The bridge to possible

SAFE Architecture Guide

Places in the Network: Secure Campus

August 2022

Contents

Overview

The Secure Campus is a place in the network (PIN), a cluster of buildings, where a company does business. This guide addresses campus business flows across all industries and the security used to defend them. Campus examples are company headquarters, or any group of buildings that requires network services. More complex than branches due to physical and logical scale, they support network access for employees, third parties, and customers across multiple buildings and floors.

The Secure Campus 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 Campus architecture guide provides:

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

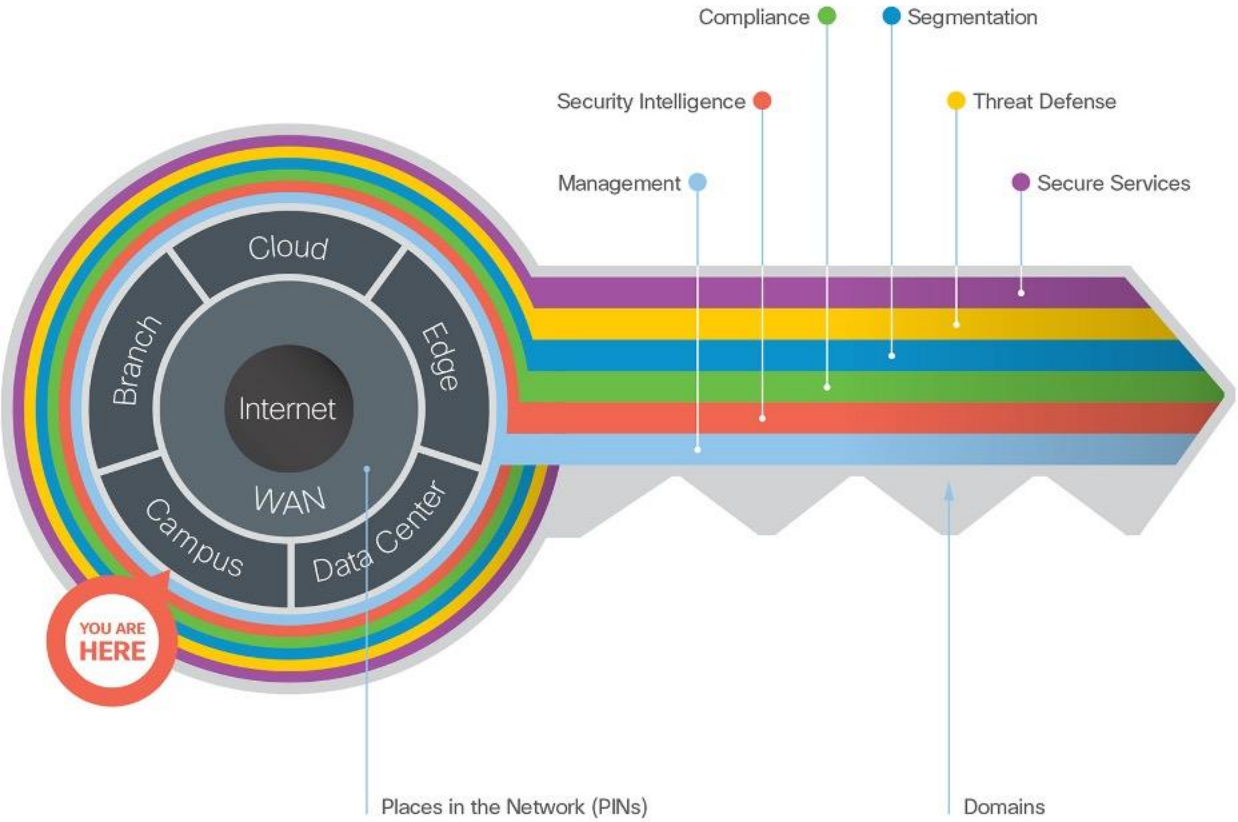


Figure 1. The Key to SAFE. SAFE provides the Key to simplify cybersecurity into Secure Places in the Network (PINs) for infrastructure and Secure Domains for operational guidance.

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.

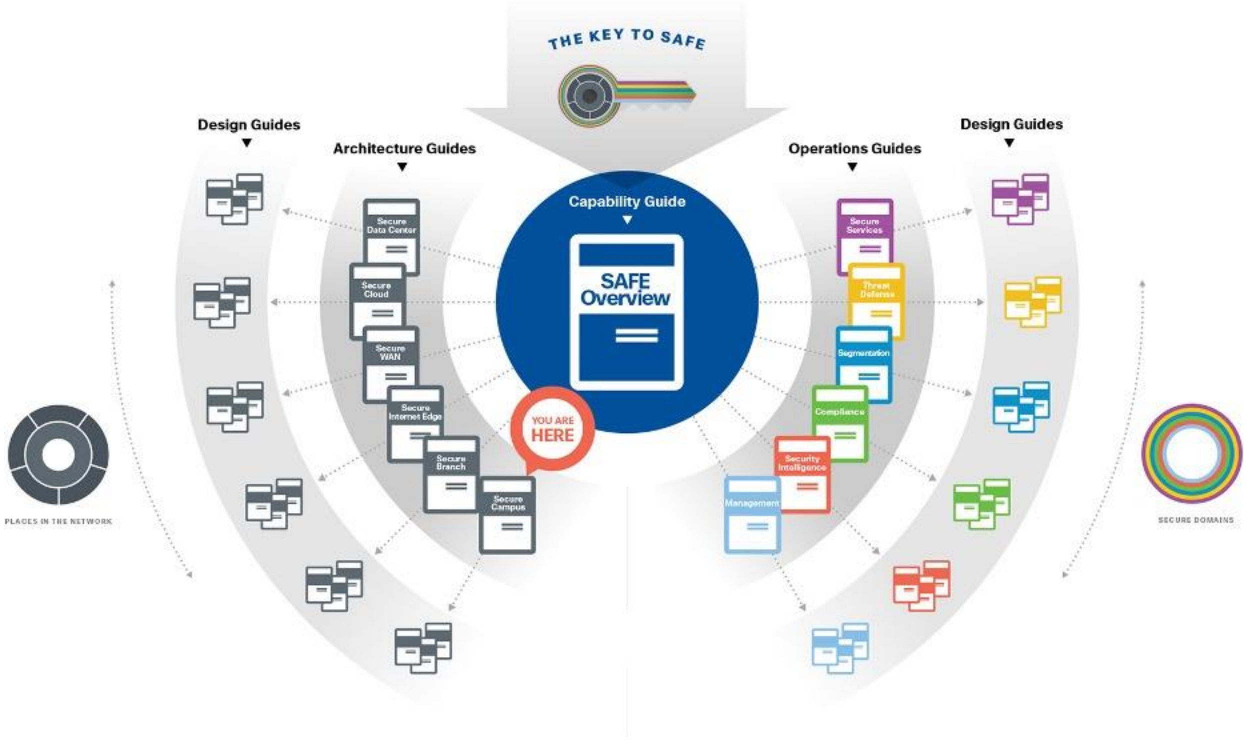


Figure 2. **SAFE Guidance Hierarchy**

Business Flows

The Secure Campus is where physical presence is important for internal employees, third-party partners, and customers over multiple physical buildings.

- Internally, employees use devices (PCs, laptops, phones, tablets, and other tools) that require access to campus-critical applications, 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 campus use guest Internet access on their phones or tablets.

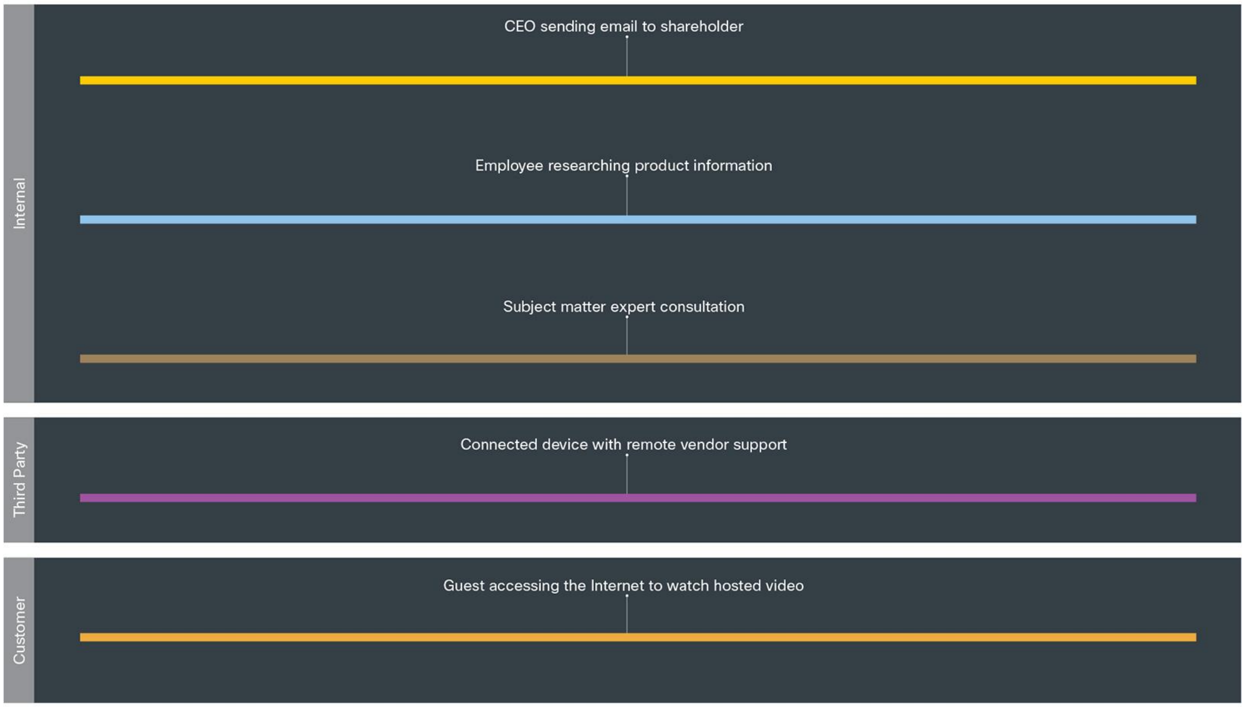

Internal
CEO sending email to shareholder
Employee researching product information
Subject matter expert consultation
Third Party
Connected device with remote vendor support
Customer
Guest accessing the Internet to watch hosted video

Figure 3. **Campus 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.

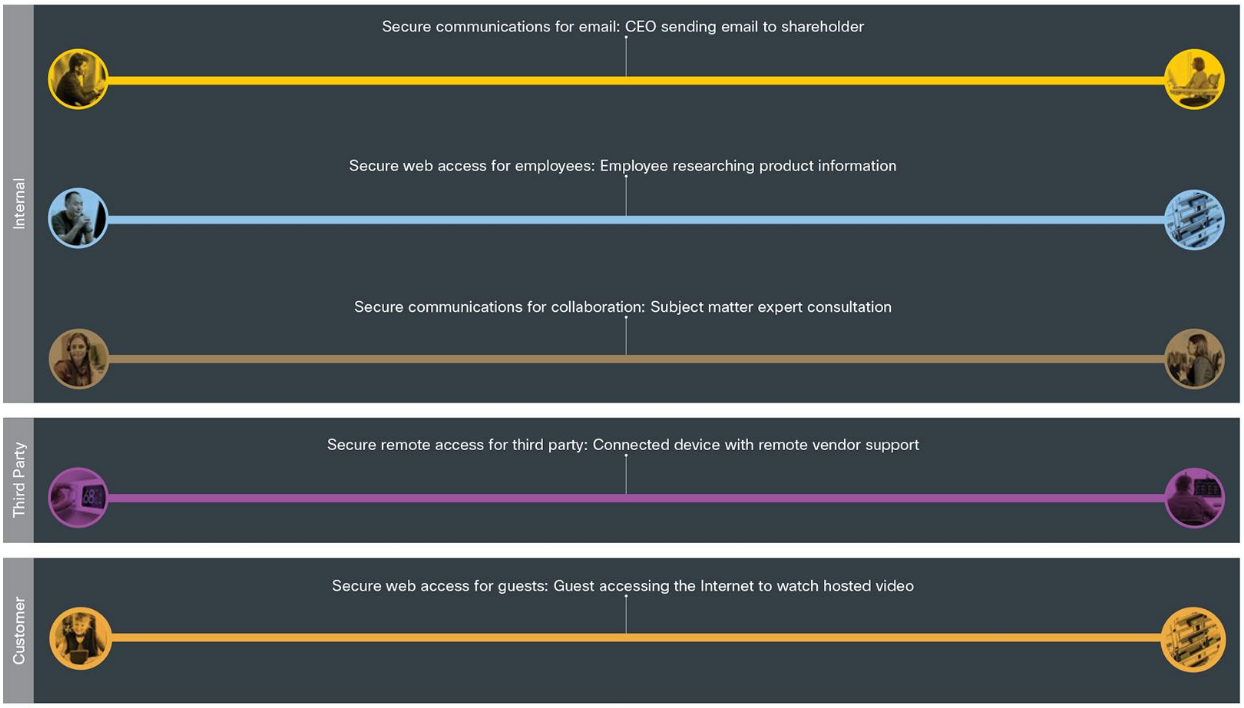

Internal
Secure communications for email: CEO sending email to shareholder
Secure web access for employees: Employee researching product information
Secure communications for collaboration: Subject matter expert consultation
Third Party
Secure remote access for third party: Connected device with remote vendor support
Customer
Secure web access for guests: Guest accessing the Internet to watch hosted video

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

Capability Groups

Campus 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-campus capabilities).

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

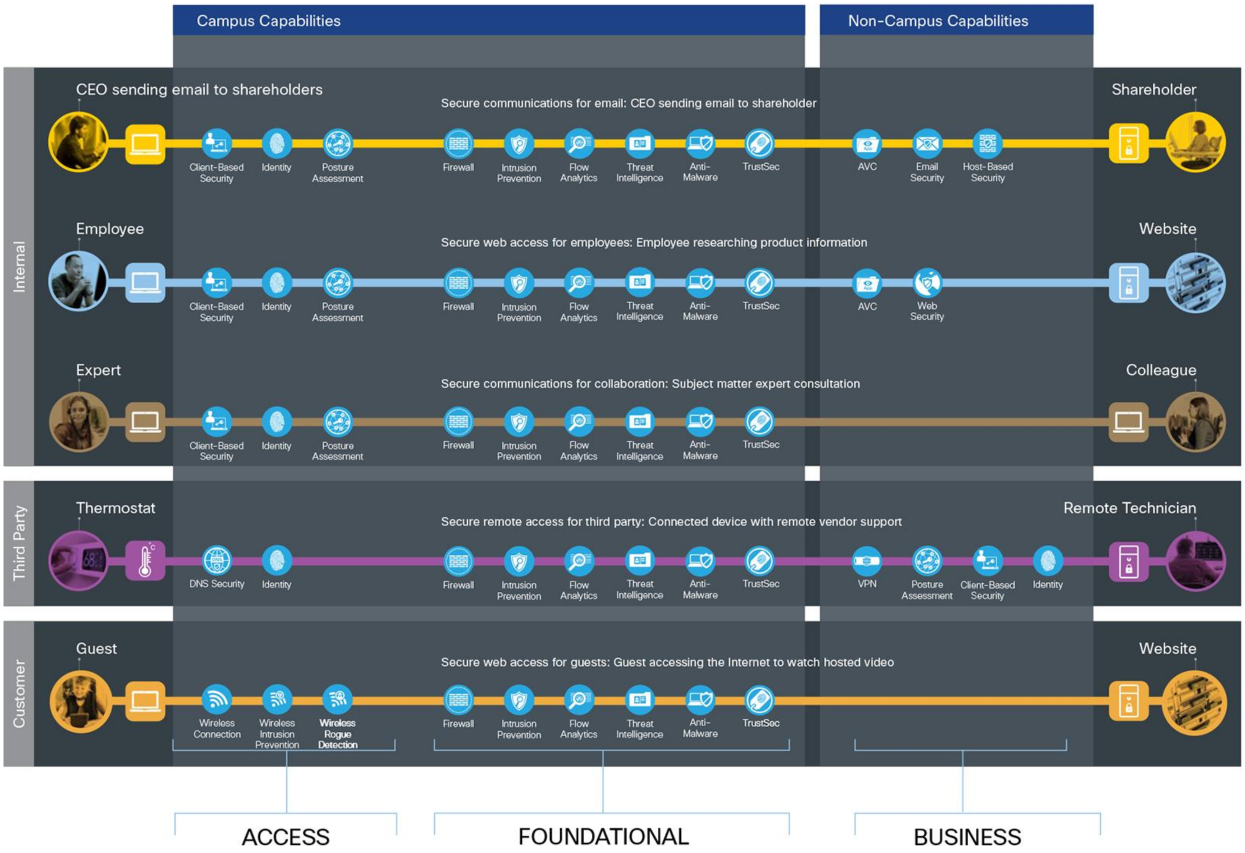


Figure 5. **Campus security simplified into capability groups**

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

Threats

Campuses have many employees, partner and guest users who use email, browse the web, collaborate. With a combination of wired and wireless access, the attack surface extends beyond the building.

The campus has six primary threats:

Phishing

Phishing is social engineering to trick people into clicking on a malicious link or opening an infected attachment of an email.

Messages looks as if they are from a legitimate organization, usually a financial institution, but contains a link to a fake website that replicates the real one

Unauthorized network access

The act of gaining access to a network, system, application or other resource without permission. The attacker could cause damage in many ways, perhaps by accessing sensitive files from a host, by planting a virus, or by hindering network performance by flooding your network with illegitimate packets.

Malware propagation

Devices present in the campus are a big 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. Devices accepting credit cards and the Internet of Things are common attack points.

Web-based exploits

Malvertizing and compromised sites hosting exploit kits to take over employee devices using browser vulnerabilities.

BYOD - Larger attack surface

Mobile devices can roam networks increasing chances of compromise, and the spread of infection. The large variety of mobile devices makes security policies and posture checking almost impossible when no device standardization exists. Limited on-device security capabilities (e.g., firewall, anti-malware, browser sand-boxing).

Botnet infestation

Botnets are networks made up of remote-controlled computers, or “bots.” These computers have been infected with an advanced form of malware which allows the devices to be remotely controlled. The controller of a botnet is able to direct the activities of these compromised computers to perform other attacks, steal data, or send spam.

Security Capabilities

The attack surface of the campus 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 campus security capabilities are listed in table 1. The placement of these capabilities are discussed in the architecture section.

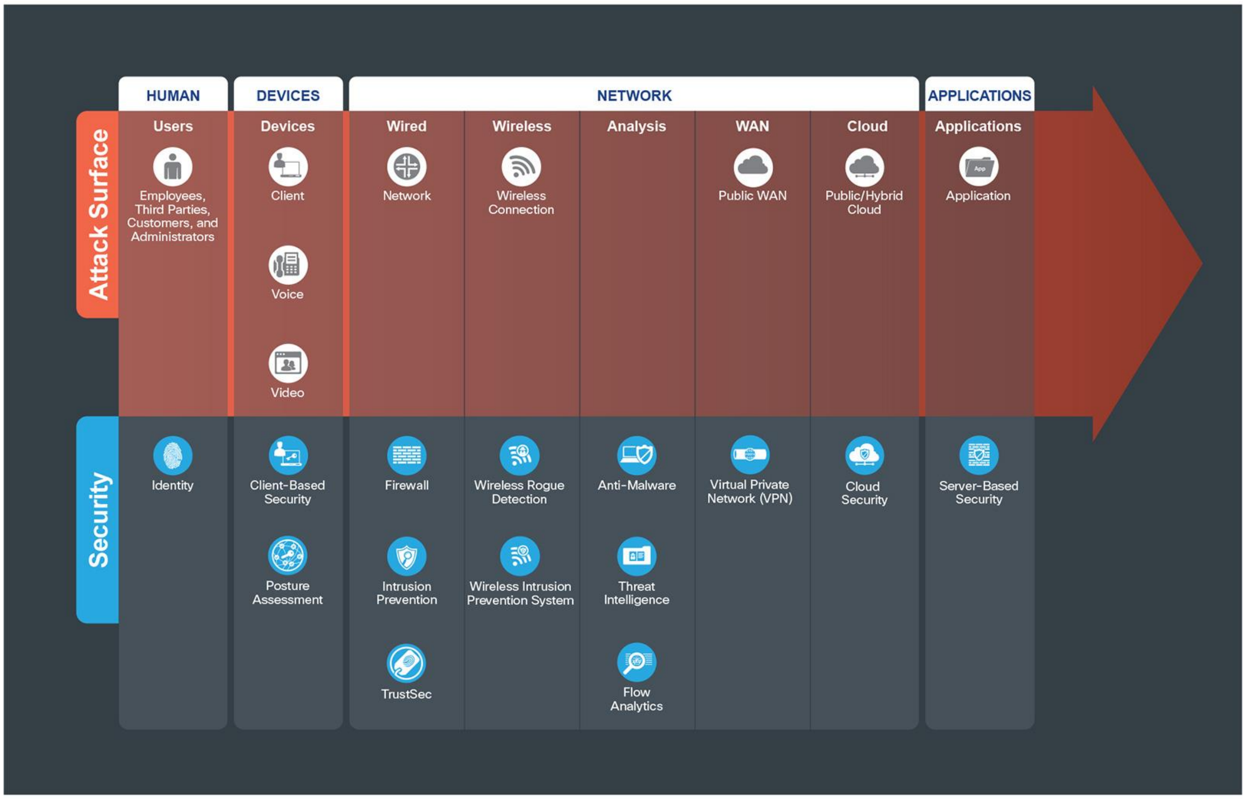


Figure 6. **Secure Campus Attack Surface and Security Capabilities**

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 campus layers and the outside Internet, and service provider connections to the data center.		Unauthorized access and malformed packets between and within the campus.
	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 campus 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 campus.

Security Capability		Threat	
	Anti-Malware: Identify, block, and analyze malicious files and transmissions.		Malware distribution across networks or between servers and devices.
	Threat Intelligence: Contextual knowledge of existing and emerging hazards.		Zero-day malware and attacks.
	Flow Analytics: Network traffic metadata identifying security incidents.		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	
	Web Security: Web, DNS, and IP-layer security and control for the campus.		Attacks from malware, viruses, and redirection to malicious URLs.
	Virtual Private Network(VPN): Encrypted communication tunnels.		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 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 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
These security capabilities are required across all PINs:
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 Campus architectures are logical groupings of security and network capabilities that support campus business use cases. It follows a classic access/distribution/core architecture, scaling as needed by increasing distribution blocks as floors or buildings are added.

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.

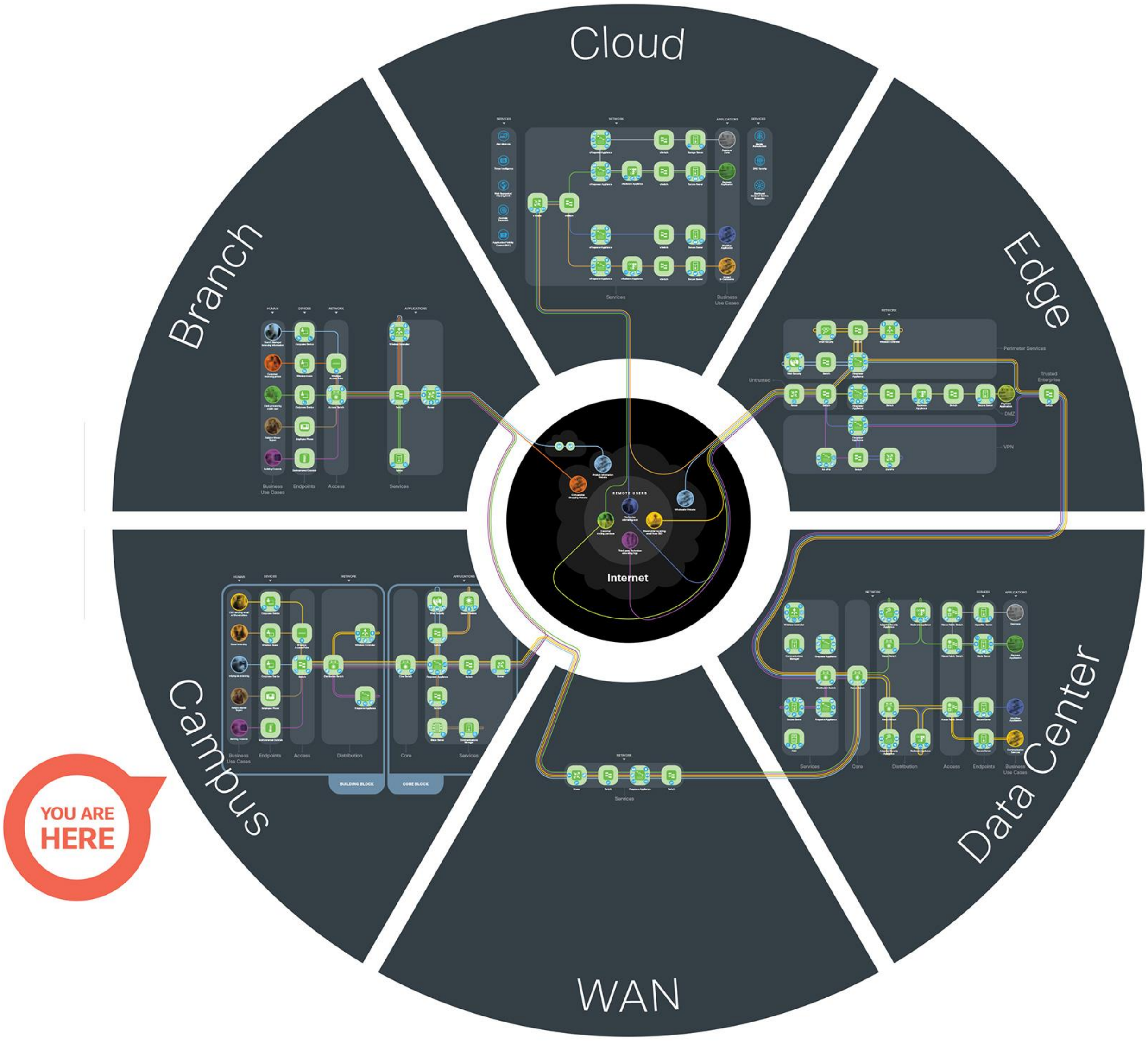


Figure 7. **SAFE Model. The SAFE Model simplifies complexity across a business by using Places in the Network (PINs) that it must secure.**

Secure Campus

The Secure Campus architecture has the following characteristics:

- Location size consists of multiple buildings/floors that may have multiple business flows
- Many varied devices requiring network connectivity
- Devices (sensors, thermostats, printers, etc.)
- Separate appliances for services for redundancy and maximum uptime
- Wireless connectivity
- Local application services (also in data center or cloud)

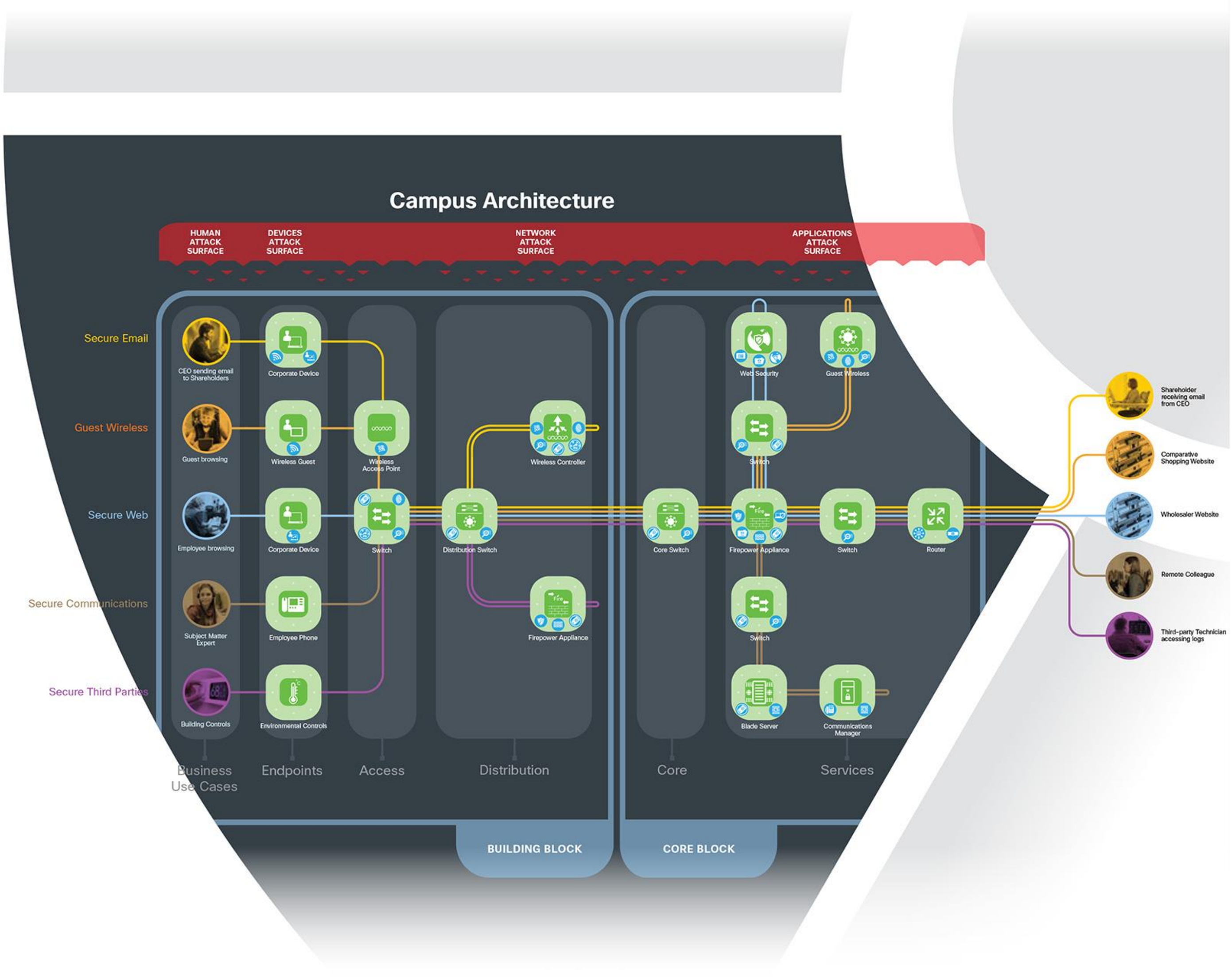


Figure 8. Secure Campus. The Secure Campus business flows and security capabilities are arranged into a logical architecture. The colored business use cases flow through the green architecture icons with the required blue security capabilities.

Attack Surface

The Secure Campus attack surface consists of Humans, Devices, Network, and Applications. The sections below discuss the security capability that defends the threats associated with that part 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, andserved 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 campus are employees, partners, or customers. No amount of technology can prevent successful attacks if the humans in the company, both internal and partner users, are not trained to keep security in mind. One of the biggest problems is that humans are prone to compromise by various types of social exploits such as phishing.

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.

It is not the purpose of this guide to advise on the specifics. Appropriate identity services defined by policy must be supplied with associated, approved clients and devices.

Primary Security Capability

Identity

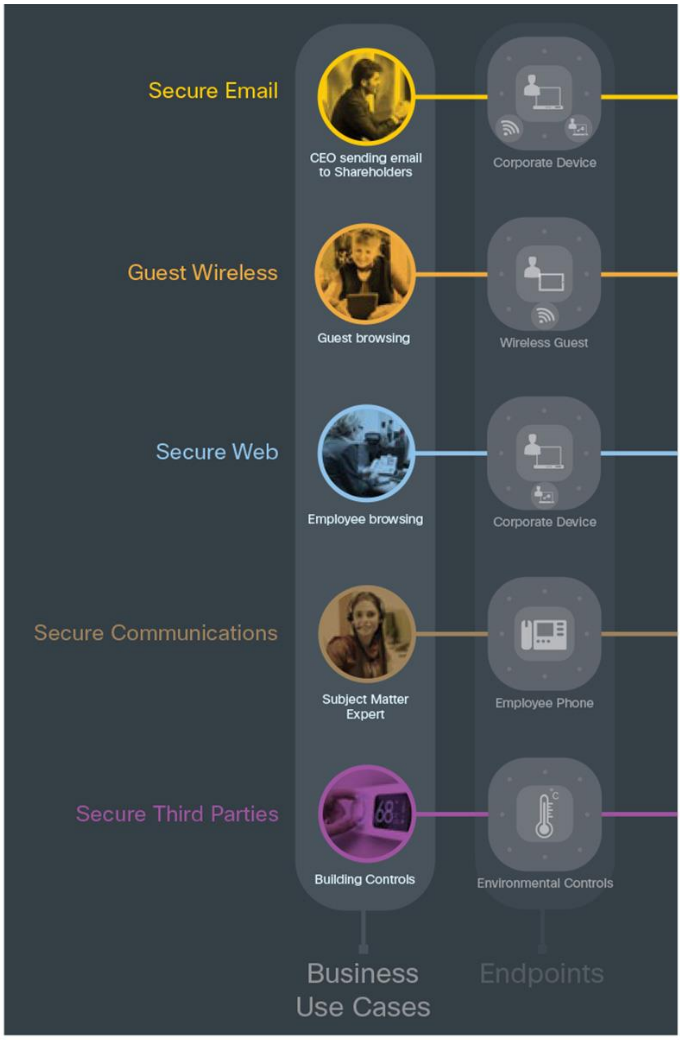
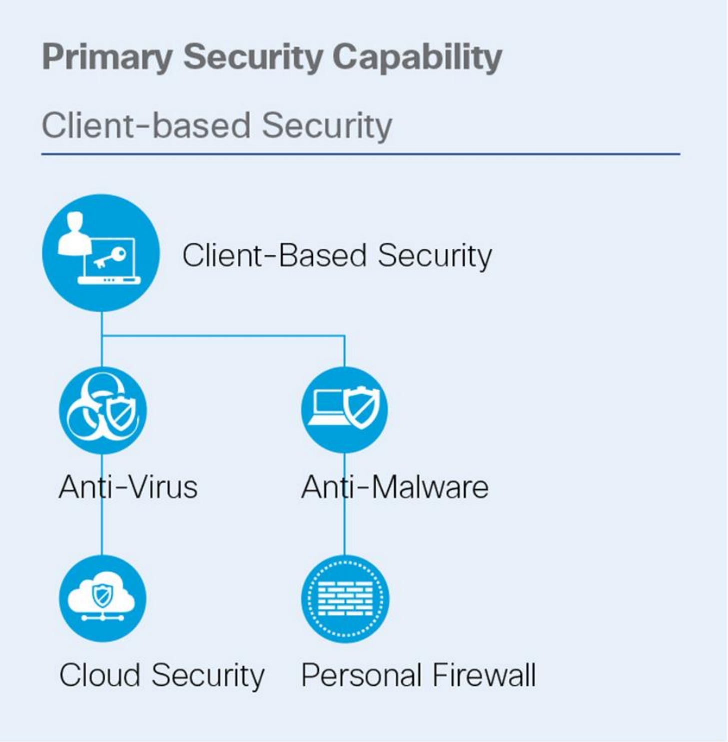


Figure 9. **Business Use Cases**

Devices

Malware propagation, Botnet infestation and a large attack surface are campus threats targeting devices. Perimeter defenses are no longer (if ever) sufficient.

Devices are part of the security reference architecture. 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 devices) are participating in security and that malicious devices are quarantined.



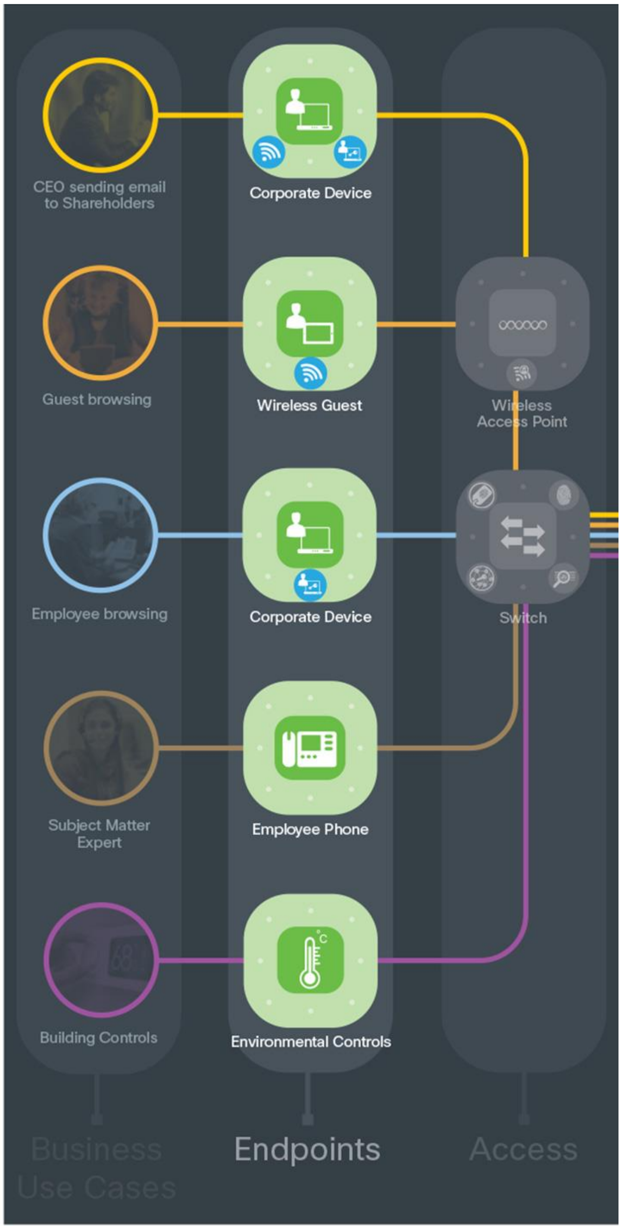


Figure 10. **Campus Devices**

Access Layer

Unauthorized network access is the primary threat addressable by the access layer.

The access/distribution/core is classic network hierarchy. The access layer is where users and devices connect to the company network. This layer connects to the distribution or core layer. Its hierarchical organization simplifies network troubleshooting and segments traffic for security. It is the first line of defense within the Secure Campus architecture. The network as a sensor utilizes flow analytics to capture anomalies and provide visibility to attacks.

Its purpose is to identify the users, to assess compliance to policy of devices seeking access to the network, and to respond appropriately. Violations of posture, identity, or anomalous behavior can be enforced.

Primary Security Capability

Identity

Flow Analytics

Posture Assessment

TrustSec

Wireless Rogue Detection

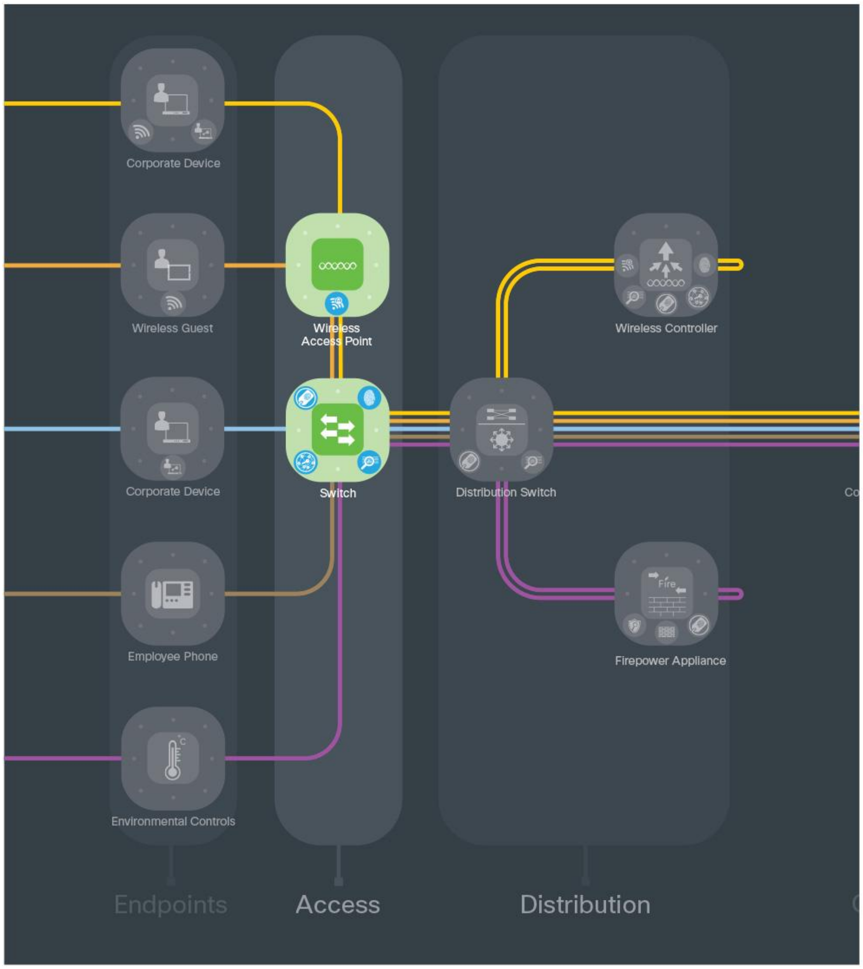


Figure 11. **Access Layer**

Distribution Layer

Distribution layers segregate the access layer from the services layer. These layers provide a distribution method of services that discretely separates business-based traffic into flows, and allows scale as employees are moved, added, or changed.

Primary Security Capability

Identity	Flow Analytics
Posture Assessment	TrustSec

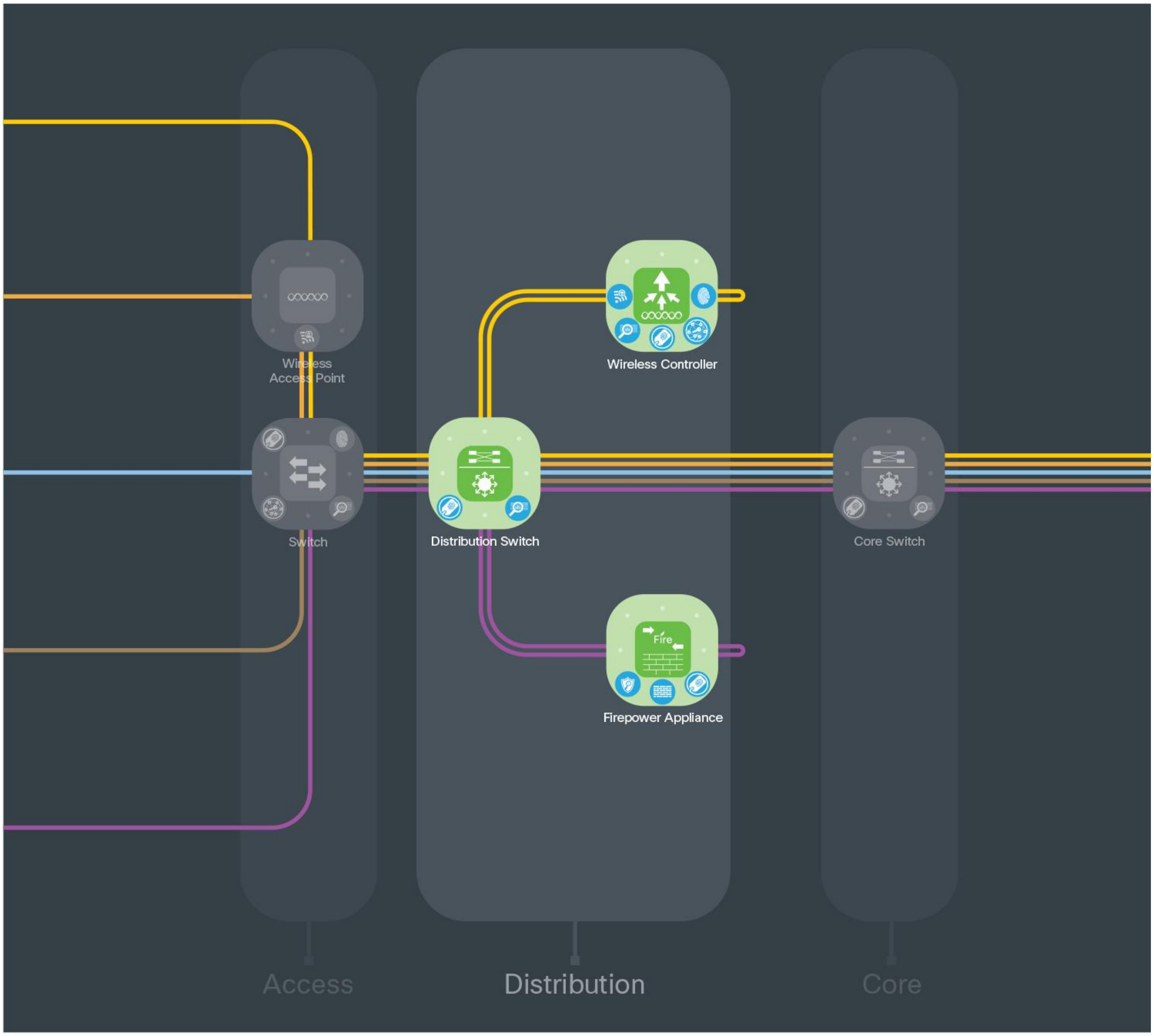


Figure 12. Distribution Layer

Core Layer

The core layer provides scale to the distribution blocks and connects them to the foundational security capabilities in the services layer.

Primary Security Capability

Flow Analytics

TrustSec

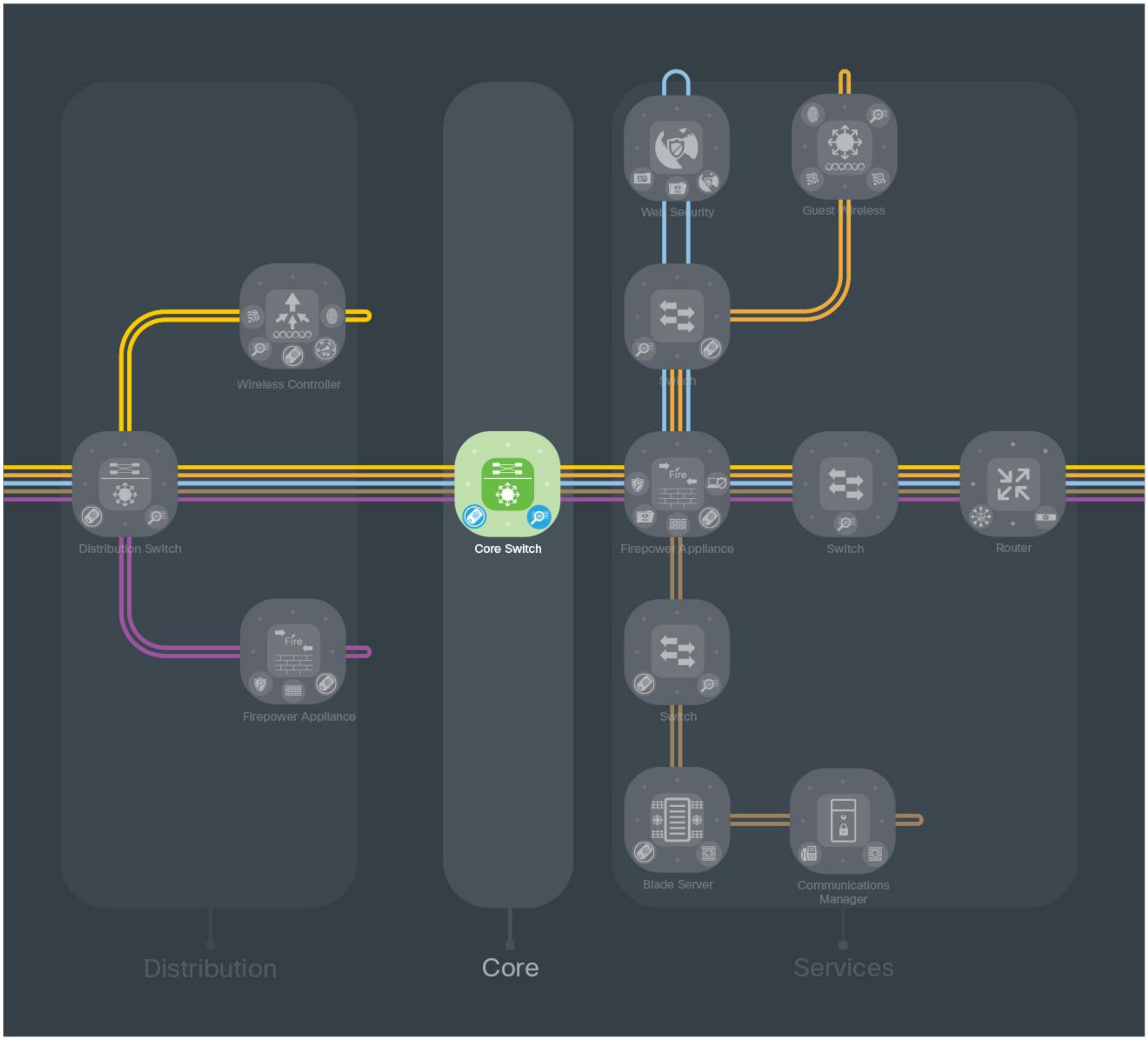


Figure 13. **Core Layer**

Services Layer

Web-based exploits are threat vectors that large campus populations need protection from.

The services layer connects the Secure Campus to the data center via service providers. It connects the access and distribution layers inside the campus to the security and inspection capabilities that secure the separate business flows coming into and out of the campus. Depending on the size of the campus, some security controls are brought into the campus as appliances rather than being served centrally as a service. See the Appendix for proposed options.

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

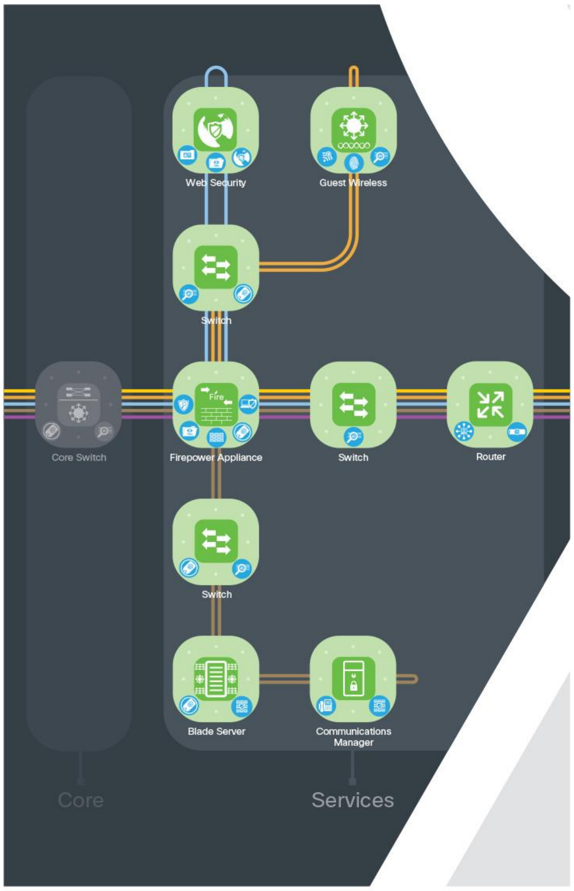


Figure 14. Services Layer

Summary

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

Cisco’s Secure Campus 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 Campus has been deployed in Cisco’s laboratories. Portions of the design have been validated and documentation is available on Cisco Design Zone.

Figure 15 depicts the specific products that were selected within Cisco’s laboratories. It is important to note that the Secure Campus 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.

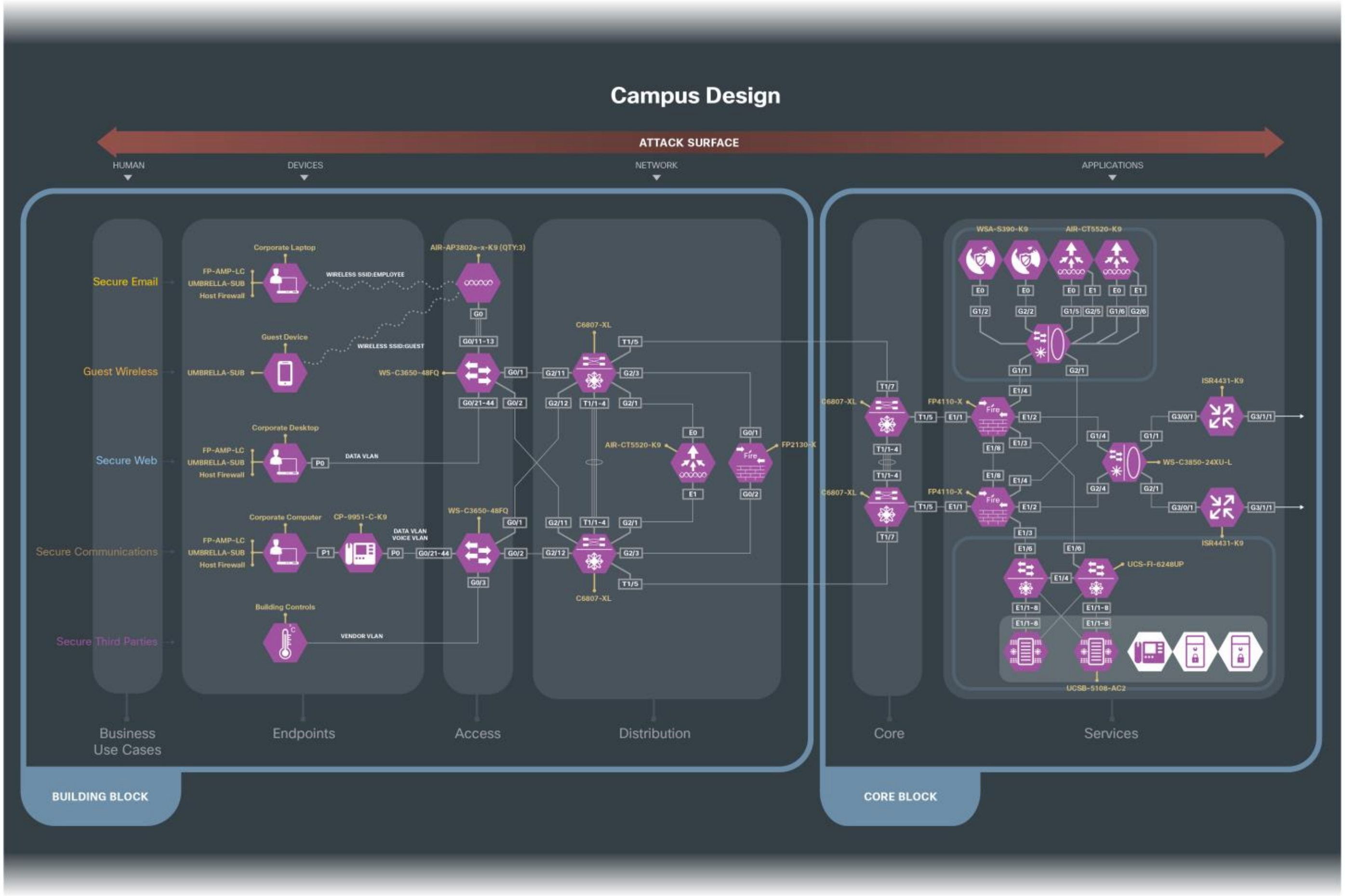


Figure 15. **Secure Campus Proposed Design, part 1. The building block is connected to the core block.**

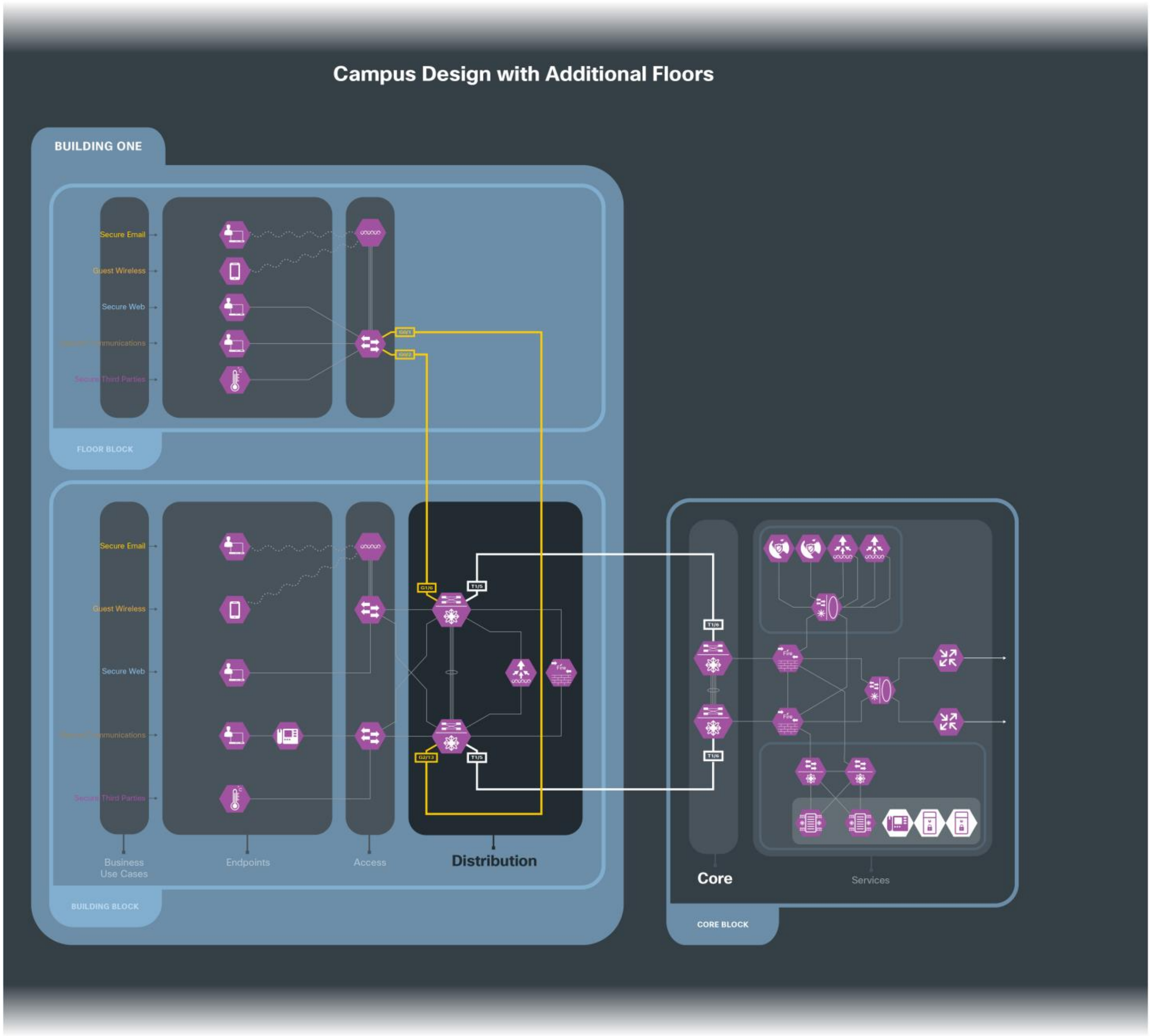


Figure 16. **Secure Campus Proposed Design, part 2 shows how multiple floors can be connected to the distribution layer.**

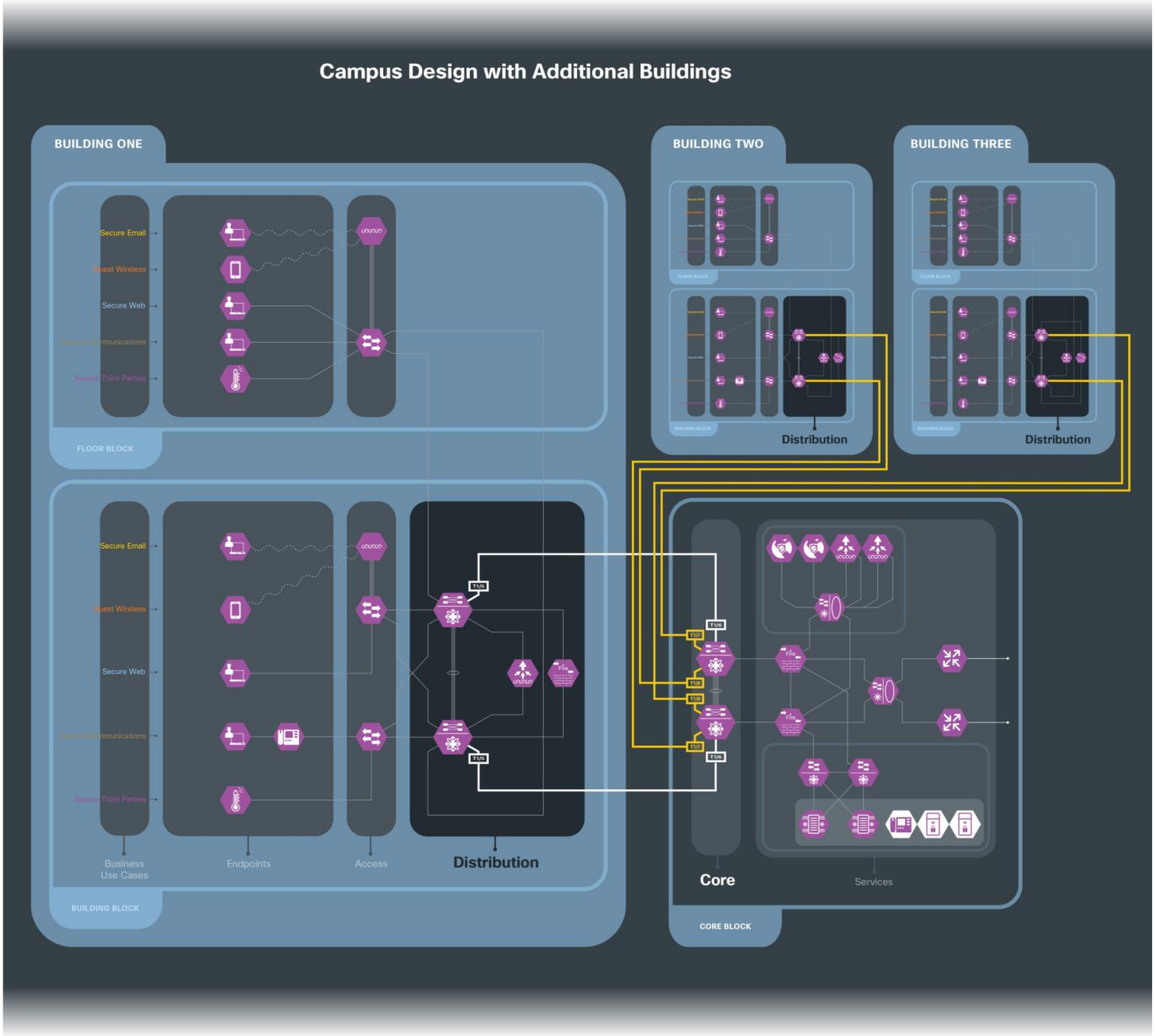


Figure 17. Secure Campus Proposed Design, part 3 illustrates multiple buildings connected to the core block.

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**.