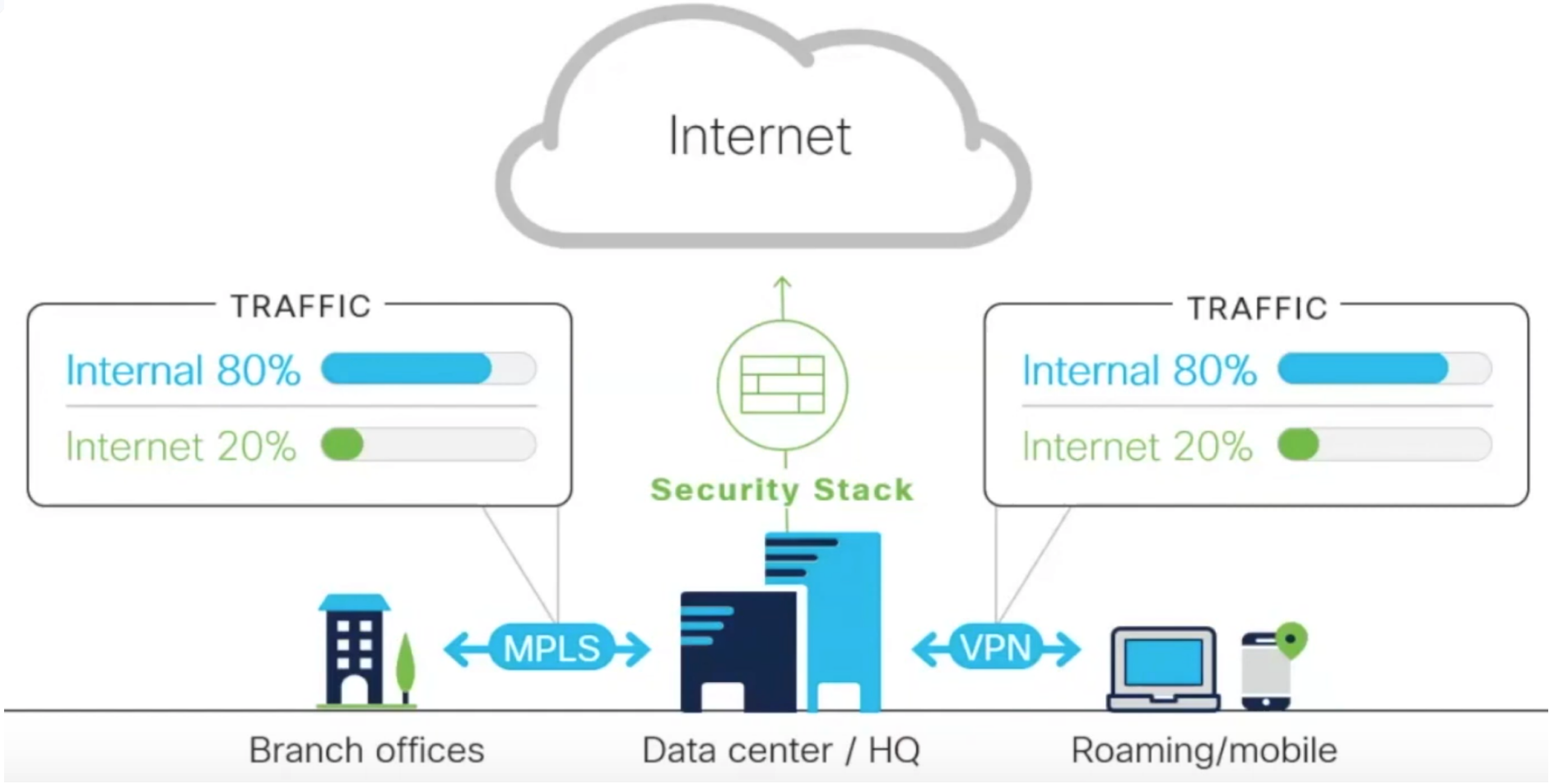
- Monitor cloud service usage across applications
- Establish cloud-related policy controls
- Enable regulatory compliance
- Do threat protection

If you are hosting your applicationss and data on the cloud, then CASB is the right solution.

SASE – Secure Access Service Edge

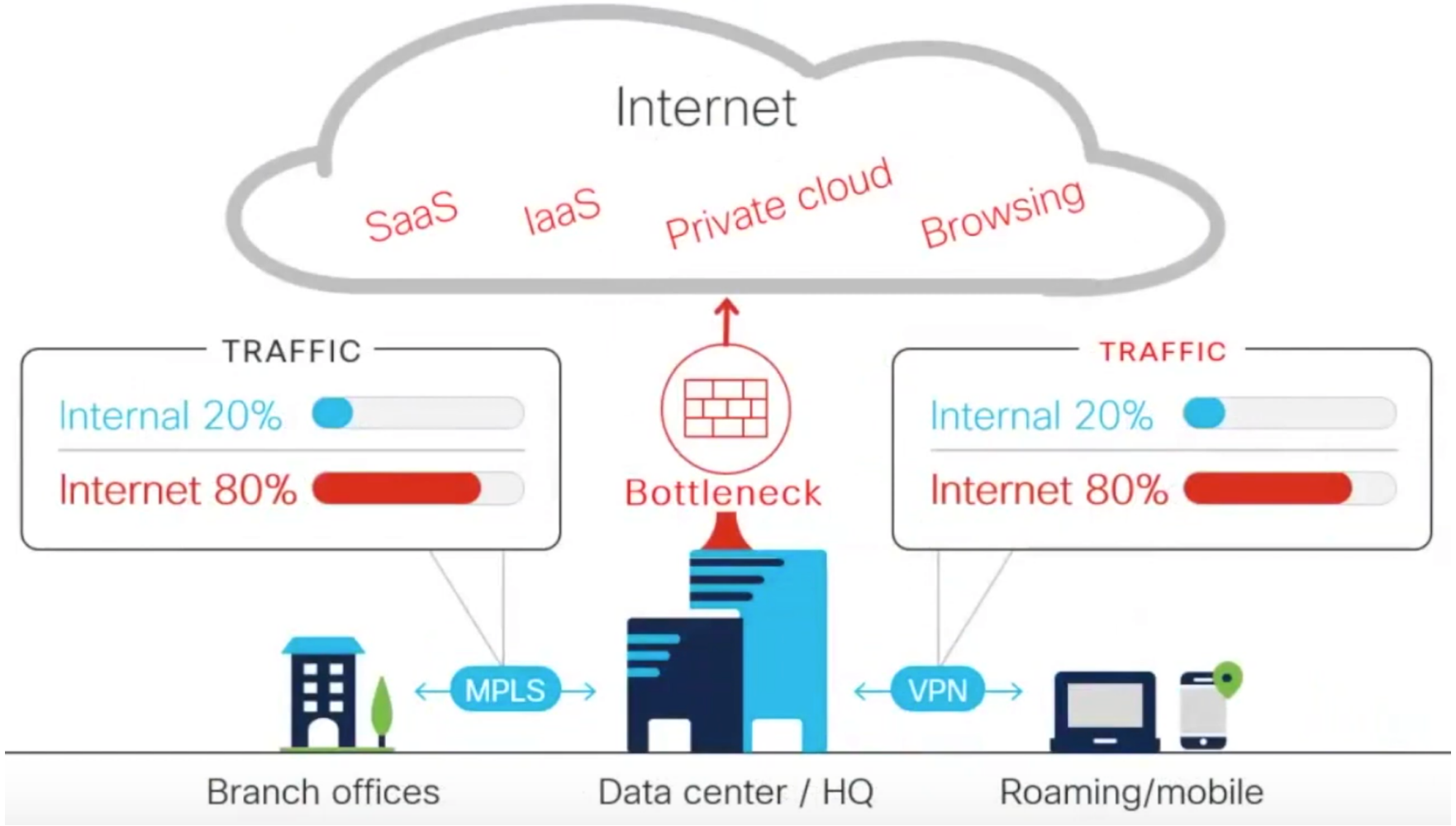
- ✓ A New Buzzword Coined by Gartner in 2019
- ✓ Convergence of Network Security & Cloud Security
- ✓ Everythhing is moving to the cloud (Apps & Data)
- ✓ 80%+ of enterprises have remote work capabilitie.
- ✓ SASE Solves Network Latency Problem

SASE – Secure Access Service Edge



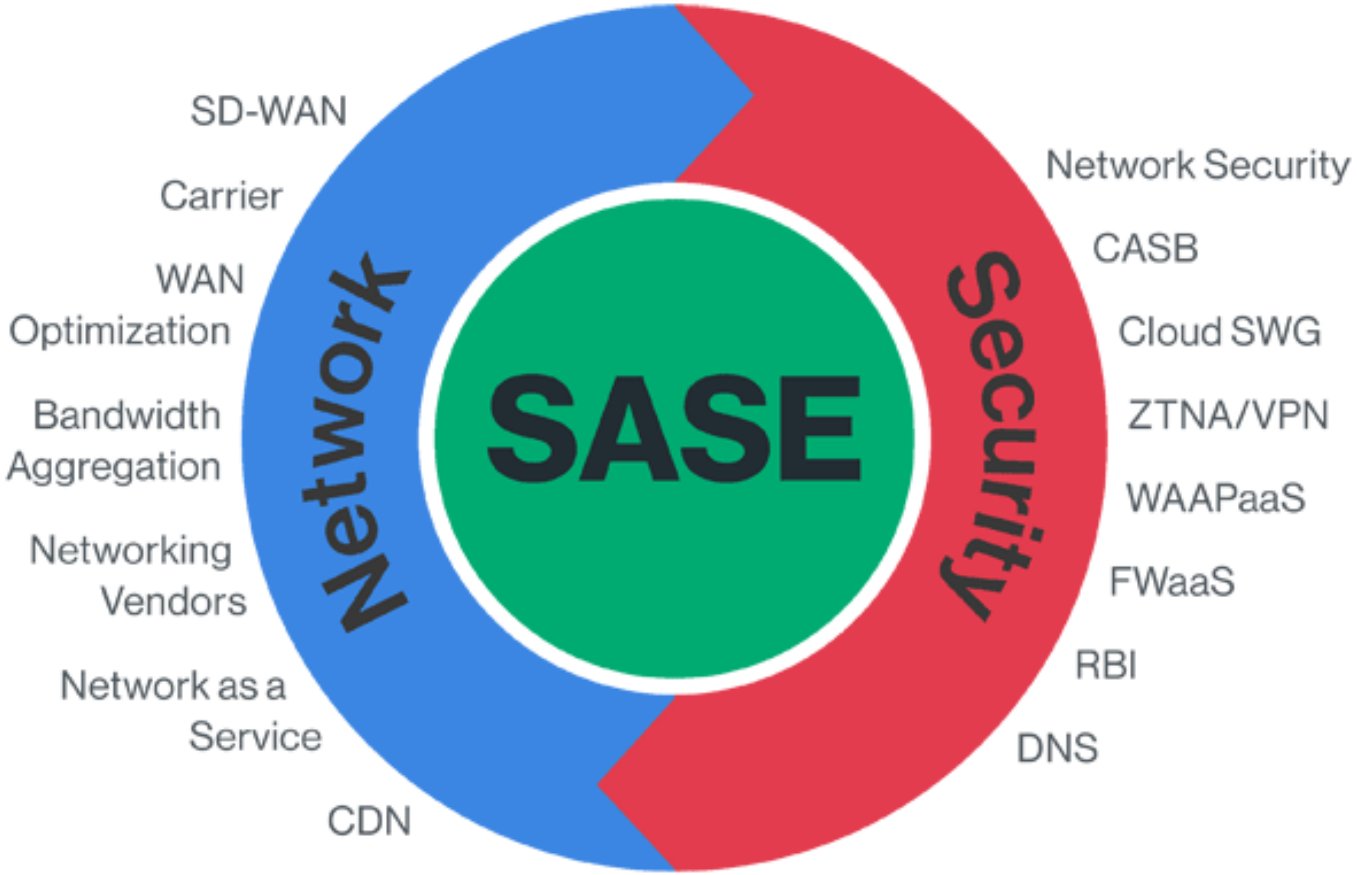
Source: Cisco Umbrella Youtube Channel

SASE – Secure Access Service Edge



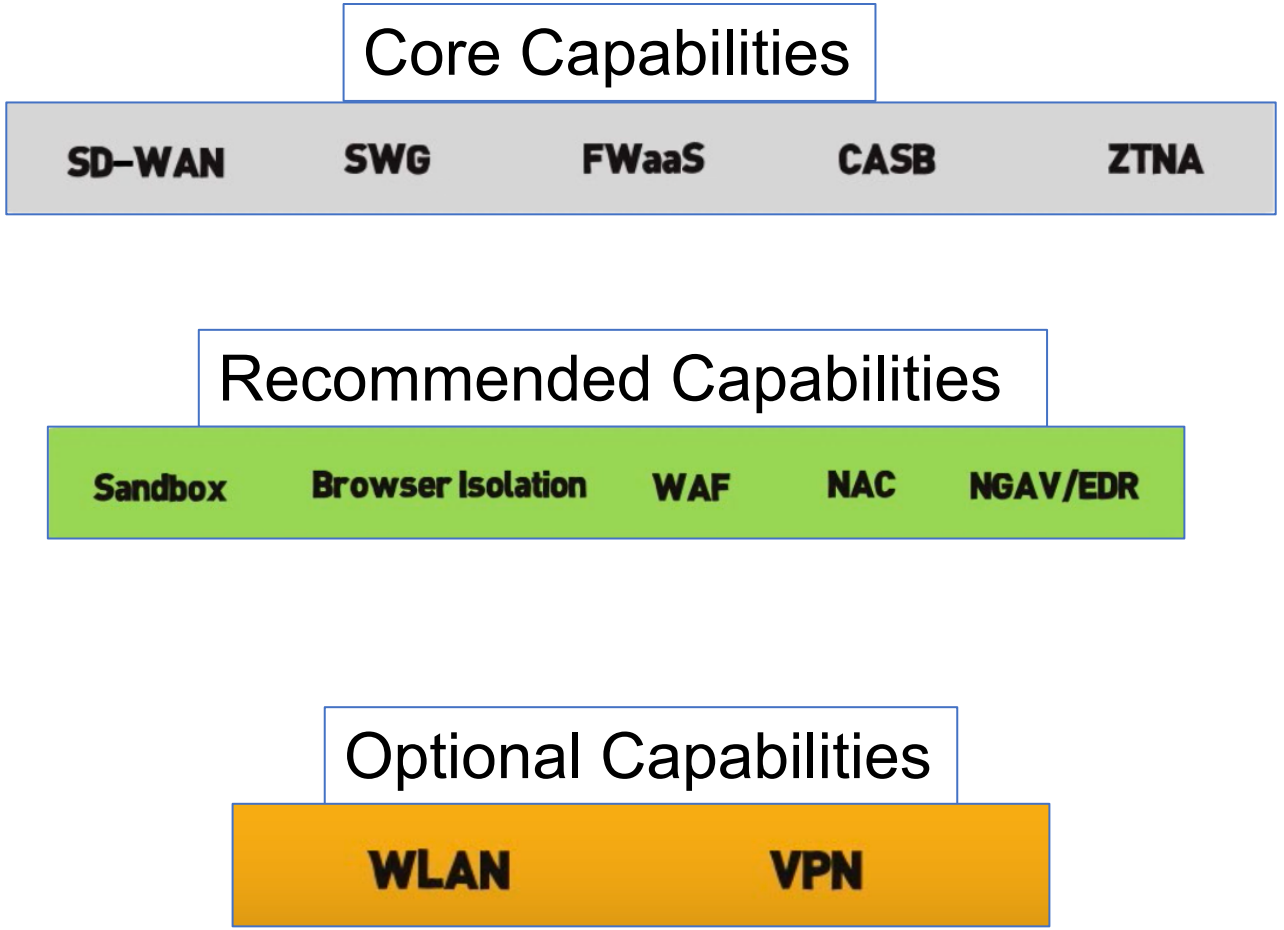
Source: Cisco Umbrella Youtube Channel

SASE – Secure Access Service Edge



Convergence of Network and Security

SASE – Secure Access Service Edge



Resources

Useful Zero Trust resources on github
https://github.com/pomerium/awesome-zero-trust

Pritunl Zero, Free Open Source SSH and Web ZT
https://zero.pritunl.com/

Conusl Community Version
https://www.consul.io/community.html

Infection Monkey – Zero Trust Assessment
https://www.guardicore.com/infectionmonkey/zero-trust.html

End

سبحانك اللهم و بحمدك
أشهد أن لا إله إلا أنت
أستغفرك و أتوب إليك

Your Questions ?