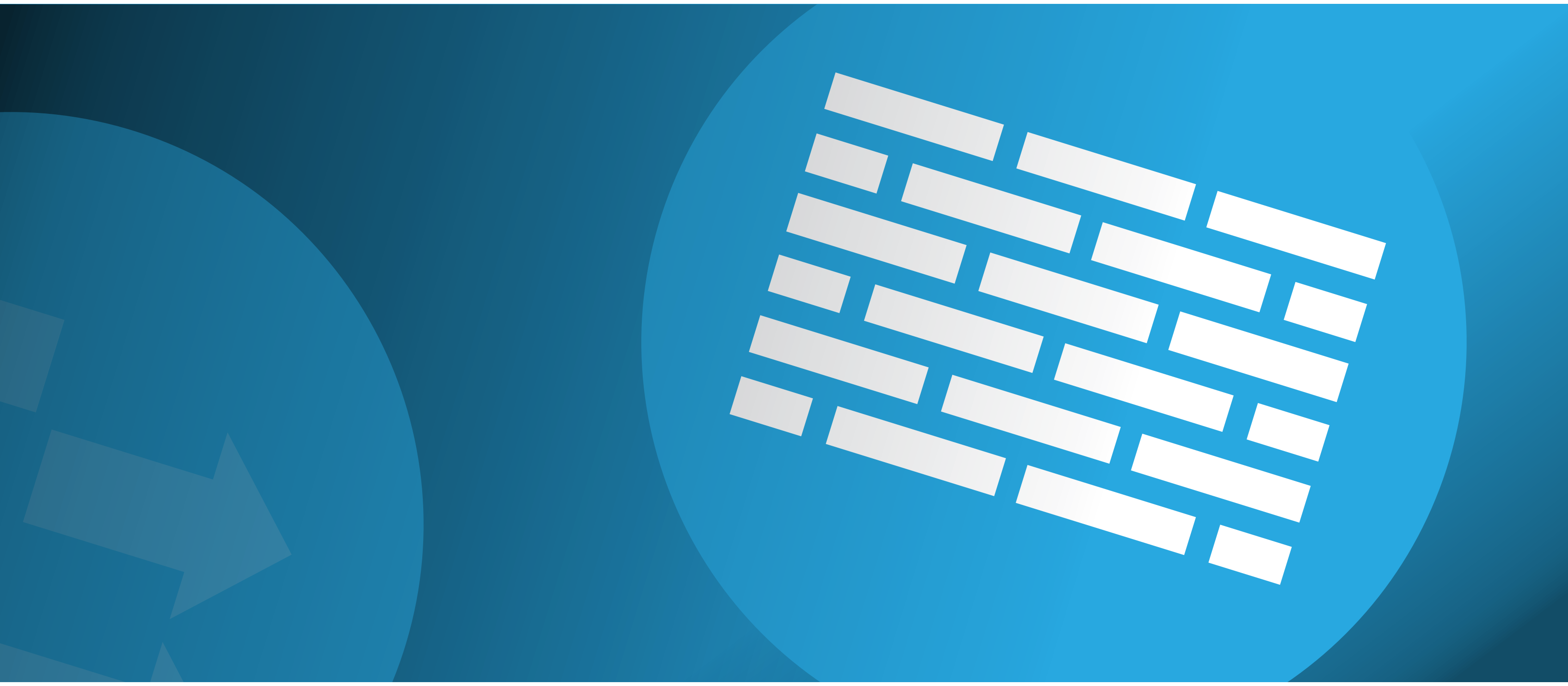


SAFE Overview Guide

Threats, Capabilities, and the Security Reference Architecture

January 2018

SAFE
SIMPLIFIES SECURITY

Contents

The Need for SAFE

Today, attacks like phishing, ransomware, and advanced persistent threats are common. No single product can successfully secure your business from these risks. An architectural approach that addresses the full range–from people, to devices, to applications–is needed. Your data flows from offices to the data center to the cloud. And you must understand where your data is to protect it.

Cisco's John Chambers famously said, "There are two types of companies: ones that have been breached and those that do not realize it…" When attackers violate your network, having a threat defense that helps you react and minimize the impact of the attack is critical.

Complexity is one of the main challenges facing security professionals. Technology constantly fragments into new uses, and organizations utilize dozens of products that do not interoperate seamlessly. This multiplies attack surfaces, which in turn complicates defenses. Fraudsters exploit this weakness to develop advanced threats for more lucrative schemes.

The industry desperately needs a resource that simplifies the problem. The solution must be comprehensive, credible, and about more than just products; it needs to focus on the threats to your business.

SAFE meets this need.

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.

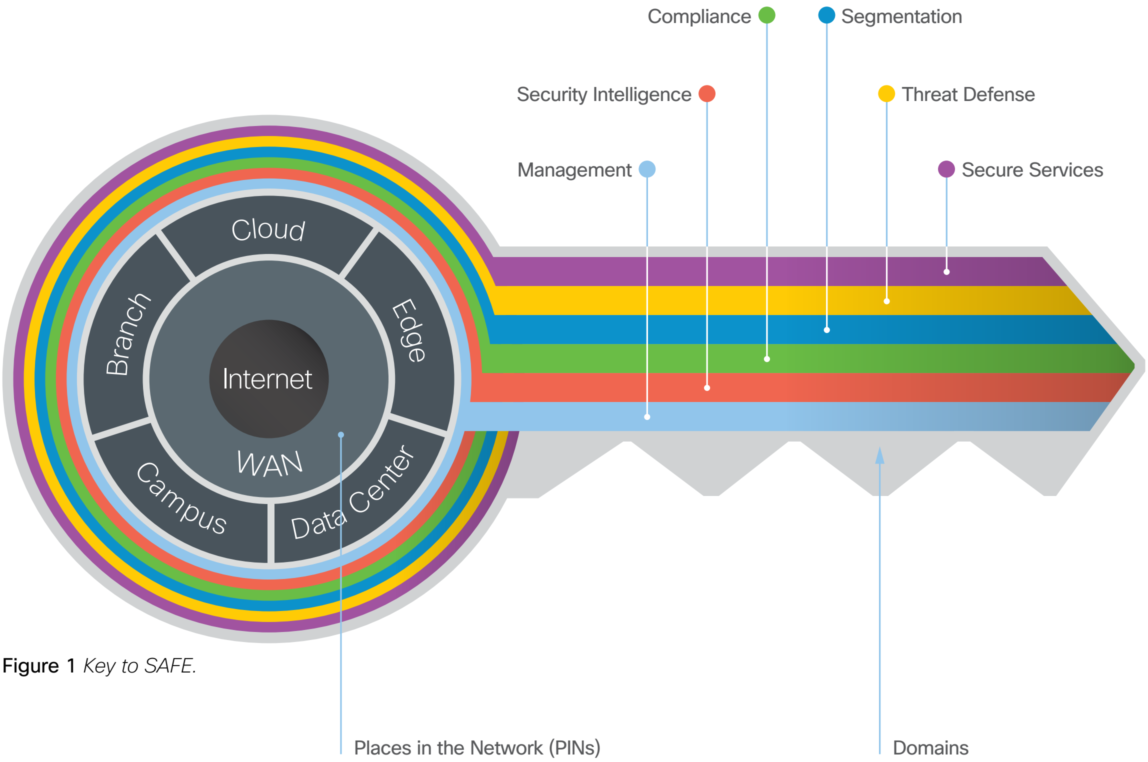


Figure 1 *Key to SAFE.*

SAFE provides the Key to simplify cybersecurity into Secure Places in the Network (PINs) for infrastructure and Secure Domains for operational guidance.

Return to Contents

The SAFE Security Reference Model

Using a security reference model, the challenges of securing today's business functions are simplified into a building block approach. The model incorporates today's security best practices, architectural discussions, and laboratory-tested designs from the brightest security minds across Cisco, its customers, and partners. SAFE's Cisco Validated Designs address critical security topics. They have been deployed, tested, and they document "how to do it."

SAFE includes:

- Business use cases illustrating the surface that fraudsters can attack
- Security **capabilities** mapped to common threats within business use cases
- Reference **architectures** that logically arrange the security capabilities into blueprints
- **Designs** using the reference architectures for common deployment scenarios and solutions

The SAFE Method

The SAFE method customizes the model for individual companies. Using the SAFE toolkit and collateral, companies can analyze the threats and risks to their own business. Contact your Cisco account team to use the method in a guided SAFE workshop. The workshop can be refreshingly helpful because it brings departments of the company together that might not normally interact. Executives come together with stakeholders from business and compliance as well as security and Infrastructure technologists to map out concerns related to how security affects the business. The workshop results in a tailored security architecture for your business.

Return to Contents

How to Use SAFE

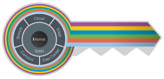
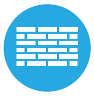
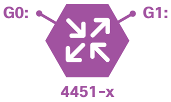
SAFE is not a single answer.

The **model** is a reference for common threats, risks, and policies across the business of a company. This does not mean that all companies are the same. Obviously, the concerns of retailers are not the same as the needs of healthcare organizations. However, when viewing the challenges of security in its entirety, patterns begin to emerge. Regardless of the industry, certain business methods are likely to be employed and, consequently, exploited. Foundational capabilities and functional controls are necessary to defend the attack surface. For example, access to the network, utilization of business applications, and communications using email are common across all companies. Connections to the Internet for web browsing and to access services coming from the cloud present additional business security concerns. SAFE provides guidance to common business functions that require security capabilities, culminating in a reference for end-to-end security.

The SAFE **method** customizes the best practices of the reference model to individual companies. It ensures that business goals are measurably secured according to each company's security policy and risk appetite, using the following steps:

- Identify business goals
- Break down the network into manageable pieces
- Establish a criteria for the success of the business
- Categorize risks, threats, and policies
- Build the security solution

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

The three phases of the SAFE method are:

1 Capability phase

Business flows, or use cases, are defined in this phase. Using them as a basis, security capabilities are applied to address threats, risks, and policy.

Small Branch Capabilities and Business Flows

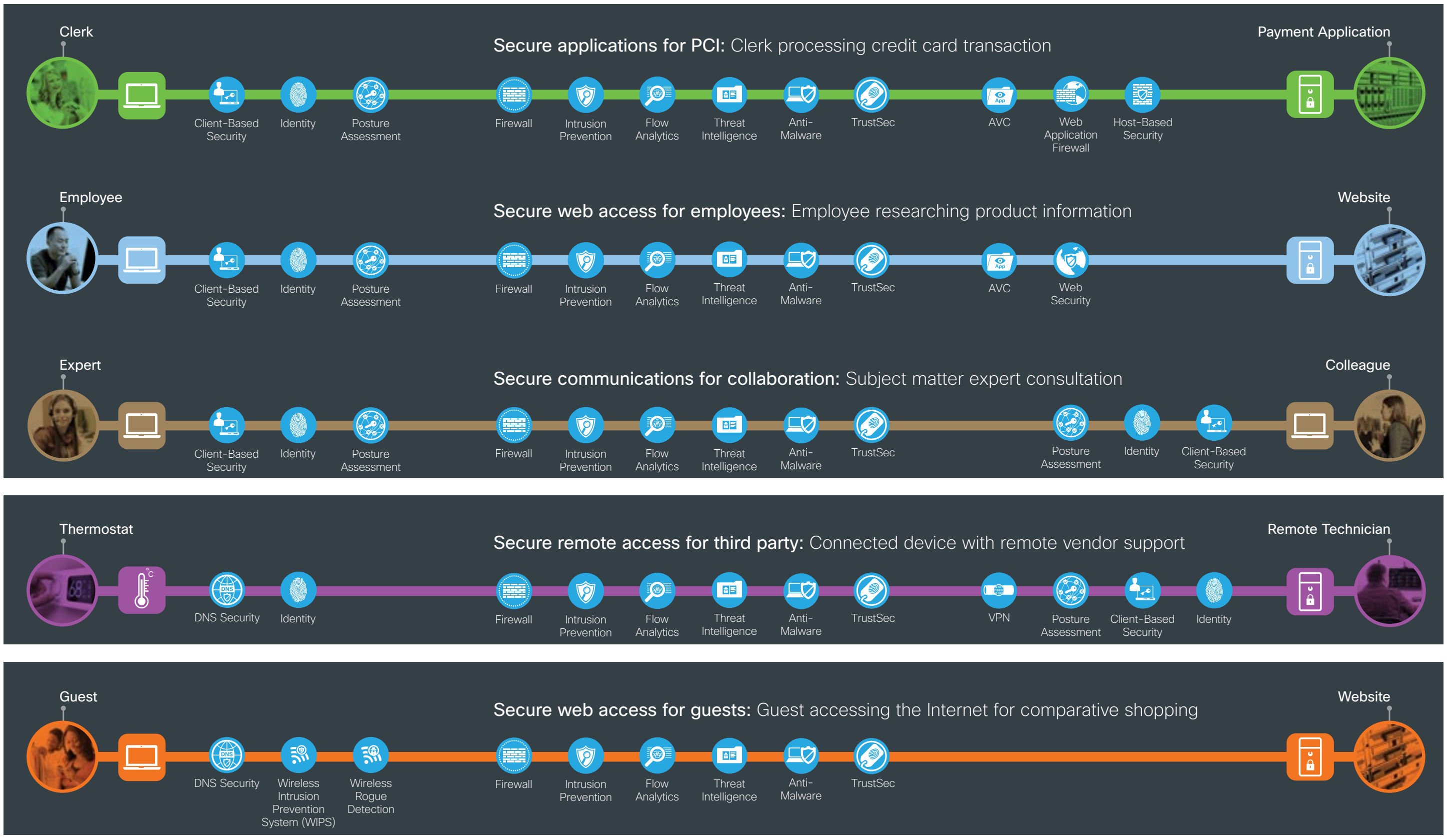


Figure 1 *In the capability phase, business flows are analyzed to determine the required security capabilities.*

Return to Contents

2 Architecture phase

A logical security architecture is defined using the security capabilities that were identified in the business flows.

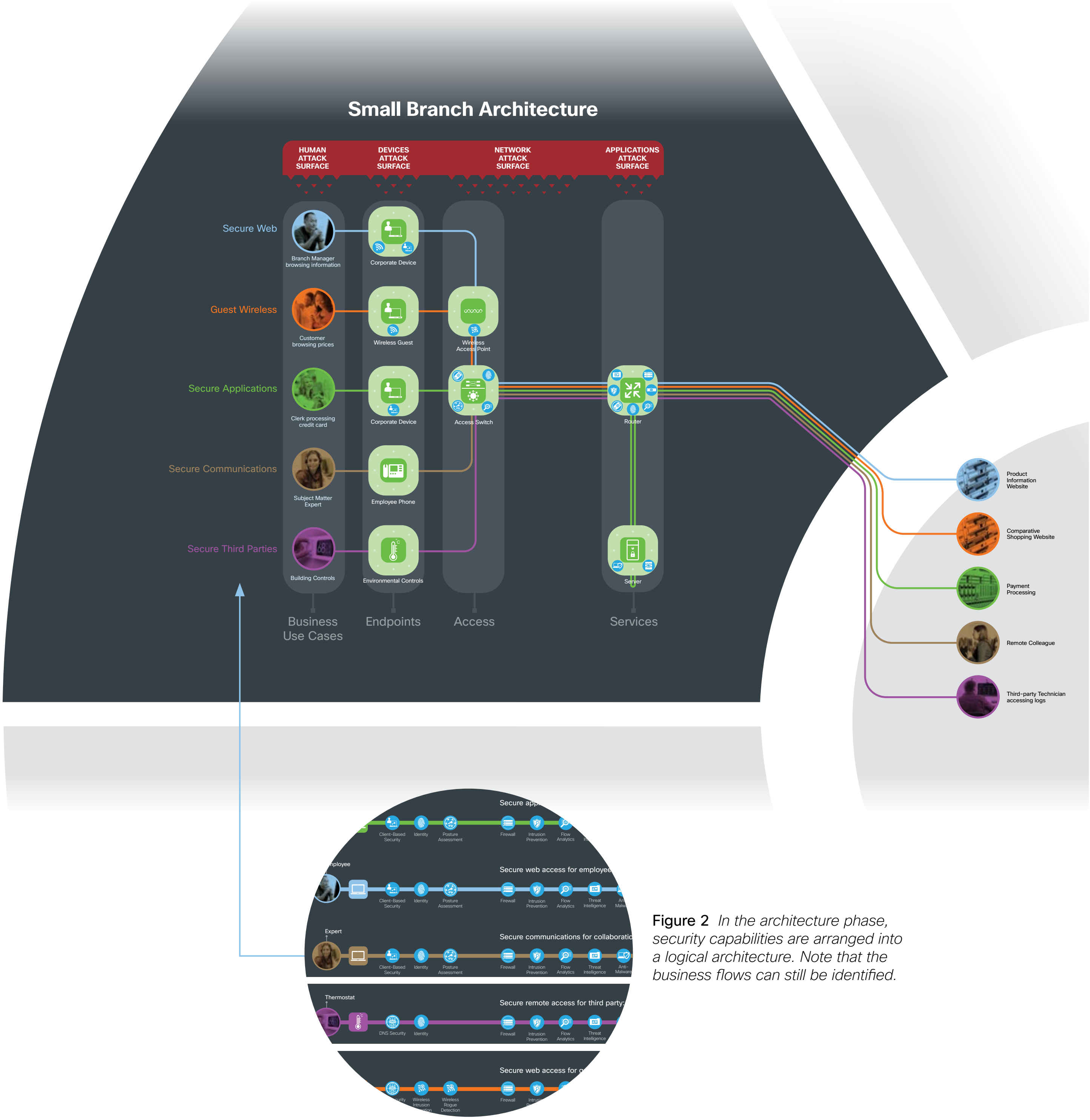
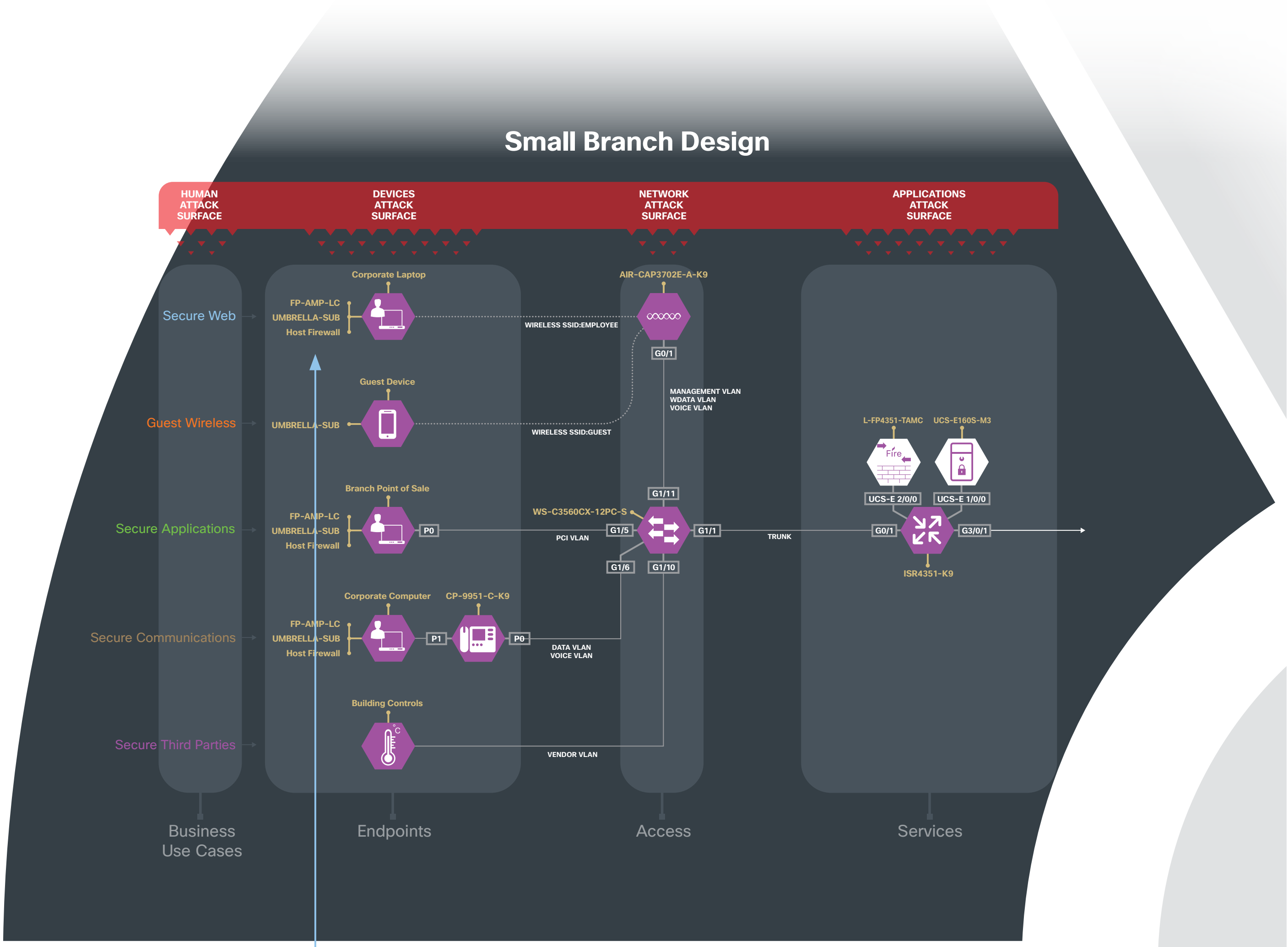


Figure 2 *In the architecture phase, security capabilities are arranged into a logical architecture. Note that the business flows can still be identified.*

3 Design phase

Using the security architecture, a specific design is created to implement the required security capabilities, complete with a product list, configuration, services, and cost.



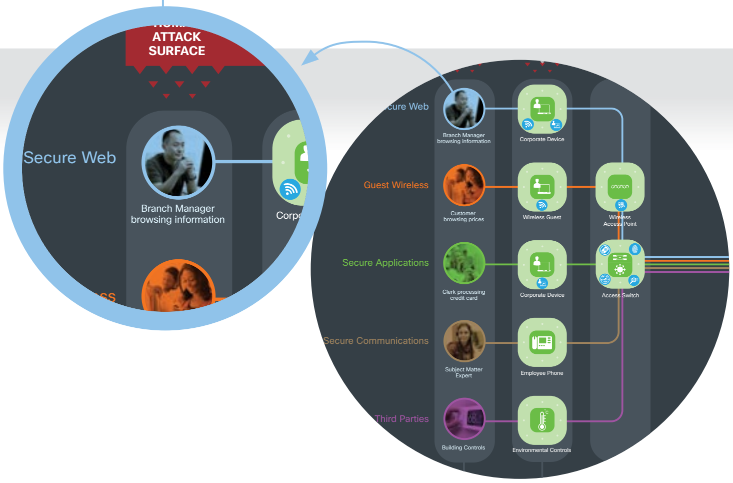


Figure 3 *In this phase, the design is created to implement the logical architecture. Although the emphasis is on the specifics of the solution, the original business flows are still present.*

SAFE's toolkit and collateral simplify the discussion

SAFE bridges the gap between business and technical audiences by providing a communal security-centric language for business concerns and technical solutions. Using innovative icons, each business line can visualize the security required, including accounting for the gaps.

SAFE tools include:

- Capability icons to represent business flows and the appropriate security controls
- Architecture guides to reference appropriate layers of security and their justifications
- Design guides that provide solutions with step-by-step instructions on how to configure the infrastructure based on Cisco's validated laboratory testing

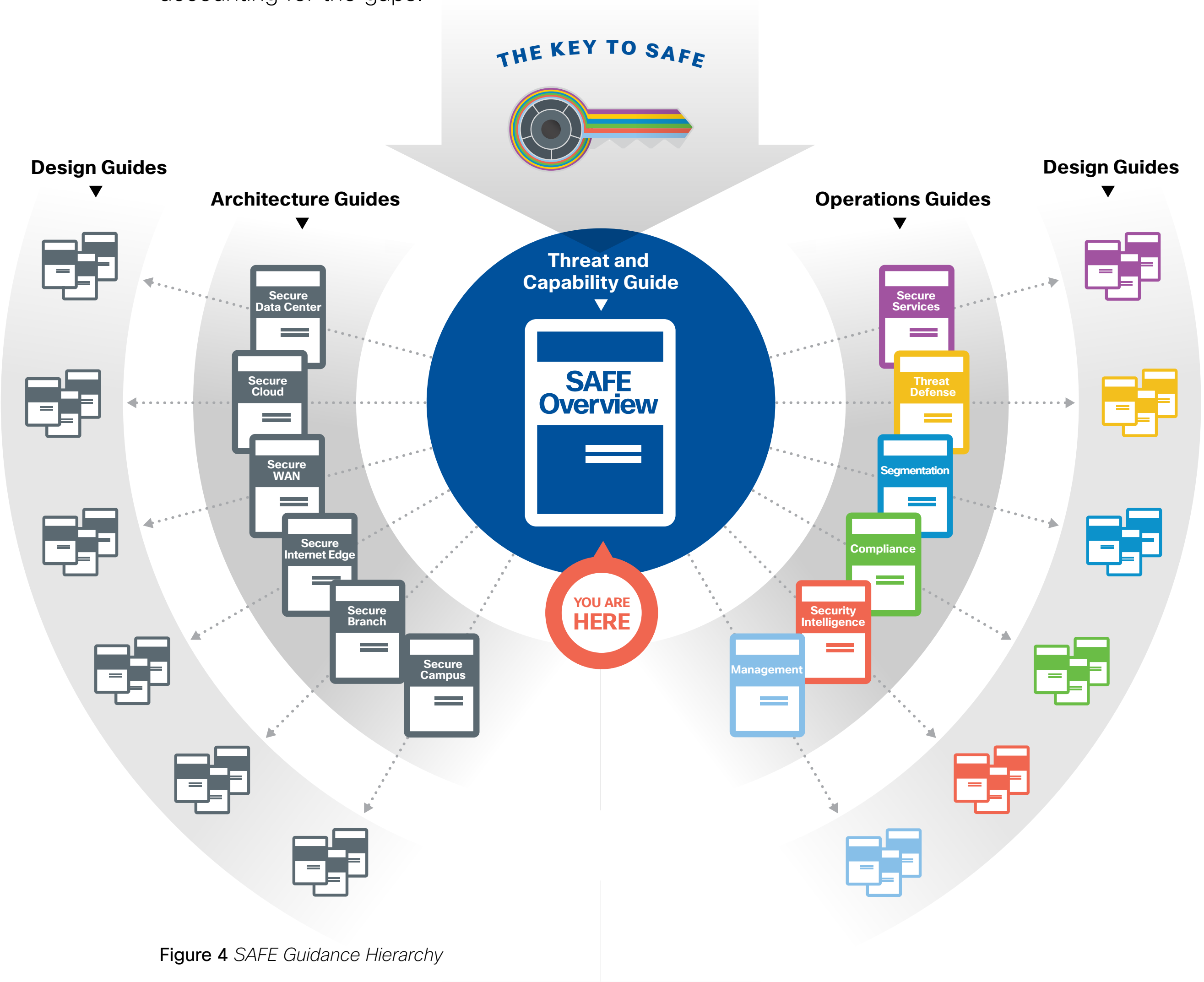


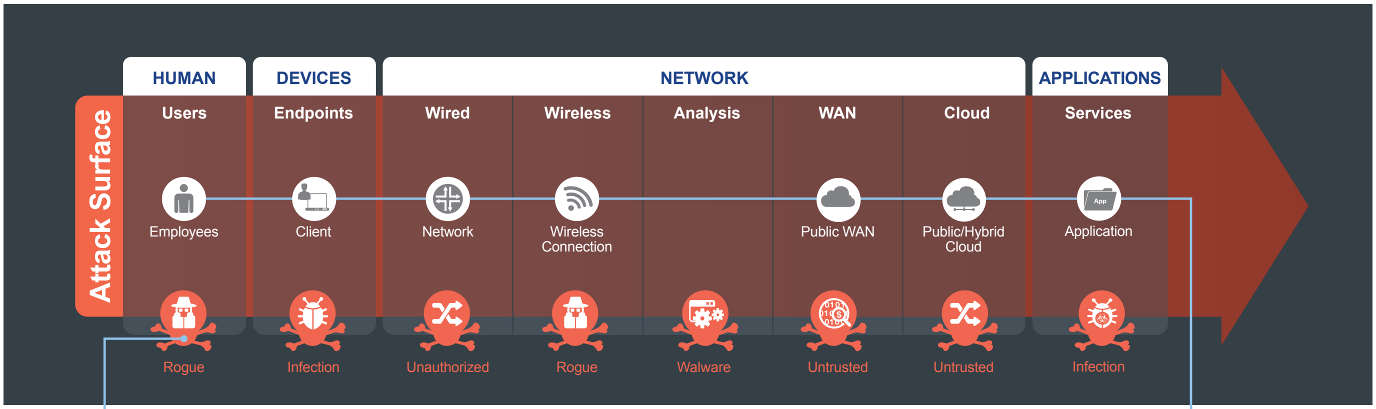
Figure 4 *SAFE Guidance Hierarchy*

Attack Surface

The attack surface of a company is anyone or anything that can be targeted.

Any human, using any device, on any network, accessing any application can be attacked.

HUMAN	Know who is on your network
DEVICE	Know that devices are not infected
NETWORK	Networks can be compromised
APPLICATIONS	Services can be exploited



Threat

Figure 5 *The attack surface that needs to be secured.*

Attack Surface

Securing the Attack Surface

The attack surface needs to be secured by appropriate capabilities. Each target may be part of a larger overall attack. By identifying a company's business flows which represent the companys attack surface, proper security capabilities can be applied.

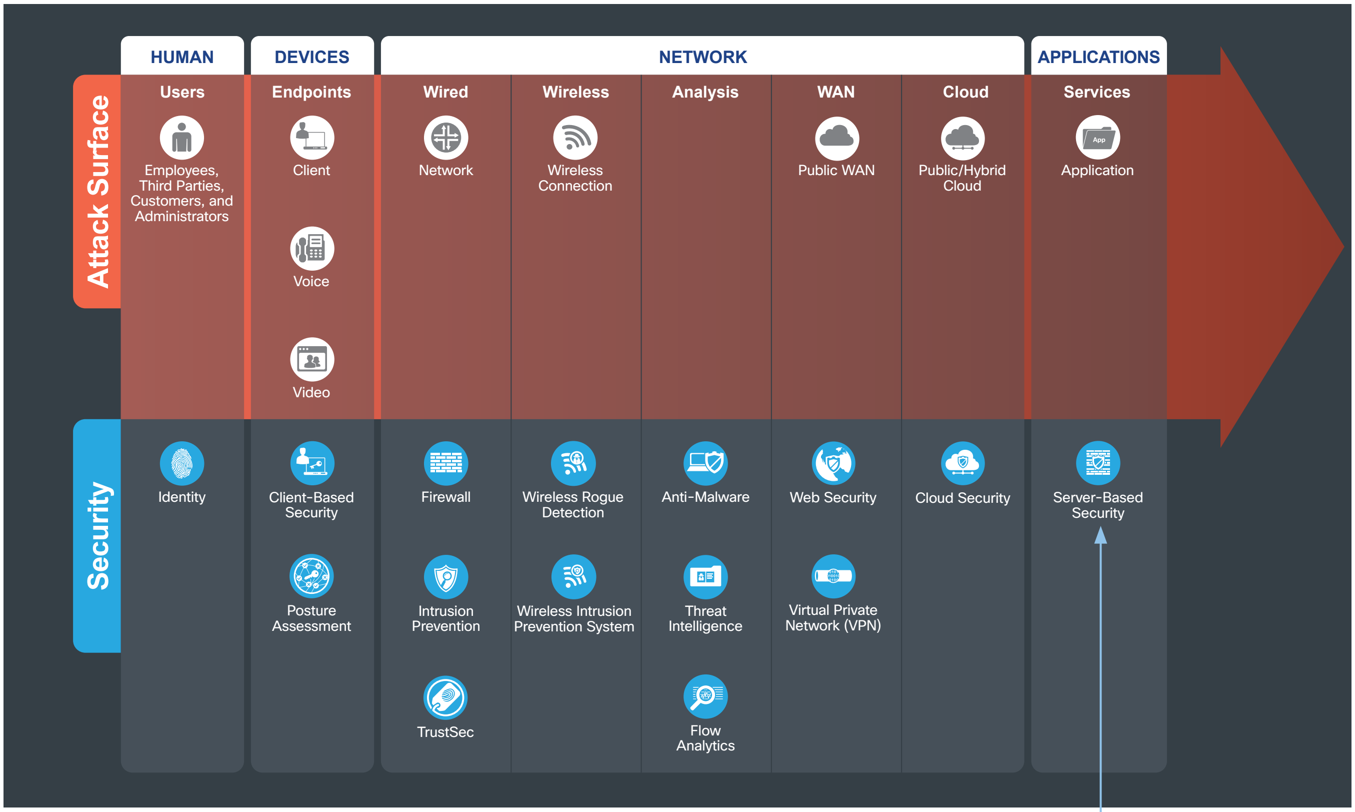


Figure 6 *Security capabilities are applied logically to mitigate the threats along the attack surface.*

Capability

Return to Contents

Business Flows

Three categories of users have a role on your network:

Internal: Internal flows are activities that employees perform on the company network.

Third Party: Third-party flows are guests, vendors, service providers, or partners who access the company network.

Customers: Customer flows can be a variety of services, such as website portals and customer information.

Policy, risks, and threats affect each of them, requiring security capabilities for protection.

SAFE's color-coded business flows illustrate the security needed for each role. These flows depict the attack surface, ensuring that controls are easily accounted for. For example, when an employee goes online to do research, or a customer makes a purchase on your e-commerce site, these activities provide fraudsters something to attack.

By documenting and planning the security of all business flows within your company, maintaining security is simplified.

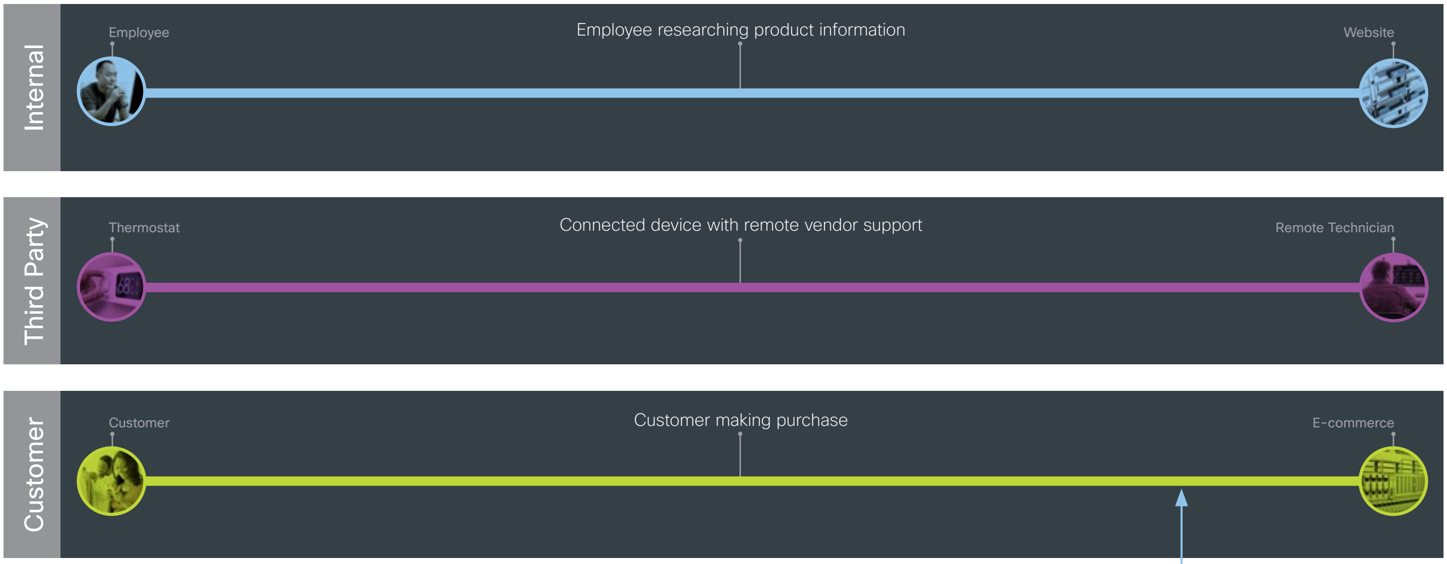


Figure 7 *SAFE color codes business use cases as business flows.*

Color Code

Return to Contents

Functional Controls

Functional controls are common security considerations that are derived from the technical aspects of the business flows.

Secure Applications	Applications require sufficient security controls for protection.
Secure East/West Traffic	Data that securely moves between internal or external resources.
Secure Access	Employees, third parties, customers, and devices securely accessing the network.
Secure Remote Access	Secure remote access for employees and third-party partners that are external to the company network.
Secure Communications	Email, voice, and video communications connect to potential threats outside of company control and must be secured.
Secure Web Access	Web access controls enforce usage policy and help prevent network infection.

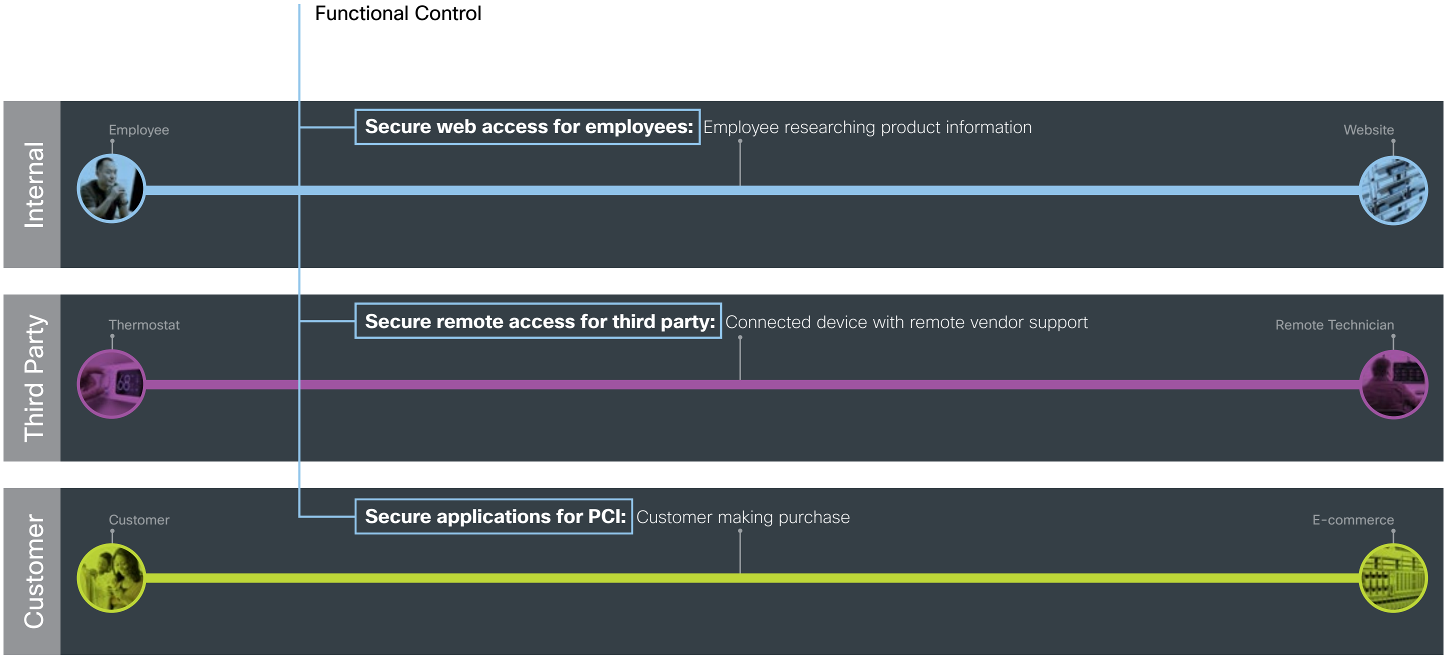

Functional Control
Internal
Employee
Secure web access for employees: Employee researching product information
Website
Third Party
Thermostat
Secure remote access for third party: Connected device with remote vendor support
Remote Technician
Customer
Customer
Secure applications for PCI: Customer making purchase
E-commerce

Figure 8 *Business flows reveal functional controls to be secured.*

Capabilities

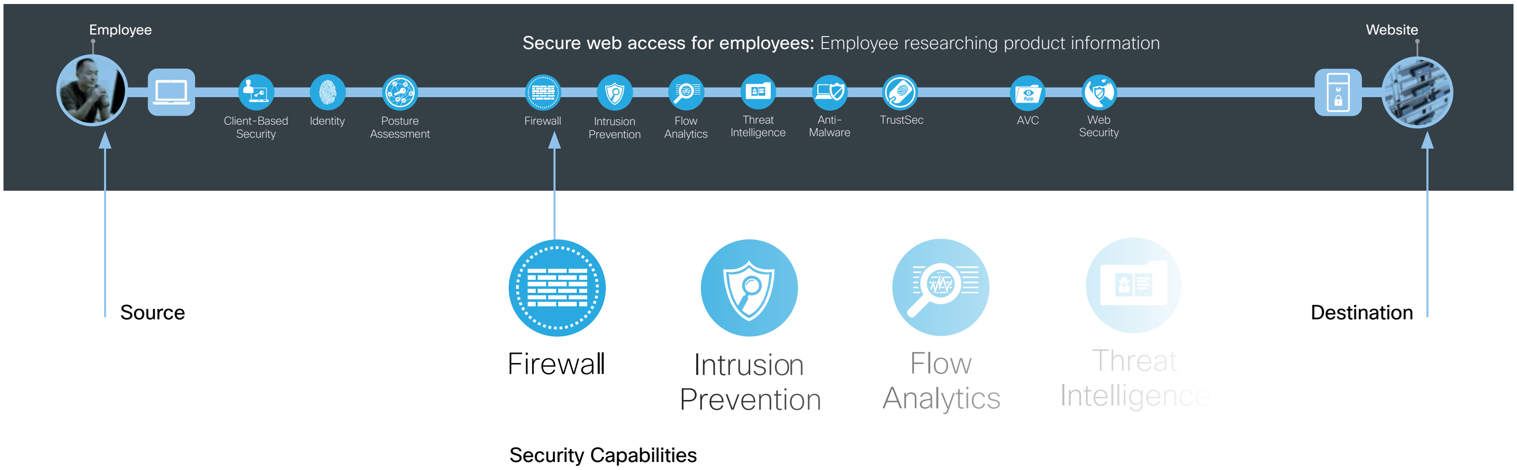
SAFE's capability icons simplify the security discussion by putting the focus on the **function** necessary to perform a specific feature before identifying a product.

For example, Cisco sells Adaptive Security Appliances, Firepower appliances, Meraki routers with firewalls, Cat6k with firewalls, and Cisco ISR with firewalls. For simplicity, any of these are identified by their capability (firewall). Subsequent SAFE steps will specify model and feature requirements.

Security capabilities are used to mitigate threats on the attack surface of a business flow. The appropriate capability icons are applied along the business flow based on the policy, risk, and threats of its attack surface.

For example, the "Employee researching product information" business flow is analyzed from source to destination.

Figure 9 *Business Flow with Required Security Capabilities*



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*

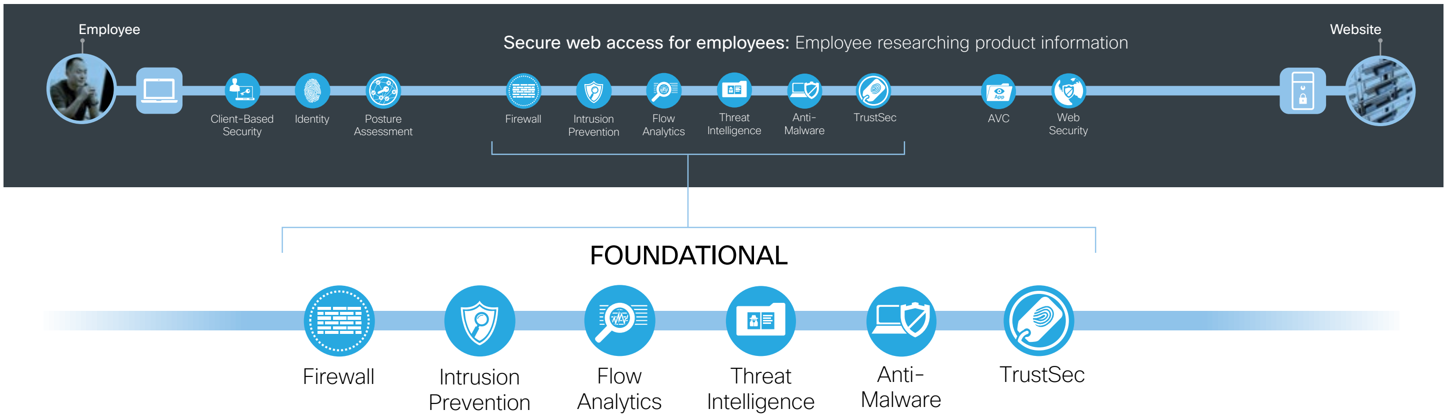


Table 2 *Foundational Capabilities*

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

Access Capabilities

Access capabilities secure users, devices, and servers as they access or provide network services.

Figure 11 *Access Capability Group: Secure Access*

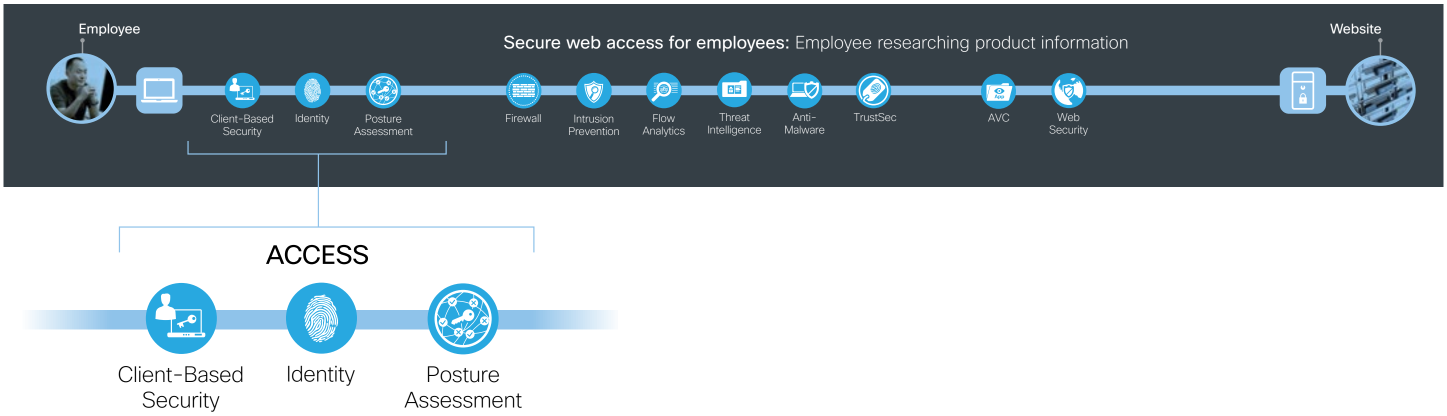


Table 3 *Access Capabilities*

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

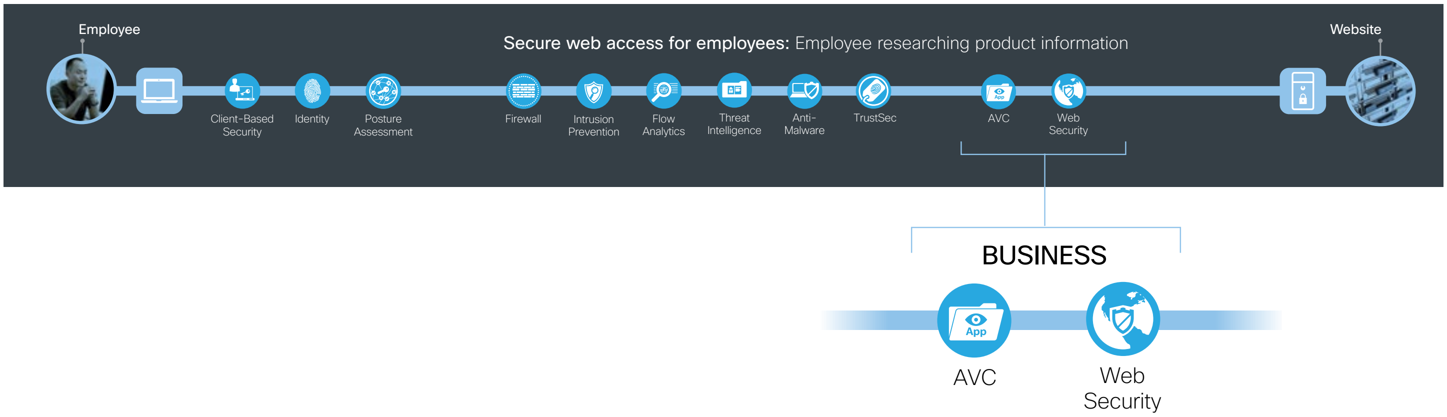


Table 4 *Business Capabilities*

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.

Return to Contents

The Business Flow Capability Diagram

Combining capabilities with business flows creates a security capability map to the business. This map is used as the basis for the next phase in SAFE: The Security Architecture.

See the Appendix for all of these SAFE use cases with their capabilties.

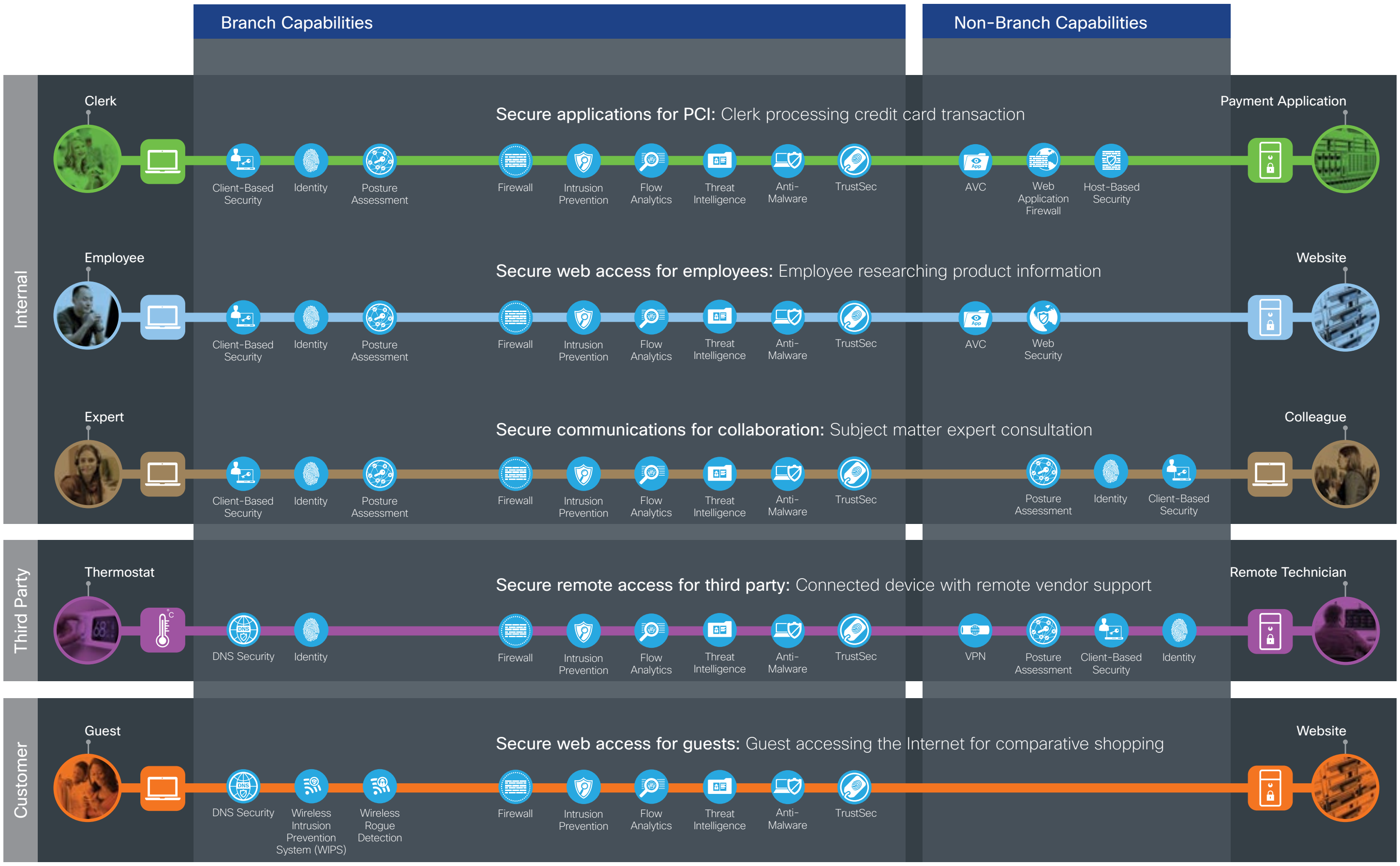


Figure 13 *The Secure Branch Business Flow Capability Diagram*

Places in the Network

SAFE simplifies network security by providing solution guidance using the Places in the Network (PINs).

- Branch
- Campus
- WAN
- Data Center
- Edge
- Cloud

PINs are locations that are commonly found in networks (see Figure 14) and conceptually represent the infrastructure deployed in these locations. They are blueprints for the fundamentals that comprise today's organizations: authentication, routing, switching, wireless, firewall, intrusion detection, and so on. Specific industry guidance for healthcare, retail, financial, and other verticals is covered in the Secure Domains.

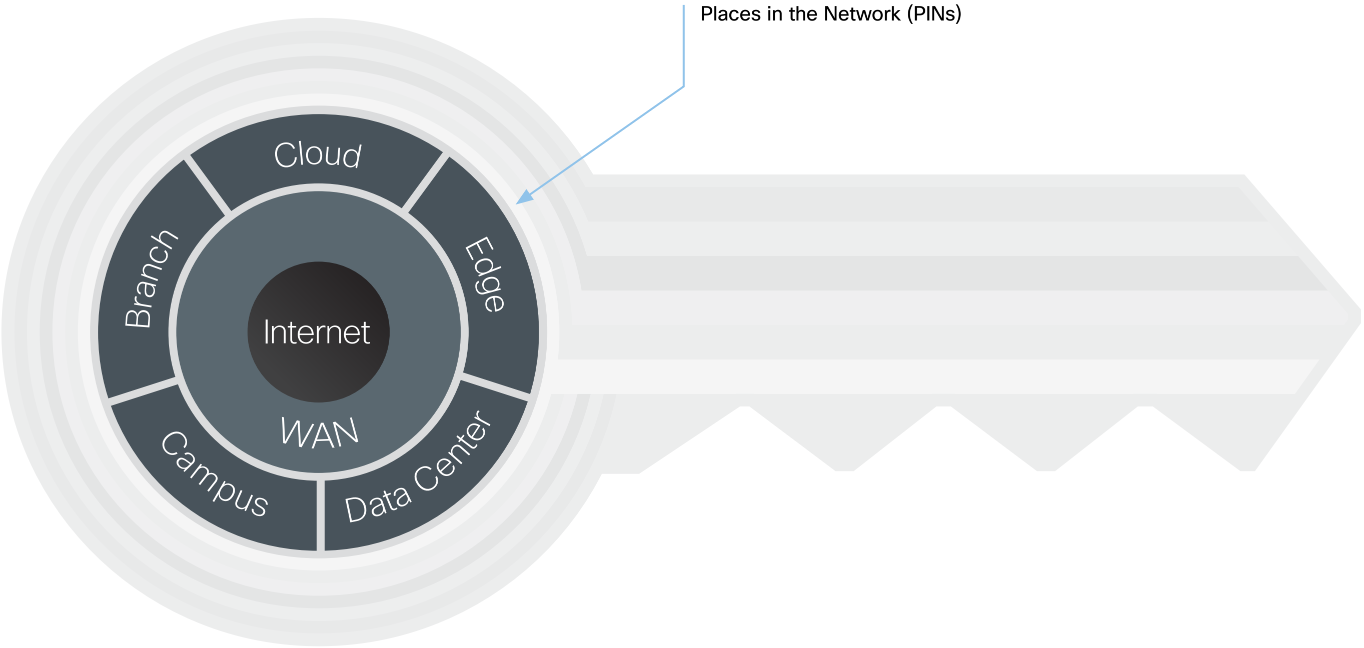


Figure 14 *Places in the Network*

Secure Branch

Branches are typically less secure than their campus and data center counterparts. Economics often dictate that it is cost prohibitive to duplicate all the security controls typically found at locations when scaling to hundreds of branches. However, this makes branch locations prime targets and more susceptible to a breach. In response, it is important to include vital security capabilities while ensuring cost-effective designs in the branch.

Figure 15 shows the progression of security capabilities used to help defend against the attacks common in a branch.

Top Threats Mitigated in the Branch

- Endpoint malware (POS malware)
- Wireless infrastructure exploits (rogue AP, Man in the Middle)
- Unauthorized/malicious client activity
- Exploitation of trust

For a deeper discussion on defending attacks within the Secure Branch, see www.cisco.com/go/SAFE.

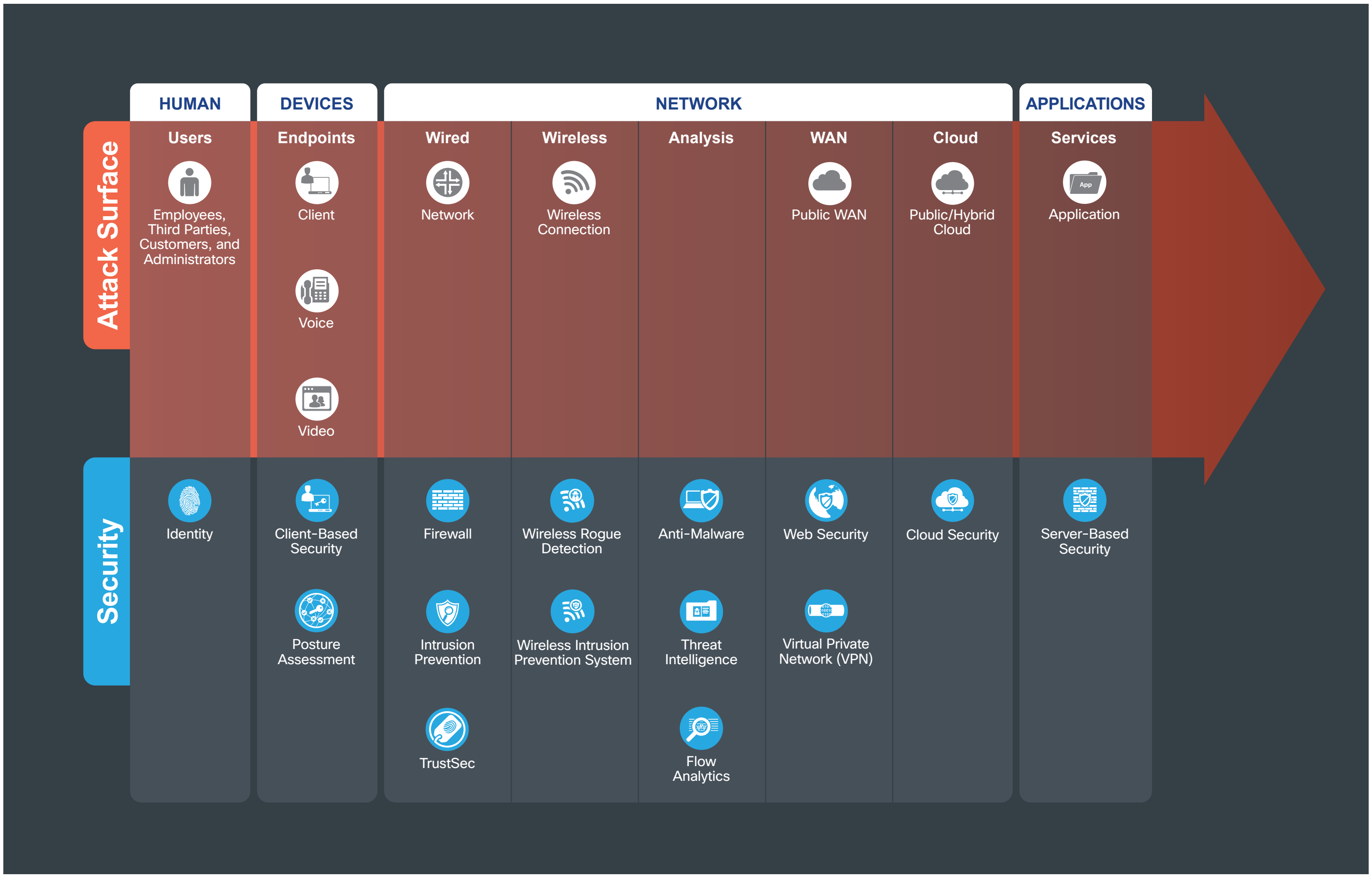


Figure 15 *Secure Branch Attack Surface and Security Capabilities*

Secure Campus

Campuses contain large user populations with a variety of device types and traditionally few internal security controls. Due to the large number of security zones (subnets and VLANs), secure segmentation is difficult. Because of the lack of security control, visibility, and guest/partner access, campuses are prime targets for attack.

Figure 16 shows the progression of security capabilities that are used to help defend against the attacks common in a campus.

Top Threats Mitigated in the Campus

- Phishing
- Web-based exploits
- Unauthorized network access
- Malware propagation
- BYOD–Larger attack surface/ increased risk of data loss
- Botnet infestation

For a deeper discussion on defending attacks within the Secure Campus, see www.cisco.com/go/SAFE.

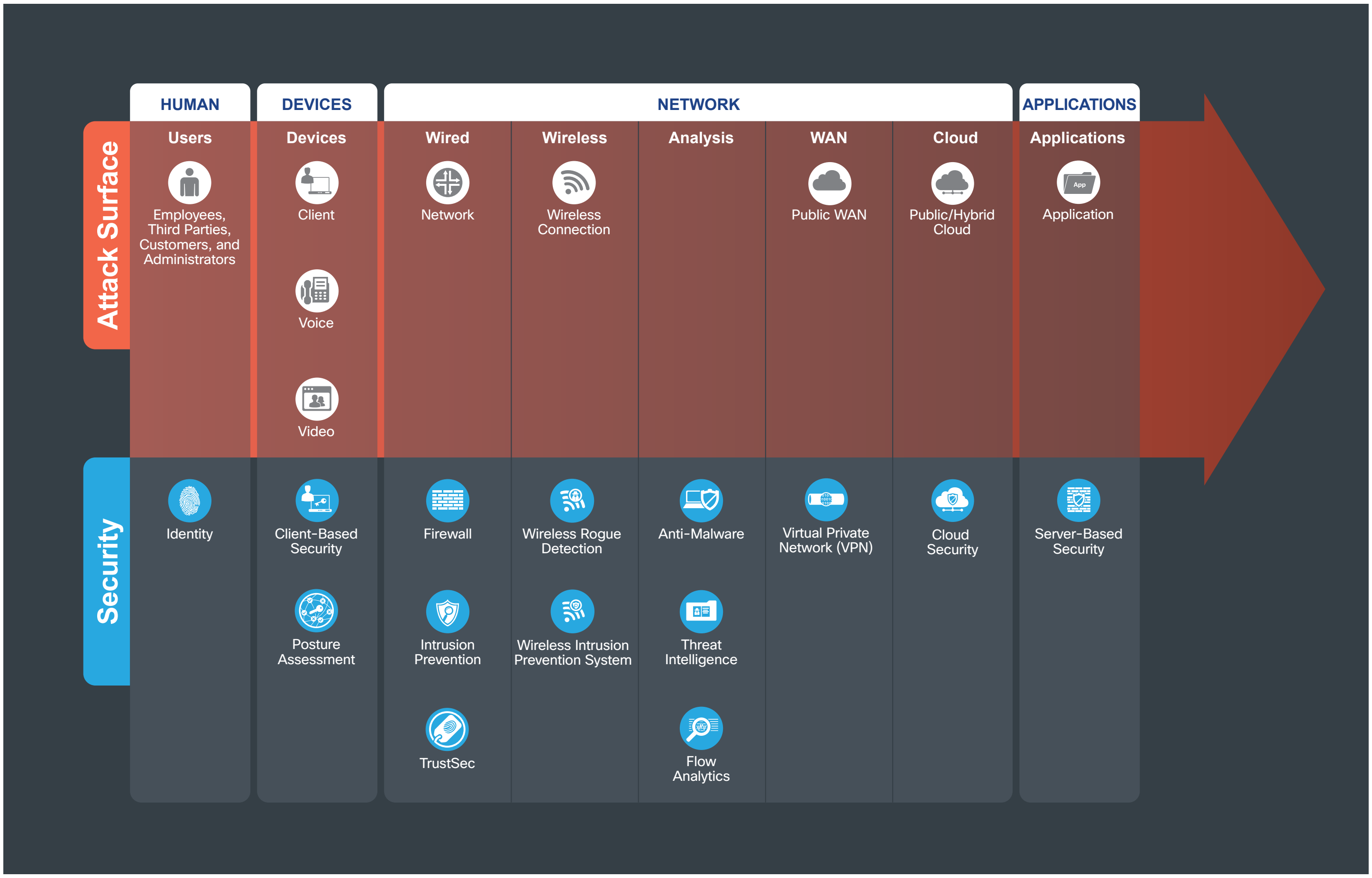


Figure 16 *Secure Campus Attack Surface and Security Capabilities*

Secure Data Center

Data centers contain the majority of information assets and intellectual property. These are the primary goals of all targeted attacks and thus require the highest level of effort to secure. Data centers contain hundreds to thousands of physical and virtual servers that are segmented by application type, data classification zone, and other methods. Creating and managing proper security rules to control access to (north/south) and between (east/west) resources can be exceptionally difficult.

Figure 17 shows the progression of security capabilities that are used to help defend against the attacks common in a data center.

Top Threats Mitigated in the Data Center

- Data extraction (data loss)
- Malware propagation
- Unauthorized network access (application compromise)
- Botnet infestation (scrumping) data loss, privilege escalation, reconnaissance)

For a deeper discussion on defending attacks within the Secure Data Center, see www.cisco.com/go/SAFE.

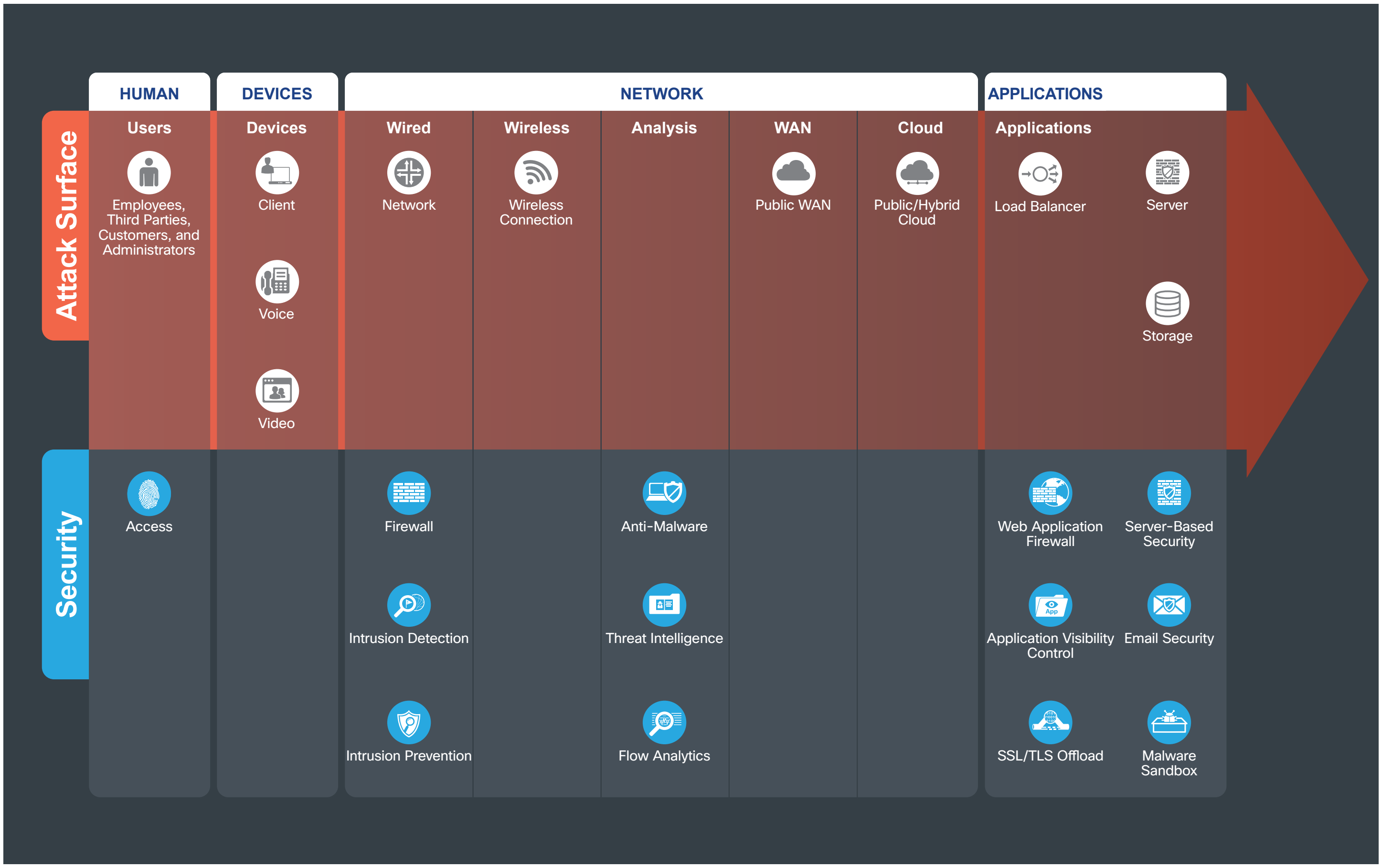


Figure 17 *Secure Data Center Attack Surface and Security Capabilities*

Secure Edge

The edge is the highest-risk PIN because it is the primary ingress point for public traffic from the Internet and the primary egress point for corporate traffic to the Internet. Simultaneously, it is the most critical business resource in today's Internet-based economy.

Figure 18 shows the progression of security capabilities that are used to help defend against the attacks common at the network edge.

Top Threats Mitigated in the Edge

- Webserver vulnerabilities
- Distributed denial of service (DDoS)
- Data loss
- Man-in-the-Middle (MitM)

For a deeper discussion on defending attacks within the Secure Edge, see www.cisco.com/go/SAFE.

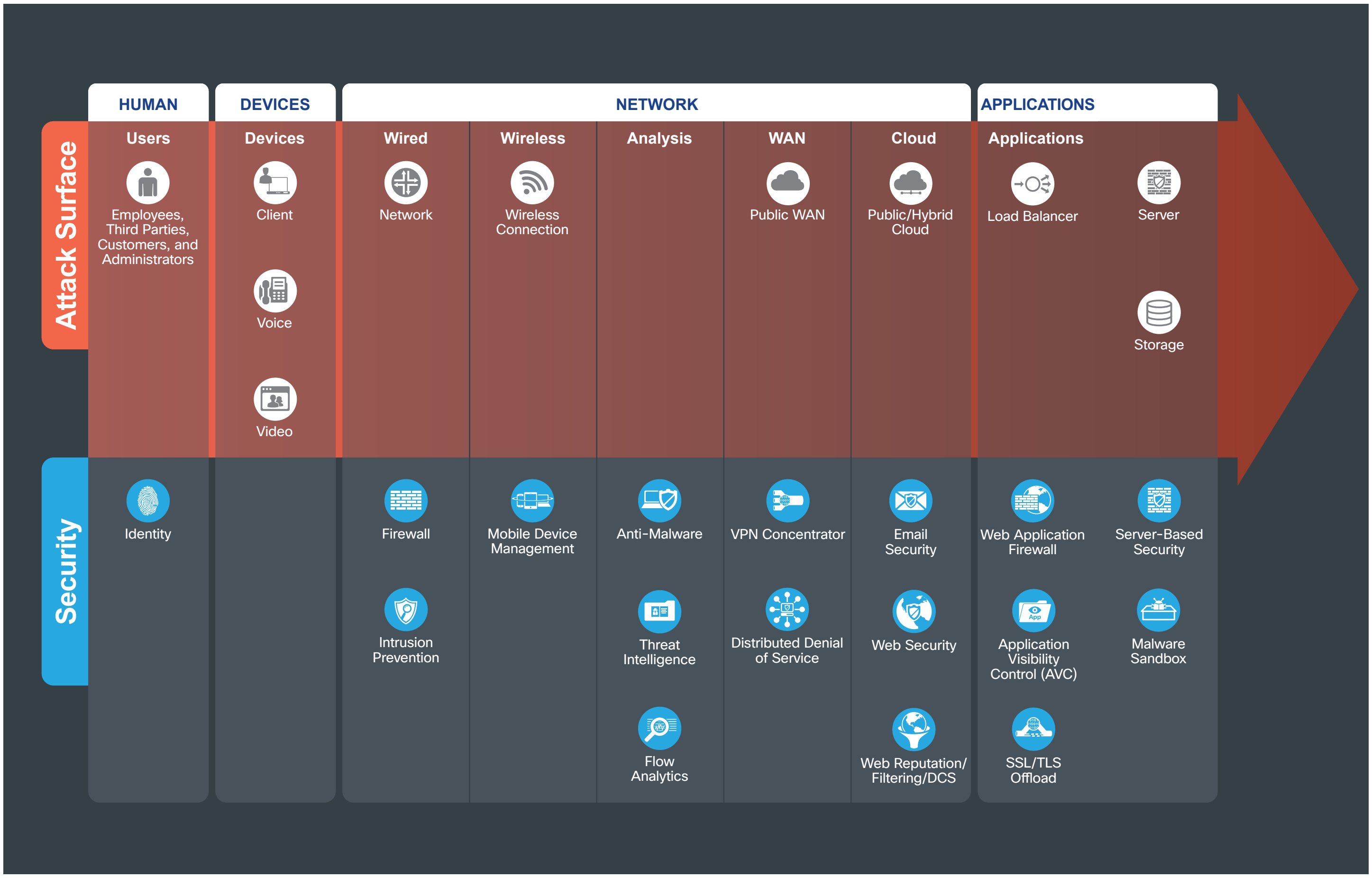


Figure 18 *Secure Internet Edge Attack Surface and Security Capabilities*

Secure Cloud

The majority of cloud security risk stems from loss of control, lack of trust, shared access, and shadow IT. Service Level Agreements (SLAs) are the primary tool for businesses to dictate control of security capabilities selected in cloud-powered services. Independent certification and risk assessment audits should be used to improve trust.

Figure 19 shows the progression of security capabilities used to help defend against the attacks common in the cloud.

Top Threats Mitigated in the Cloud

- Webserver vulnerabilities
- Loss of access
- Virus and malware
- Man-in-the-Middle (MitM)

For a deeper discussion on defending attacks within the Secure Cloud, see www.cisco.com/go/SAFE.

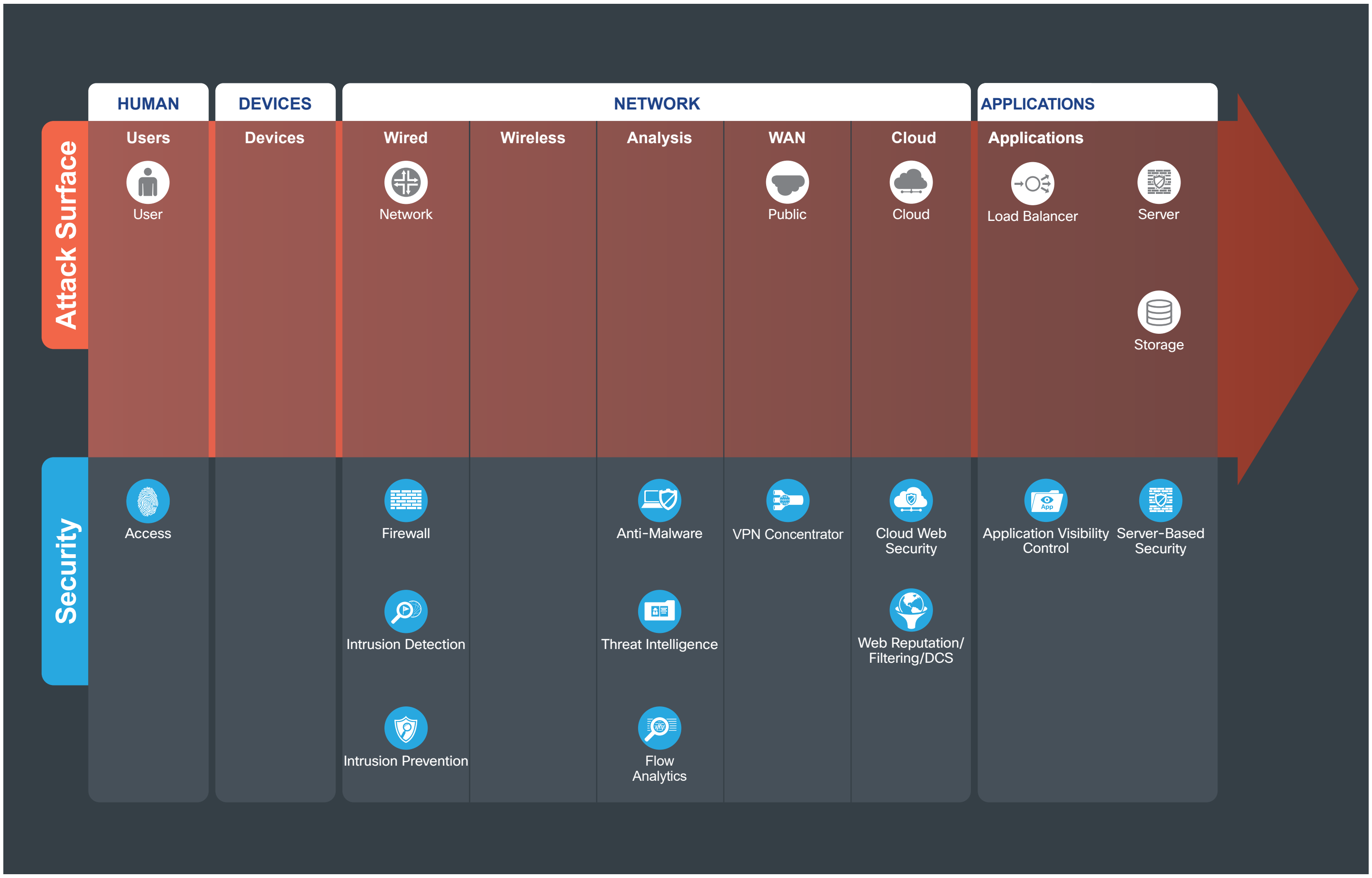


Figure 19 *Secure Cloud Attack Surface and Security Capabilities*

Return to Contents

Secure WAN

The WAN connects all company locations together to provide a single point of control and access to all resources. Managing security and quality of service (QoS) policies to control communication can be exceptionally difficult and complex.

Figure 20 shows the progression of security capabilities used to help defend against the attacks common in a WAN.

Top Threats Mitigated in the WAN

- Malware propagation
- Unauthorized network access
- WAN sniffing and MitM attacks

For a deeper discussion on defending attacks within the Secure WAN, see www.cisco.com/go/SAFE.

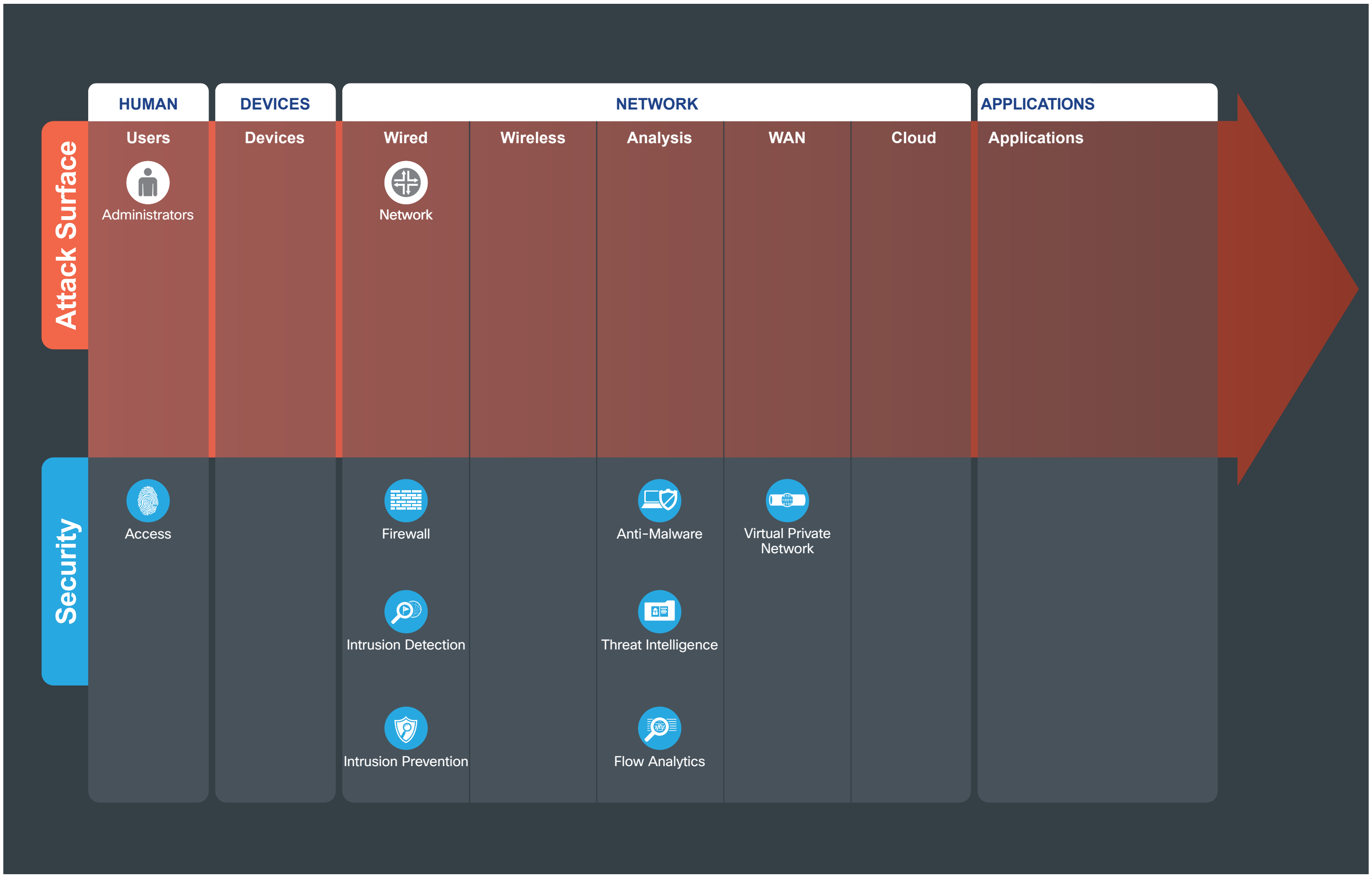


Figure 20 *Secure WAN Attack Surface and Security Capabilities*

Secure Domains

The Secure Domains represent the operational side of the Key. Operational security is divided by function and the people in the organization that are responsible for them. Each domain has a class of security capabilities and operational aspects that must be considered. (See Figure 21.)

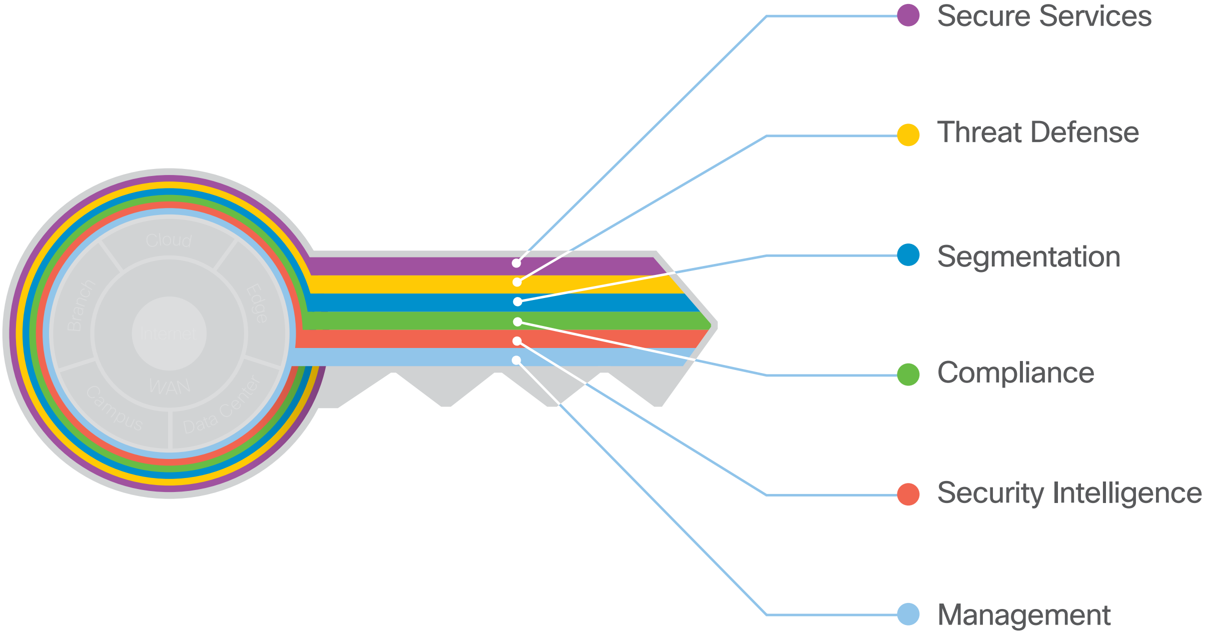


Figure 21 *SAFE Model Secure Domains*

Management

Management of devices and systems using centralized services is critical for consistent policy deployment, workflow change management, and the ability to keep systems patched. Management coordinates policies, objects, and alerting.

Figure 22 shows the progression of security capabilities used for the operations of Management.

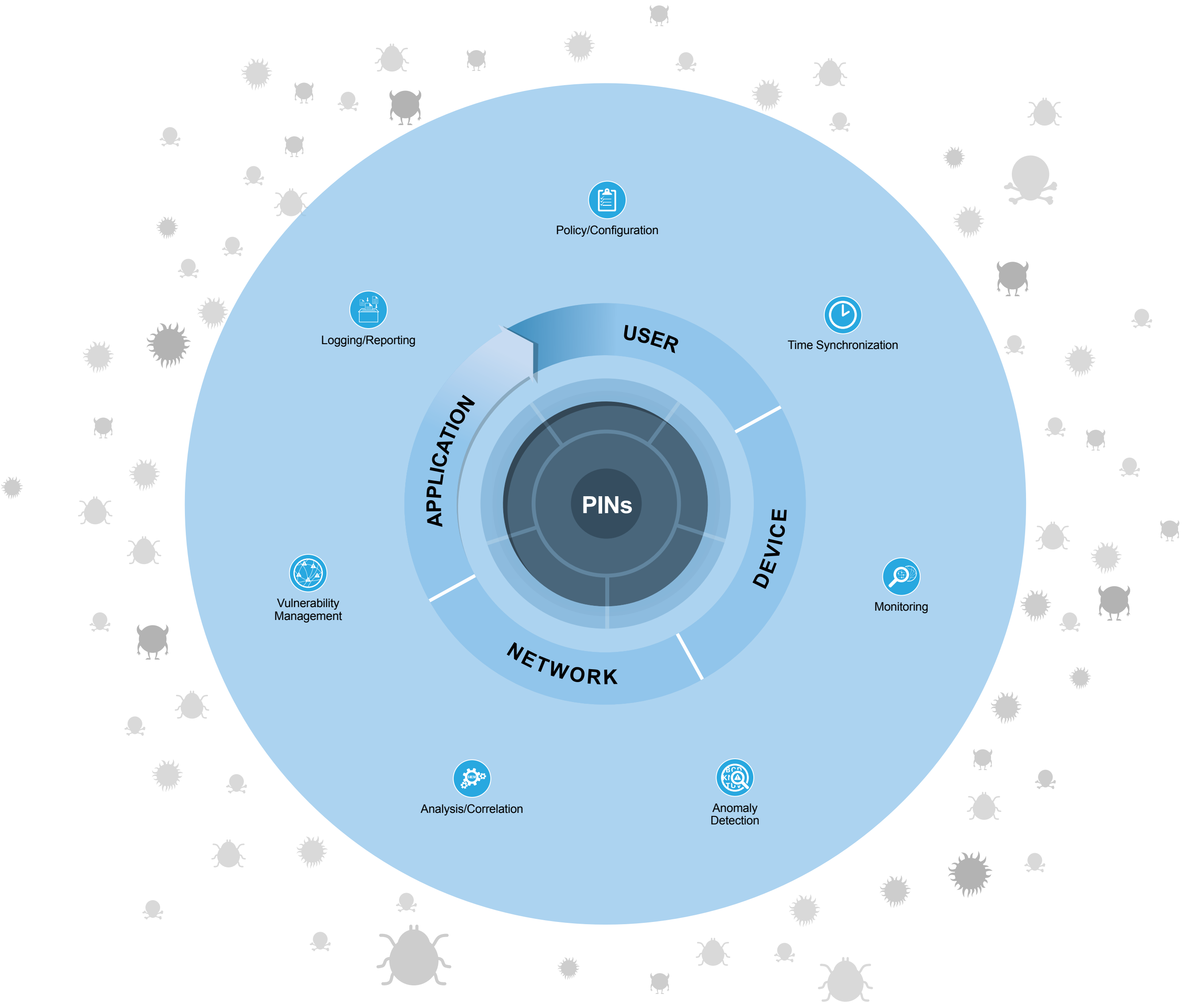


Figure 22 *Management Domain Capabilities*

Security Intelligence

Security Intelligence provides global detection and aggregation of emerging malware and threats. It enables an infrastructure to enforce policy dynamically, as reputations are augmented by the context of new threats, providing accurate and timely security protection.

Figure 23 shows the progression of security capabilities used for the operations of Security Intelligence.

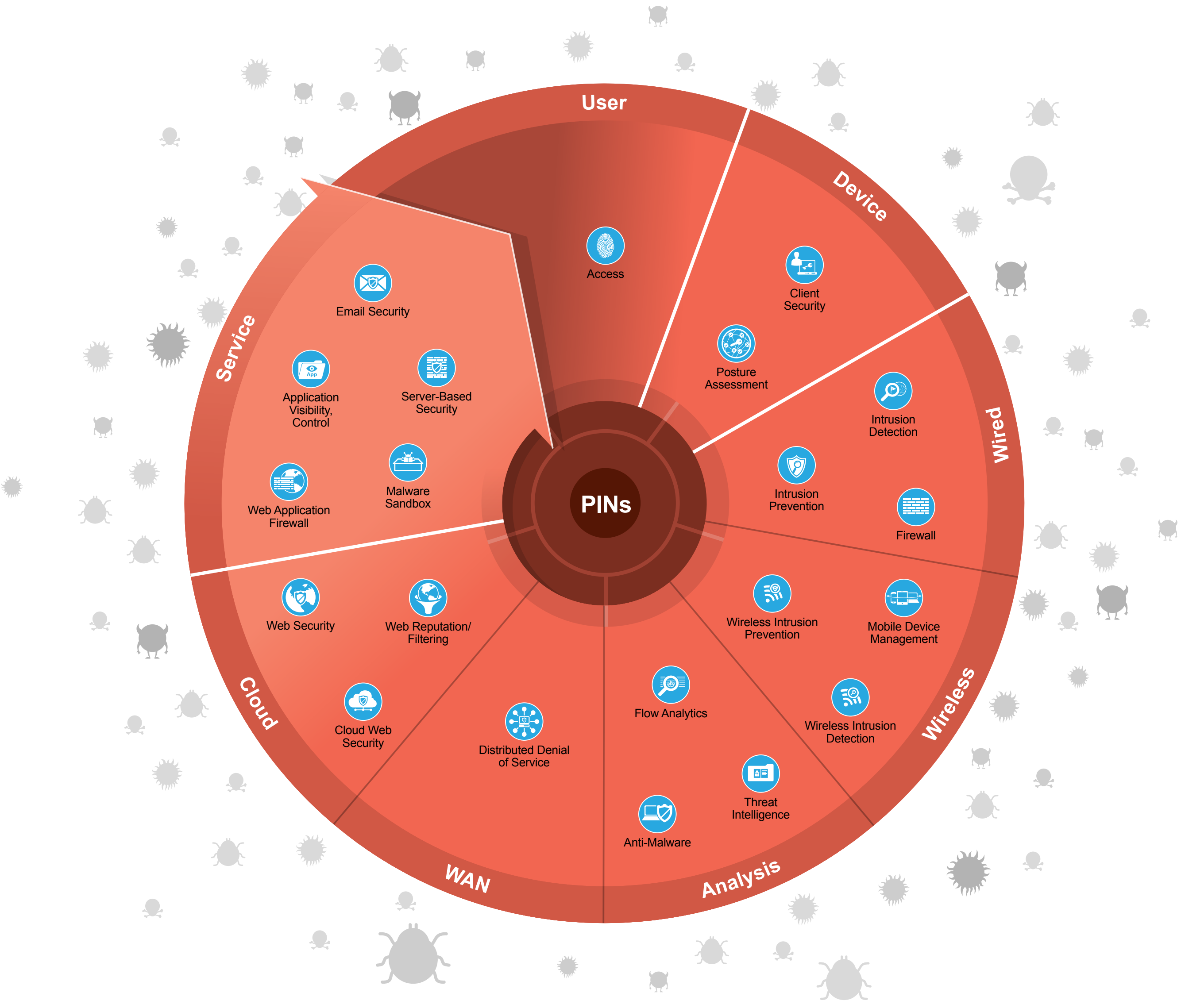


Figure 23 *Security Intelligence Capabilities*

Compliance

Compliance addresses internal and external policies. It shows how multiple controls can be satisfied by a single solution. Examples of external compliance include PCI, HIPAA, and Sarbanes-Oxley (SOX).

Figure 24 shows the progression of security capabilities used for Compliance.

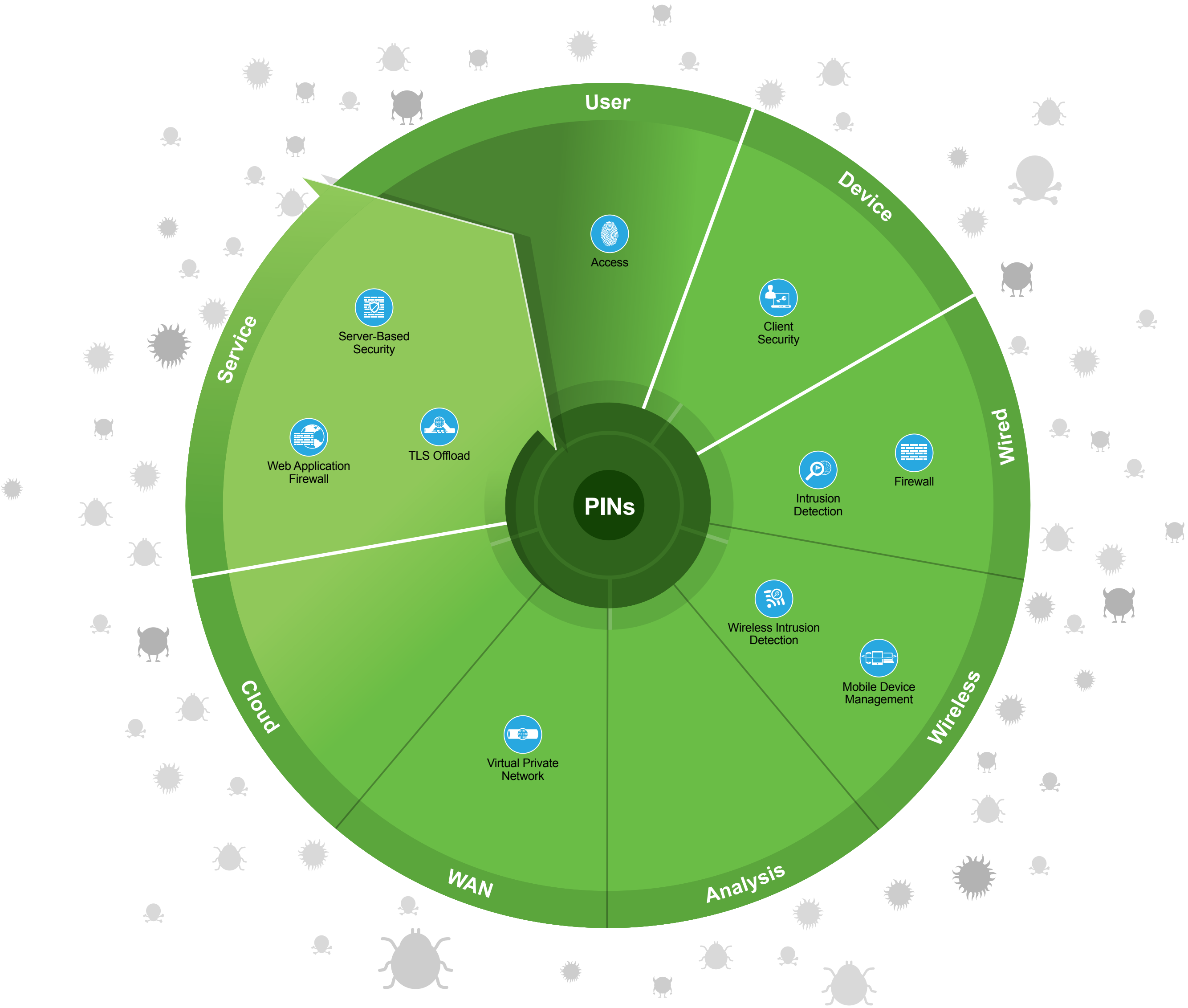


Figure 24 *Compliance Capabilities*

Segmentation

Segmentation establishes boundaries for data and users. Traditional manual segmentation uses a combination of network addressing, VLANs, and firewalls for policy enforcement. Advanced segmentation leverages identity-aware infrastructure to enforce automated and scalable policies.

Figure 25 shows the progression of security capabilities used for Segmentation.

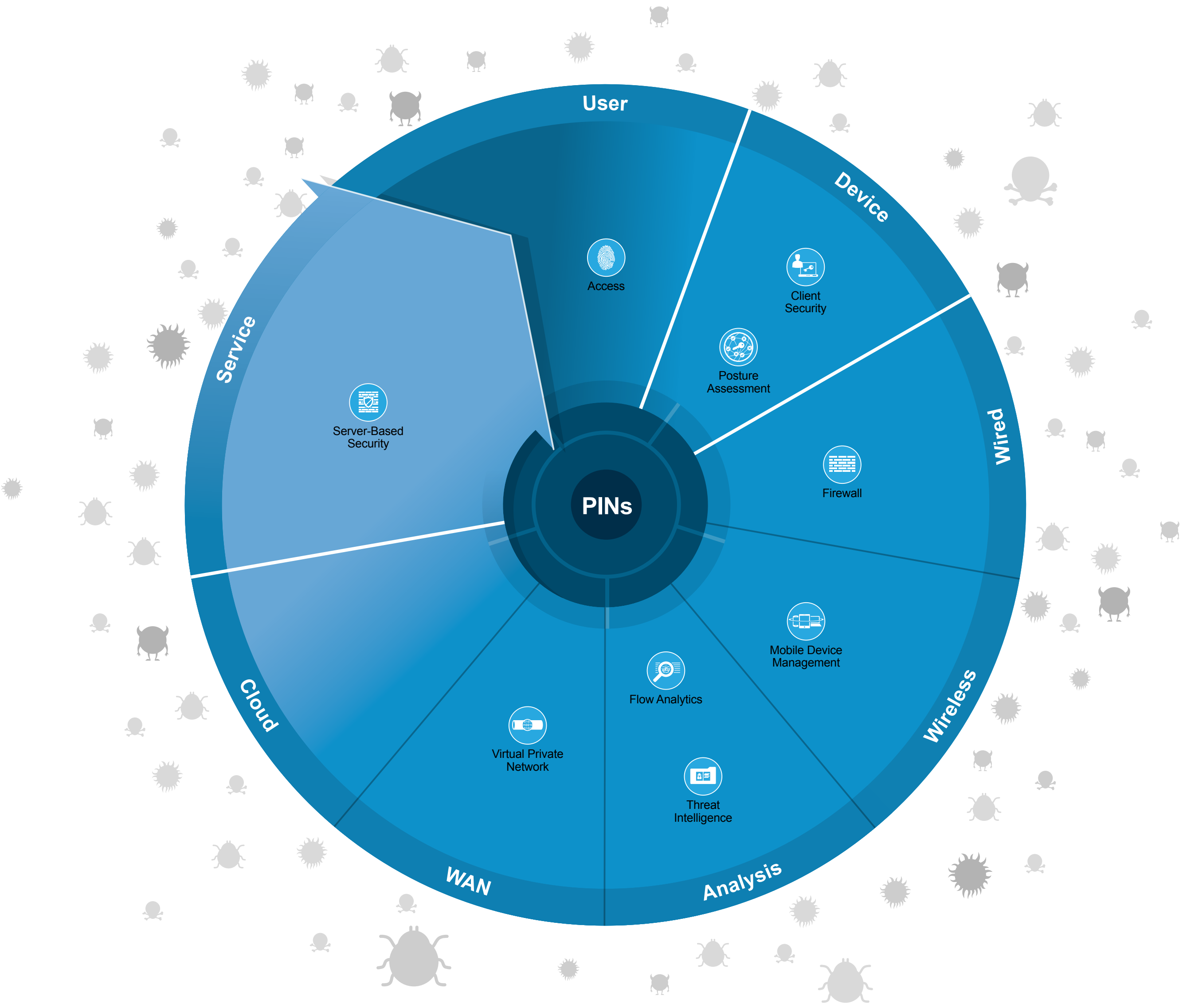


Figure 25 *Segmentation Capabilities*

Threat Defense

Threat Defense provides visibility into the most evasive and dangerous cyber threats. Using network traffic telemetry, reputation, and contextual information, it enables assessment of the nature and potential risk of the suspicious activity so you can take corrective action.

Figure 26 shows the progression of security capabilities used for the operations of Threat Defense.

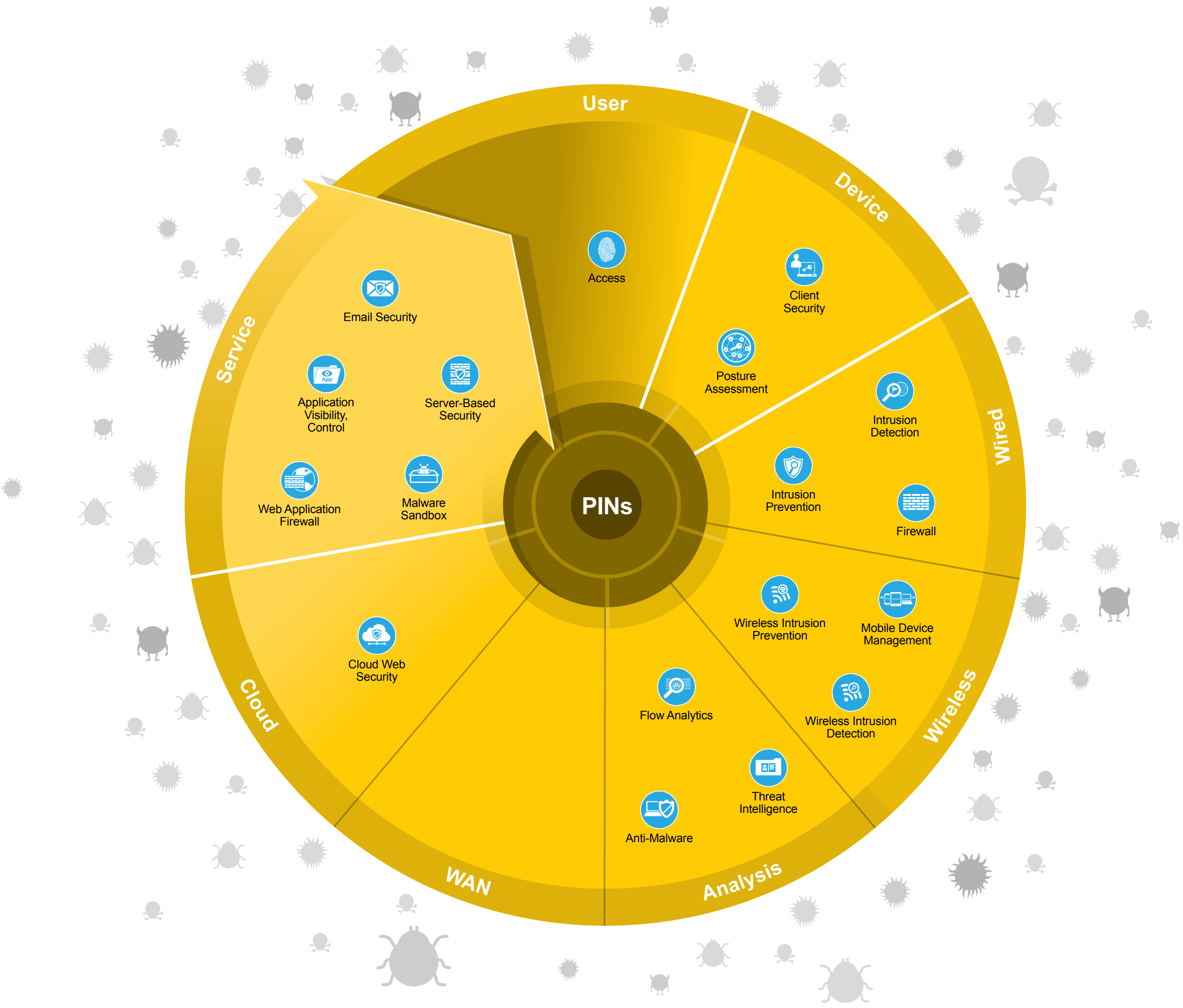


Figure 26 *Threat Defense Capabilities*

Secure Services

Secure Services provide technologies such as access control, virtual private networks, and encryption. This domain includes protection for insecure services such as applications, collaboration, and wireless.

Figure 27 shows the progression of security capabilities used for Secure Services.

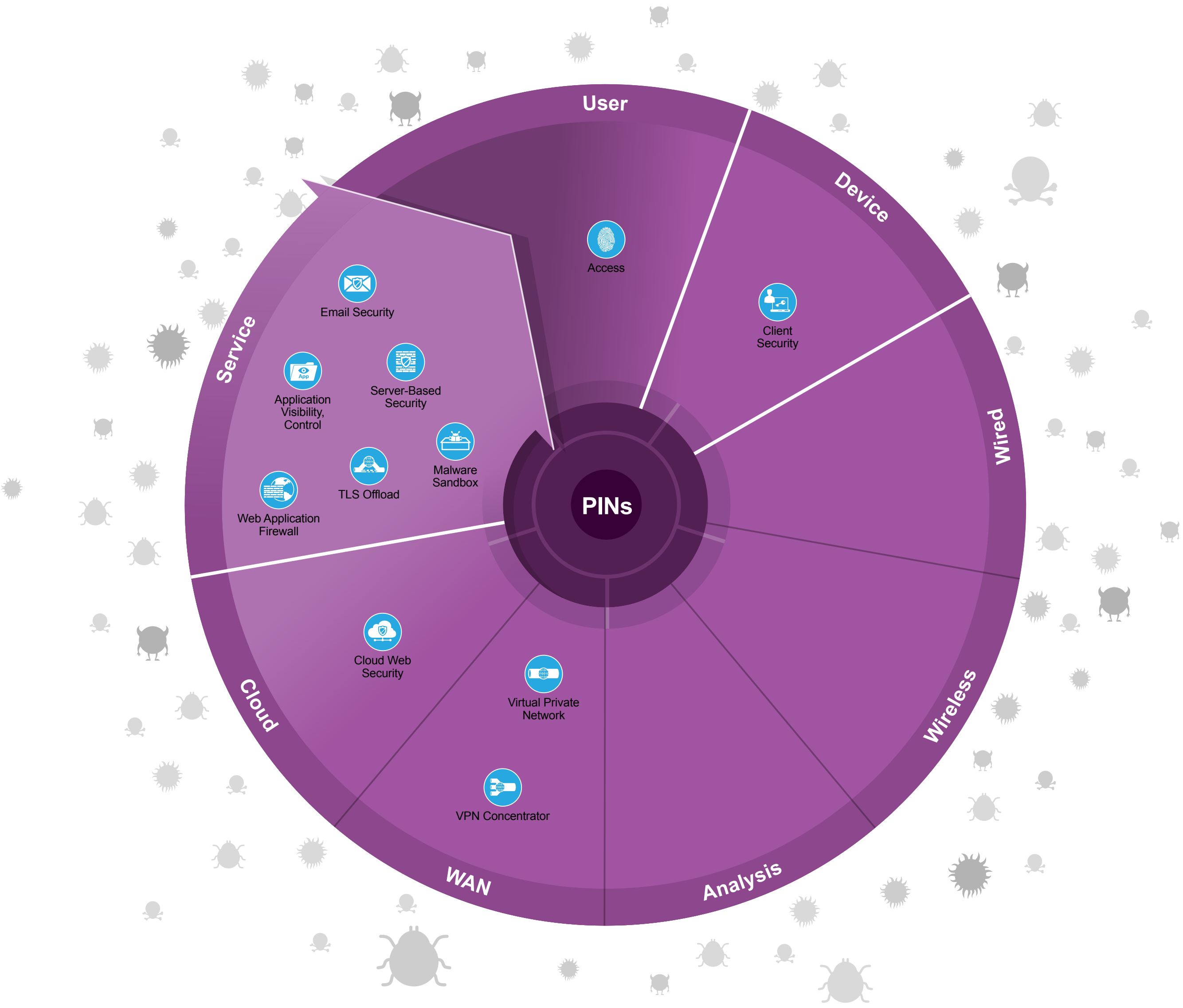


Figure 27 *Secure Services Capabilities*

SAFE Capabilities

Capabilities describe the primary functions of a security service. Table 5 provides a definition for the capabilities used in SAFE. The recommended products are mapped to each capability, where and when it is used, and the top threats mitigated.

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 compliance verification and authorization.	**Virus and Malware:** Compromised devices connecting to infrastructure.	Secure Branch Secure Campus Secure External Zones	AnyConnect Agent Centralized Identity Services Engine

Table 5 *Cisco Security Capabilities and Threats*

Attack Surface	Capabilities	Threats	Places in the Network	Recommended Products
Voice: Phone.	**N/A:** Covered in Secure Services domain.	Attackers accessing private information.	Secure Branch Secure Campus	Cisco Unified Communications
Video: Displays, collaboration.	**N/A:** Covered in Secure Services domain.	Attackers accessing private information.	Secure Branch Secure Campus	Cisco TelePresence
Network				
Wired Network: Physical network infrastructure; routers, switches, used to connect access, distribution, core, and services layers together	**Firewall Segmentation:** Stateful filtering and protocol inspection.	Unauthorized access and malformed packets.	Secure Branch Secure Campus Secure Cloud Secure External Zones Secure WAN	Adaptive Security Appliance Integrated Services Router Meraki MX
			Secure Data Center Secure Edge	Adaptive Security Appliance Integrated Services Router
	Intrusion Detection and Prevention: Identification of attacks by signatures and anomaly analysis.	Attacks using worms, viruses, or other techniques.	Secure Campus Secure Data Center Secure Edge Secure External Zones Secure WAN	Cisco Firepower Services on Adaptive Security Appliance FirePOWER Appliance Firepower Virtual Appliance
			Secure Branch	Cisco FirePOWER Services on ASA and UCS-E Meraki MX
			Secure Cloud	Firepower Virtual Appliance
	Access Control + TrustSec: Contextual segmentation.	**Unauthorized Network Access:** Lateral spread of infiltration.	Secure Branch Secure Campus	Wireless Controller/ Catalyst Switch Centralized Identity Services Engine
			Secure Data Center Secure Edge	Adaptive Security Appliance Aggregation Services Router Nexus/Catalyst Switch

Return to Contents

Table 5 *Cisco Security Capabilities and Threats*

Attack Surface	Capabilities	Threats	Places in the Network	Recommended Products
Wireless Network: Branches vary from having robust local wireless controller security services to a central, cost-efficient model.	**Mobile Device Management (MDM):** Endpoint access control based on policies.	Compromised devices connecting to infrastructure.	Secure Edge	Identity Services Engine Meraki Mobile Device Management
	Wireless Rogue Detection: Detection and containment of malicious wireless devices that are not controlled by the company.	Unauthorized access and disruption of wireless network.	Secure Branch Secure Campus	Wireless LAN Controller Mobility Services Engine Centralized Mobility Services Engine Centralized Wireless LAN Controller Cisco Meraki
	Wireless Intrusion Prevention (WIPS): Blocking of wireless attacks by signatures and anomaly analysis.	Attacks on the infrastructure via wireless technology.		
Analysis: Analysis of network traffic within the campus.	**Anti-Malware:** Identify, block, and analyze malicious files and transmissions.	Malware distribution across networks or between servers and devices.	Secure Branch Secure Campus Secure Cloud Secure Data Center Secure Edge Secure WAN	Cisco Advanced Malware Protection for Networks
			Secure External Zones	Advanced Malware Protection
	Threat Intelligence: Contextual knowledge of emerging hazards.	Zero-day malware and attacks.	Secure Branch Secure Campus Secure Cloud Secure Data Center Secure Edge Secure WAN	Cisco Collective Security Intelligence Cisco Talos Security Intelligence
	Flow Analytics: Network traffic metadata identifying security incidents.	Traffic, telemetry, and data exfiltration from successful attacks.	Secure Branch Secure Campus	Integrated Services Router Adaptive Security Appliance Wireless LAN Controller Catalyst Switch
			Secure Cloud	Stealthwatch Cloud
			Secure Data Center Secure Edge Secure WAN	NetFlow Generation Appliance Stealthwatch FlowSensor Adaptive Security Appliance

Return to Contents

Table 5 *Cisco Security Capabilities and Threats*

Attack Surface	Capabilities	Threats	Places in the Network	Recommended Products
WAN: Public and untrusted Wide Area Networks that connect to the company, such as the Internet.	**VPN Concentrator:** Encrypted remote access.	Exposed services and data theft.	Secure Edge	Adaptive Security Appliance Aggregation Services Router
	Virtual Private Network (VPN): Encrypted communication tunnels.	Easily collecting information and identities.	Secure Branch Secure Campus	Adaptive Security Appliance Integrated Services Router Meraki MX
			Secure Data Center	Adaptive Security Appliance Aggregation Services Router Firepower Appliance
			Secure Cloud External Zones Secure WAN	Adaptive Security Appliance Aggregation Services Router AnyConnect Meraki MX
	DDoS Protection: Protection against scaled attack forms.	Massively scaled attacks that overwhelm services.	Secure Edge	Distributed Denial of Service Technology Partner

Return to Contents

Table 5 *Cisco Security Capabilities and Threats*

Attack Surface	Capabilities	Threats	Places in the Network	Recommended Products
Cloud	**Cloud Security:** Security and control for the distributed enterprise.	Attacks from malware, viruses, and malicious URLs.	Secure Branch Secure Campus Secure Cloud Secure Data Center Secure Edge Secure External Zones Secure WAN	Cloud Web Security Meraki MX Firepower URL Web Security Appliance AnyConnect Agent Cisco Umbrella Secure Internet Gateway (SIG) Cloudlock
	DNS Security	Redirection of user to malicious website.		
	Cloud-based Firewall	Unauthorized access and malformed packets connecting to services.		
	Software-Defined Perimeter (SDP/SD-WAN):	Easily collecting information and identities.		
	Web Security: Internet access integrity and protections.	Infiltration and exfiltration via HTTP.		
	Web Reputation/ Filtering: Tracking against URL-based threats.	Attacks directing to a malicious URL.		
	Cloud Access Security Broker (CASB)	Unauthorized access and Data loss.		
Applications				
Applications	**Web Application Firewalling:** Advanced application inspection and monitoring.	Attacks against poorly-developed applications.	Secure Data Center Secure Edge	Web Application Firewall Technology Partner
	Application Visibility Control (AVC): Deep packet inspection (DPI) of application flows.	Attack tools hiding in permitted applications.	Secure Branch Secure Edge	FirePOWER Services Module or Appliance Meraki MX Cisco ASR

Table 5 *Cisco Security Capabilities and Threats*

Attack Surface	Capabilities	Threats	Places in the Network	Recommended Products
Applications (continued)	**TLS Encryption Offload:** Hardware accelerated encryption of data services.	Theft of unencrypted traffic.	Secure Data Center Secure Edge	Transport Layer Security Offload Technology Partner
	Storage: Information storage on all media types.		Secure Branch Secure Campus Secure Cloud Secure Data Center Secure Edge	NAS/SAN (Partner)
	Server-Based Security: Security software to protect hosts.	Viruses or malware compromising systems.	Secure Cloud Secure Data Center Secure Edge	Cisco Advanced Malware Protection for Endpoint AnyConnect Cisco Umbrella Anti-Virus
	Anti-Malware: Identify, block, and analyze malicious files and transmissions.	Malware distribution across servers.		
	Anti-Virus	Viruses compromising systems.		
	Cloud Security	Redirection of user to malicious website.		
	Host-based Firewall	Unauthorized access and malformed packets connecting to server.		
	Email Security: Messaging integrity and protections.	Infiltration and exfiltration via email.	Secure Data Center Secure Edge	Email Security Appliance Cloud Web Security
	Malware Sandbox: Detonation and analysis of file behavior.	Polymorphic threats.	Secure Branch Secure Data Center Secure Edge	Cloud Web Security Cisco Threatgrid

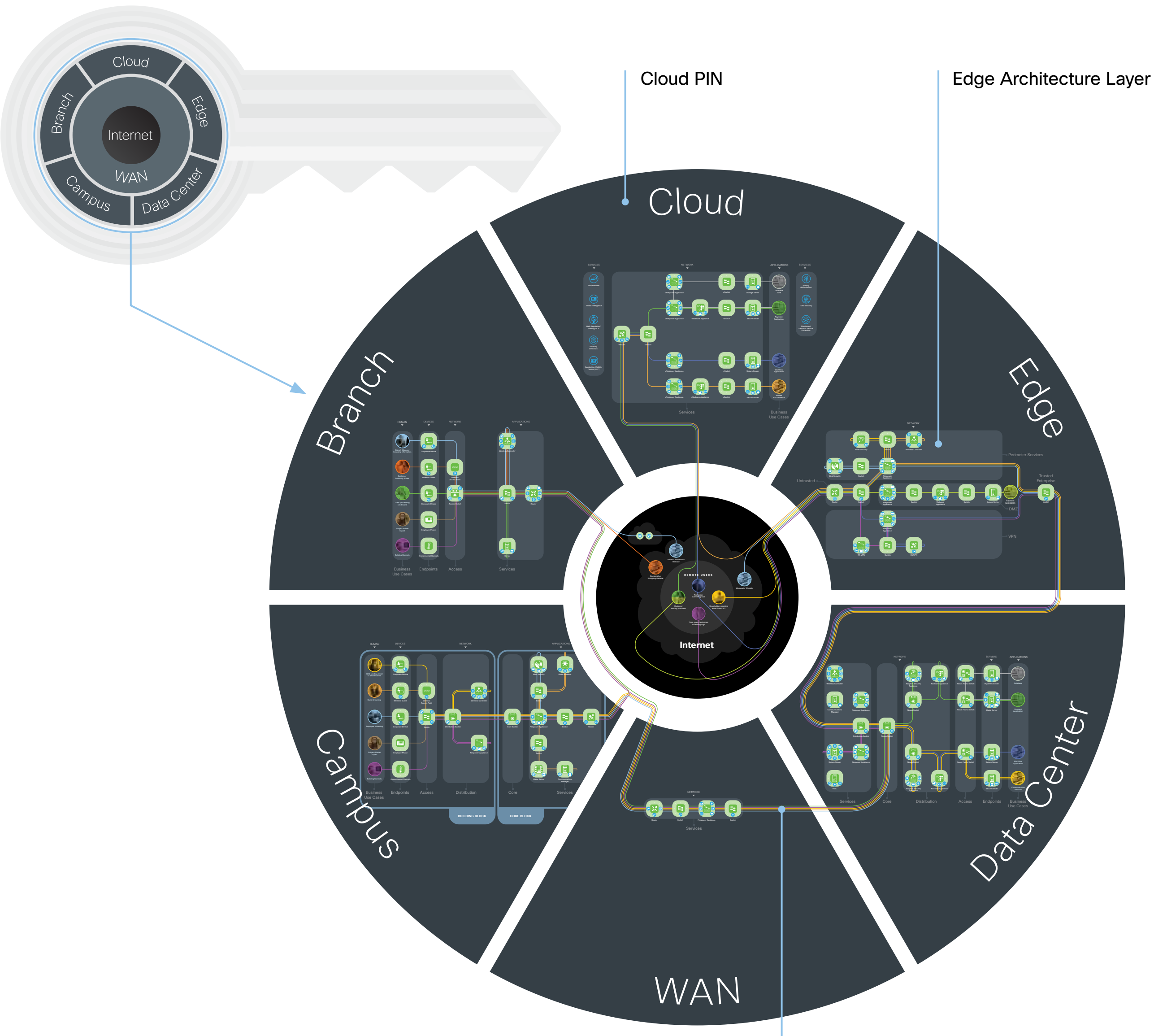
Return to Contents

Table 5 *Cisco Security Capabilities and Threats*

Attack Surface	Capabilities	Threats	Places in the Network	Recommended Products
Management				
	Logging/Reporting: Centralized event information collection.	Unauthorized network access or configuration.	All	Prime Infrastructure Manager Stealthwatch Management Console Partner Tools
	Policy/Configuration: Unified infrastructure management and compliance verification.	Seizure of infrastructure or devices.		Prime Management Suite
	Time Synchronization: Device clock calibration.	Misdirection and correlation of attacks		All systems and devices
	Vulnerability Management: Continuous scanning and reporting of infrastructure.	Malicious device connected to infrastructure.		Firepower Management Center Identity Services Engine Cisco Meraki
	Analysis/ Correlation: Security event management of real-time information.	Diverse and polymorphic attacks.		Firepower Management Center Stealthwatch Prime SIEM partner
	Anomaly Detection: Identification of infected hosts scanning for other vulnerable hosts.	Worm traffic that exhibits scanning behavior.		Fiepower Management Center Stealthwatch Management Console AMP for Endpoints Console
	Monitoring: Network traffic inspection.	Traffic, telemetry, and data exfiltration from successful attacks.		Stealthwatch Cisco NAM Cisco NGA Partner Tools

The SAFE Architecture

The SAFE security reference architecture logically maps **business flows** to security capabilities from the source to the destination using **Places in the Network (PINs)**. Each PIN has **architectural layers** that define where and why security controls are used.



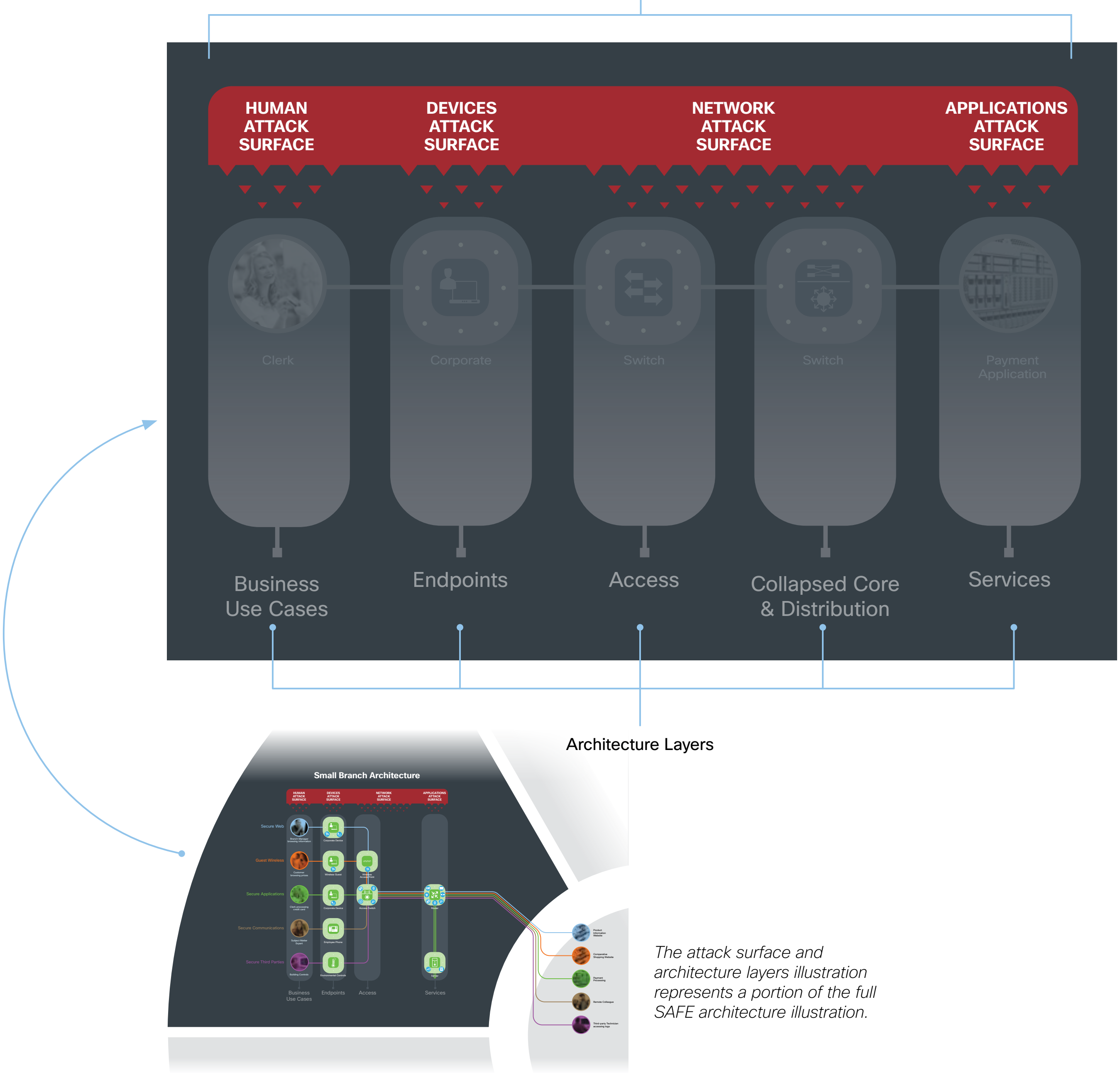
Business Flows

Figure 28 *SAFE Model. The SAFE Model simplifies complexity across a business by using Places in the Network (PINs) that it must secure.*

The Attack Surface and Architecture Layers

The SAFE architecture uses layers that align to the attack surface. Business use cases connect through the network to application services. Each layer has standardized controls relating to its function. Some layers provide access and visibility while others perform enforcement. Not all PINs contain all layers (see further definition in the architecture guide for each Place in the Network).

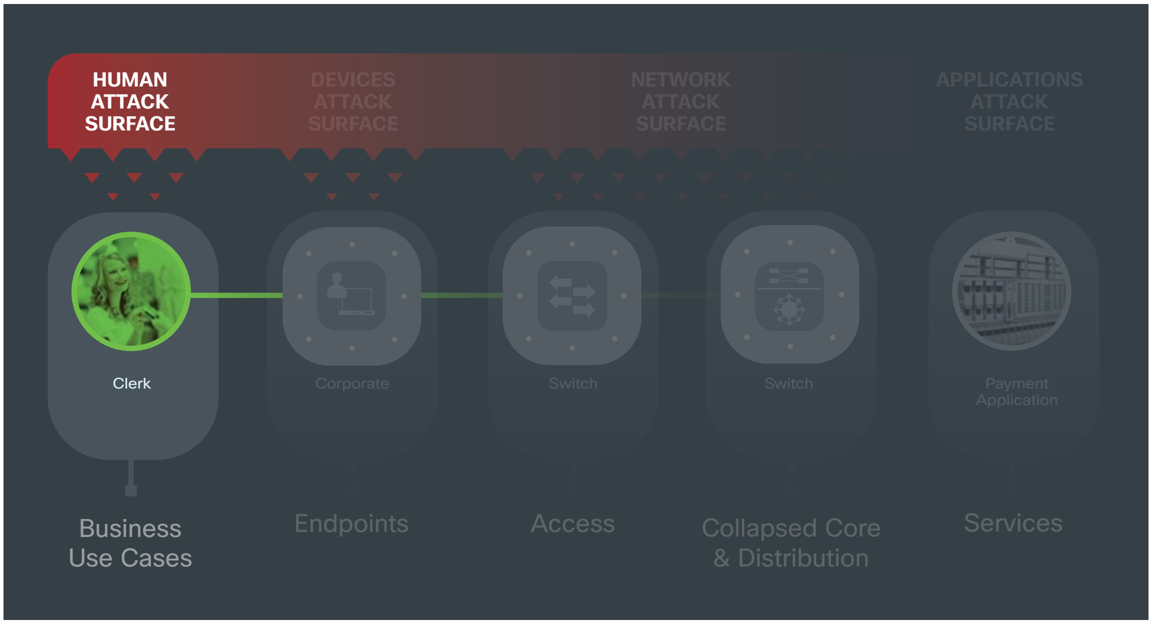
Figure X *Alignment of attack surface to architecture layers*



The attack surface and architecture layers illustration represents a portion of the full SAFE architecture illustration.

Attack Surface: Human

A Business Use Case is a role performed by a Human connecting to network services.



Business Use Case Layer

Humans use network services to perform business functions. Each business use case defines what services are needed and where the flow of data will go. Some users will perform multiple roles requiring respective security.

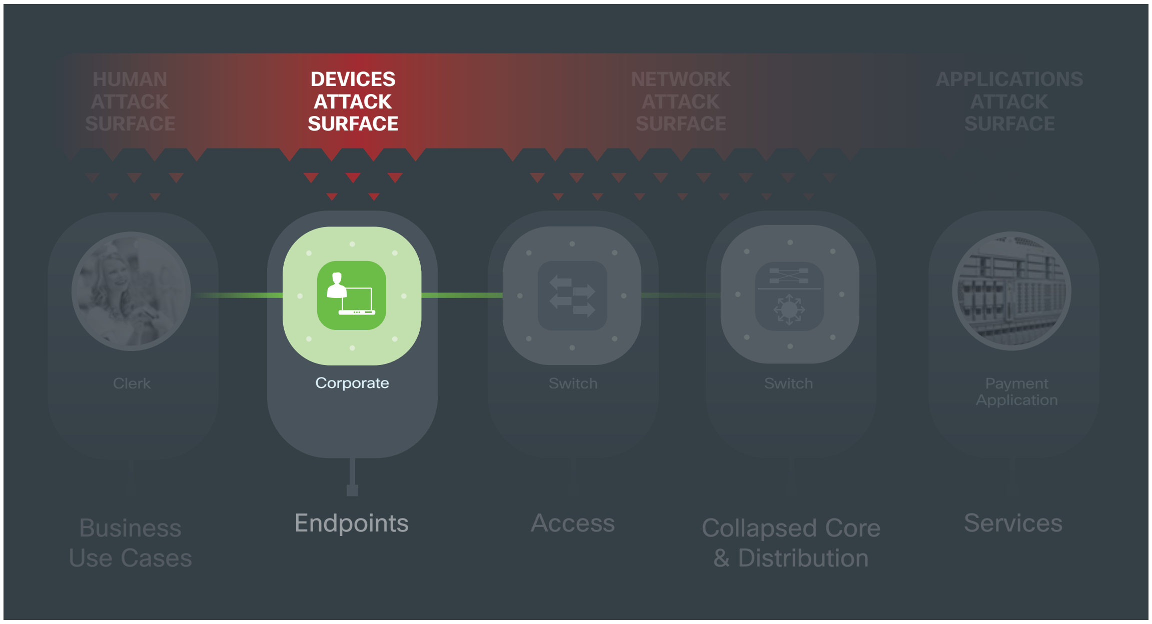
Humans can be the weakest link in your security architecture. If their identity is compromised, downstream technical controls can be bypassed. Visibility and segmentation limit the impact of compromised employees, malicious partners, or customers.

Capability

Identity – Assign each user a role-based identity that has a respective set of security capability controls.

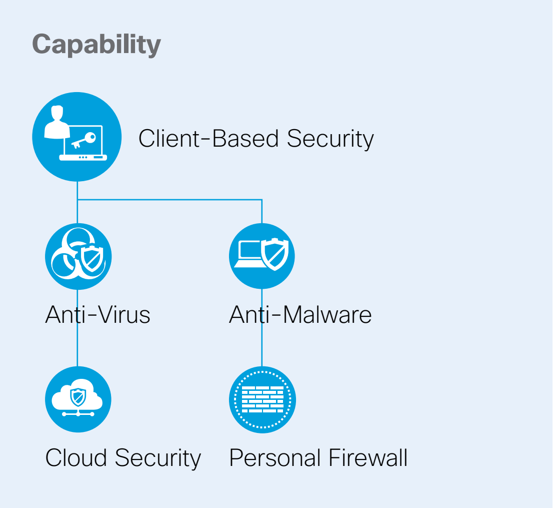
Attack Surface: Devices

The Devices layer includes devices that vary from traditional PCs and laptops to smart phones, tablets, and increasingly, things such as building controls, cameras, and robotics. Devices require respective client-based security defined by policy.



Endpoints Layer

Zero day and other advanced attacks can bypass existing security. A secure company uses the network and the devices connecting to it as baselines of behavior. Under attack, new behavior compared to baselines provides alarm. Visibility using the network as a sensor, enables effective containment through intelligent architectural design.


Capability

Client-Based Security

Anti-Virus

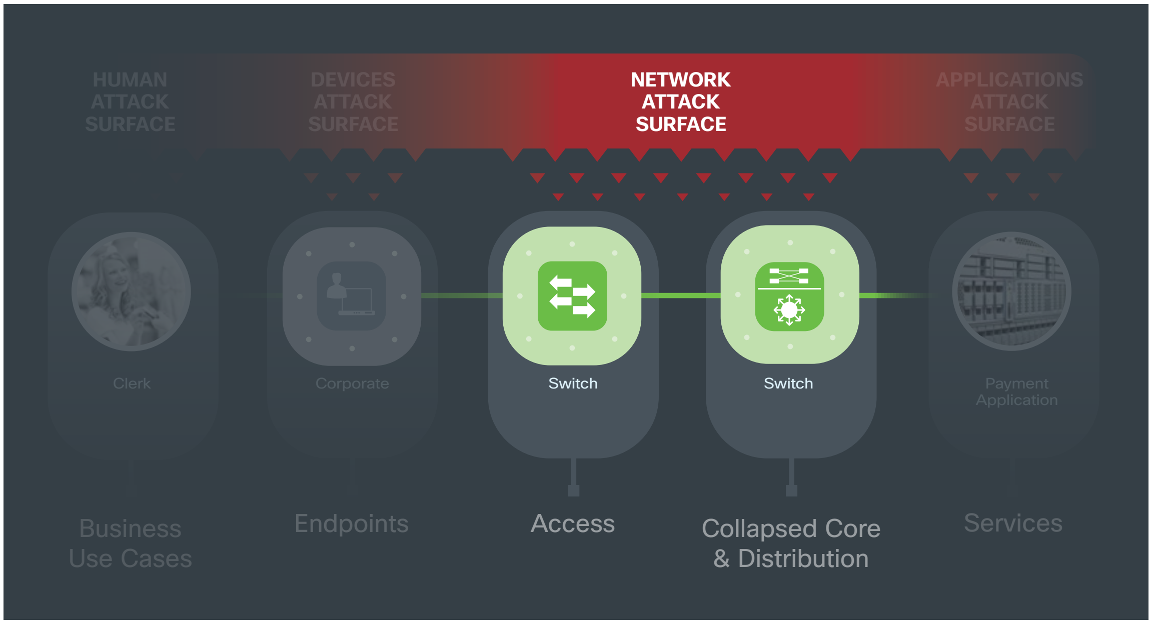
Anti-Malware

Cloud Security

Personal Firewall

Attack Surface: Network

The SAFE model aligns to the traditional network model of access, distribution, and core. Each layer in the hierarchy benefits by dividing a flat network into scalable blocks. Traffic remains local unless it is destined for other networks, and it is elevated to a higher layer. The network acts as a sensor utilizing flow analytics to capture anomalies and provide visibility to attacks.



Access Layer

The purpose of the access layer is to securely connect humans and devices to the network. It connects to the distribution layer and is the first line of enforcement to the rest of the network. Its purpose is to identify and segment users, and to assess compliance of devices seeking access. Ths layer enables enforcement of violations of posture, identity, or anomalous behavior.

Distribution Layer

This layer is an aggregation point for all of the access switches. It controls the boundary between the access and core layers and serves as an integration point for security capabilities such as IPS and network policy enforcement.

Core Layer

The core layer provides high-speed, highly redundant forwarding services, connecting the distribution layer to the services layer. In smaller locations not requiring scale, distribution or access layers connect directly to the core.

Primary Security Capability

Identity

Flow Analytics

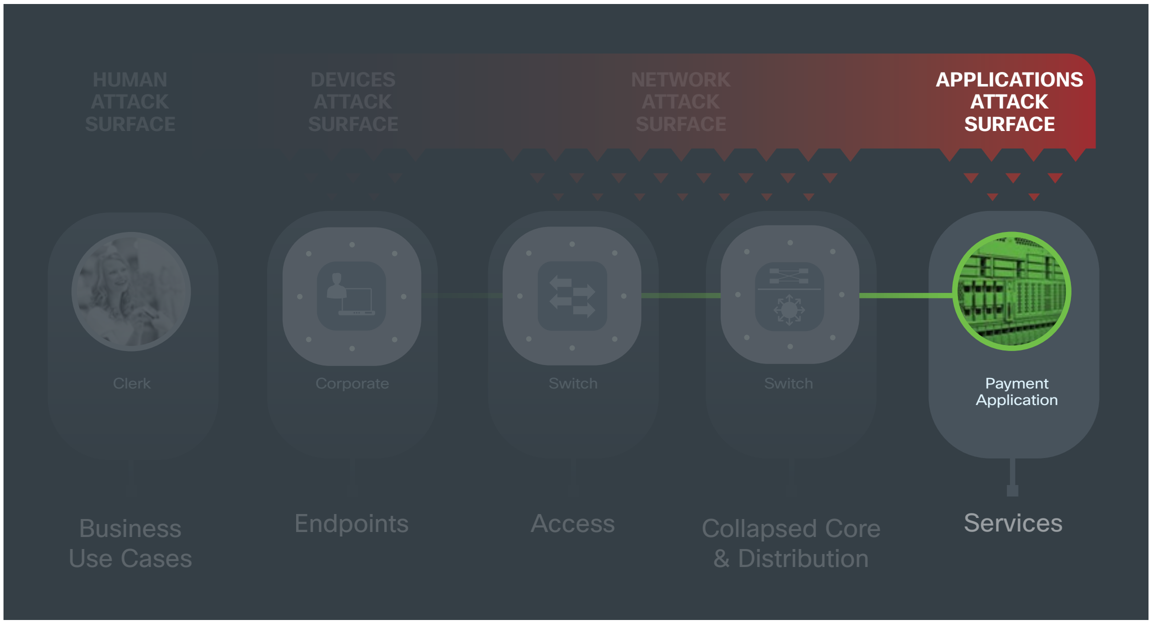
Posture Assessment

TrustSec

Wireless Rogue Detection

Attack Surface: Applications

The purpose of the services layer is to provide and secure services used by business functions.

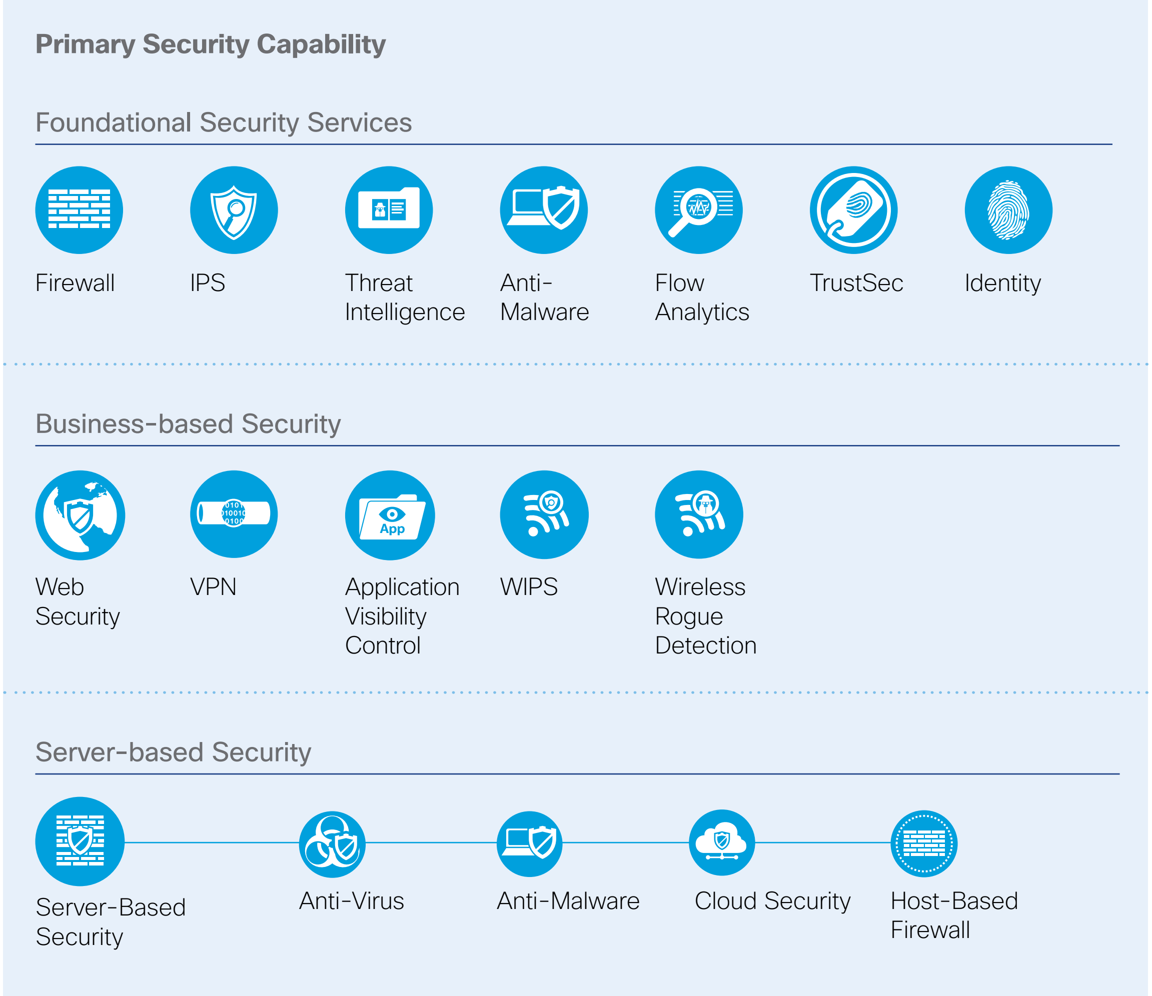


Services Layer

The services layer typically connects to the core layer and provides foundational capabilities. The security capabilities segment traffic and provide visibility into separated business flows. Through analytics, each Place in the Network has protection from known malware and other malicious intrusions. In the event of zero-day attacks where the threat has not been categorized, flow analytics identifies anomalous behavior, reducing time to detection. Policy is enforced against violations.

Business-based security protects against threats introduced outside the company, such as email correspondence, web surfing, and remote access. Many businesses need to satisfy compliance mandates using rogue wireless detection regardless of whether the company uses wireless itself. If a company uses wireless for business functions, WIPS is needed in addition to foundational IPS.

Return to Contents



Primary Security Capability

Foundational Security Services

- Firewall
- IPS
- Threat Intelligence
- Anti-Malware
- Flow Analytics
- TrustSec
- Identity

Business-based Security

- Web Security
- VPN
- Application Visibility Control
- WIPS
- Wireless Rogue Detection

Server-based Security

- Server-Based Security
- Anti-Virus
- Anti-Malware
- Cloud Security
- Host-Based Firewall

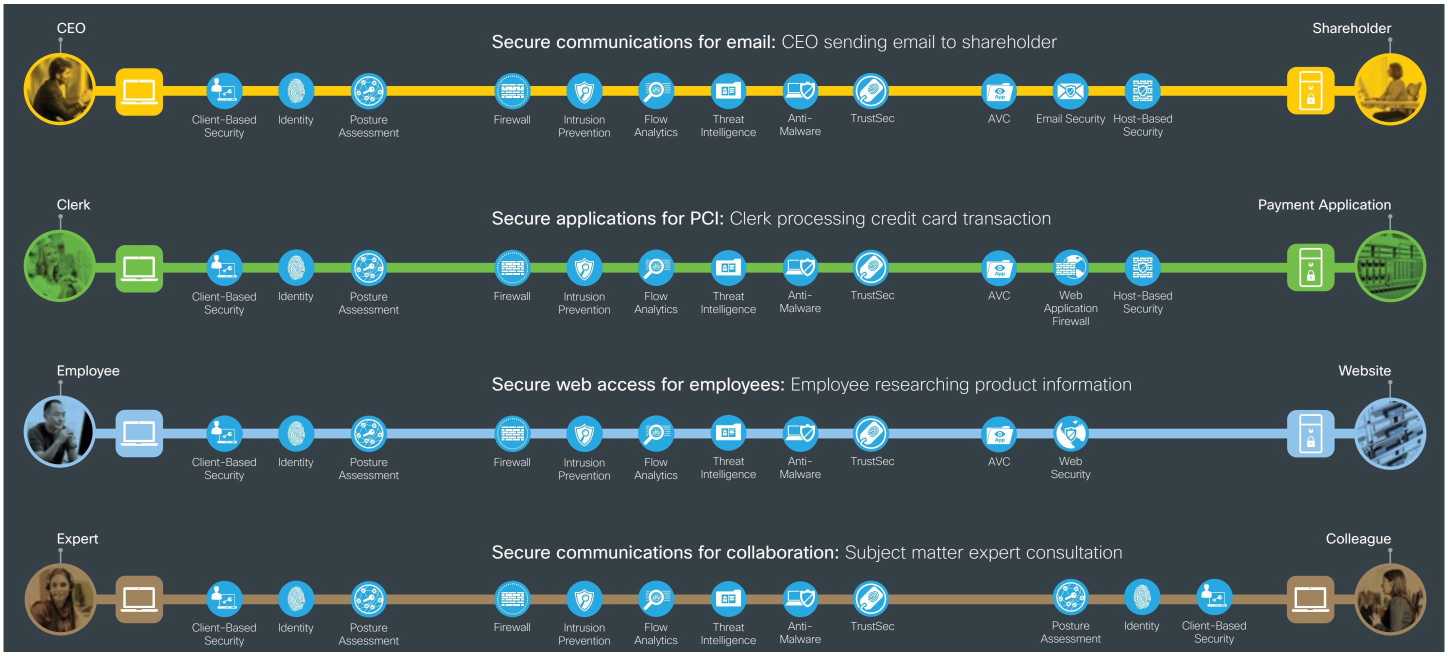
Summary

Companies are threatened by increasingly sophisticated attacks. SAFE provides a model and a method for simplifying the complexity associated with defense. By segmenting company business into role-based business flows, appropriate security capabilities are applied. Organizing these capabilities into architectures, SAFE standardizes how the business is secured. Finally, designs complete with materials, configurations, and cost are created based on these security business architectures.

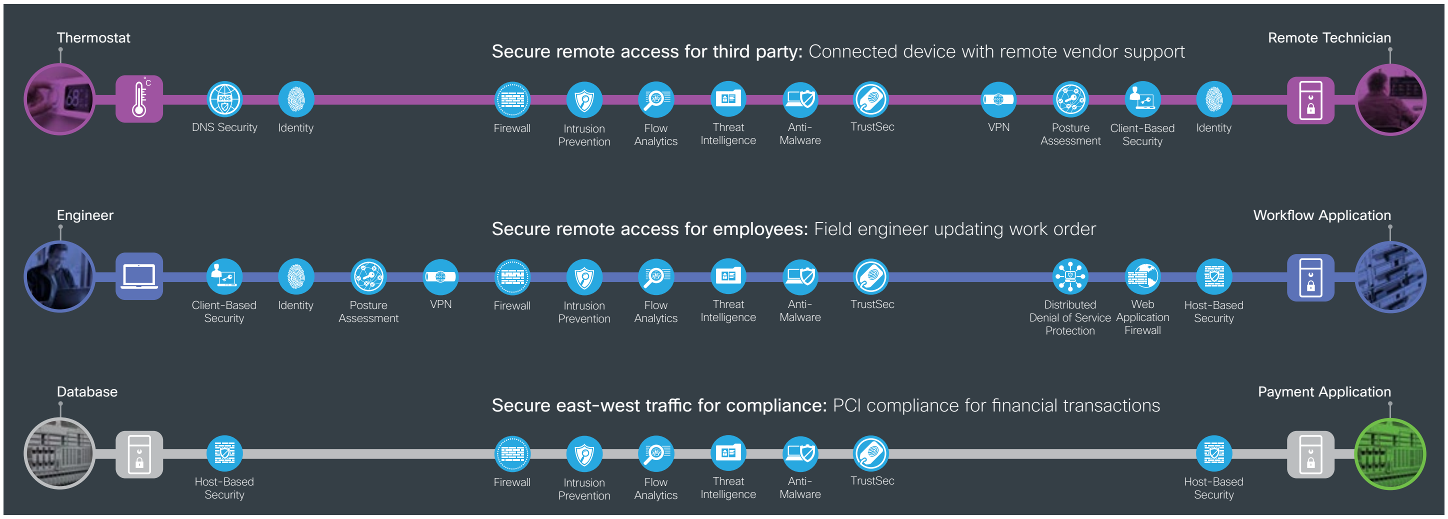
SAFE simplifies the security challenges of today and prepares for the threats of tomorrow.

Appendix

Internal Business Flows

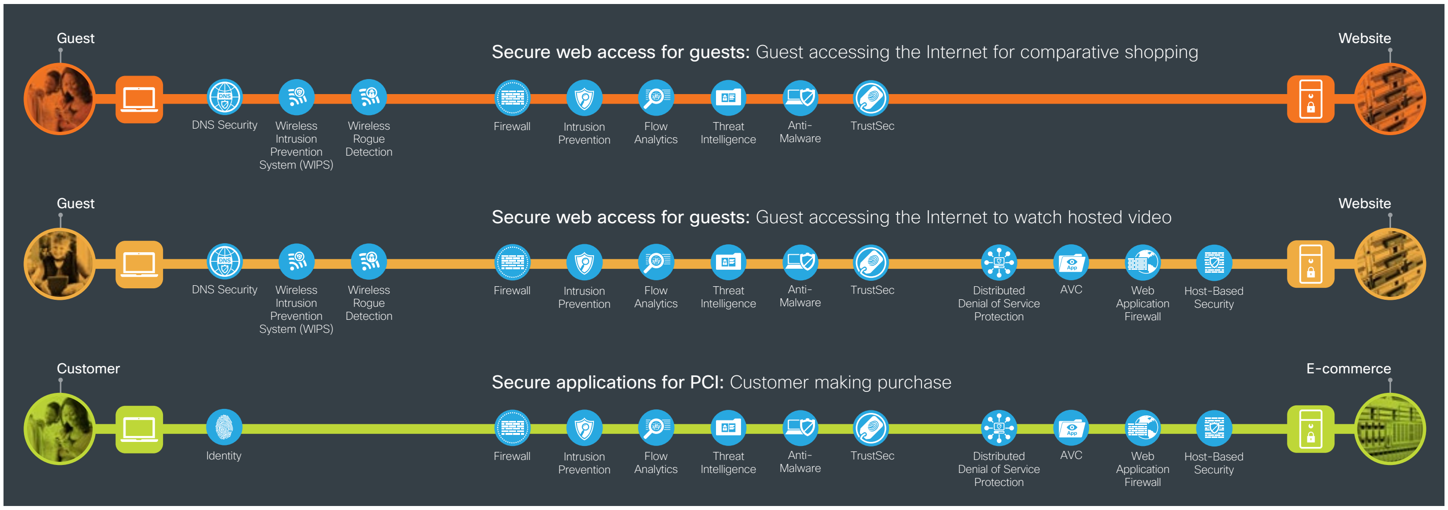


Third-Party Business Flows



Return to Contents

Customer Business Flows



↰ Return to Contents

For more information on SAFE, see www.cisco.com/go/SAFE.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.