

SAFE Architecture Guide

Places in the Network: Secure Branch

August 2022

Contents

Overview	3
Business Flows	4
Threats	7
Security Capabilities	8
Human Attack Surface	9
Devices Attack Surface - Clients	10
Network Attack Surface - Wired Network	10
Network Attack Surface - Wireless Network	11
Network Attack Surface - Analysis	12
Network Attack Surface - WAN	12
Network Attack Surface - Cloud	13
Applications Attack Surface	14
Management	14
Architecture	15
Small Branch	16
Medium Branch	17
Large Branch	19
Attack Surface	20
Human	21
Devices	21
Access Layer	23
Core and Distribution Layer	24
Services Layer	25
Summary	26
Appendix	26
Appendix A - A Proposed Design	26
Appendix B - Suggested Components	30
Appendix C - Feedback	31

Overview

The Secure Branch is a place in the network (PIN) where a company does business across dispersed locations. This guide addresses the most common branch business flows across all industries and the security used to defend them. Branch examples are stores in retail, clinics in healthcare, banks in financial markets, etc. Typically less complex and smaller in footprint than campuses or data centers, branches can have large numbers of locations supporting network access for employees, third parties, and customers.

The Secure Branch is one of the six places in the network within SAFE. SAFE is a holistic approach in which Secure PINs model the physical infrastructure and Secure Domains represent the operational aspects of a network.

The Secure Branch architecture guide provides:

- Business flows typical for branch locations
- Branch threats and security capabilities
- Business flow security architecture
- Design examples and a parts list

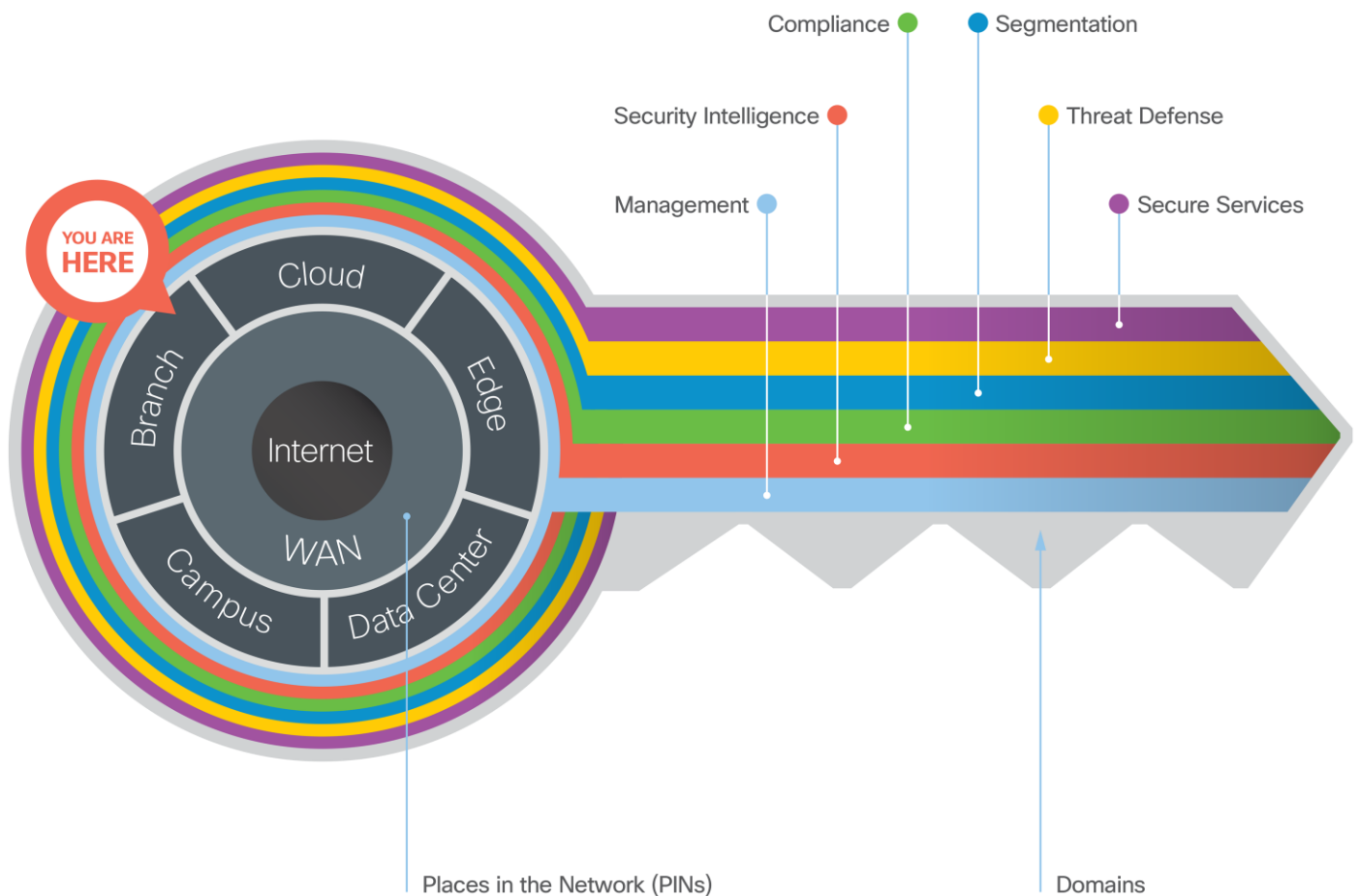


Figure 1.

The 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.

SAFE simplifies security by starting with business flows, then addressing their respective threats with corresponding security capabilities, architectures, and designs. SAFE provides guidance that is holistic and understandable.

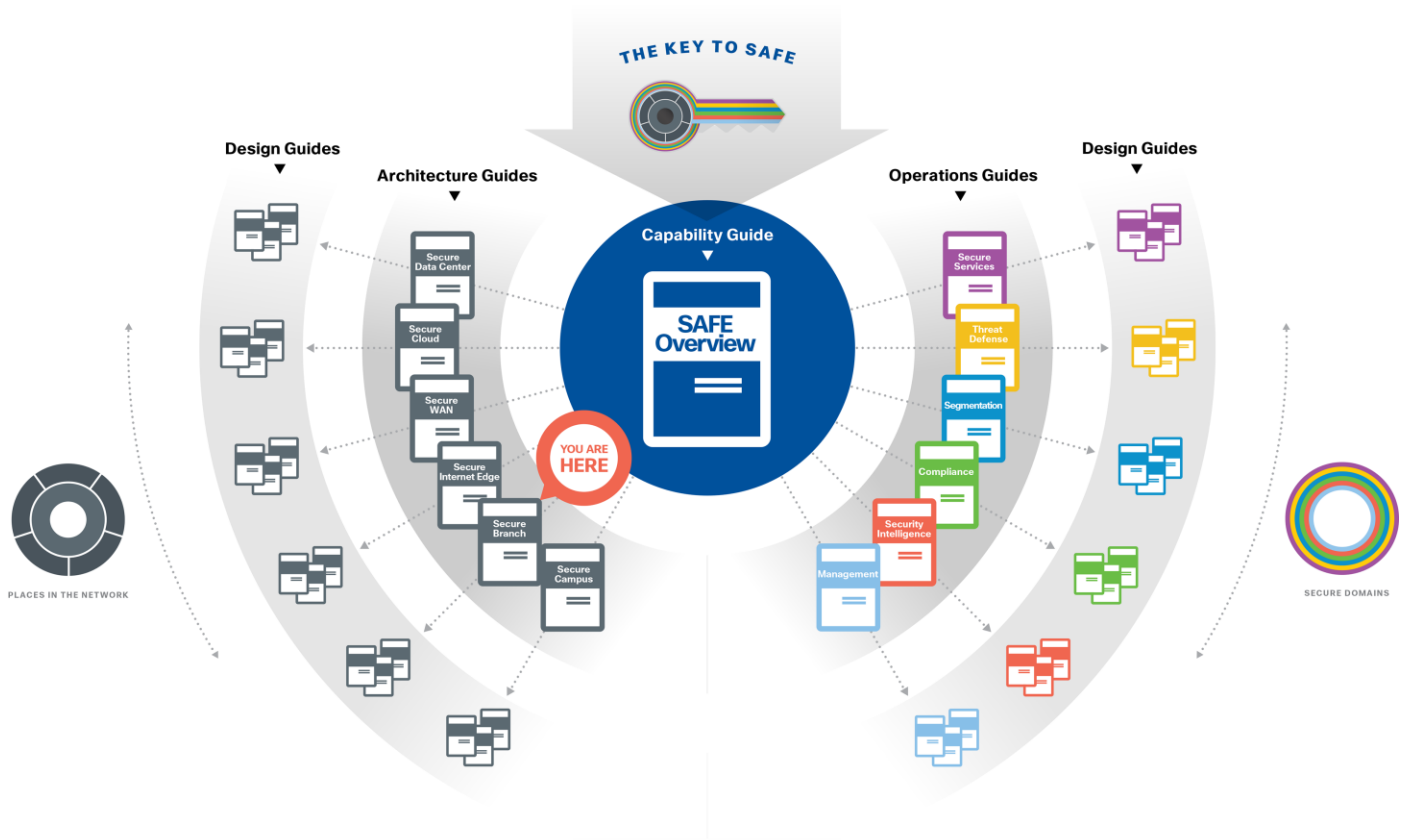


Figure 2.
SAFE Guidance Hierarchy

Business Flows

The Secure Branch is where physical presence is important for internal employees, third-party partners, and customers.

- Internally, employees use devices (PCs, laptops, phones, tablets, and other tools) that require access to branch-critical applications (i.e. payments), collaboration services like (voice, video, email) and the Internet.
- Third parties, such as service providers and partners, require remote access to applications and devices.
- Customers at the branch use guest Internet access on their phones or tablets.



Figure 3. Branch business use cases are color coded to define where they flow.

Functional Controls

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

Functional Controls	Description
Secure Applications	Applications require sufficient security controls for protection.
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.



Figure 4. Branch business flows map to functional controls based on the types of risk they present.

Capability Groups

Branch security is simplified using foundational, access and business capability groups.

Each flow requires access and foundational groups. Additional business activity risks require appropriate controls as shown in figure 5 which often reside outside the branch (non-branch capabilities).

For more information regarding capability groups, refer to the SAFE overview guide.

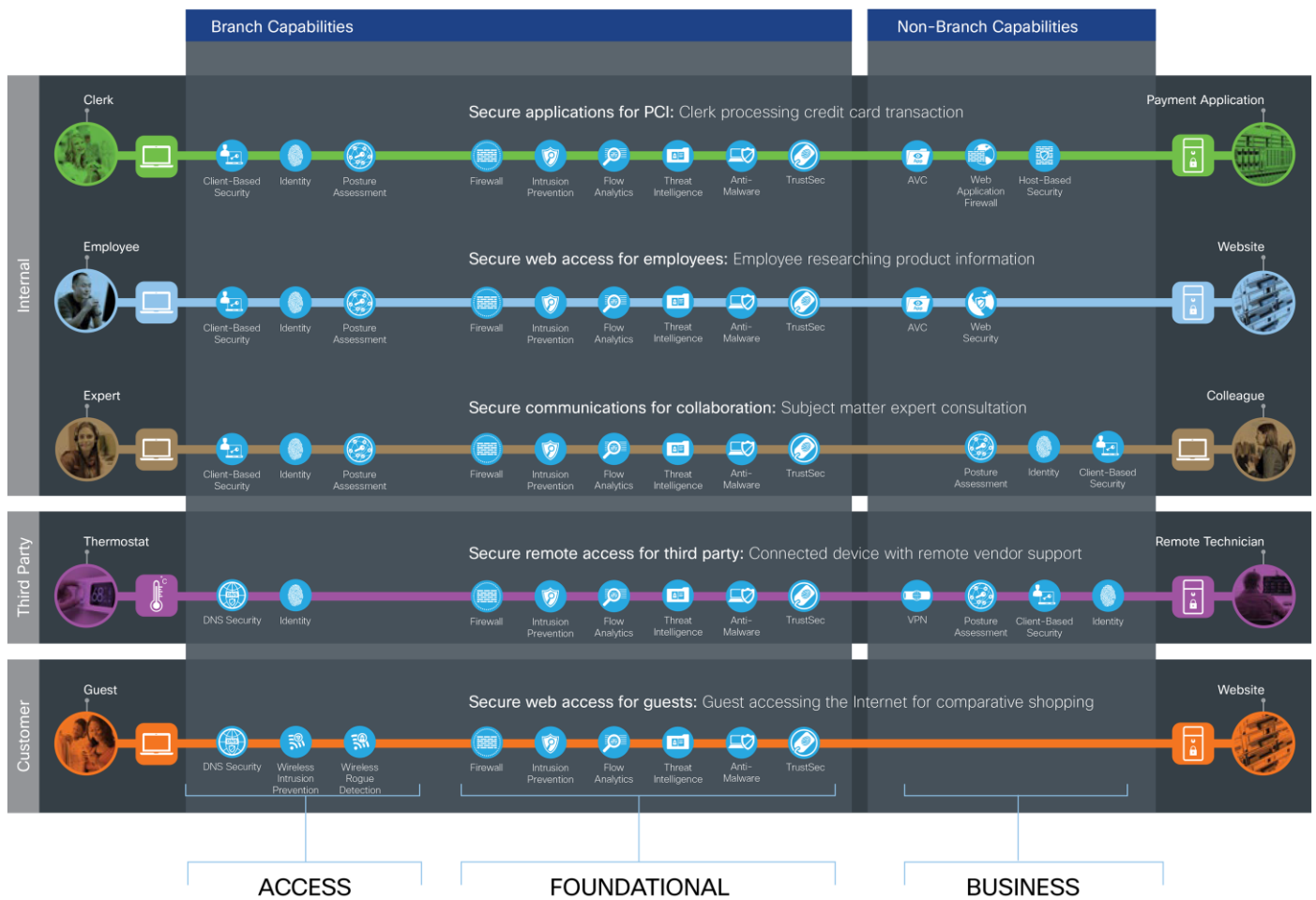


Figure 5. Branch security simplified into capability groups

Secure Branch threats and capabilities are defined in the following sections.

Threats

The branch has four primary threats, and the defense is explained throughout the rest of the document:

Exploitation of trust

People have a specific job to do. Unfortunately, the trust of employees can be compromised. Malicious employees (especially administrators) are very dangerous.

Partners can be compromised. If a trusted partner is breached, an attacker would have access via stolen credentials.

Endpoint malware

Devices present at the branch are a common source of contamination. Devices of employees, partners or customers can be infected from multiple sources such as web use, email use, or lateral infection from other devices on the network. Mobile devices can roam networks increasing chances of compromise. Devices accepting credit cards and the Internet of Things are primary attack points.

Unauthorized/malicious device activity

Devices at the branch range from Employee PCs to Temperature Controls Units. Although PCs can use client security software, zero-day attacks can bypass them. Worse, many devices are not constructed with strong security. Advanced persistent threats take advantage of exploits from various resources, and once compromised through vulnerability, can be used to contribute to a larger overall attack.

Wireless infrastructure exploits

Wireless networks expose companies to threats beyond their walls. A company's wireless service allows attackers access that they would not normally have without physical access.

Attackers with physical access can place their own (rogue) wireless access points which allow them to continue attacks from parking lots or other locations outside the physical walls of the company.



Security Capabilities

The attack surface of the branch is defined by the business flow, which includes the people and the technology present. The security capabilities that are needed to respond to the threats are mapped in Figure 6. The branch security capabilities are listed in table 1. The placement of these capabilities is discussed in the architecture section.




Figure 6.
Secure Branch Attack Surface and Security Capabilities

The branch primary threats are mitigated by security capabilities placed within architectural locations that are described in the following attack surface tables. The attack surfaces include Human, Devices, Network, Applications and Management.

Human Attack Surface














Users: Employees, third parties, customers, and administrators.

Security Capability		Threat	
	Identity: Identity-based access.		Attackers accessing restricted information resources.

Devices Attack Surface - Clients





Devices such as PCs, laptops, smartphones, tablets.





Security Capability		Threat	
	Client-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.
	Posture Assessment: Client endpoint compliance verification and authorization.		Compromised devices connecting to infrastructure.

Network Attack Surface - Wired Network



Physical network infrastructure; routers, switches, used to connect access, distribution, core, and services layers together.

Security Capability		Threat	
	Firewall: Stateful filtering and protocol inspection between branch layers and the outside Internet, and service provider connections to the data center.		Unauthorized access and malformed packets between and within the branch.

Security Capability		Threat	
	Intrusion Prevention: Blocking of attacks by signatures and anomaly analysis.		Attacks using worms, viruses, or other techniques.
	TrustSec: Policy-based segmentation.		Unauthorized access and malicious traffic between branch layers.

Network Attack Surface - Wireless Network





Branches vary from having robust local wireless controller security services to a central, cost-efficient model.

Security Capability		Threat	
	Wireless Rogue Detection: Detection and containment of malicious wireless devices that are not controlled by the company.		Unauthorized access and disruption of wireless network.
	Wireless Intrusion Prevention (WIPS): Blocking of wireless attacks by signatures and anomaly analysis.		Attacks on the infrastructure via wireless technology.

Network Attack Surface - Analysis



Analysis of network traffic within the branch.

Security Capability		Threat	
	<p>Anti-Malware:</p> <p>Identify, block, and analyze malicious files and transmissions.</p>		Malware distribution across networks or between servers and devices.
	<p>Threat Intelligence: Contextual knowledge of existing and emerging hazards.</p>		Zero-day malware and attacks.
	<p>Flow Analytics:</p> <p>Network traffic metadata identifying security incidents.</p>		Traffic, telemetry, and data exfiltration from successful attacks.

Network Attack Surface - WAN



Public and untrusted Wide Area Networks that connect to the company, such as the Internet.

Security Capability		Threat	
	<p>Web Security:</p> <p>Web, DNS, and IP-layer security and control for the branch.</p>		Attacks from malware, viruses, and redirection to malicious URLs.
	<p>Virtual Private Network(VPN):</p> <p>Encrypted communication tunnels.</p>		Exposed services and data theft of remote workers and third parties.










Network Attack Surface - Cloud



Security Capability		Threat	
	Cloud Security: Web, DNS, and IP-layer security and control in the cloud for the campus.		Attacks from malware, viruses, and redirection to malicious URLs
	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		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 Attack Surface



Security Capability		Threat	
	Server-based Security: Security software for servers with the following capabilities:		
	Anti-Malware: Identify, block, and analyze malicious files and transmissions.		Malware distribution across servers.
	Anti-Virus		Viruses compromising systems.
	Cloud Security		Redirection of session to malicious website.
	Host-based Firewall		Unauthorized access and malformed packets connecting to server.

Management

Security Capability
<p>These security capabilities are required across all PINs:</p> <ul style="list-style-type: none"> Identity/authorization Policy/configuration Analysis/correlation Monitoring Vulnerability management Logging/reporting Time synchronization/NTP

Architecture

SAFE underscores the challenges of securing the business. It enhances traditional network diagrams to include a security-centric view of the company's business. The Secure Branch architectures are logical groupings of security and network capabilities that support branch business use cases. Branches are not easily defined across multiple industries; SAFE uses several sizes of branches to address a large cross-section of scenarios.

SAFE business flow security architecture depicts a security focus. Traditional design diagrams that depict cabling, redundancy, interface addressing, and specificity are depicted in SAFE design diagrams. Note that a SAFE logical architecture can have many different physical designs.

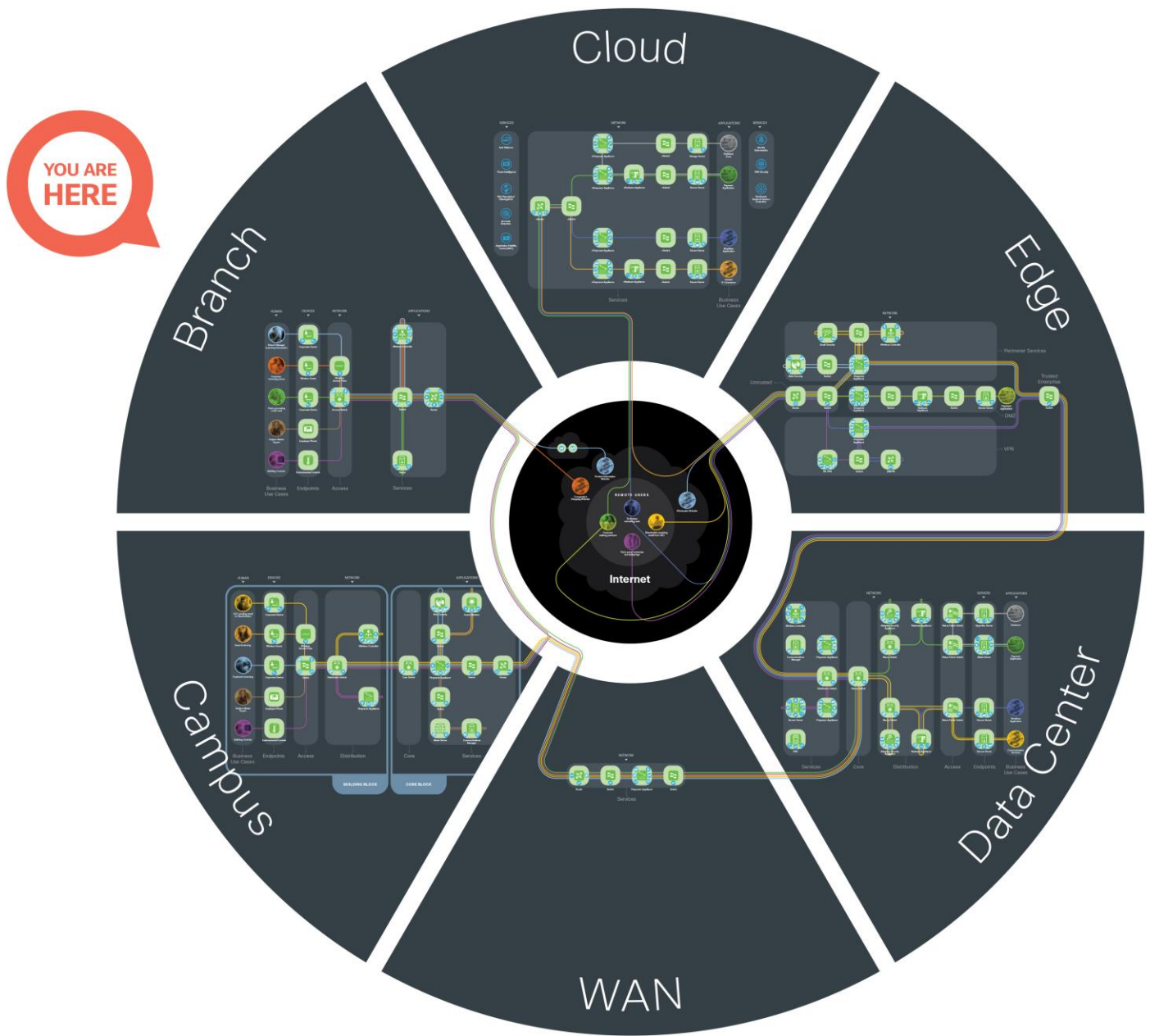


Figure 7.

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

Small Branch

The Secure Small Branch architecture has the following characteristics:

- Location size averages between 1,000 and 6,000 square feet
- Preference for integrated services within fewer network components because of physical space requirements
- Wireless connectivity
- Single router with firewall/IPS, integrated Ethernet switch, compact switch, and power-over-Ethernet (PoE)
- Web security via the cloud
- Survivable Remote Site Telephony (SRST)
- Majority of applications in data center or cloud
- Fewer than 25 traditional devices (PCs, laptops, tablets, phones, etc.) requiring network connectivity
- Fewer than 25 low-bandwidth devices (sensors, thermostats, printers, etc.)

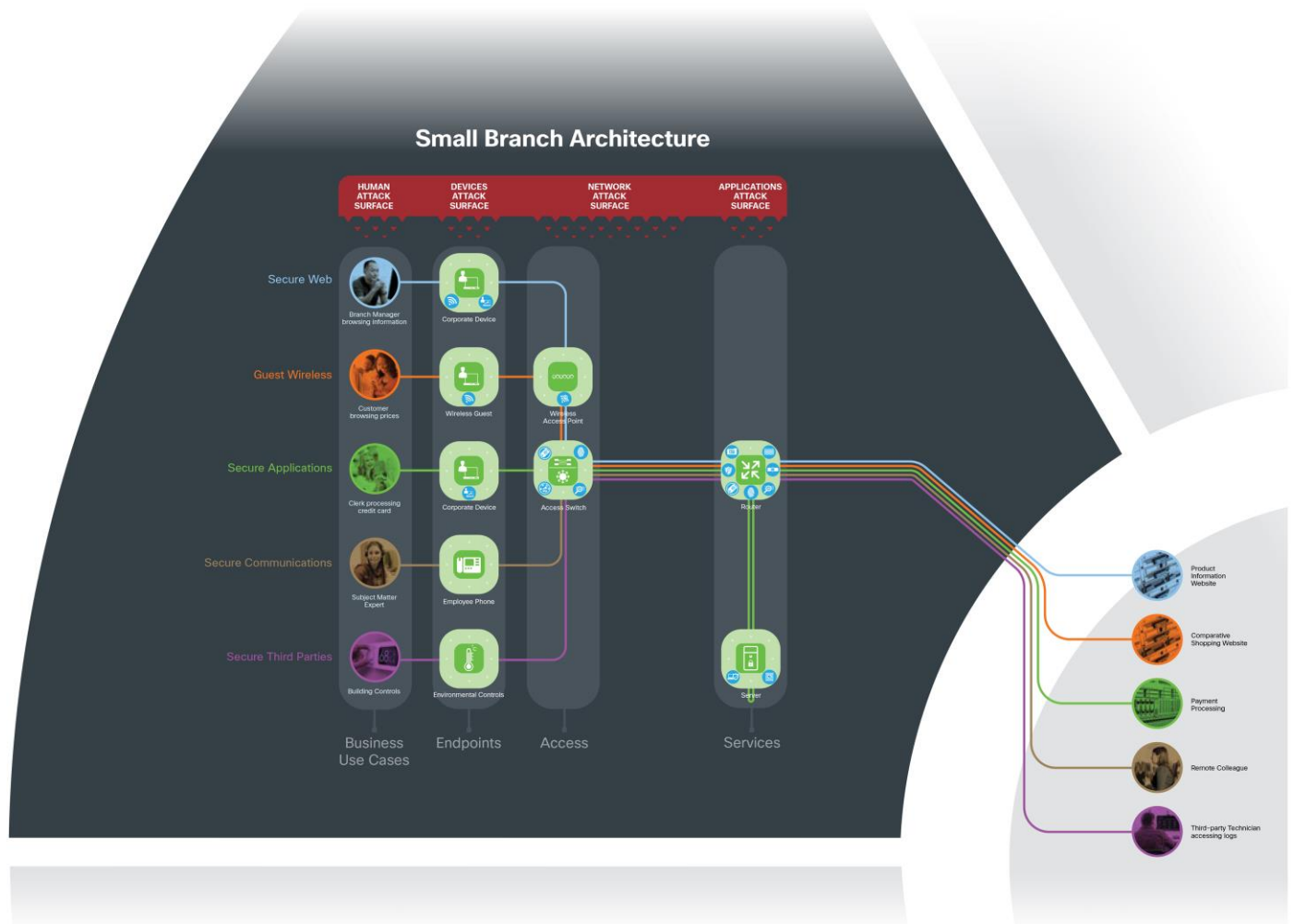


Figure 8.

Secure Small Branch. The Secure Small Branch business flows and security capabilities are arranged into a logical architecture. The colored business use cases flow through the green architecture icons with the required blue security capabilities.

Medium Branch

The Secure Medium Branch architecture uses the following characteristics:

- Location size averages between 6,000 and 18,000 square feet
- Redundant LAN and WAN infrastructures with firewall/IPS
- The physical size is smaller than a large branch, so a core and distribution layer of network switches is not required
- Web security via the cloud
- Wireless connectivity
- Survivable Remote Site Telephony (SRST)
- 25-100 traditional devices (PCs, laptops, tablets, phones, etc.) requiring network connectivity
- Fewer than 100 low-bandwidth devices (sensors, thermostats, printers, etc.)

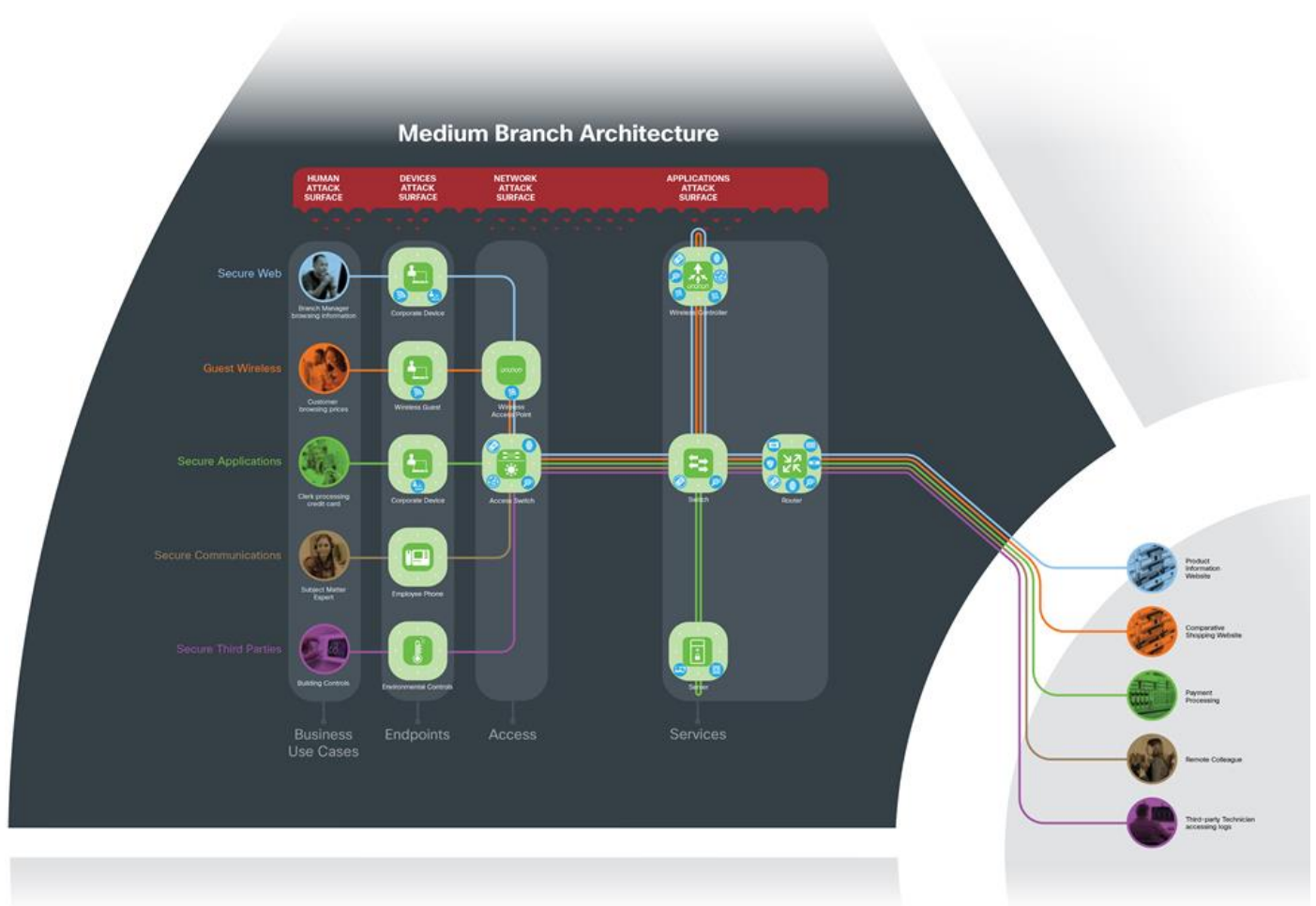


Figure 9.

Secure Medium Branch. The Secure Medium Branch business flows and security capabilities are arranged into a logical architecture. The colored business use cases flow through the green architecture icons with the required blue security capabilities.

Large Branch

The Large Branch architecture includes the following design requirements:

- Location size averages between 15,000 and 150,000 square feet
- Multiple routers for primary and backup network connectivity requirements
- Preference for a combination of network services distributed across the facility to meet resilience and application availability requirements
- Tiered network architecture within the branch; distribution layer switches are employed between the central network services core and the access layer connecting to the network endpoints (endpoints, wireless APs, servers)
- Unified Communications with centralized or distributed PSTN access and services
- 100 or more traditional devices (PCs, laptops, tablets, phones, etc.) requiring network connectivity
- 100 or more low-bandwidth devices (sensors, thermostats, printers, etc.)

Large Branch Design

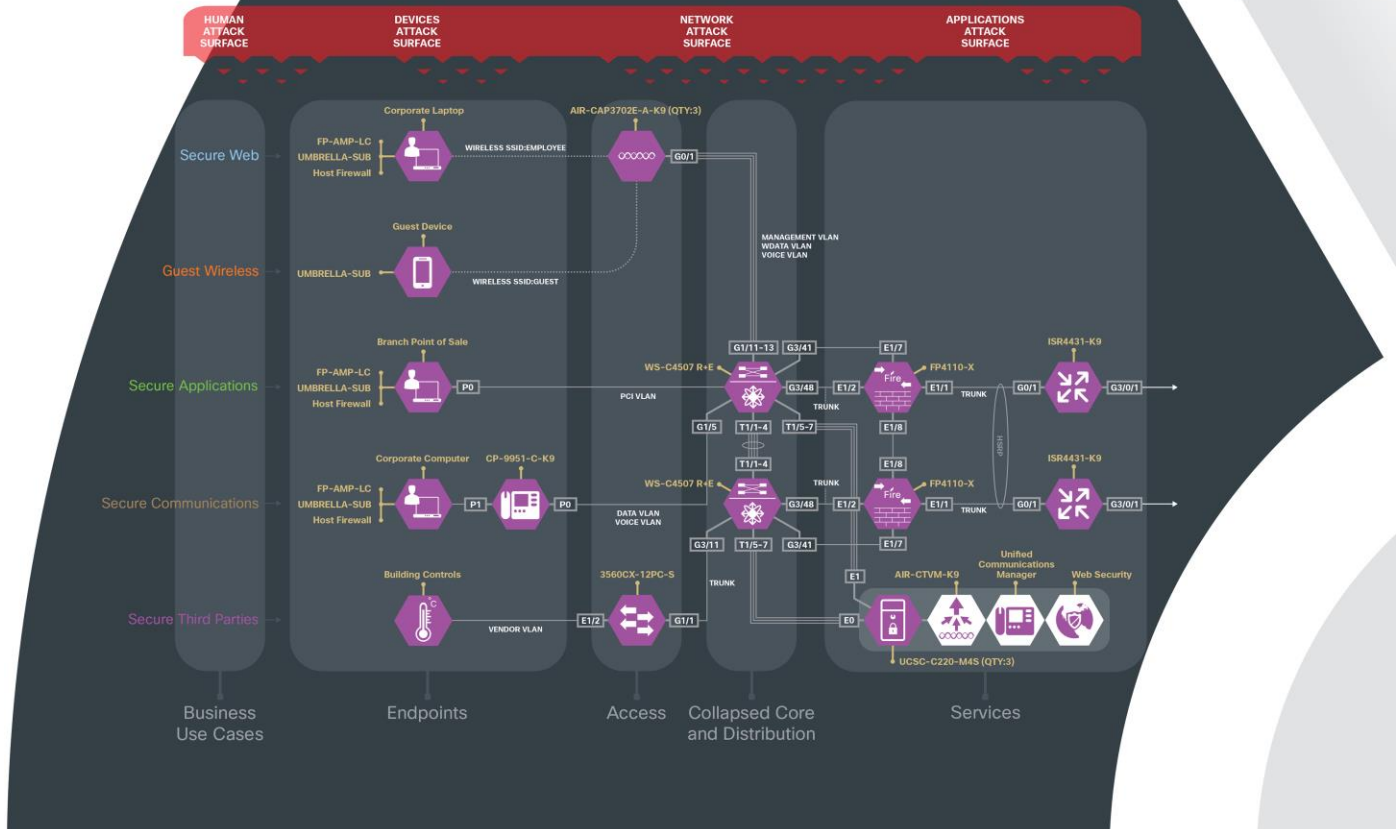


Figure 10.

Secure Large Branch. The Secure Large Branch business flows and security capabilities are arranged into a logical architecture. The colored business use cases flow through the green architecture icons with the required blue security capabilities.

Attack Surface

The Secure Branch attack surface of Human, Devices, Network, and Applications is consistent across all sizes of branch architectures. The sections below discuss the security capability that defends the threats associated with each layer of the surface. Note that the capability might be a service that is supplied from another PIN. For example, the Identity service is prompted to a human, on a user's device, enforced at the switch, and served from the Data Center. However, for the sake of simplifying, Identity is depicted logically where the risk exists of supplying credentials: the human.

Human

Typically, humans in the branch are employees, customers, and remote access users such as partners. Exploitation of Trust attacks happen most frequently at this layer. Credential management of employees, partners and customers with effective role-based segmentation minimized the risk of this threat.

Security technology should be augmented with security awareness training and acceptable use policies for internal, partner, and customer users. No amount of technology can prevent successful attacks if humans in your company, both internal and partner users, are not trained to keep security in mind. Security training and metrics of adoption are critical elements to reducing the risk of this attack surface.

Administrators have more authority than normal users and the systems they have access to. Additional controls should be used like two-factor authentication, limited access to job function, and logging of their changes.

Appropriate identity services defined by policy must be supplied with associated, approved clients and devices.



Figure 11. Business Use Cases

Devices

Devices are part of the security reference architecture. Endpoint Malware and Malicious device activity attacks occur at this layer. Combining identity, posture assessments with the capabilities of the device layer minimize the risk of these threats.

Perimeter defenses are no longer (if ever) sufficient. A secure company uses the network and the devices connecting to it as baselines for comparison. If you are not using the network as a sensor, you are not secure. This visibility allows for effective containment through intelligent architectural design. It is equally important to ensure that clients (PCs, tablets, phones, and other connected devices) are participating in security and that malicious devices are quarantined.

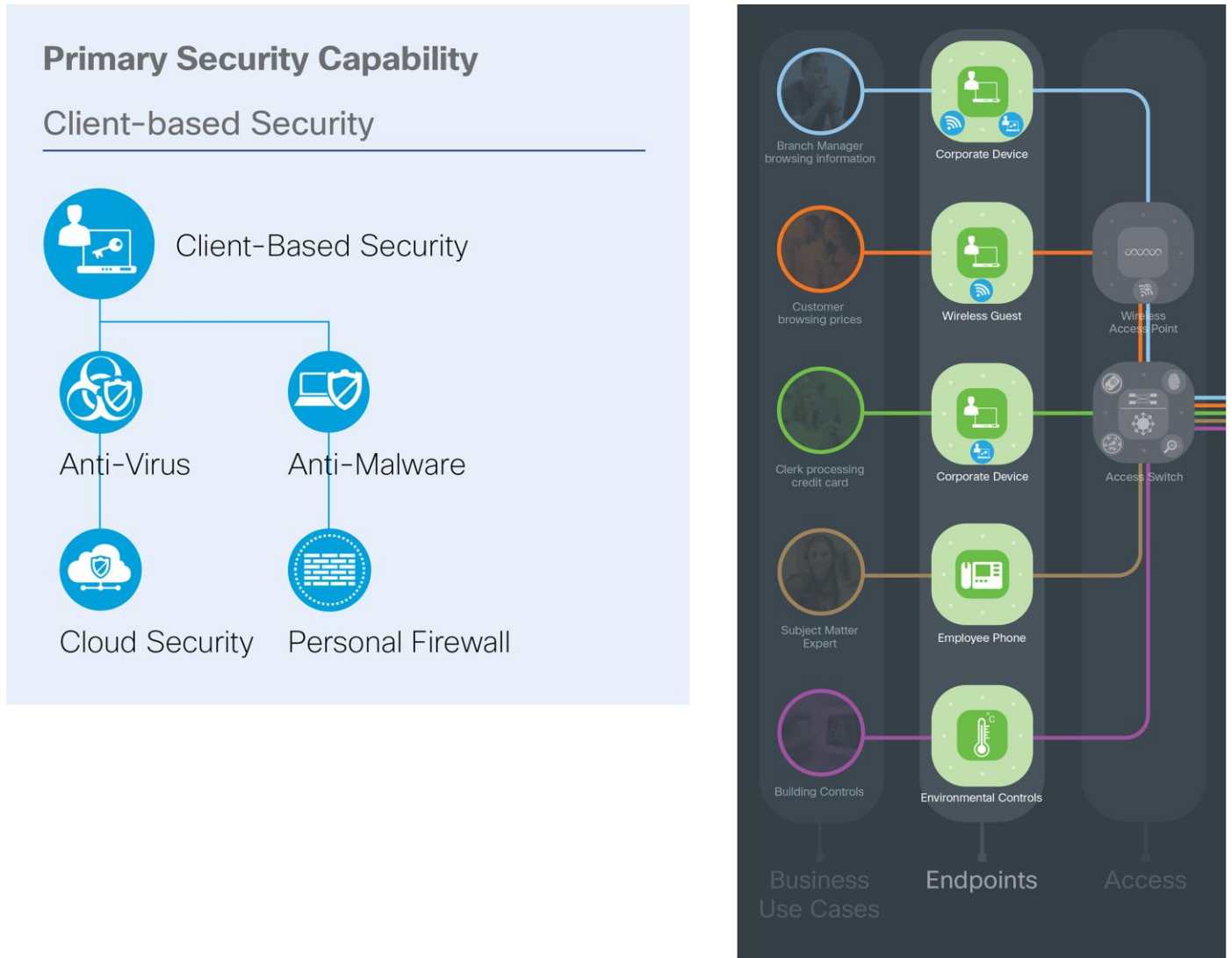


Figure 12. Branch Devices

Access Layer

The access layer is where users and devices connect to the company network. It is the first line of defense within the Secure Branch architecture. Its purpose is to identify the users, to assess compliance to policy of devices seeking access to the network, and to respond appropriately.

Wireless infrastructure exploits typically happen at the access layer. Unauthorized wireless access points and attacks on the wireless communication are mitigated by security capabilities.

This layer connects to the distribution or core layer in a hierarchical organization that simplifies network troubleshooting and segments traffic for security. The network as a sensor utilizes flow analytics to capture anomalies and provide visibility to attacks. Violations of posture, identity, or anomalous behavior can be enforced.

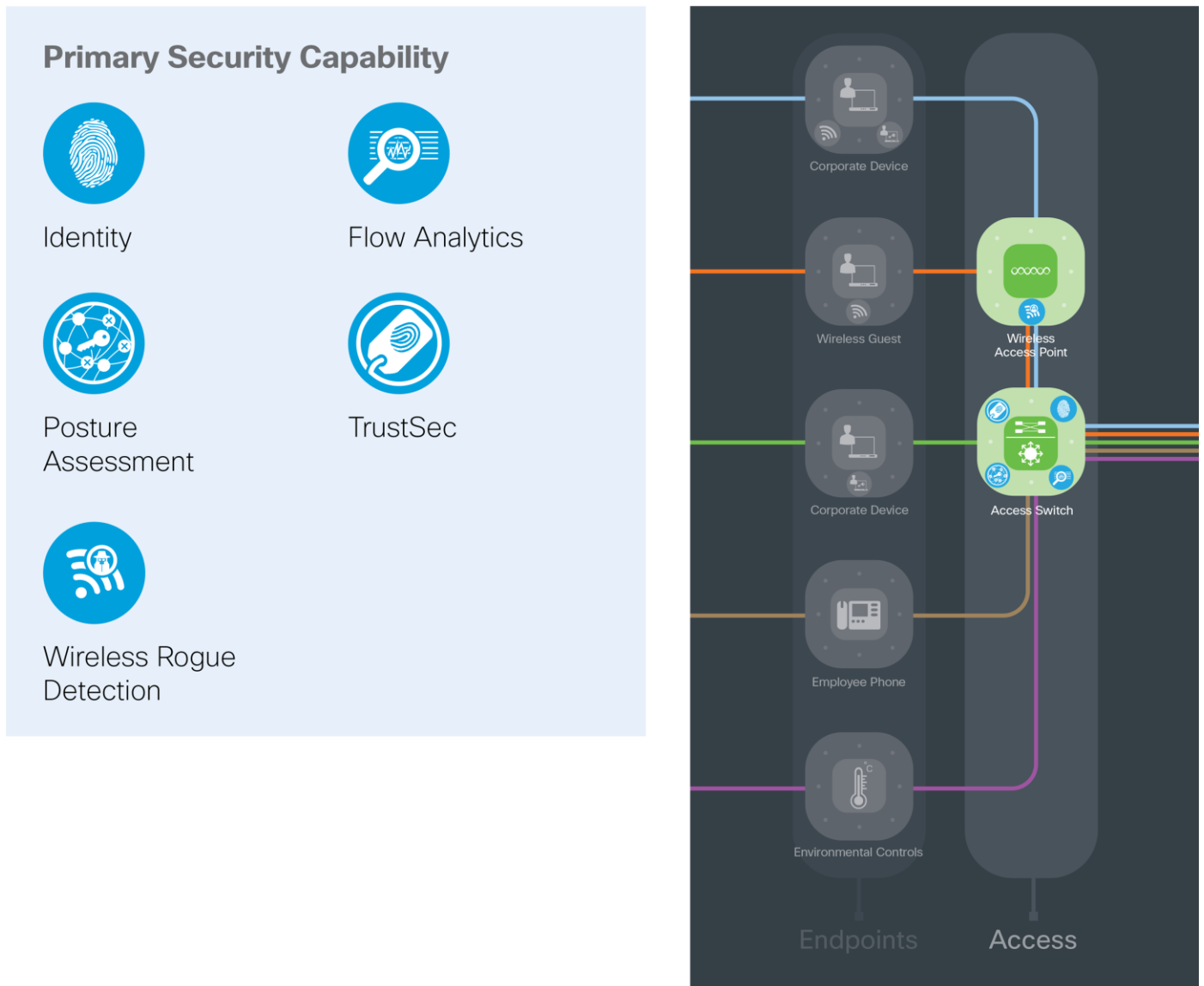


Figure 13. Access Layer

Core and Distribution Layer

The access/distribution/core is classic network hierarchy. Due to branches having smaller footprints, these functions may be collapsed. By segregating the access layer from the services layer, this layer provides a distribution method of services that discretely separates business-based traffic into flows.

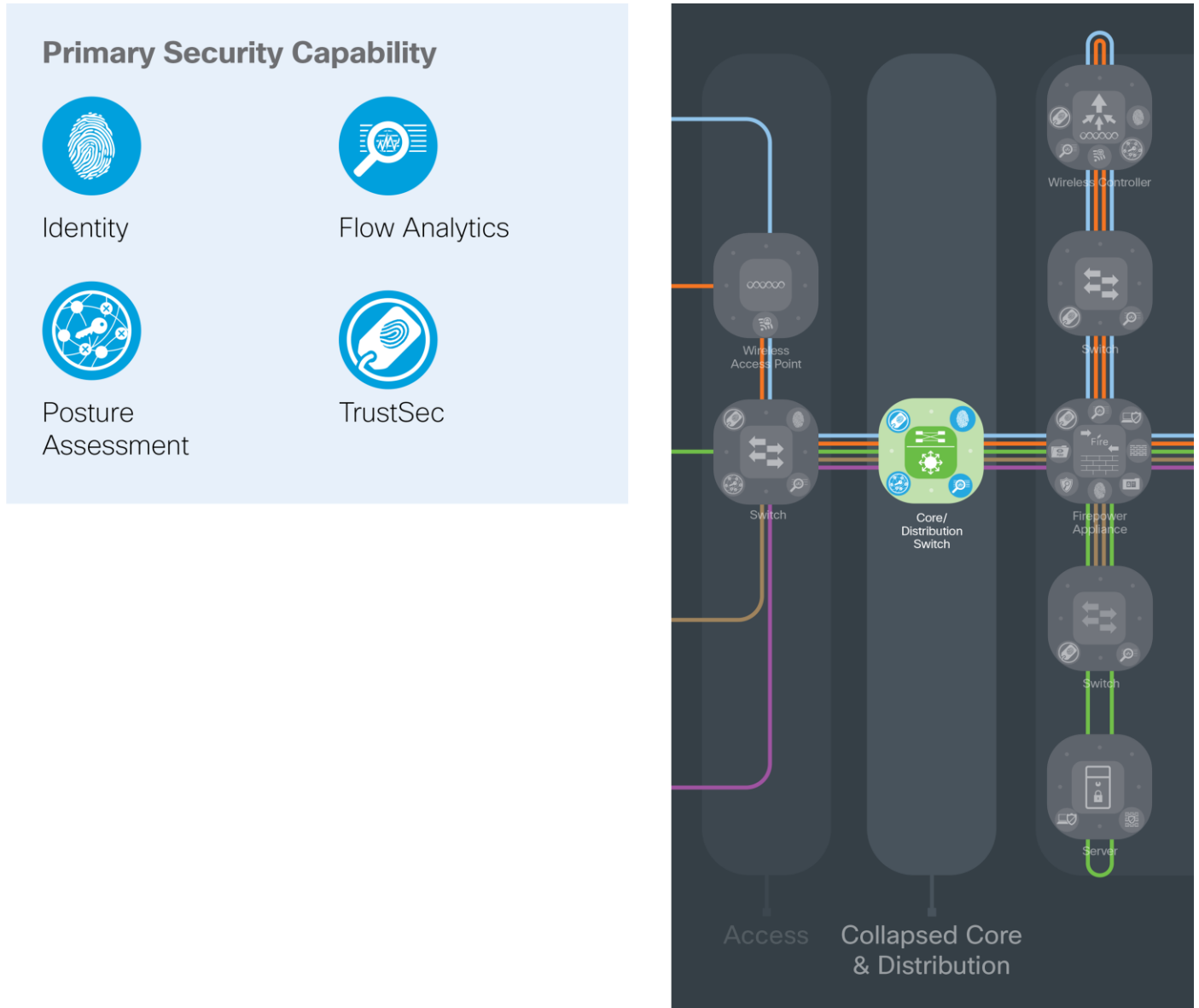


Figure 14. Collapsed Core and Distribution

Services Layer

The services layer connects the Secure Branch to the outside data center and Internet via service providers. It connects the access and distribution layers inside the branch to the security and inspection capabilities that secure the separate business flows coming into and out of the branch.

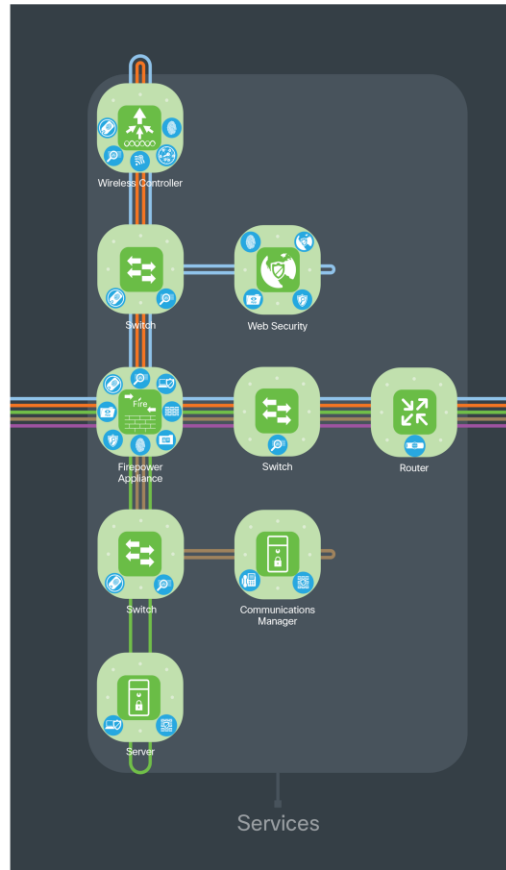


Figure 15. Services Layer

Summary

Today's companies are threatened by increasingly sophisticated attacks. Branches are commonly targeted because they are susceptible to physical access and have a large mix of services across increasingly complicated devices.

Cisco's Secure Branch architecture and solutions defend the business against corresponding threats.

SAFE is Cisco's security reference architecture that simplifies the security challenges of today and prepares for the threats of tomorrow.

Appendix

Appendix A - A Proposed Design

The Secure Branch has been deployed in Cisco's laboratories. Portions of the design have been validated and documentation is available on [Cisco Design Zone](#).

Figures 16–18 depict the specific products that were selected within Cisco's laboratories. It is important to note that the Secure Branch architecture can produce many designs based on performance, redundancy, scale, and other factors. The architecture provides the required logical orientation of security capabilities that must be considered when selecting products to ensure that the documented business flows, threats, and requirements are met.

Small Branch Design

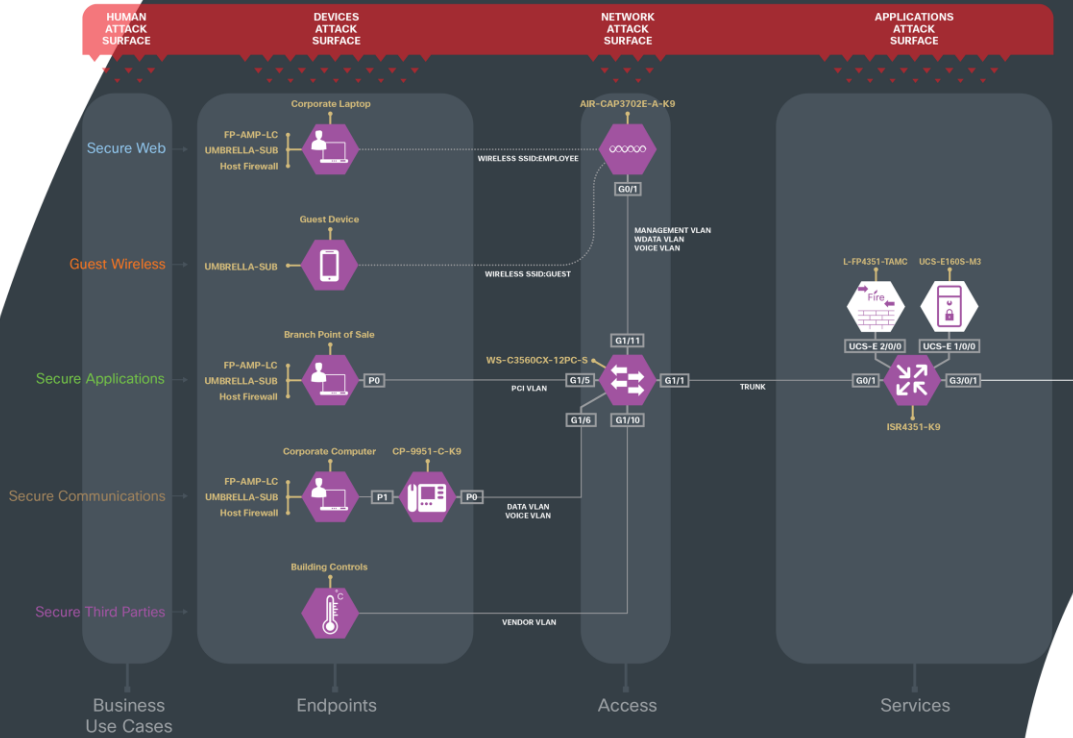


Figure 16. Secure Small Branch Proposed Design

Medium Branch Design

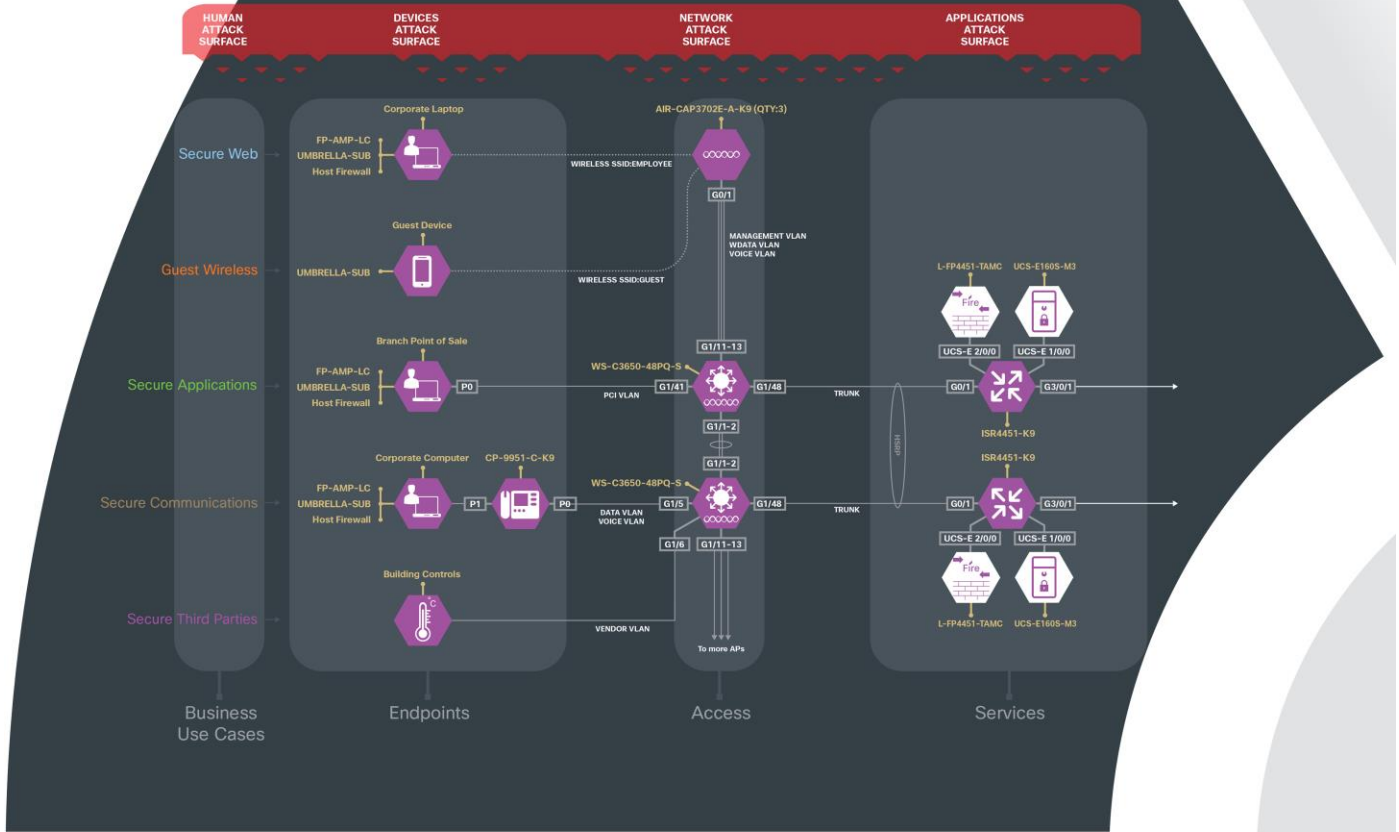


Figure 17. Secure Medium Branch Proposed Design

Large Branch Design

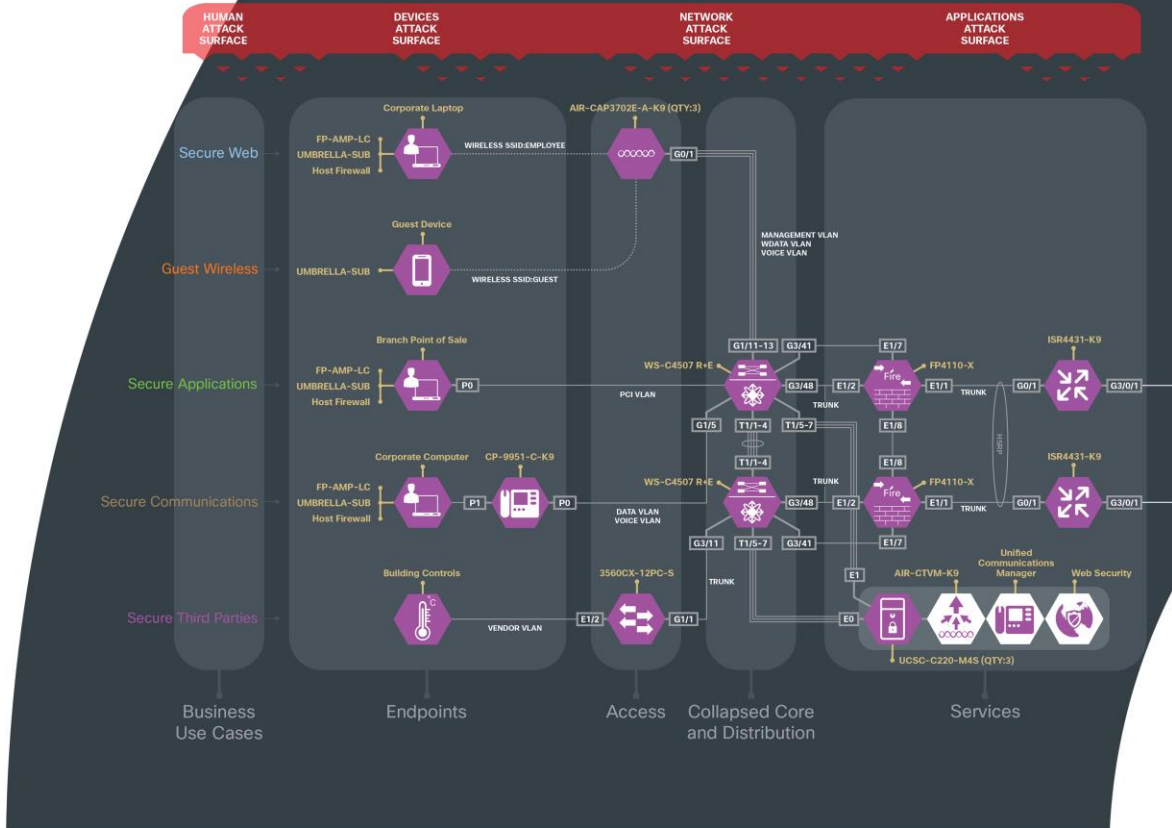















Figure 18. Secure Large Branch Proposed Design

Appendix B - Suggested Components

Branch Attack Surface		Branch Security		Suggested Cisco Components
Human	Users		Identity	Identity Services Engine (ISE) Cisco Secure Access by Duo Meraki Management
Devices	Endpoints		Client-based Security	Cisco Secure Endpoint Cisco Umbrella Cisco AnyConnect Secure Mobility Client
			Posture Assessment	Cisco AnyConnect Secure Mobility Client Identity Services Engine (ISE) Meraki Mobile Device Management
Network	Wired Network		Firewall	Cisco Secure Firewall Integrated Services Router (ISR) Meraki MX
			Intrusion Prevention	Cisco Secure Firewall Cisco Secure Firewall on UCS-E Meraki MX
			Access Control+ TrustSec	Wireless Controller/Catalyst Switch Identity Services Engine (ISE) Meraki MX
	Analysis		Anti-Malware	Cisco Secure Endpoint Advanced Malware Protection (AMP) for Networks Advanced Malware Protection (AMP) for Web Security Integrated Services Router (ISR) with SecureX Network Analytics SecureX Malware Analytics
			Threat Intelligence	Talos Security Intelligence SecureX Malware Analytics Cognitive Threat Analytics (CTA)

Branch Attack Surface		Branch Security		Suggested Cisco Components
			Flow Analytics	Cisco Secure Firewall Catalyst Switches ISR with SecureX Network Analytics SecureX Network Analytics (Flow Sensor and Collectors) Wireless LAN Controller Meraki MX
	WAN		Web Security	Cisco Secure Firewall Cisco Secure Web Umbrella Secure Internet Gateway (SIG) Meraki MX
			VPN	Cisco Secure Firewall Integrated Services Router (ISR) Aggregation Services Router (ASR) Meraki MX
	Cloud		Cloud Security	Umbrella Secure Internet Gateway (SIG) Cloudlock Meraki MX
Applications	Service		Server-based Security	Cisco Secure Workload Cisco Umbrella

Appendix C - Feedback

If you have feedback on this design guide or any of the Cisco Security design guides, please send an email to ask-security-cvd@cisco.com.

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 <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)