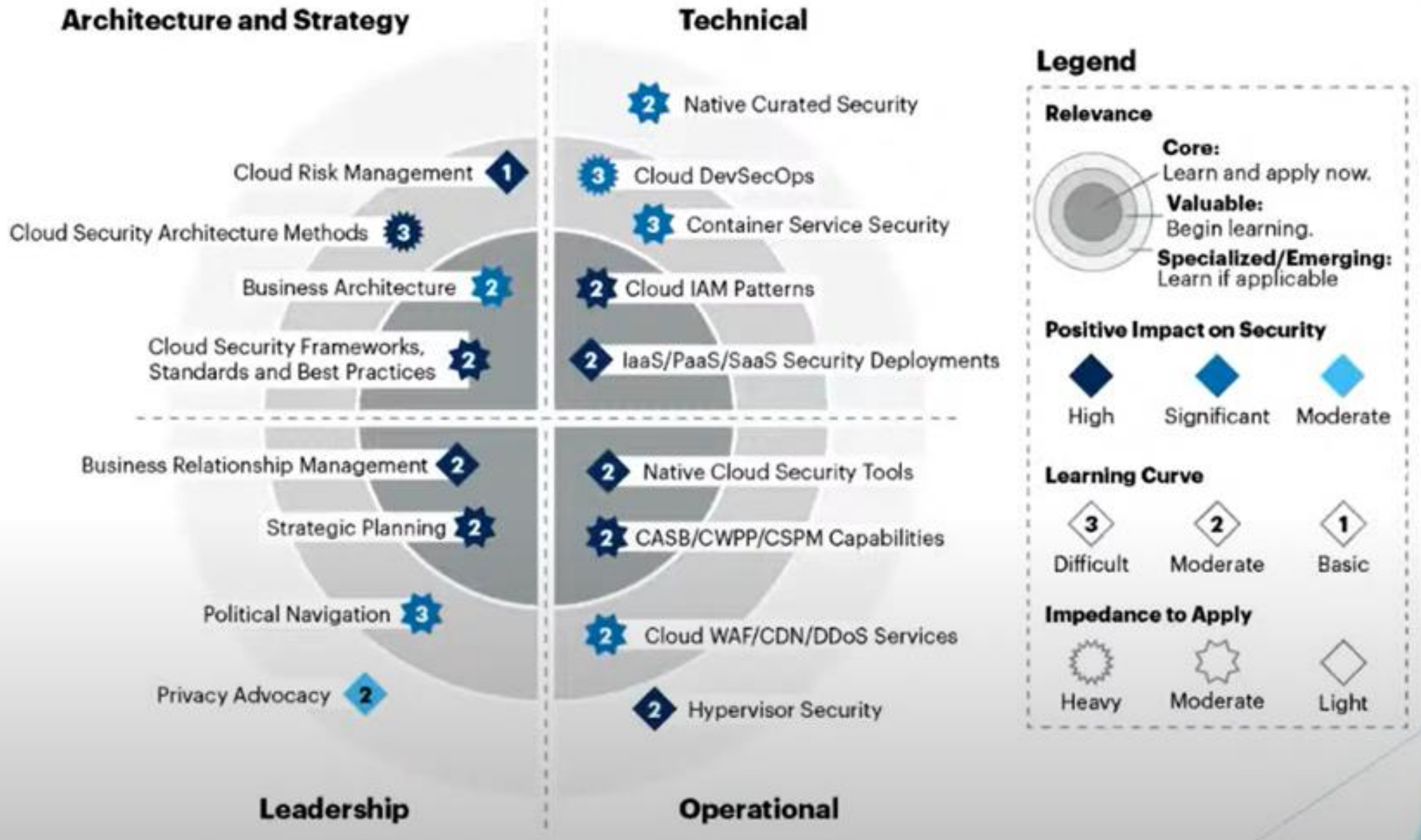
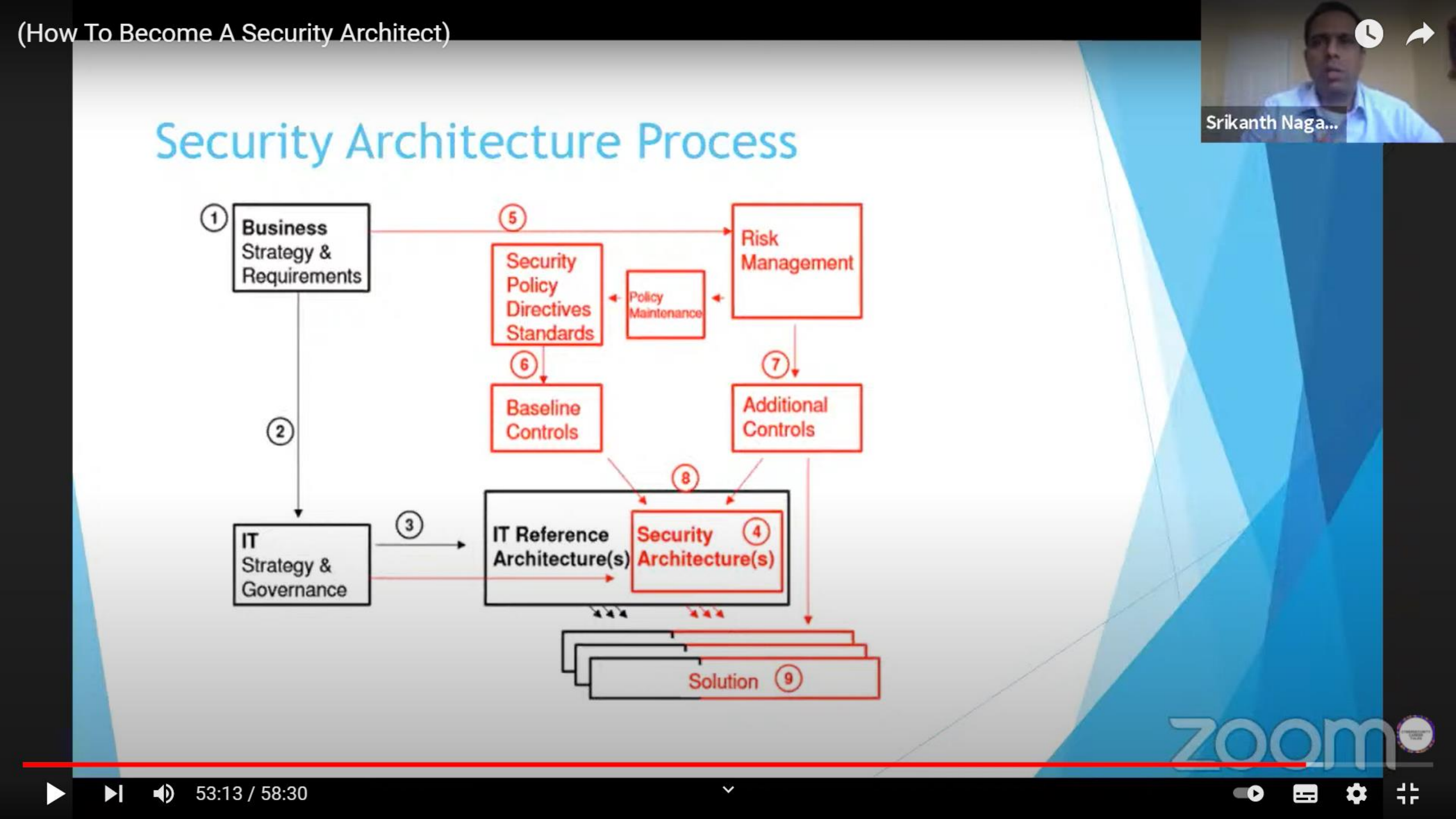
Cloud Security Architecture Skills Scope



(How To Become A Security Architect)



What is SAFE?

SAFE is a security **model** and **method** used to secure business. It focuses on threats–and best practices for defending against them. SAFE illustrates today's business challenges in a language that changes the way we think about security. It uses simple concepts to focus on the complexities of today, so that we're prepared for the challenges of tomorrow.

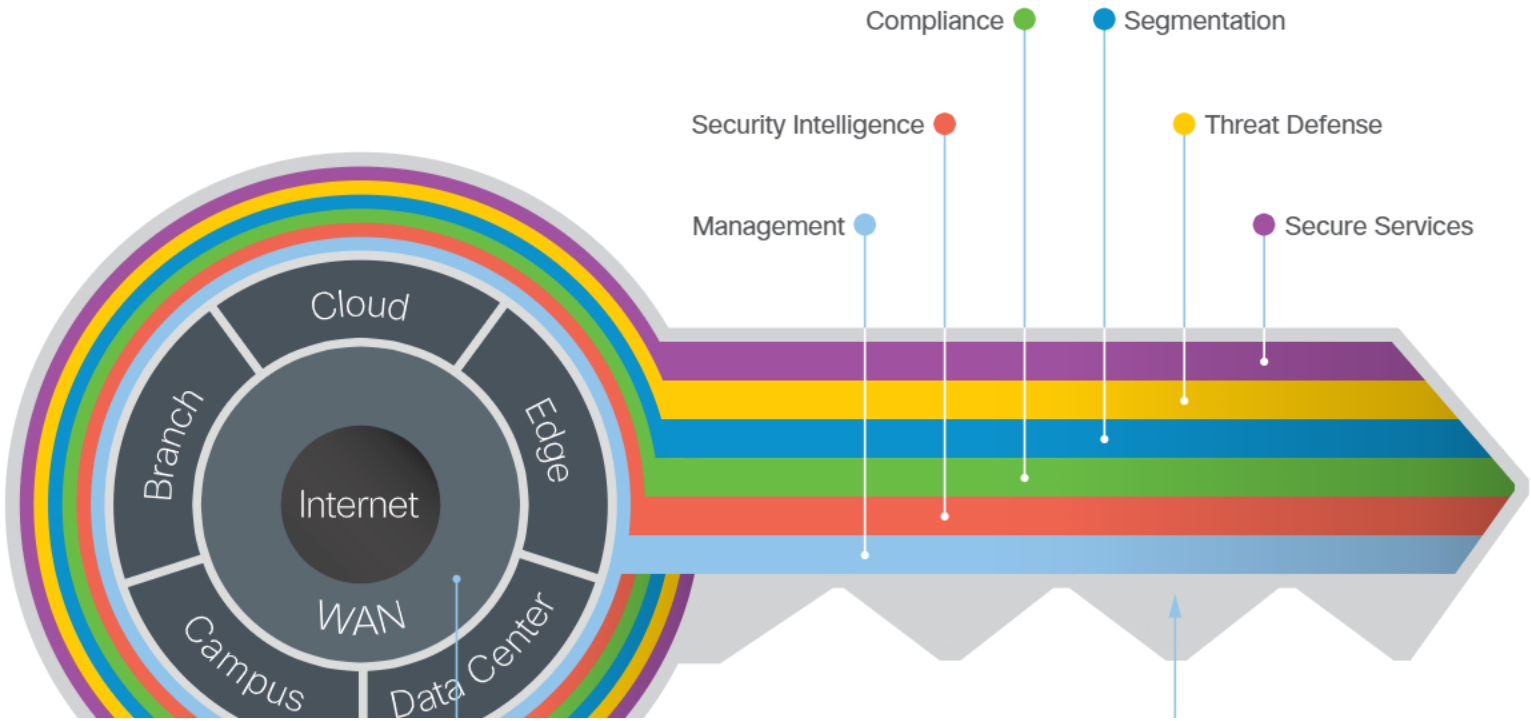
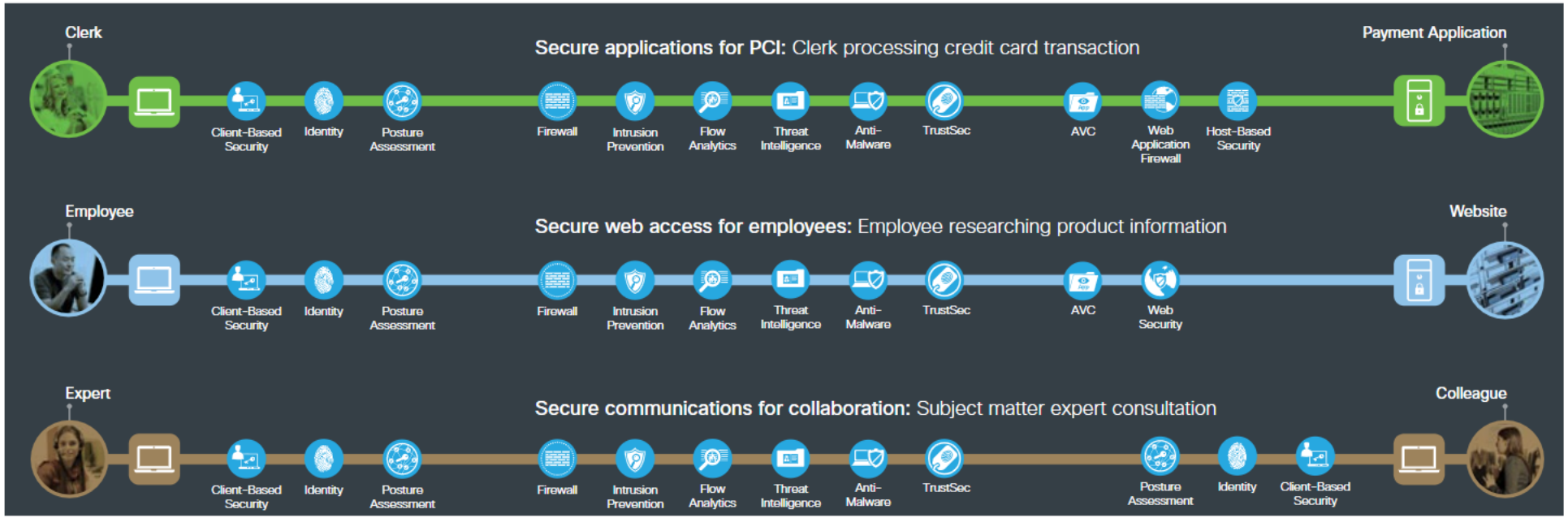


Table 1 *The SAFE Model Icons*

Phase/Example Icon	Description	Function
Key 	Organizational Model	The Key to SAFE provides the Key to simplify cybersecurity into Secure Places in the Network (PINs) for infrastructure and Secure Domains for operational guidance.
Business Flow 	Use Case	Business flows use colored lines to depict use cases and show where data flows through a network.
Threat 	Unauthorized Packets. This threat is blocked by firewalls.	The top security threats of an organization are catalogued.
Capability 	Firewall	Capabilities are used to describe security functions.
Architecture 	Logical Router. This logical router has firewall capability.	Architectures are used to logically arrange the security capabilities.
Design 	4451x with Firewall	Designs are used to provide specific products and services.

Return to Contents

Small Branch Capabilities and Business Flows



Based on where they are applied on the business flows, security capabilities can be grouped into three types: Foundational, Access, and Business.

Foundational Capabilities

Foundational Capabilities work together to protect applications and traffic. They use segmentation, visibility, and analysis in a comprehensive architectural approach. All business flows require foundational security capabilities.

Figure 10 *Foundational Capability Group: Secure Applications and Secure East West Traffic*

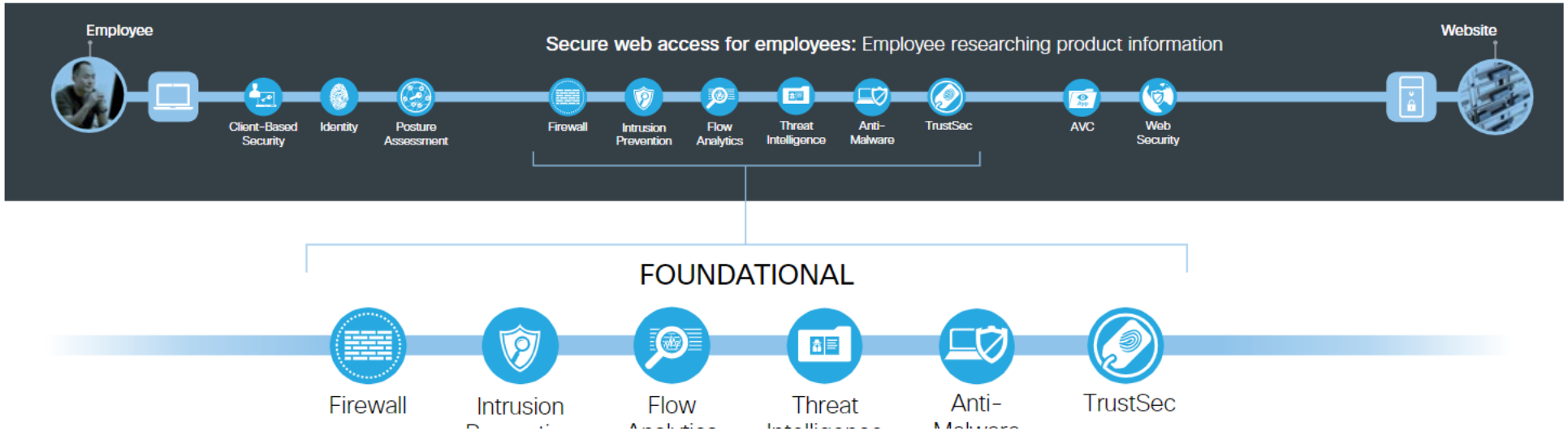


Table 2 *Foundational Capabilities*

Security Capability	Threat
Firewall: Stateful filtering and protocol inspection between layers and the outside Internet and service provider connections.	Unauthorized access and malformed packets between and within the branch.
Intrusion Prevention: Blocking of attacks by signatures and anomaly analysis.	Attacks using worms, viruses, or other techniques.
Flow Analytics: Network traffic metadata identifying security incidents.	Traffic, telemetry, and data exfiltration from successful attacks.
Threat Intelligence: Contextual knowledge of existing and emerging hazards.	Zero-day malware and attacks.
Anti-Malware: Identify, block, and analyze malicious files and transmissions.	Malware distribution across networks or between servers and devices.
TrustSec: Policy-based segmentation.	Unauthorized access and malicious traffic between branch layers.

Return to Contents

Figure 11 *Access Capability Group: Secure Access*

Table 3 *Access Capabilities*

Security Capability	Threat
Client-/Server-based Security: Security software for devices with the following capabilities:	
Anti-Malware	Malware compromising systems

Security Capability	Threat
Client-/Server-based Security: Security software for devices with the following capabilities:	
Anti-Malware	Malware compromising systems.
Anti-Virus	Viruses compromising systems.
Cloud Security	Redirection of user to malicious website.
Personal Firewall	Unauthorized access and malformed packets connecting to client.
Identity: Identity-based access.	Attackers accessing restricted information resources.
Posture Assessment: Client endpoint compliance verification and authorization.	Compromised devices connecting to infrastructure.

Business Capabilities

Business capabilities are used to secure risks introduced by business practices that are not handled by the foundational and access groups. Email, web access, and remote access directly connect to potential malicious entities (like the web, phishing, and compromised partners) which are outside the control of a company and require additional security capabilities.

Figure 12 *Business Capability Group: Secure Communications, Secure Web Access, Secure Remote Access*

Table 4 *Business Capabilities*

Table 4 *Business Capabilities*

Security Capability	Threat
Web Security: Web, DNS, and IP-layer security and control for the branch.	Attacks from malware, viruses, and redirection to malicious URLs.
Email Security: Messaging integrity and protections.	Infiltration and exfiltration via email.
Application Visibility and Control (AVC): Deep packet inspection (DPI) of application flows.	Attack tools hiding in permitted applications.
Web Application Firewalling: Advanced application inspection and monitoring.	Attacks against poorly-developed applications.
DDoS Protection: Protection against scaled attack forms.	Massively scaled attacks that overwhelm services.
Virtual Private Network (VPN): Encrypted communication tunnels.	Exposed services and data theft of remote workers and third parties.

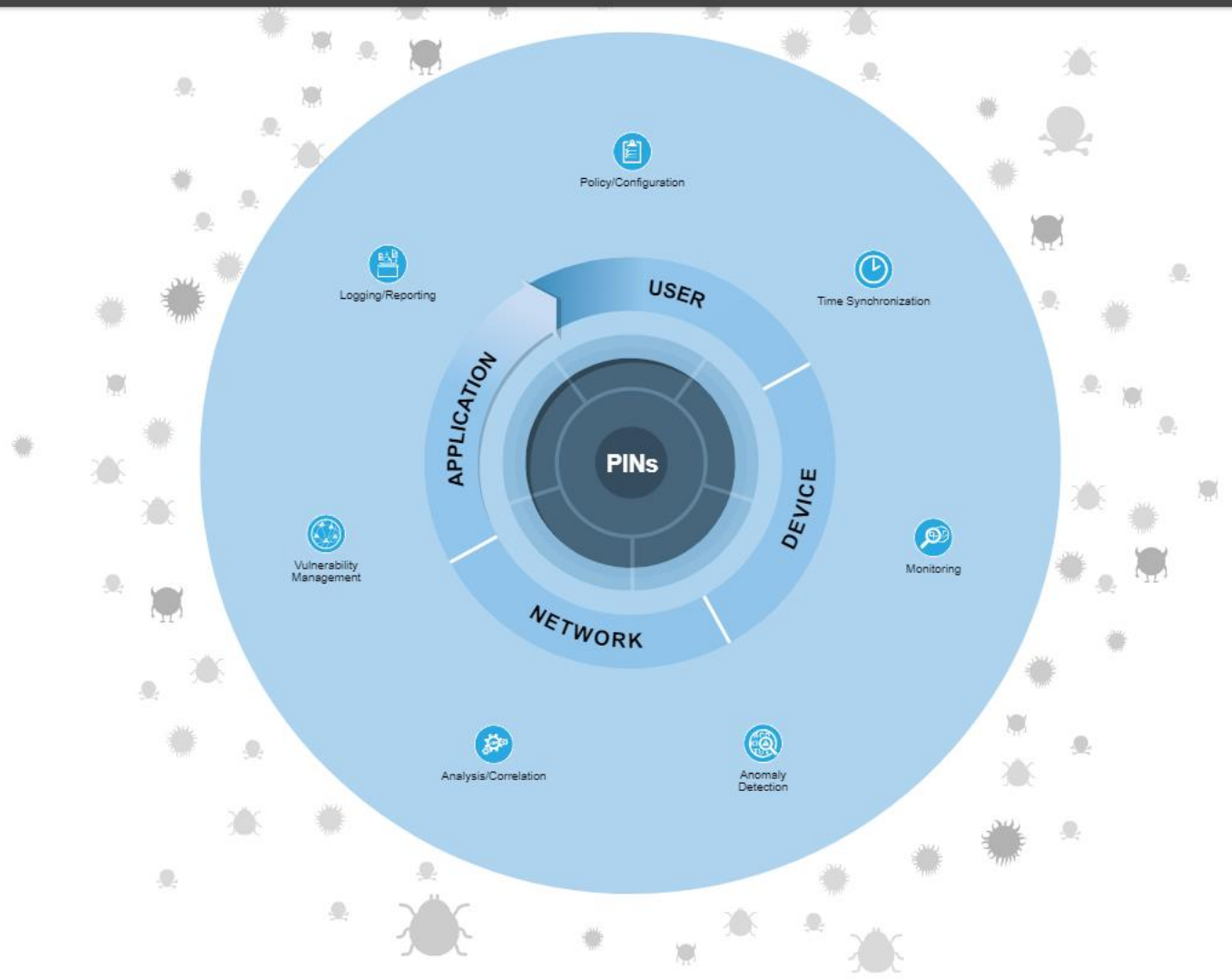


Figure 22 *Management Domain Capabilities*

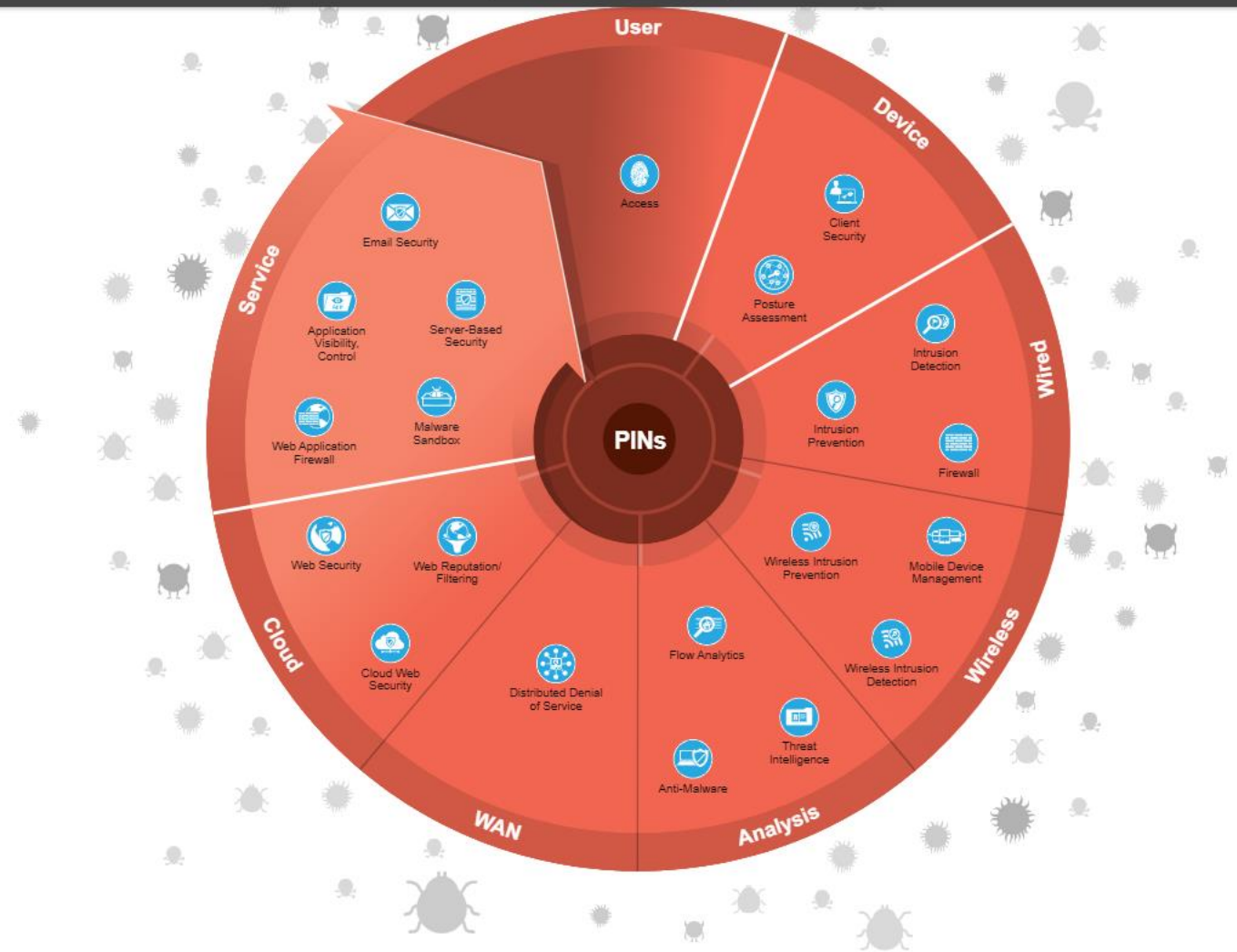


Figure 23 *Security Intelligence Capabilities*

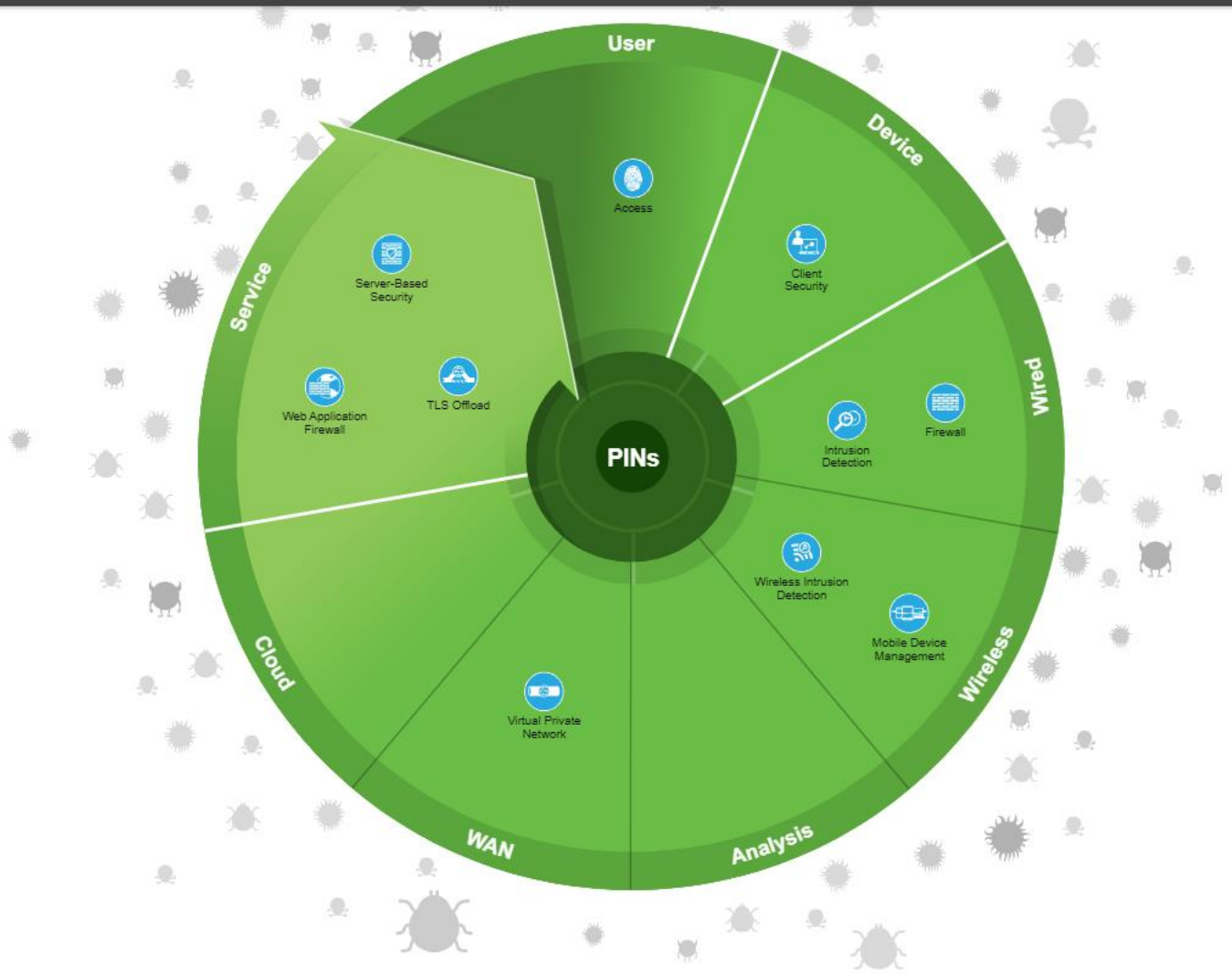


Figure 24 *Compliance Capabilities*

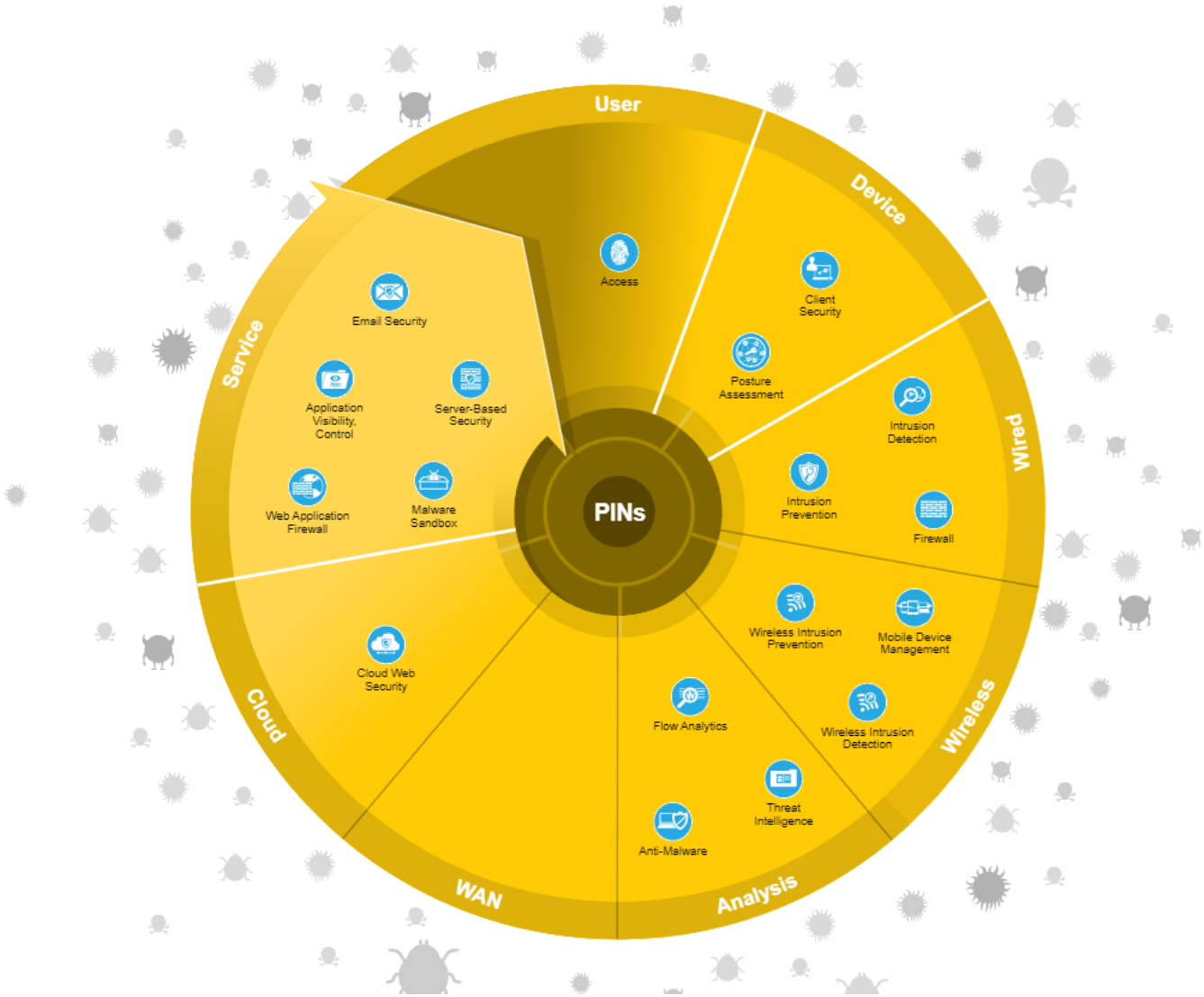
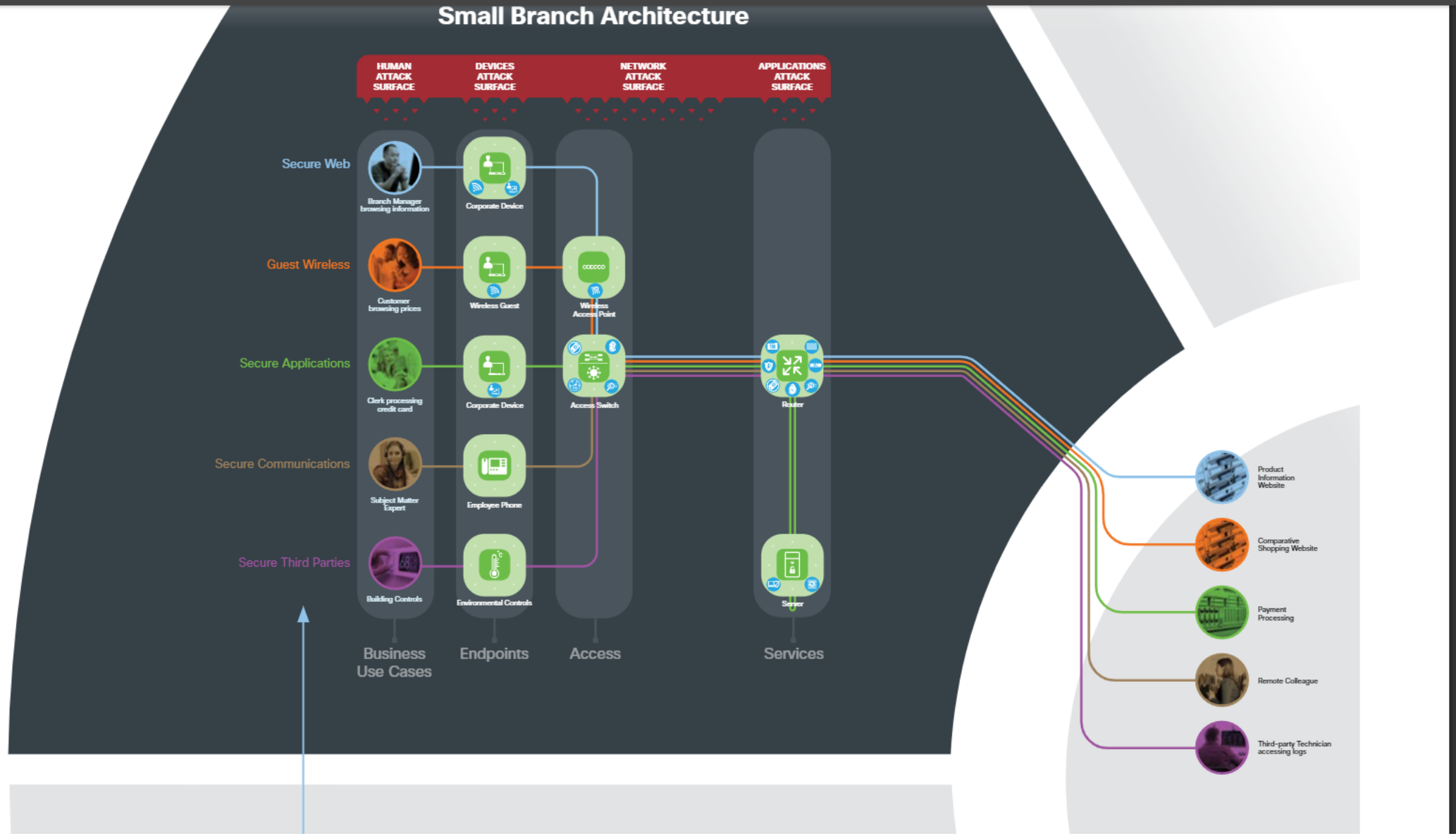

User
Device
Wired
Wireless
Analysis
WAN
Cloud
Service
PINs
Access
Client Security
Posture Assessment
Intrusion Detection
Intrusion Prevention
Firewall
Wireless Intrusion Prevention
Mobile Device Management
Wireless Intrusion Detection
Threat Intelligence
Anti-Malware
Flow Analytics
Cloud Web Security
Web Application Firewall
Malware Sandbox
Application Visibility, Control
Server-Based Security
Email Security

Table 5 *Cisco Security Capabilities and Threats*

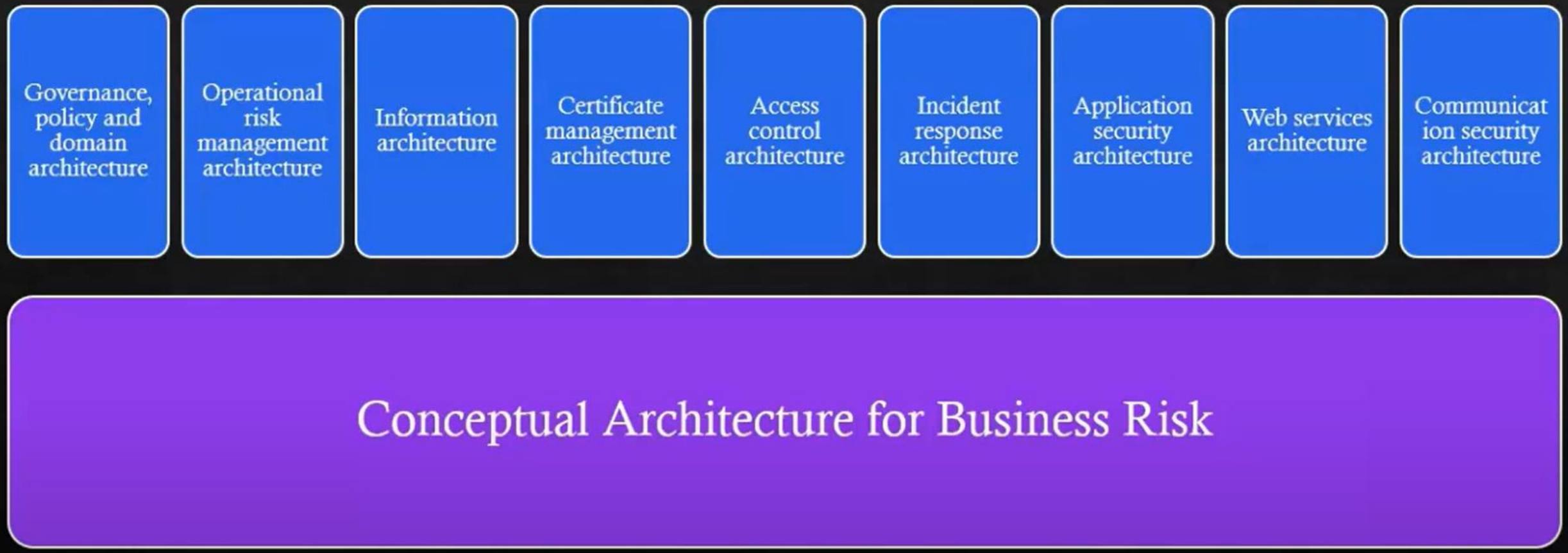
Attack Surface	Capabilities	Threats	Places in the Network	Recommended Products
Human				
Users: Employees, third parties, customers, and administrators.	**Identity/Authorization:** Restriction of user access to services and resources.	**Unauthorized Network Access:** Attackers accessing restricted information.	Secure Branch Secure Campus Secure Cloud Secure Data Center Secure Edge Secure WAN	Identity Services Engine
Devices				
Clients: Devices such as PCs, laptops, smartphones, tablets.	**Client-Based Security:** Security software to protect clients.	**Malware:** Viruses or malware compromising systems.	Secure Branch Secure Campus Secure External Zones	Cisco Advanced Malware Protection for Endpoint Anti-Virus AnyConnect Cisco Umbrella
	Anti-Malware	Malware compromising systems.		
	Anti-Virus	Viruses compromising systems.		
	Cloud Security	Redirection of user to malicious website.		
	Personal Firewall	Unauthorized access and malformed packets		
	Posture Assessment: Client endpoint	**Virus and Malware:**	Secure Branch Secure Campus	AnyConnect Agent Centralized Identity



To Design a Security Architecture

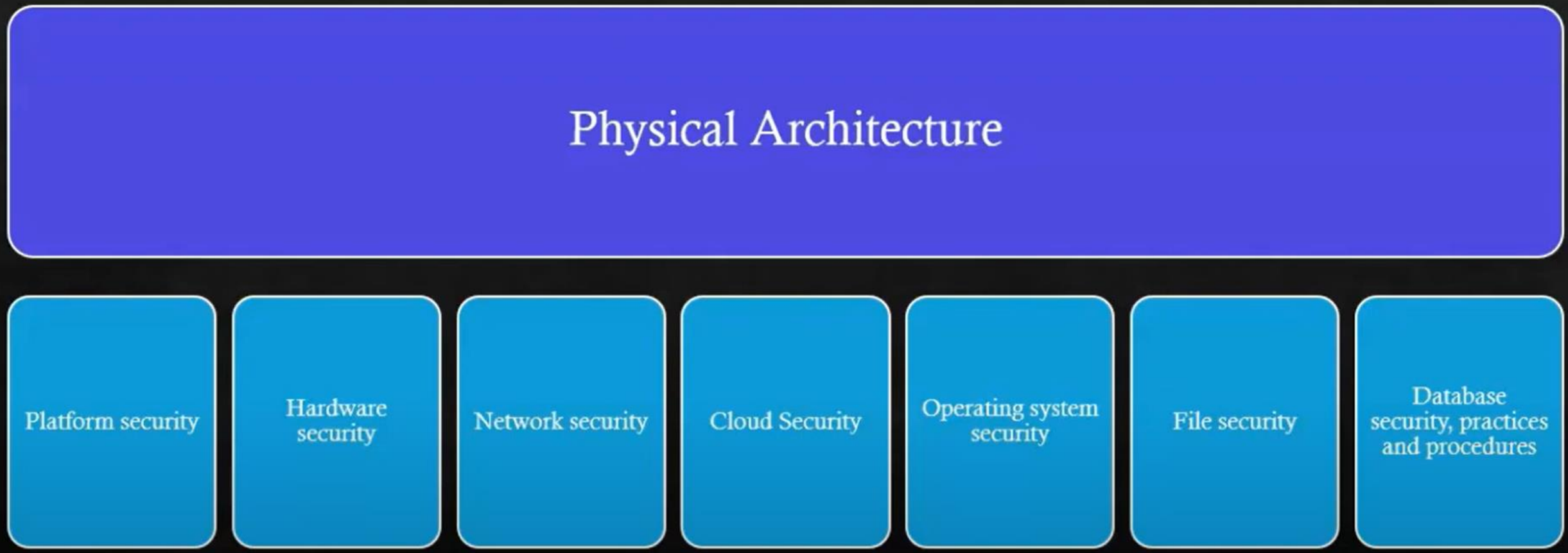
- **Identify business objectives, goals and strategy**
- Identify business attributes that are required to achieve those goals
- Identify all the risk associated with the attributes that can prevent a business from achieving its goals
- Identify the required controls to manage the risk
- Define a program to design and implement those controls

What Security Architecture means & How to create one ?



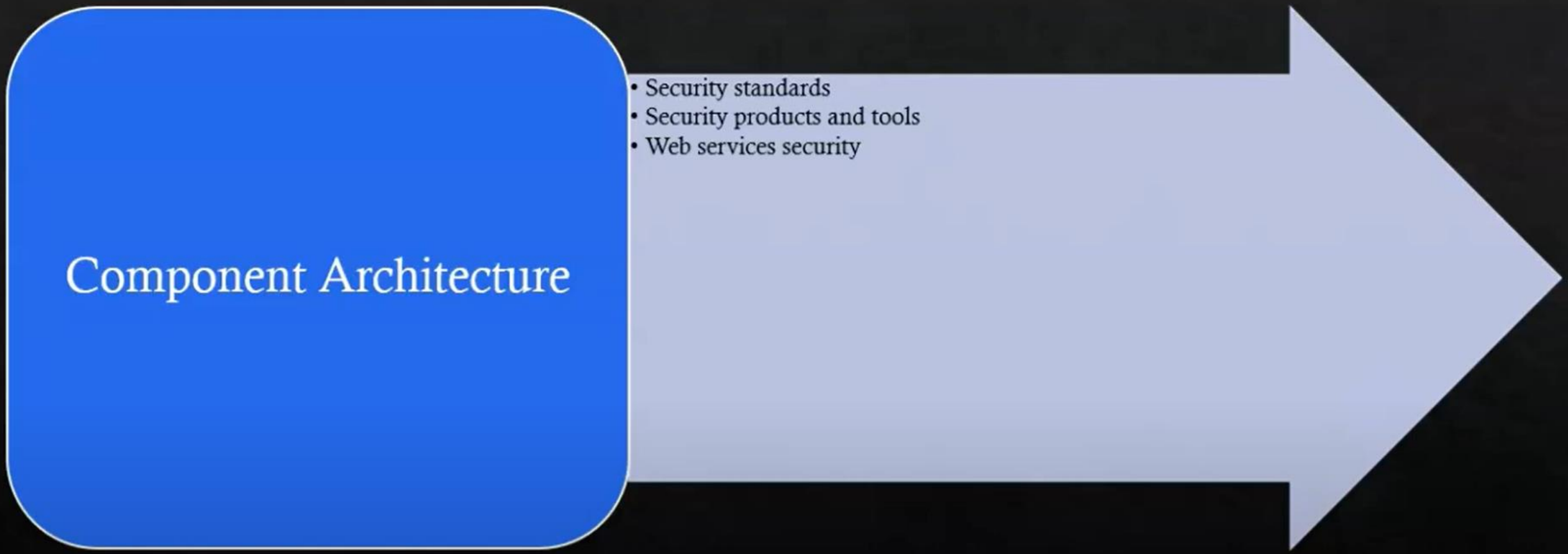
What Security Architecture means & How to create one ?

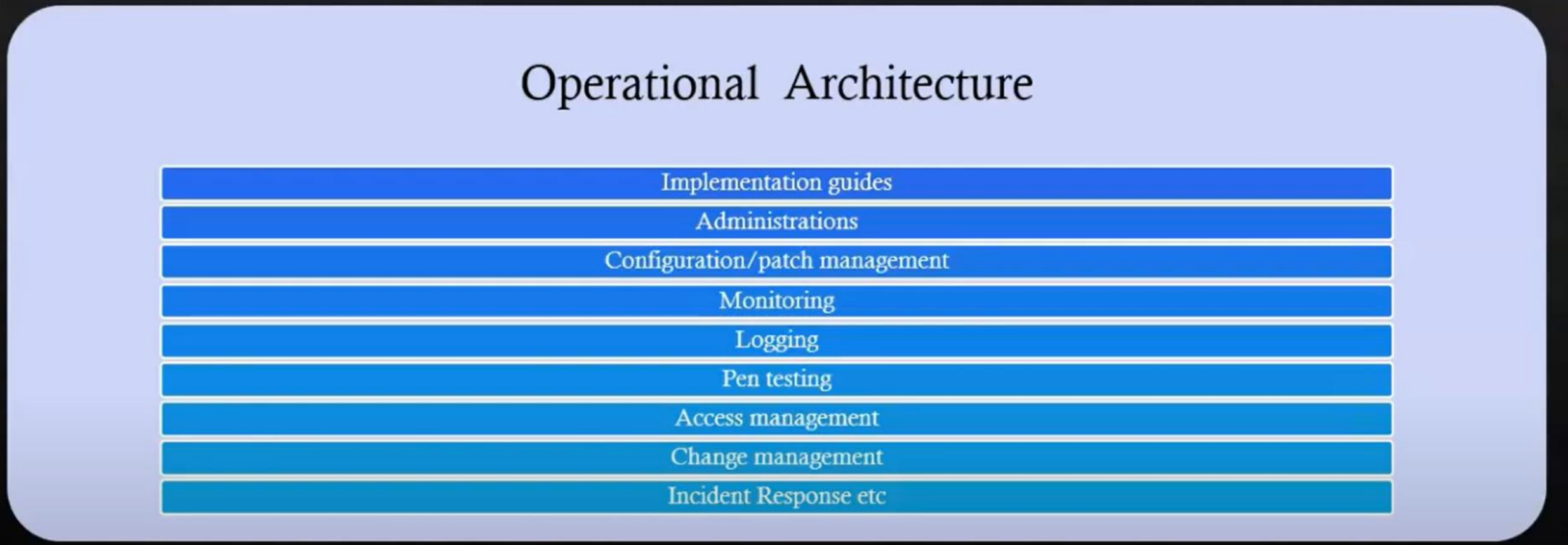
Press Esc to exit full screen



2:56 / 4:44

What Security Architecture means & How to create one ?





What Security Architecture means & How to create one ?

Press Esc to exit full screen

4:25 / 4:44

Security Controls

		CONTROL FUNCTIONS		
		Preventative	Detective	Corrective
CONTROL TYPES	Physical	Fences, gates, locks	CCTV and surveillance camera logs	Repair physical damage, re-issue access cards
	Technical	Firewall, IPS, MFA solution, antivirus software	Intrusion detection systems, honeypots	Patch a system, terminate a process, reboot a system, quarantine a virus
	Administrative	Hiring and termination policies, separation of duties, data classification	Review access rights, audit logs, and unauthorized changes	Implement a business continuity plan or incident response plan

https://www.f5.com

Introduction to Security Architecture

OSI MODEL

Application	Layer 7
Presentation	Layer 6
Session	Layer 5
Transport	Layer 4
Network	Layer 3
Data Link	Layer 2
Physical	Layer 1

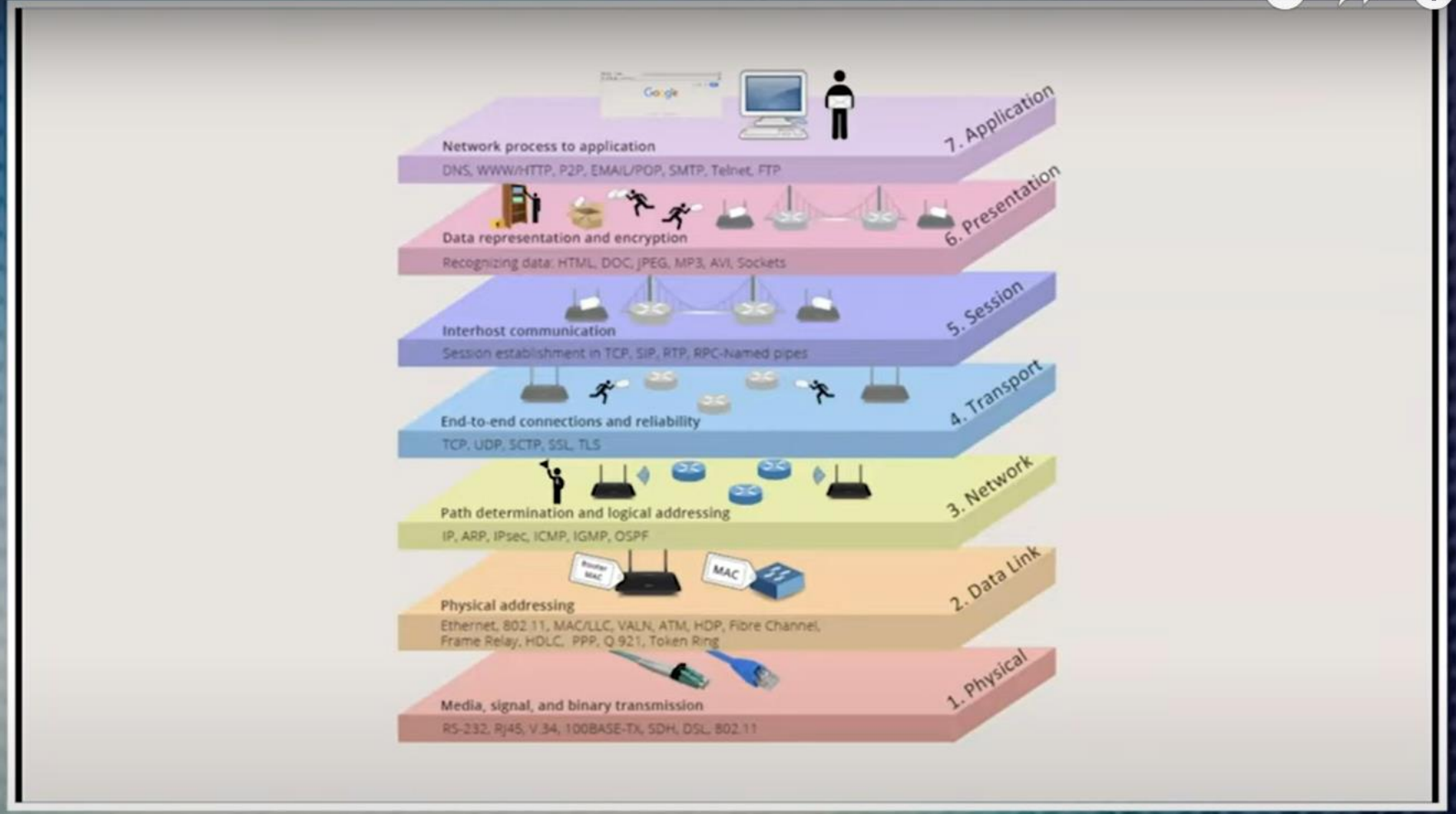
30:10

NEW TO CYBER
Summit 2021

SANS SUMMITS

23:07 / 58:32

Introduction to Security Architecture



NEW TO CYBER
Summit 2021

SANS SUMMITS

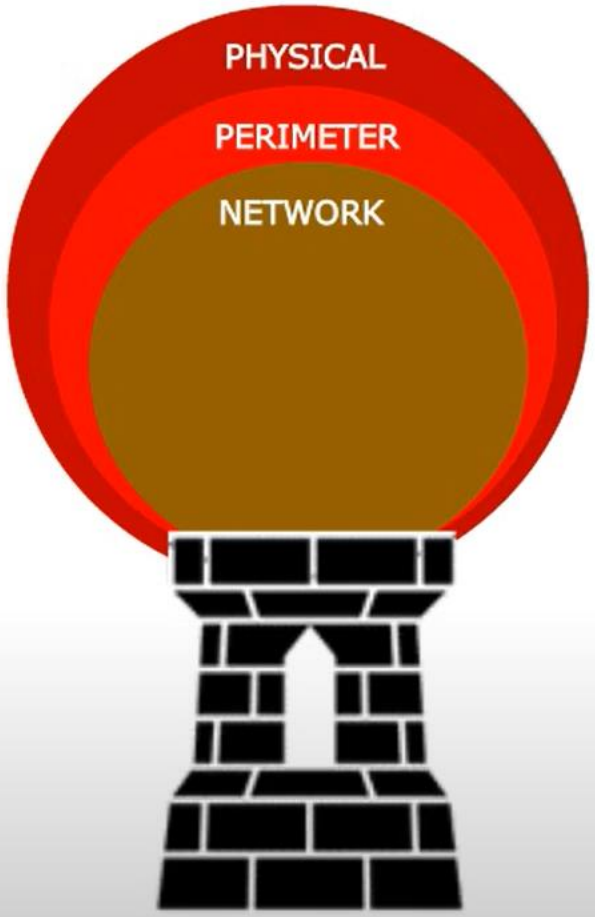
27:53 / 58:32

Application	XXS, SQL injection, data leaks, spam	Application Attacks
Presentation	SSL, XML encryption, images	
Session	Sockets, RPC, NetBIOS auth., SNMP	DDoS
Transport	SYN/ACK attacks, port scans, MitM	
Network	Port filters, IP frag, spoofing, smurfs	Network Attacks
Data Link	VLANs, ARP poisoning	
Physical	Management interface segmentation	

NEW TO CYBER
Summit 2021

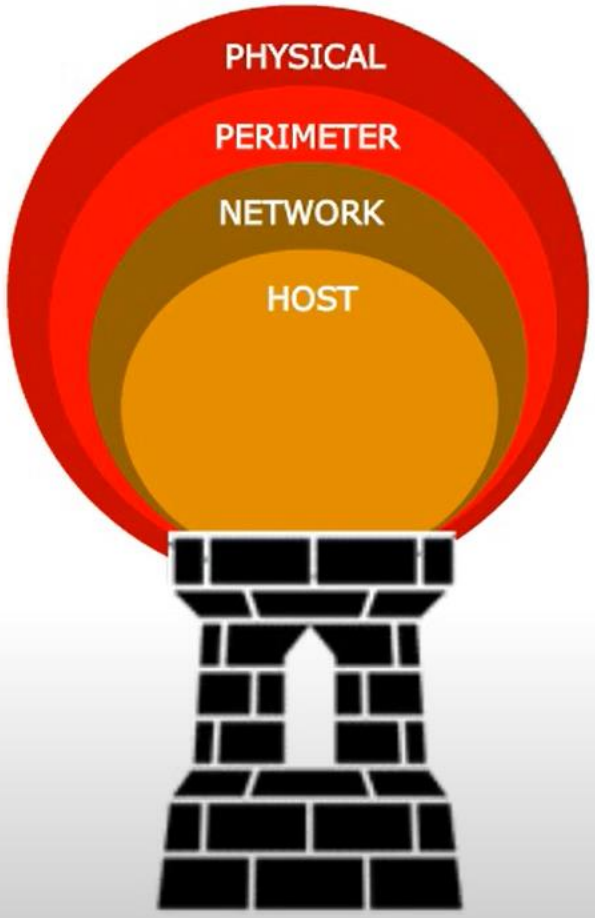
SANS SUMMITS

Security Architecture: Network Layer



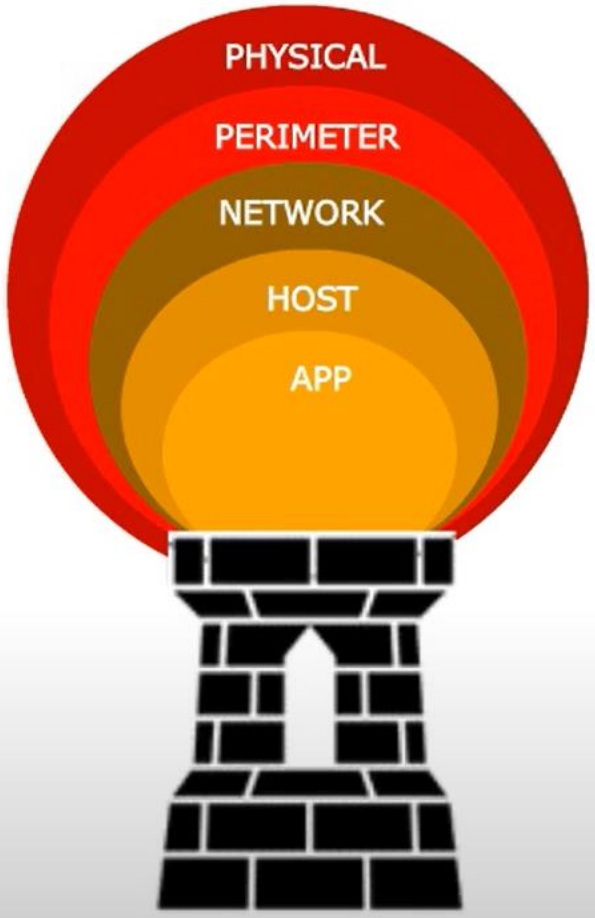
- IPS
- Email
- Window communication control
- Web application firewall (WAF)
- Data acquisition network (DAN/SIEM)
- Network Access Control (NAC) & Logical Access Controls
- Network time protocol (NTP)
- Wireless network security
- Password management (vaults)
- Security Operations Center (SOC)

Security Architecture: Host Layer



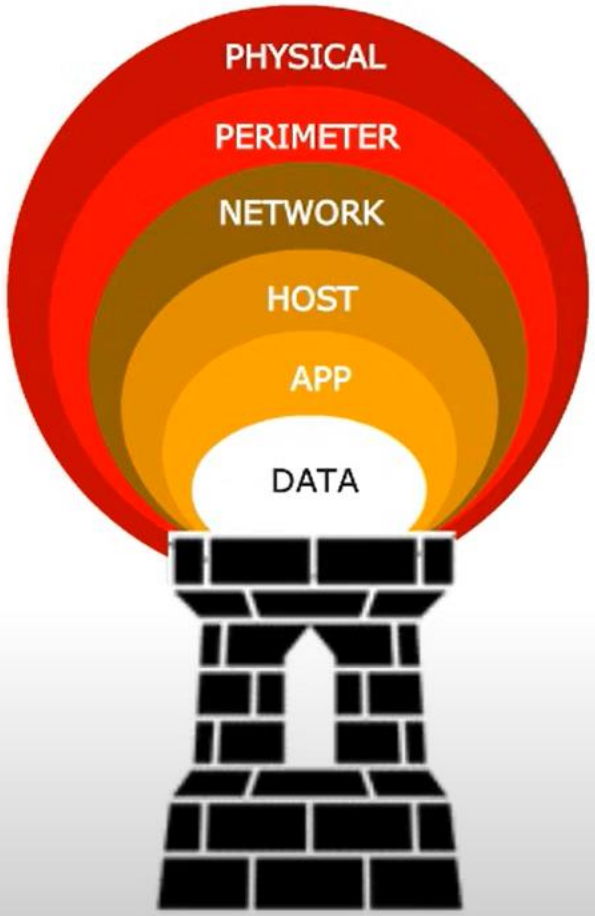
- Host based FWs
- Anti virus & malware
- Vulnerability scanning & patching
- CMDB and asset management
- Server Access Controls
- OS hardening guidelines
- Mobile devices and MDM
- Privileged access management
- Thumb drive protection

Security Architecture: Application Layer



- SSL certs (data-in-flight)
- Role Base Access Control (RBAC/ABAC)
- Application code review
- Key management systems
- Sourcecode management security

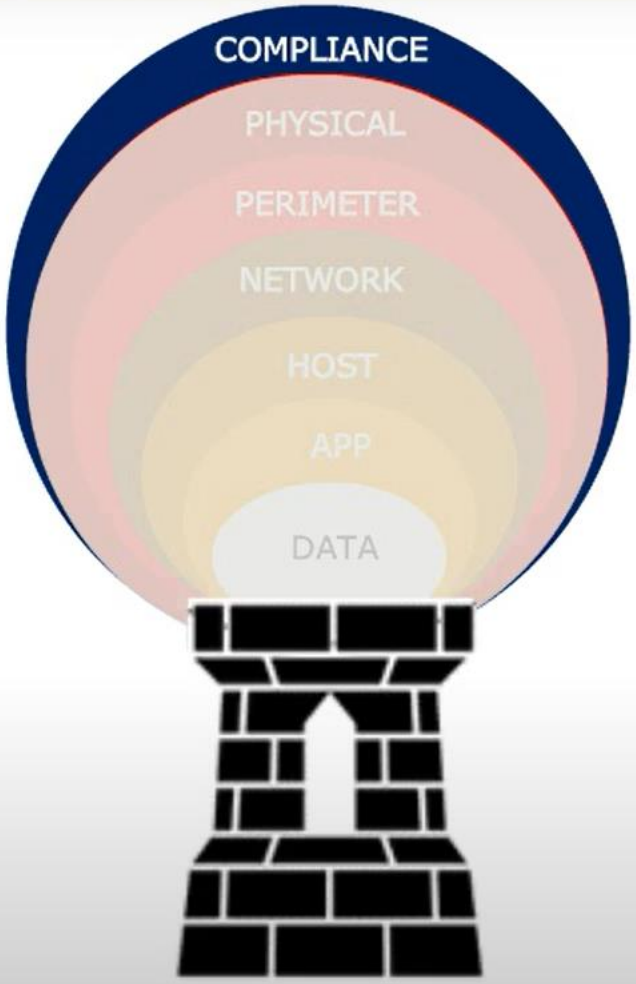
Security Architecture: Data Layer



- SSL certs (data-in-flight)
- Role Base Access Control (RBAC/ABAC)
- Application code review
- Key management systems
- Sourcecode management security

- Data encryption
- Data loss prevention (DLP)
- Distributed denial of Service
- Data backup (recovery)

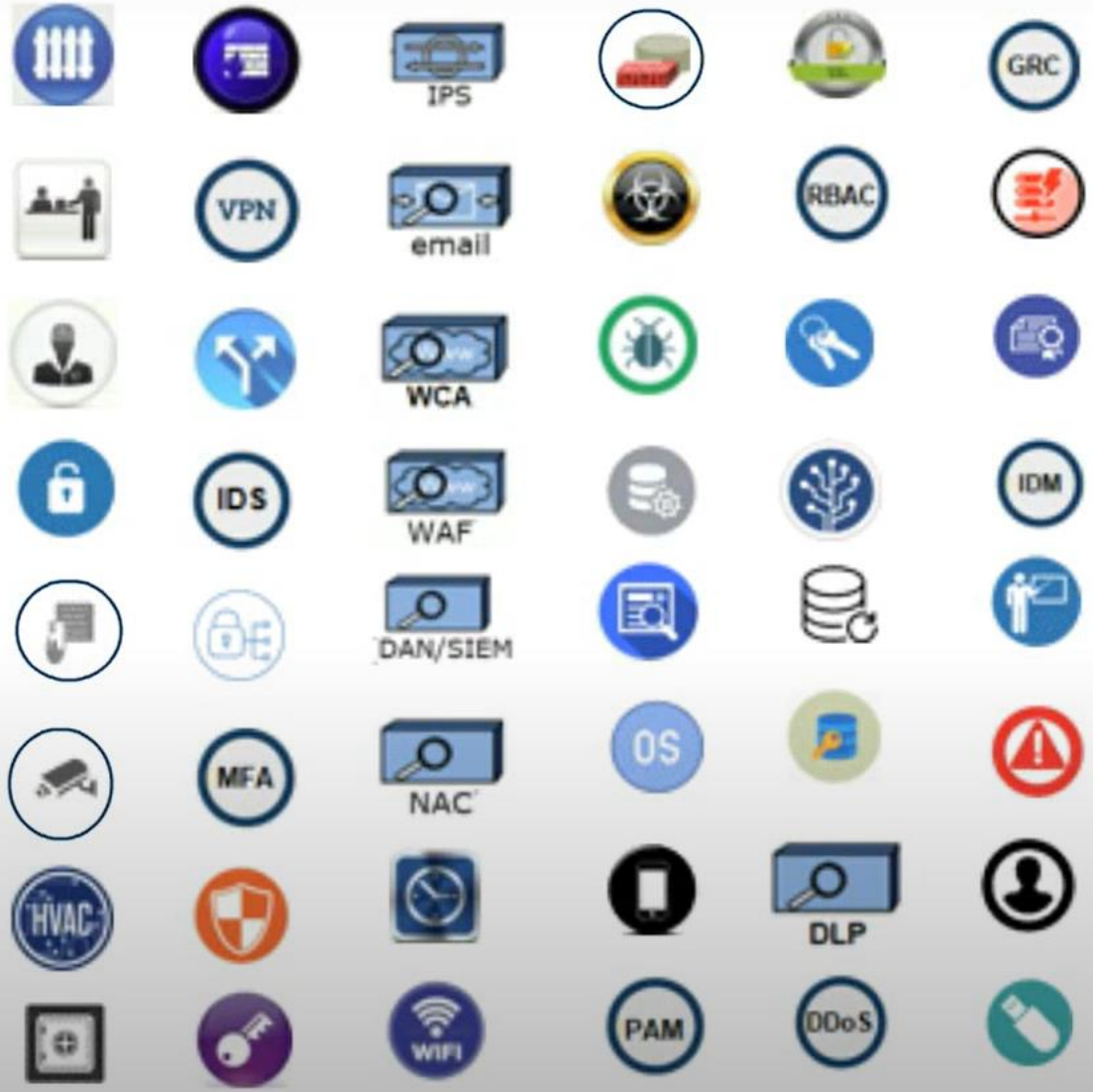
Security Architecture: Compliance Layer



Compliance – Policy, Procedures & Awareness

- Governance, Risk and Compliance tools
- Business continuity and Disaster Recovery
- Certifications: SOC 2, ISO 27001, Privacy Shield, GDPR?
- Change Management
- Identity Management and Identity Governance
- Security Awareness Training
- Incident Management
- HR Background Checks

Security Controls



Modern Cyber Threats

No. 1: Socially engineered malware & Ransom-based attacks

No. 2: Password phishing attacks

No. 3: Unpatched software

No. 4: Social media threats

No. 5: Advanced persistent threats

philosophy. Under this model, we make no assumptions about trust — other than the assumption that no user or device is trusted until they have proved both their identity and their authorization. With this new mindset in place, we then explore five adaptations of the customer's security controls to better support a zero trust approach.

1. Segment the Network

Proper network segmentation is the cornerstone of a zero trust architecture. Organizations must segregate systems and devices according to the types of access they allow and the categories of information that they process. These network segments can then serve as the trust boundaries that allow other security controls to enforce the zero trust philosophy.

2. Enhance Identity and Access Management

The second prerequisite for implementing zero trust is a strong identity and access management infrastructure. The use of multifactor authentication provides added assurance of identity and protects against credential theft. Deploying role-based access control allows applications to limit access in a manner that enforces the principle of least privilege.

3. Implement Least Privilege at the Firewall

Least privilege also applies to networks. After building out network segments, cybersecurity teams should lock down access between networks to only traffic required to meet business needs. For example, if remote offices do not need direct communication with each other, that access should not be allowed by default.

4. Add Application Context to the Firewall

Modern firewalls go far beyond the simple rule-based inspection of years past. Cybersecurity teams should add application inspection technology to their existing firewall deployments, ensuring that traffic being passed over a connection bears appropriate content. For example, application context controls can verify that outbound Domain Name System traffic actually corresponds to queries and responses and is not being abused by an attacker to stealthily exfiltrate sensitive information.

5. Log and Analyze Security Events

Design Zero- trust model 5 steps

- 1. data discovery - sensitivity, data store, rules, access, sso, MTA
- 2. workstations- identified, patched, verified
- 3. data flow- segmentation of the core engine, NGFW, priviegd access control policy
- 4. pretend the application– enable rules and RBAS for the applicatinos
- 5. monitor-- logs, analytics, and threat alerting

Why a 'new' architecture? Tips for a safer migration

- Graph thinking
- Why VPN into the network?
- Trusted Internet Connection (Federal IDS/IPS)
- Ransomware from client-side spreading through network
  - to other laptops, to fileshare servers
- Phishing/Browser attacks
- Social engineering for passwords (MFA/SSO everywhere)
- Segmentation:
  - Identity (Mimikatz)
  - Network vs Apps: Gmail/O365 vs. VPN+Local Exchange Server
  - Supply chain
  - Old and dangerous protocols

Typosquatting (example DNS control)

- DNS logging/control, something you should be doing but probably aren't
- Some (not enough) do it at HQ and branch offices
- What about remote workers? (No full time VPN backhaul w/ no split tunneling)
- DNS logging/control should be on every desktop/laptop/server
- Typosquatting to $HRsite, user wants to go to portal and miskeys one letter
- Option 1: Infected
- Option 2: DNS blocks Typosquatting site due to rules, policies and some AI

Benefits of mobile DNS logging/control w/ no VPN:

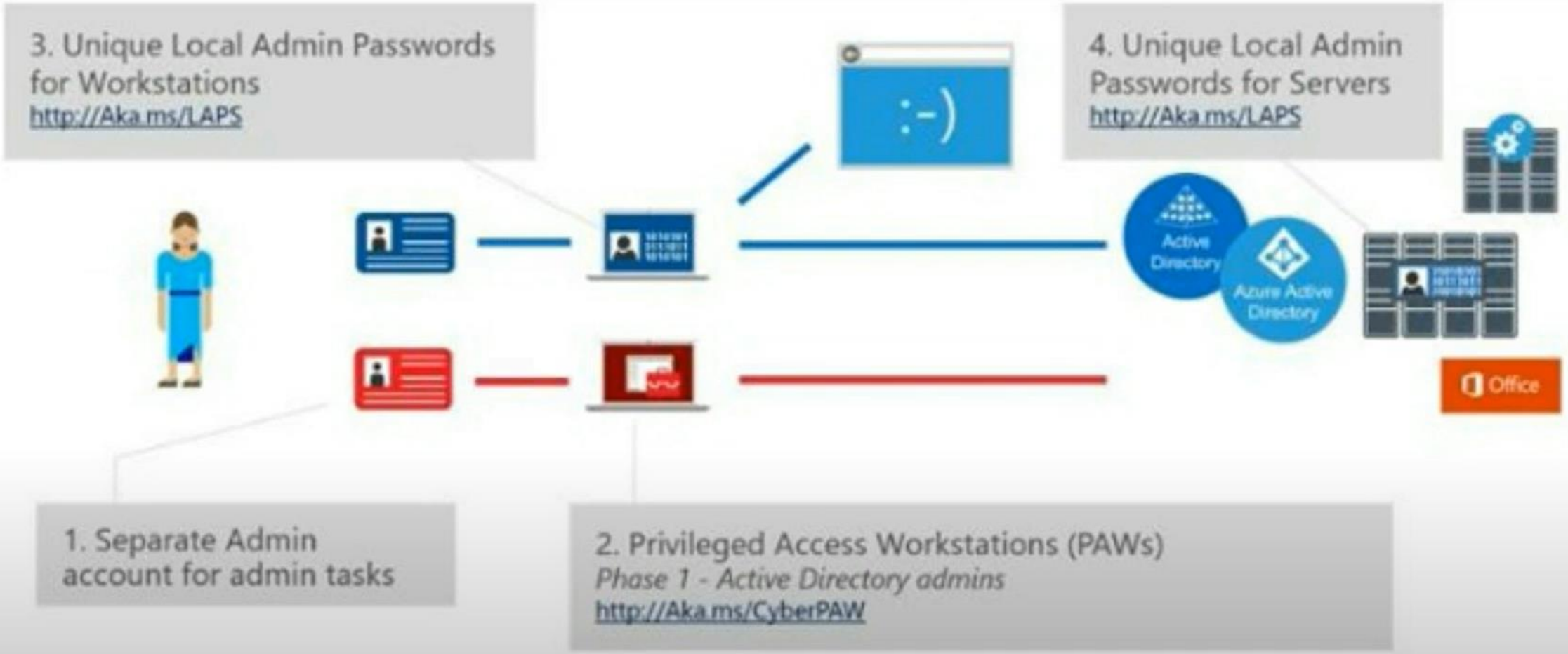
- Flexibility of movement for mobile users
- Reduced latency due to no need for network backhaul (trombone)
- Reduced helpdesk calls due to VPN clients

Identity Management as Segmentation

- Mimikatz allows theft of credentials from Windows
- Grabs credentials from RAM, in plaintext
  - No need for offline decryption of SAM file
  - Instantly use credentials to get Local Admin skeleton key
  - Domain Admin on ANY infected machine where credential is used

  - https://github.com/gentilkiwi/mimikatz
  - "It's now well known to extract plaintext passwords, hash, PIN code
    - And Kerberos tickets from memory. Mimikatz can also perform
    - Pass-the-hash, pass-the-ticket or build *Golden tickets*."

Privileged Identity protection strategy

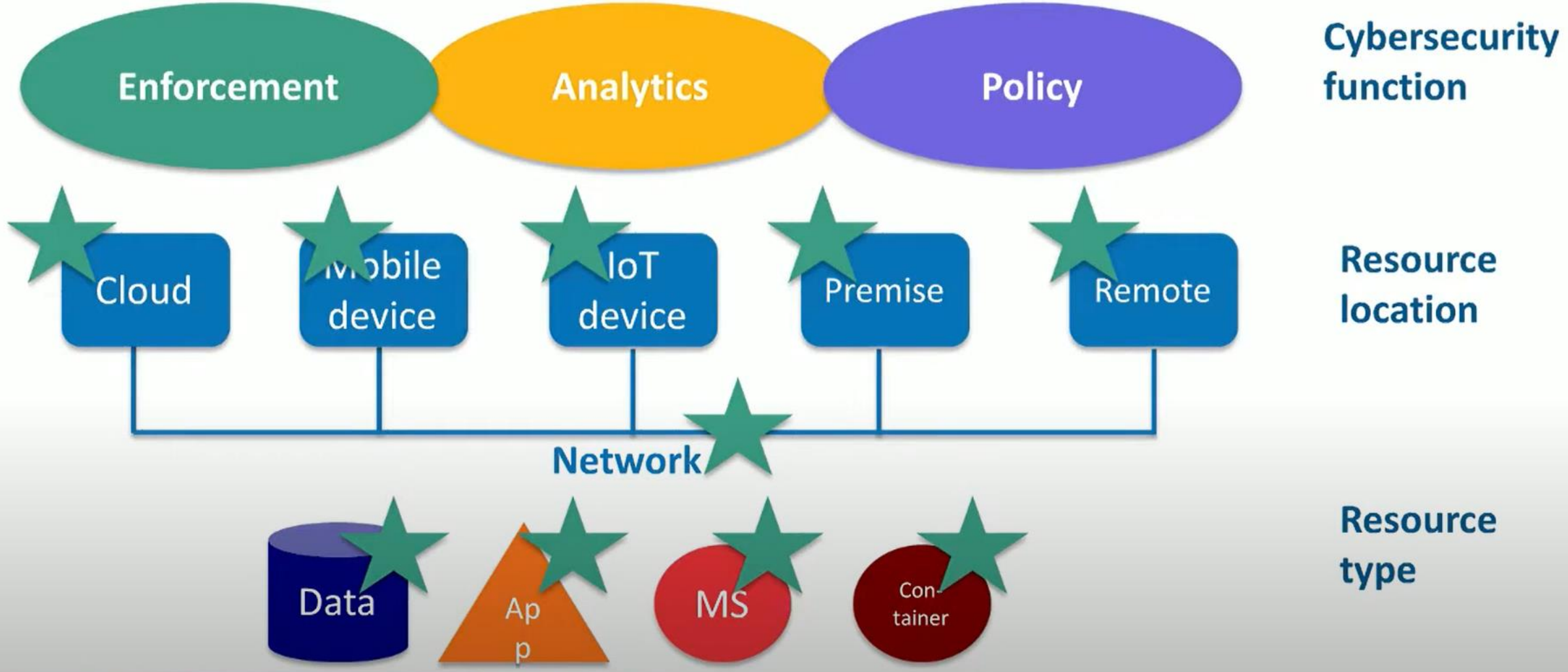


- Next-Generation Cybersecurity Architecture - YouTube

Cybersecurity Scope

- **Data**
  - Structured
  - Unstructured
  - Multimedia
  - Etc
- **Applications**
  - Executables
  - Services/microservices
  - Containers
  - Etc
- **Infrastructure and hardware**
  - Compute resources
  - Network resources
  - Devices

Cybersecurity Architecture



Challenges

- **Policy:** no product currently positioned to serve as a universal policy engine; currently function fragmented across a range of devices/services
- **Analytics:** Mix of embedded and external (BTA)
- **Enforcement:** Lack of integration with analytics and policy; limited automation

Bellwether Technology:AST

What it Is	• Automated application security testing (SAST, DAST, IAST, RAST)
Why We Selected It	• Automated application security testing requires “table stakes” of a mature application security practice • Automation enables next-gen development methodologies (eg Agile, DevOps)
Example Providers	• Contrast, Fortify, Veracode, Waratek

Bellwether Technology: Behavioral Threat Analytics

What it Is	• Software that integrates multiple sources of data (logs, analytics platforms such as Splunk, SEIM) to capture and display anomalous behavior of users, devices, and systems
Why We Selected It	• Effective use of BTS requires "table stakes" of solid analytics already in place; therefore characterizes more mature organizations • UBA enables proactive protection against attacks
Example Providers	• Bay Dynamics, Gurucul, Exabeam, Splunk/Caspida

Bellwether Technology: Advanced Endpoint Security

What it Is

- Software that protects endpoints from malware, using a variety of mechanisms (eg microsegmentation)
- Goes far beyond list-based protection offered by traditional anti-malware

Why We Selected It

- Represents an architectural/technical “step function” increase over existing technology
- Aligns well with additional strategic initiatives (eg virtualization)

Example Providers

- Bromium, Crowdstrike, Invincea, Tanium, Carbon Black (also current versions of Trend Micro, McAfee, Sophos Symantec, some capability in Microsoft)

Bellwether Technology: Network Access Control

What it Is	• Tools that authorize devices on the network based on security policies
Why We Selected It	• To deploy NAC, organizations need to have a solid authorization and authentication policy in place; that policy becomes the foundation of the zero-trust environment
Example Providers	• Cisco, Forescout, HP/Aruba, Trustwave

Bellwether Technology: CASB

What it Is

- Premise or cloud based software that automatically detects cloud usage by employees, assesses business and technical risk, and enforces policies

Why We Selected It

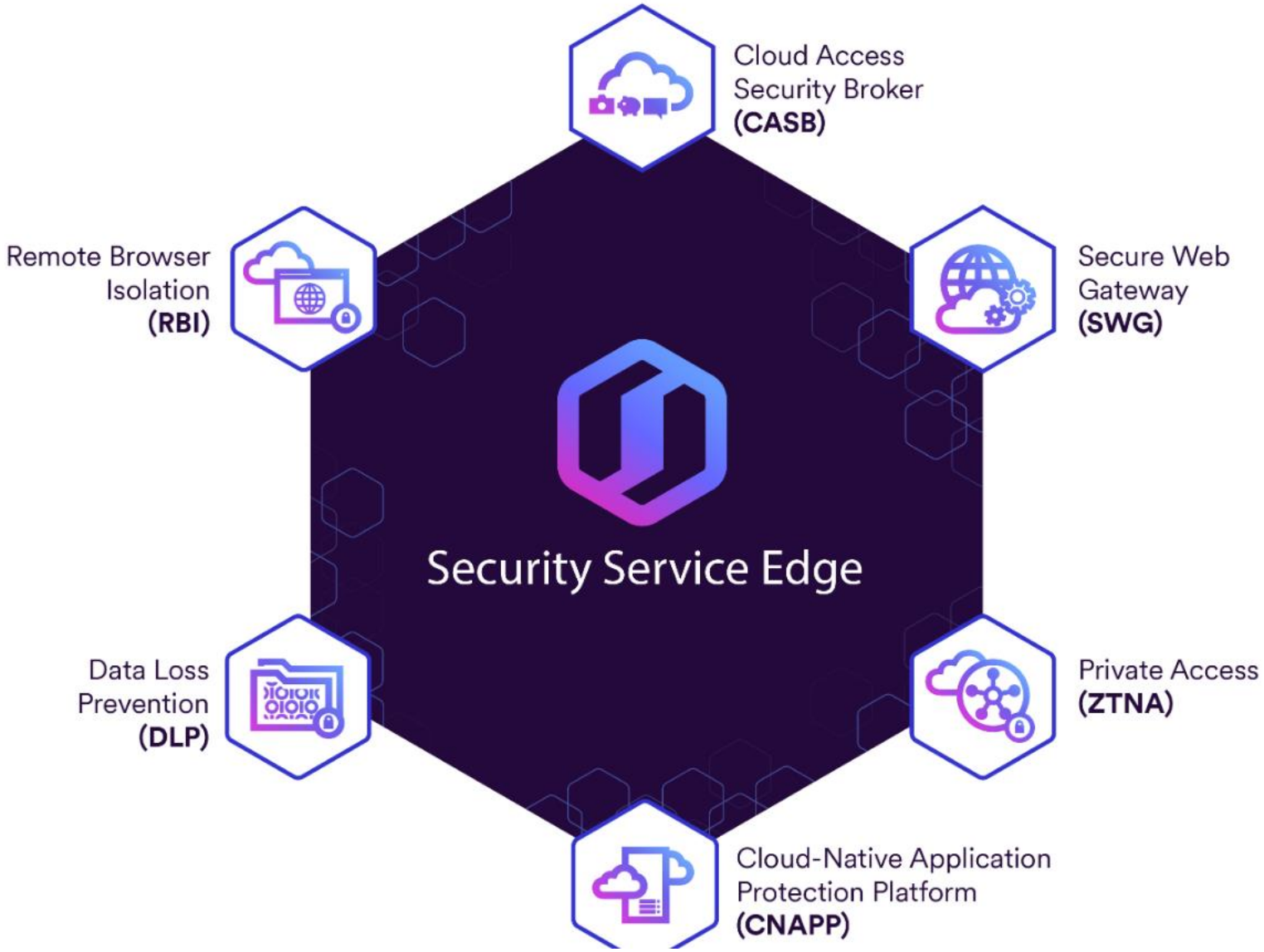
- Critical to manage cloud use by employees
- Use implies a relatively mature cloud initiative, including defined policies

Example Providers

- BitGlass, BlueCoat/Symantec, Microsoft, Netskope, Skyhigh

Bellwether Technology: Cloud DLP

What it Is	• Premise or cloud based software that protects content stored on clouds
Why We Selected It	• Critical to manage cloud use by employees • Use implies a relatively mature cloud initiative, including defined policies
Example Providers	• Skyhigh, GTB, Cyphercloud, Vormetric


Cloud Access Security Broker (CASB)
Remote Browser Isolation (RBI)
Secure Web Gateway (SWG)
Security Service Edge
Data Loss Prevention (DLP)
Private Access (ZTNA)
Cloud-Native Application Protection Platform (CNAPP)

Bellwether Technology: Single Signon as a Service

What it Is	• Cloud based software that enables single signon to cloud and on-premise resources
Why We Selected It	• Critical to manage cloud and on-premise use by employees • Use implies a relatively mature cloud initiative, including defined policies
Example Providers	• Microsoft, Okta, Ping

(How To Become A Security Architect)

Press Esc to exit full screen

Certifications

- CEH: Certified Ethical Hacker
- CISSP: Certified Information Systems Security Professional
- CISSP-ISSAP: Information Systems Security Architecture Professional
- CISM: Certified Information Security Manager
- CSSA: Certified SCADA Security Architect
- GSEC / GCIH / GCIA: GIAC Security Certifications
- TOGAF / SABSA / Zachman - Enterprise Architect

29:03 / 58:30