

Cisco Secure Architecture for Everyone (SAFE)

Overview Guide

September 2023

Contents

The Need for Cisco SAFE.....	4
What is Cisco SAFE?.....	4
The Cisco SAFE Security Reference Model.....	5
The Cisco SAFE Method.....	5
How to Use Cisco SAFE?	5
The three phases of SAFE.....	7
Capability phase	7
Architecture phase	8
Design phase	9
SAFE's toolkit and collateral simplify the discussion.....	10
Attack Surface	11
Securing the Attack Surface.....	12
Business Flows	12
Functional Controls	13
Capabilities.....	14
Foundational Capabilities	15
Access Capabilities.....	16
User Access	16
Device Access	17
Server and Application Access	18
Business Capabilities	19
The Business Flow Capability Diagram.....	21
Places in the Network.....	22
Secure Branch.....	23
Secure Campus.....	24
Secure Cloud	25
Secure Data Center	26
Secure Edge.....	26
Secure WAN.....	28
Secure Domains	29
Management.....	30
Security Intelligence.....	31
Compliance.....	32
Segmentation.....	33
Threat Defense.....	34

Secure Services	35
SAFE Capabilities	36
The SAFE Architecture	47
The Attack Surface and Architecture Layers	48
Attack Surface: Human	49
Business Use Case Layer	49
Attack Surface: Devices	50
Endpoints Layer	50
Attack Surface: Network	51
Access Layer	51
Distribution Layer	51
Core Layer	52
Attack Surface: Applications	52
Services Layer	53
Summary.....	54
Appendix	54
Appendix A – Business Flows	54
Internal Business Flows	54
Third-Party Business Flows	54
Customer Business Flows	55
Appendix B – Feedback	55

The Need for Cisco 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.

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.

What is Cisco SAFE?

Cisco Secure Architecture for Everyone (SAFE) is a security model and method used to secure business. It focuses on threats—and best practices for defending against them. Cisco 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.

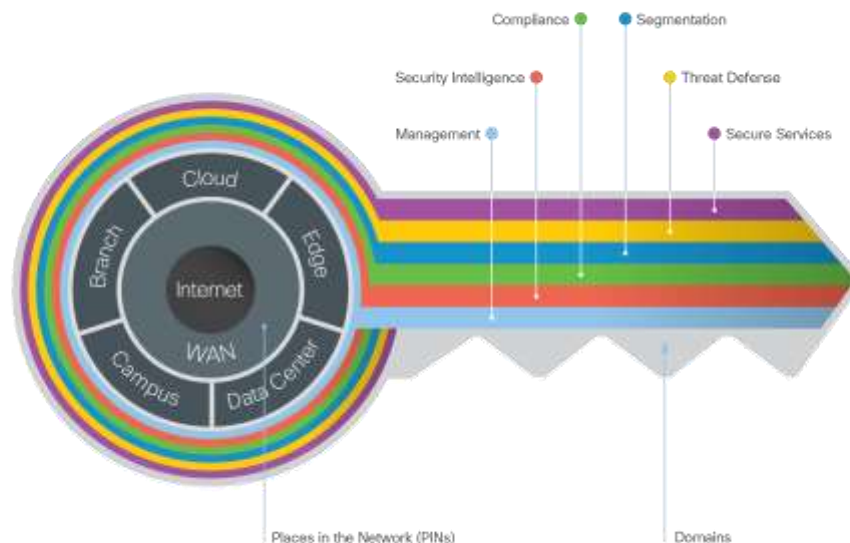


Figure 1. Key to SAFE

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

The Cisco 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. Delivered as Cisco Validated Designs (CVDs).

The Cisco 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.

How to Use Cisco 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


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 Cases	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.

Table 1. The SAFE Model Icons

The three phases of SAFE

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

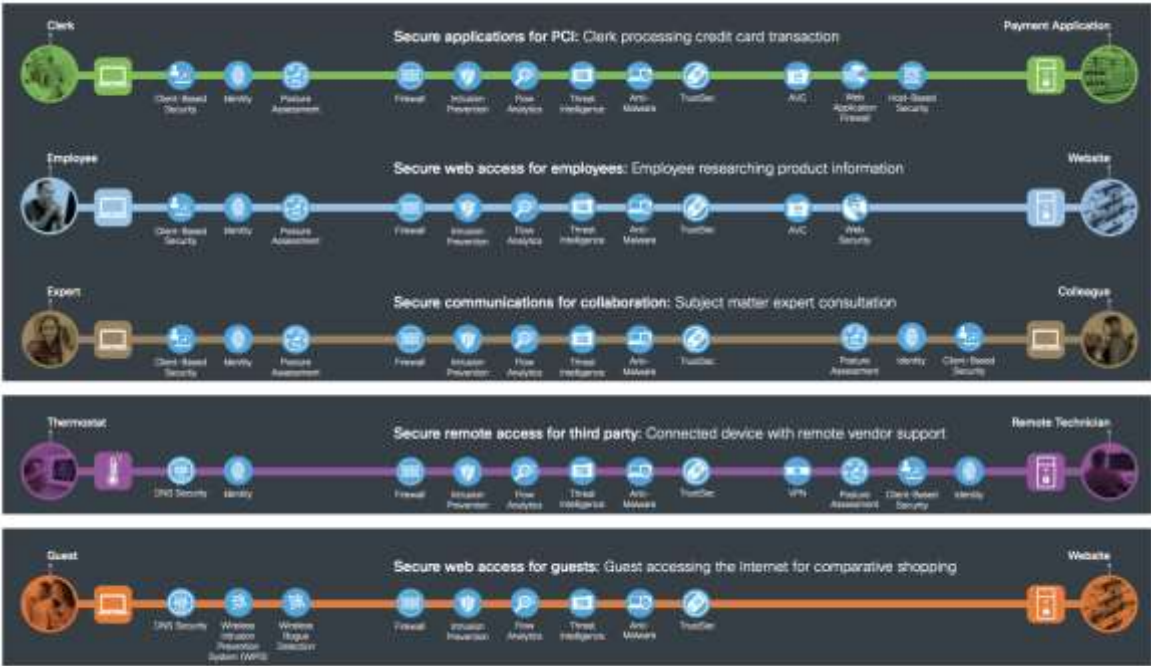


Figure 2. In the capability phase, business flows are analyzed to determine the required security capabilities.

Architecture phase

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

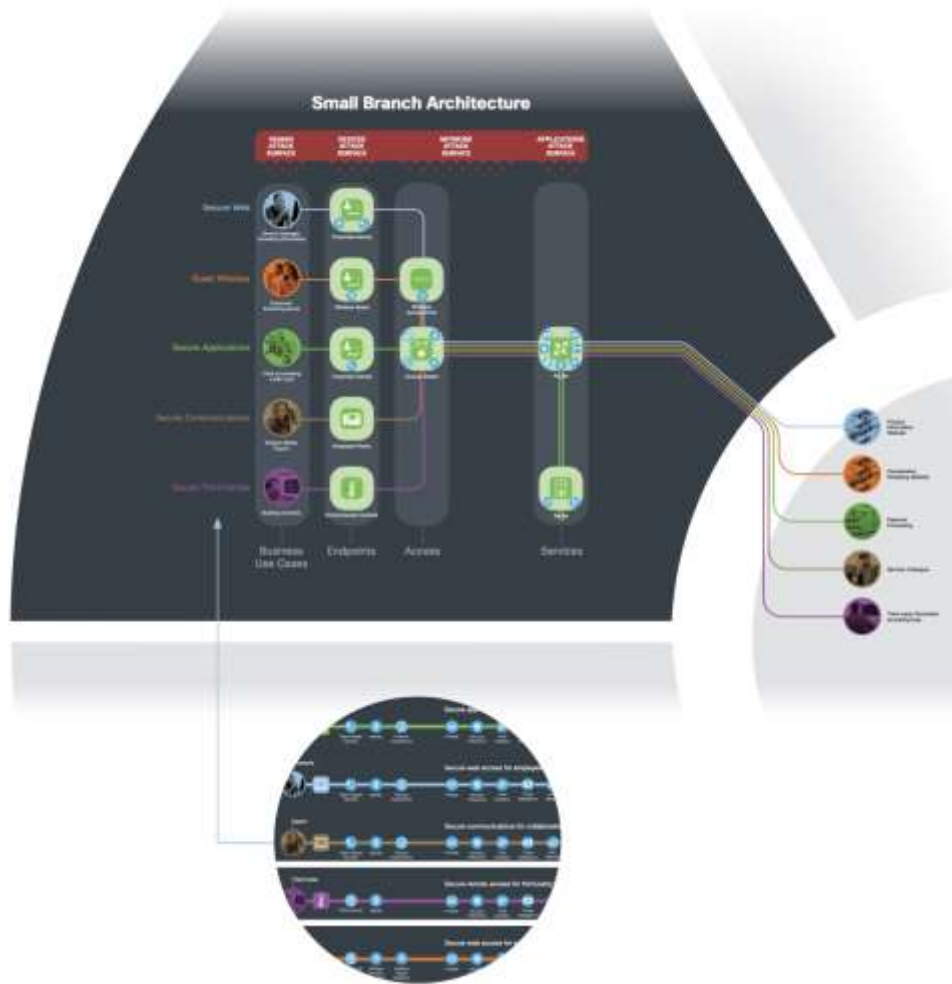


Figure 3. In the architecture phase, a logical architecture. Note that the security capabilities are arranged into business flows can still be identified.

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

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 5. 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.

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

Table 2. Attack Surface

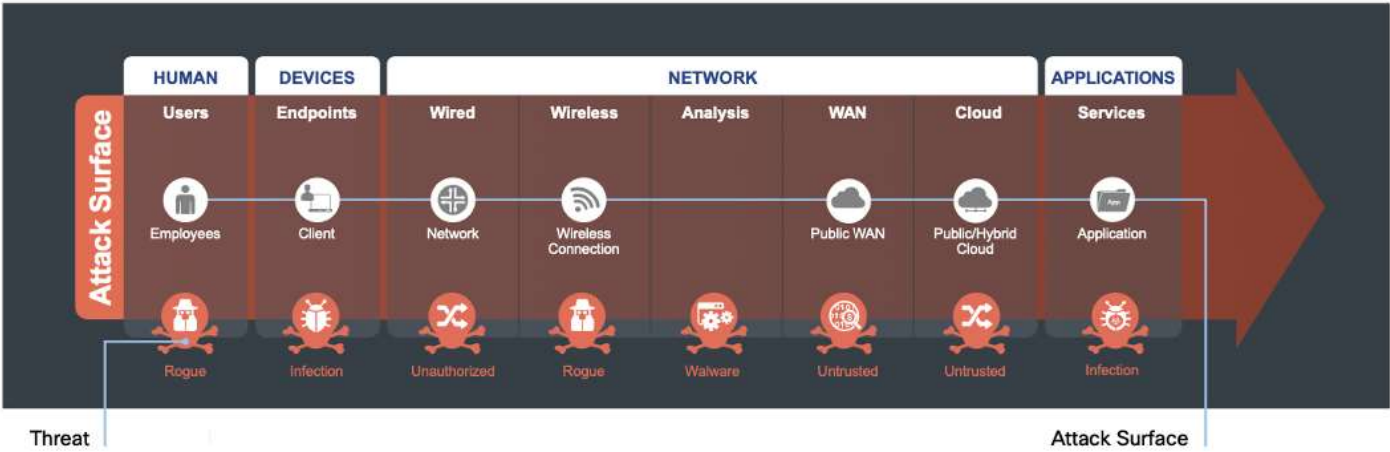


Figure 6. The attack surface that needs to be secured.

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 company's attack surface, proper security capabilities can be applied.

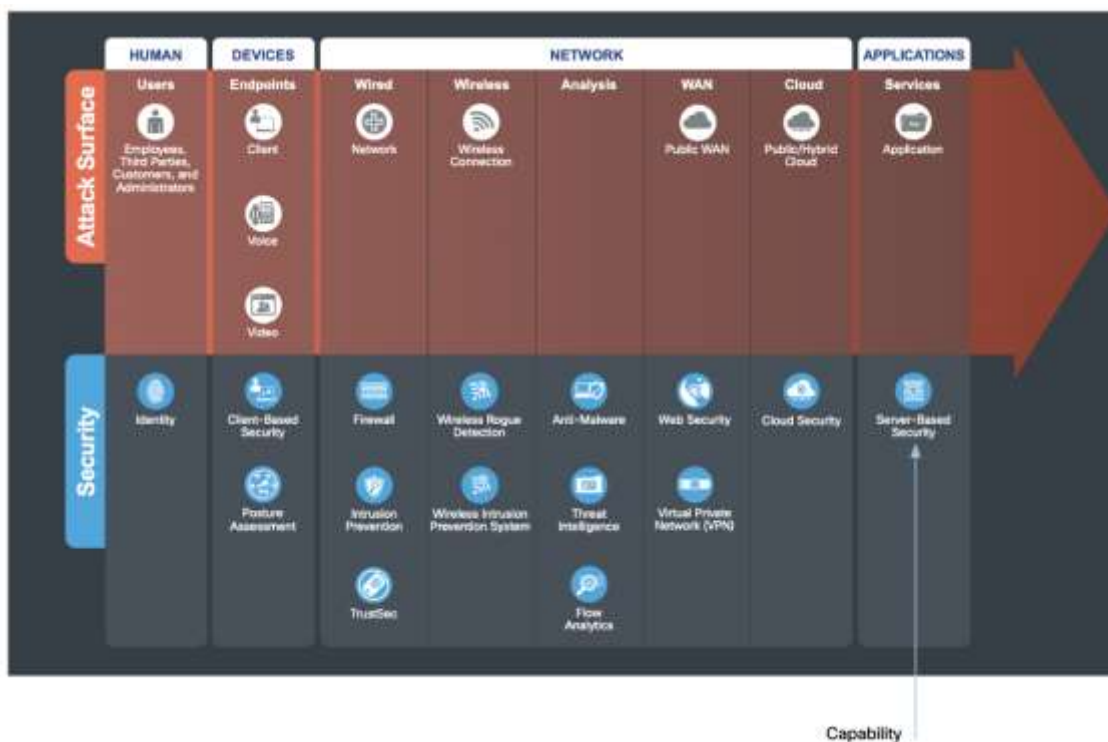


Figure 7. Security capabilities are applied logically to mitigate the threats along the attack surface.

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.

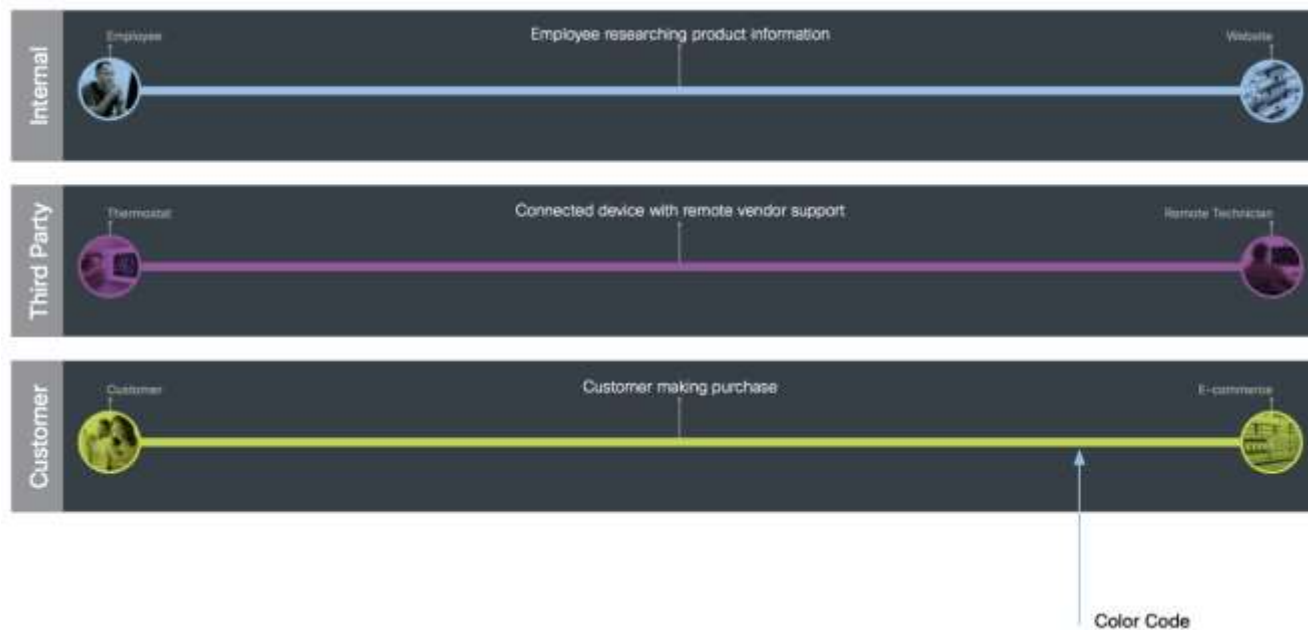


Figure 8. SAFE color codes business use cases as business flows.

Functional Controls

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

Functional Control	Definition
Secure Applications	Applications require sufficient security controls for protection.
Secure East/West Traffic	Data that securely moves between internal and external resources.
Secure Access	Employeea, 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 prevent network infection.

Table 3. Functional Controls



Figure 9. 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 10. 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 11. Foundational Capability Group: Secure Applications and Secure East West Traffic

Security Capability Icon	Security Capability Description	Threat Icon	Threat Description
	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 data center.
	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 segments.

Table 4. Foundational Capabilities

Access Capabilities

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



Figure 12. Secure Access Capability Group: Secure Access

User Access



Users: Employees, contractors, customers, and administrators.

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

Table 5. User Access Capabilities

Device Access



Devices such as PCs, laptops, smartphones, tablets.

Security Capability Icon	Security Capability Description	Threat Icon	Threat Description
	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.

Table 6. Device Access Capabilities

Server and Application Access



Security Capability Icon	Security Capability Description	Threat Icon	Threat Description
	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: Security services from the cloud		Redirection of session to malicious website.
	Host-based Firewall: Provides micro-segmentation and policy enforcement.		Unauthorized access and malformed packets connecting to server.
	Posture Assessment: Server compliance verification, authorization, and patching.		Targeted attacks taking advantage of known vulnerabilities.
	Disk Encryption: Encryption of data at rest.		Theft of unencrypted data.
	Flow Analytics: Network traffic metadata identifying security incidents.		Traffic, telemetry, and data exfiltration from successful attacks.
	Application Dependency Mapping:		Exploiting a misconfigured firewall policy.
	Vulnerability Assessment and Software Inventory:		Exploiting unpatched or outdated applications.







Security Capability Icon	Security Capability Description	Threat Icon	Threat Description
	Process Anomaly Detection & Forensics:		Exploiting privileged access to run shell code.
	Tagging: Grouping for Software Defined Policy		Unauthorized access and malicious traffic between segments.
	Policy Generation, Audit, and Change Management:		Targeted attacks taking advantage of known vulnerabilities.

Table 7. Server and Application Access Capabilities

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 13. Business Capability Group: Secure Communications, Secure Web Access, Secure Remote Access













Security Capability Icon	Security Capability Description	Threat Icon	Threat Description
	Web Security: Web, DNS, and IP-layer security and control for the campus.		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.

Table 8. Business Capabilities

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 capabilities.

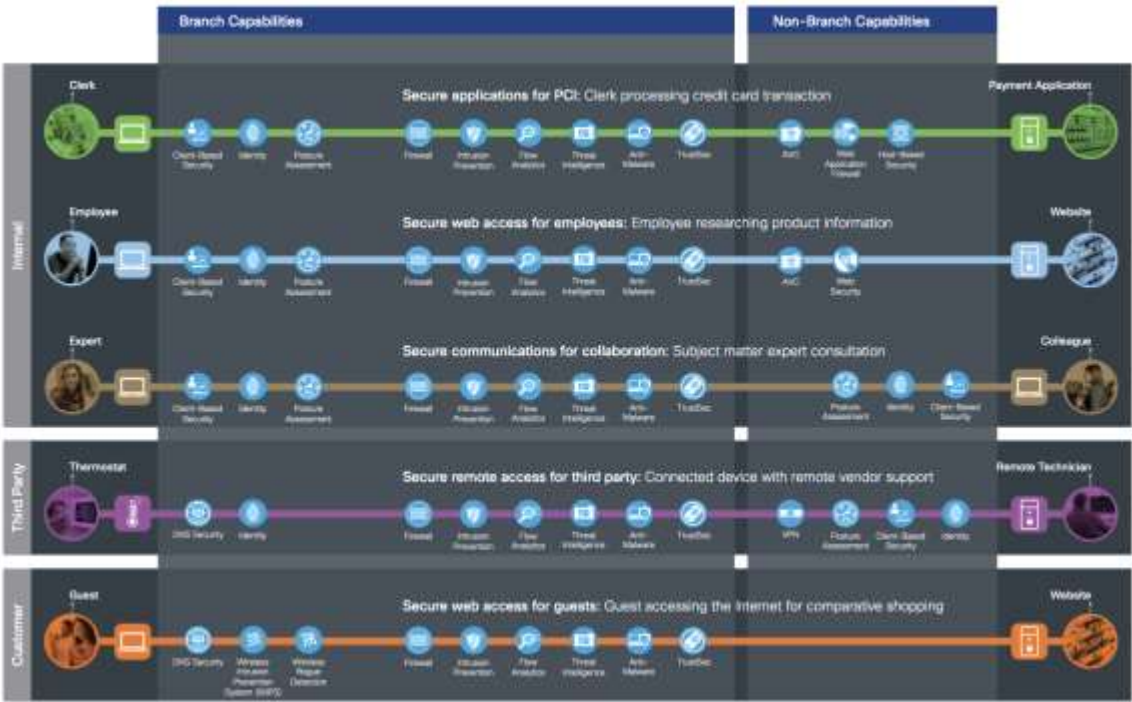


Figure 14. The Secure Branch Business Flow Capability Diagram

Places in the Network

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

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

PINs are locations that are commonly found in networks 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.

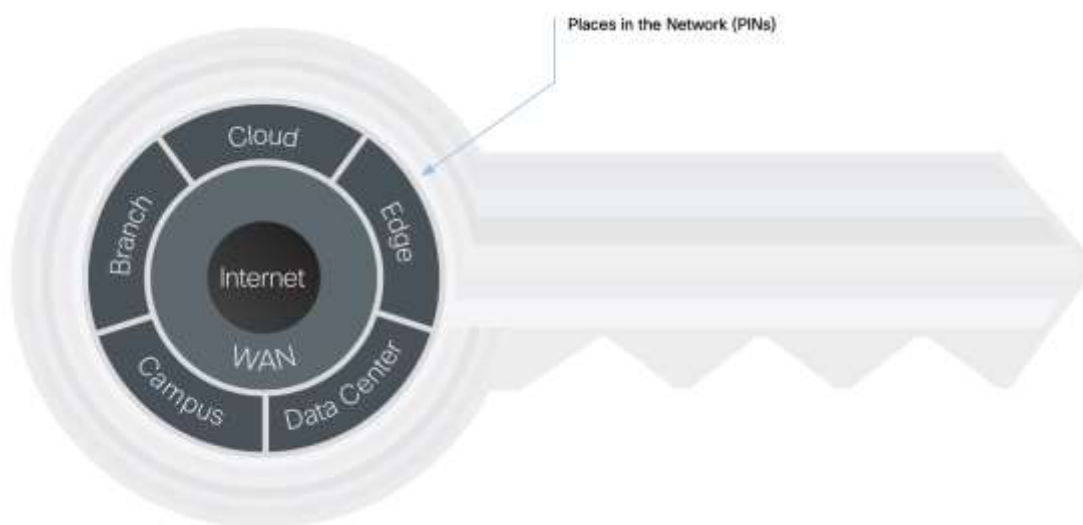


Figure 15. Places in the Network

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.

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 more information, refer to the [SAFE Secure Branch Architecture Guide](#).

The following figure shows the progression of security capabilities used to help defend against the attacks common in a branch.



Figure 16. 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.

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 more information, refer to the [SAFE Secure Campus Architecture Guide](#).

The following figure shows the progression of security capabilities that are used to help defend against the attacks common in a campus.



Figure 17. Secure Campus 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.

Top Threats Mitigated in the Cloud:

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

For more information, refer to the [SAFE Secure Cloud Architecture Guide](#).

The following figure shows the progression of security capabilities used to help defend against the attacks common in the cloud.



Figure 18. Secure Cloud 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.

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 more information, refer to the [SAFE Secure Data Center Architecture Guide](#).

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



Figure 19. 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.

Top Threats Mitigated in the Edge:

- Webserver vulnerabilities

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

For more information, refer to the [SAFE Secure Edge Architecture Guide](#).

The following figure shows the progression of security capabilities that are used to help defend against the attacks common at the network edge.



Figure 20. Secure Edge Attack Surface and Security Capabilities

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.

Top Threats Mitigated in the WAN:

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

The following figure shows the progression of security capabilities used to help defend against the attacks common in a WAN.



Figure 21. 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.

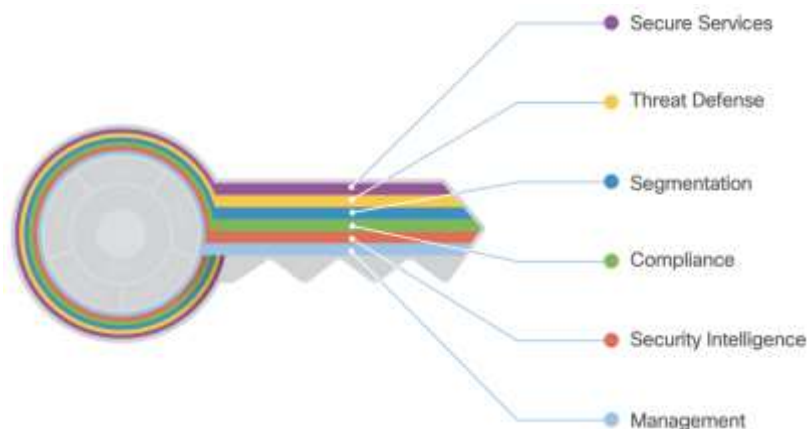


Figure 22. SAFE Model Secure Domains

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.

The following figure shows the progression of security capabilities used for the operations of Management.

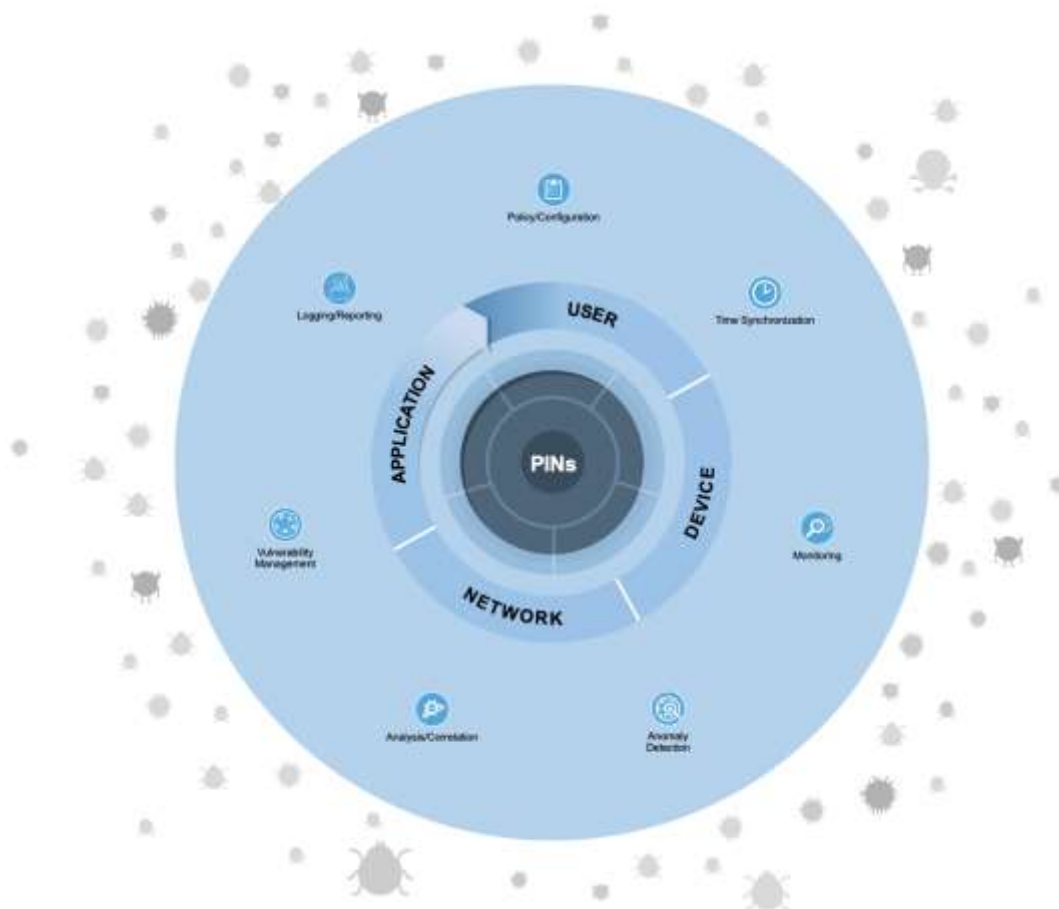


Figure 23. Management Domain Capabilities

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.

The following figure shows the progression of security capabilities used for the operations of Security Intelligence.

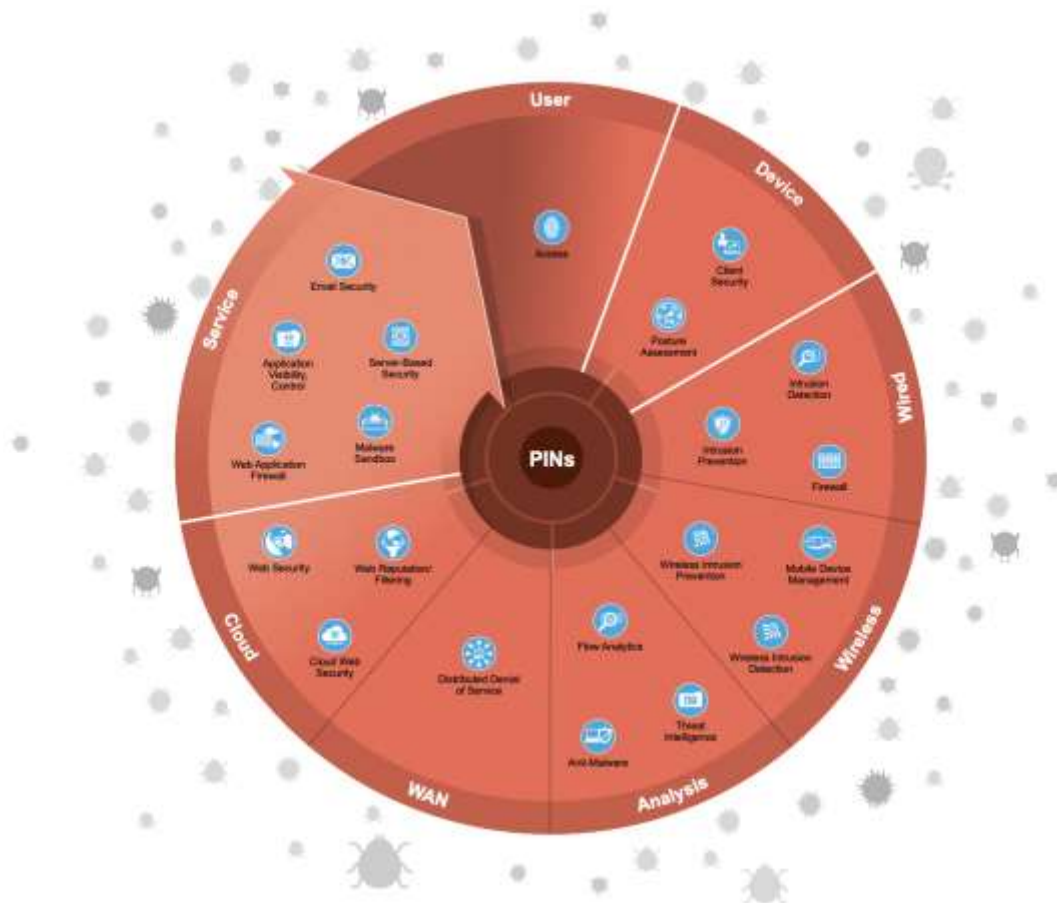


Figure 24. Security Intelligence Capabilities

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).

The following figure shows the progression of security capabilities used for Compliance.



Figure 25. 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.

The following figure shows the progression of security capabilities used for Segmentation.

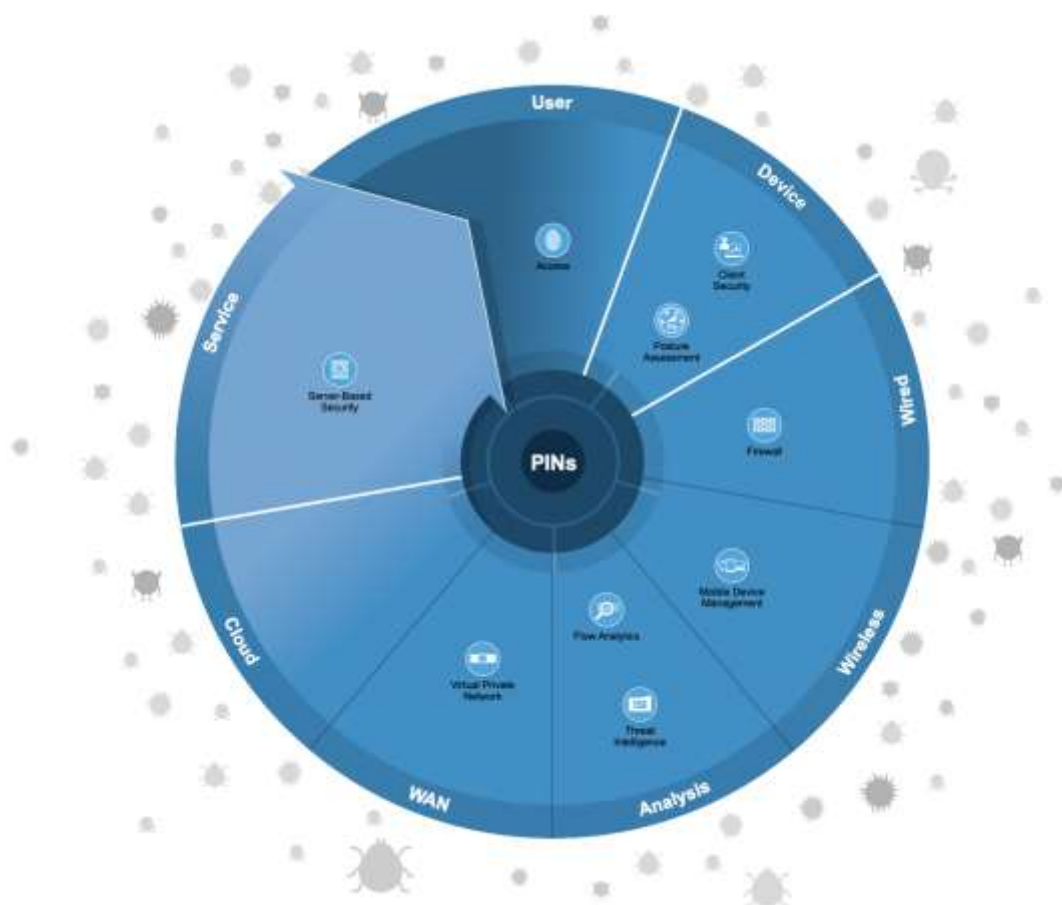


Figure 26. Segmentation Capabilities

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.

The following figure shows the progression of security capabilities used for the operations of Threat Defense.



Figure 27. 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 .

The following figure shows the progression of security capabilities used for Secure Services.

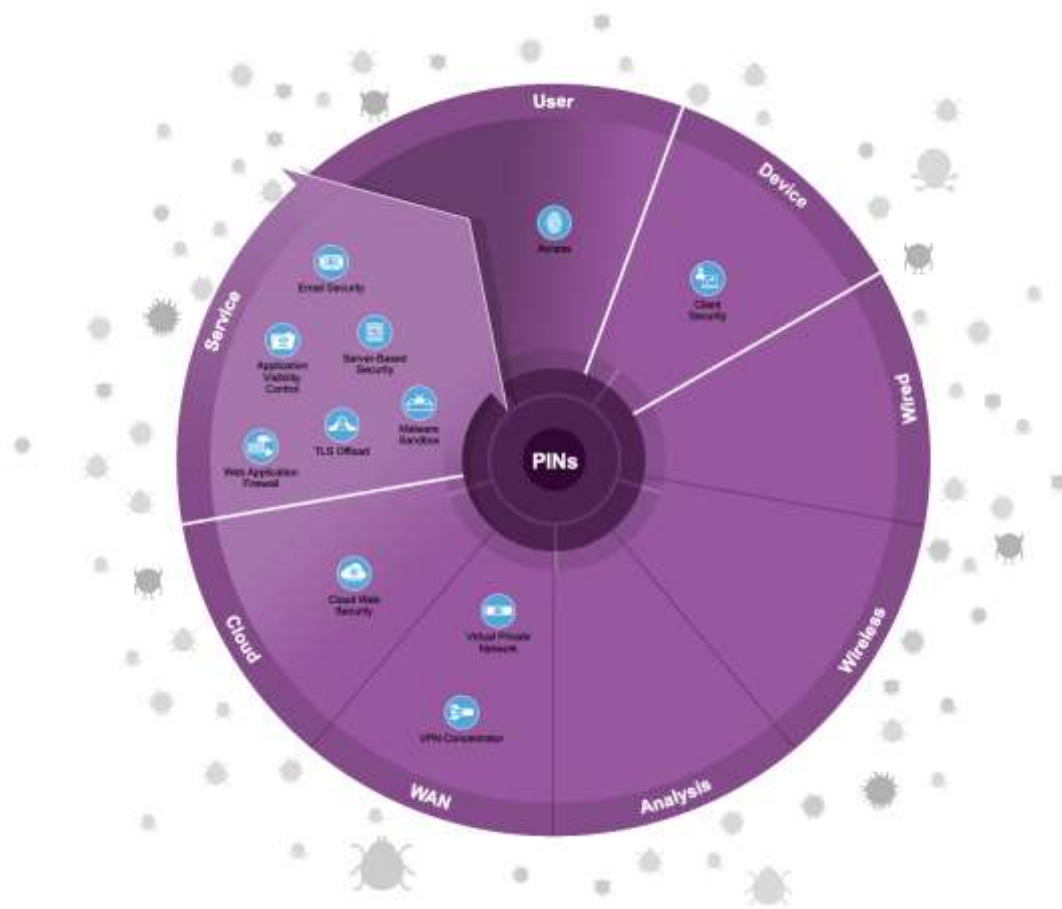






















Figure 28. Secure Services Capabilities






SAFE Capabilities




Capabilities describe the primary functions of a security service. The following table 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.






Attack Surface	Attack Surface Examples	Security Capability Icon	Security Capability Description	Places in the Network	Suggested Cisco Components
Human	Users: Employees, contractors, customers, and administrators.		Identity/ Authorization: Restriction of user access to services and resources.	Secure Branch Secure Campus Secure Cloud Secure Data Center Secure Edge Secure WAN	Identity Services Engine (ISE) Duo Meraki Mobile Device Management
Devices	Clients: Devices such as PCs, laptops, smartphones, tablets.		Client-Based Security: Security software to protect clients.	Secure Branch Secure Campus Secure External Zones	Secure Endpoint Secure Client Secure Access Umbrella
			Anti-Malware		
			Anti-Virus		
			Cloud Security		
			Personal Firewall		
			Posture Assessment: Client endpoint compliance verification and authorization.	Secure Branch Secure Campus Secure External Zones	Secure Client Duo Identity Services Engine




Attack Surface	Attack Surface Examples	Security Capability Icon	Security Capability Description	Places in the Network	Suggested Cisco Components
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.	Secure Branch Secure Campus Secure Data Center Secure External Zones Secure WAN	Secure Firewall Meraki MX
				Secure Cloud	Multicloud Defense Secure Firewall
			Intrusion Prevention System: Identification of attacks by signatures and anomaly analysis.	Secure Campus Secure Cloud Secure Data Center Secure Edge Secure External Zones Secure WAN	Secure Firewall
			Tagging: Contextual Segmentation	Secure Branch Secure Campus Secure Data Center Secure Edge	Nexus/Catalyst/Meraki Switch VLANs Identity Services Engine, pxGrid, TrustSec Application Centric Infrastructure (ACI) Endpoint Group (EPG)
	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.	Secure Edge	Meraki Mobile Device Management Identity Services Engine
			Wireless Rogue Detection: Detection and containment of malicious wireless devices that are not controlled by the company.	Secure Branch Secure Campus	Meraki Wireless Wireless LAN Controller
			Wireless Intrusion Prevention (WIPS): Blocking of wireless attacks by signatures and anomaly analysis.		





Attack Surface	Attack Surface Examples	Security Capability Icon	Security Capability Description	Places in the Network	Suggested Cisco Components
	Analysis: Analysis of network traffic within the campus.		Anti-Malware: Identify, block, and analyze malicious files and transmissions.	Secure Branch Secure Campus Secure Cloud Secure Data Center Secure Edge Secure WAN Secure External Zones	Secure Endpoint
			Threat Intelligence: Contextual knowledge of emerging hazards.	Secure Branch Secure Campus Secure Cloud Secure Data Center Secure Edge Secure WAN	Talos Threat Intelligence
			Flow Analytics: Network traffic metadata identifying security incidents.	Secure Branch Secure Campus Secure Cloud Secure Data Center Secure Edge Secure WAN	Secure Network Analytics Secure Cloud Analytics XDR
	WAN: Public and untrusted Wide Area Networks that connect to the company, such as the Internet.		VPN Concentrator: Encrypted remote access.	Secure Edge	Secure Firewall Meraki MX
			Virtual Private Network (VPN): Encrypted communication tunnels.	Secure Branch Secure Campus Secure Cloud Secure Data Center Secure WAN External Zones	Secure Firewall Meraki MX
			DDoS Protection: Protection against scaled attack forms.	Secure Edge	Secure DDoS
	Cloud:		Cloud Security: Secure Internet Gateway or Secure Access Service Edge	Secure Branch Secure Campus	Secure Access Umbrella







Attack Surface	Attack Surface Examples	Security Capability Icon	Security Capability Description	Places in the Network	Suggested Cisco Components
			(SASE)	Secure Cloud	
				Secure Data Center	
				Secure Edge	
				Secure External Zones	
				Secure WAN	
			DNS Security: Enforces security at the DNS layer to block malware, phishing, and command and control callbacks over any port.		
			Firewall: Macro segmentation is the process of separating a network topology into smaller sub-networks, often known as zones. A firewall is typically the enforcement point between zones in a network.		
			Intrusion Prevention: An intrusion prevention system (IPS) provides network visibility, security intelligence, automation, and advanced threat protection.		
			Web Security: A full proxy that can log and inspect all your web traffic for greater transparency, control, and protection. IPsec tunnels, PAC files and proxy chaining can be used to forward traffic for full visibility, URL and application-level controls, and advanced threat protection.		
			Web Reputation Filtering: Compares each new website visited		










Attack Surface	Attack Surface Examples	Security Capability Icon	Security Capability Description	Places in the Network	Suggested Cisco Components
			against known sites and then blocks access to sites that launch malicious code.		
			TLS/SSL Decryption: Ability to decrypt and inspect encrypted web traffic and block hidden attacks.		
			Remote Browser Isolation: Provides an added layer of protection against browser-based security threats for high-risk users. RBI moves the most dangerous part of browsing the internet away from the end user's machine and into the cloud.		
			Network Anti-Malware: Advanced malware's goal, in general, is to penetrate a system and avoid detection. Once loaded onto a computer system, advanced malware can self-replicate and insert itself into other programs or files, infecting them in the process. Anti-malware protection should be implemented in both the network (to prevent initial infection and detect attempts of spread) and in the endpoint (to prevent endpoint infection and remove unwanted threats). This capability represents network anti-malware.		

Attack Surface	Attack Surface Examples	Security Capability Icon	Security Capability Description	Places in the Network	Suggested Cisco Components
			Malware Sandbox: Inspects and Analyzes suspicious files.		
			Cloud Access Security Broker (CASB): An intermediary between cloud providers, cloud-based applications, and cloud consumers to enforce an organization's security policies and usage.		
			Data Loss Prevention: Designed to stop sensitive information from leaving an organization. The goal is to stop information such as intellectual property, financial data, and employee or customer details from being sent, either accidentally or intentionally, outside the corporate network.		
			Application Visibility & Control: Visibility and access control to approved web applications.		
Applications	Application		Application Dependency Mapping: Creates a map of all the components of an application. Enables network admins to build tight network security policies based on various signals such as network flows, processes, and other side information like	Secure Cloud Secure Data Center	Secure Workload

Attack Surface	Attack Surface Examples	Security Capability Icon	Security Capability Description	Places in the Network	Suggested Cisco Components
			load balancer configs.		
			<p>Process Anomaly Detection & Forensics:</p> <p>Anomaly detection is provided by performing hash analysis of all httpd binaries on the system, and reporting any mismatches. For all processes across the workloads if the rootscope, executable binary path, OS version or package info does not match the expected value, it is reported. Forensics enables monitoring and alerting for possible security incidents by capturing real-time forensic events and applying user-defined rules.</p>	<p>Secure Cloud</p> <p>Secure Data Center</p>	Secure Workload
			<p>Continuous Vulnerability Scanning:</p> <p>Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunities for attackers.</p>	<p>Secure Cloud</p> <p>Secure Data Center</p>	Secure Workload
			<p>Tagging/Grouping for Software Defined Policy:</p> <p>Segmentation using Endpoint Groups (EPG), TrustSec Security Group Tag (SGT), or VLANs.</p>	<p>Secure Cloud</p> <p>Secure Data Center</p>	<p>Secure Workload</p> <p>Secure Firewall</p>

Attack Surface	Attack Surface Examples	Security Capability Icon	Security Capability Description	Places in the Network	Suggested Cisco Components
			<p>Policy Generation, Audit and Change Management:</p> <p>The output of application dependency mapping provide an allowed access list policy. This policy will need to be audited and changed as required.</p>	<p>Secure Cloud</p> <p>Secure Data Center</p>	Secure Workload
			<p>Micro-Segmentation:</p> <p>Micro-segmentation secure applications by expressly allowing particular application traffic and, by default, denying all other traffic. Granular east-west policy control provides a scalable way to create a secure perimeter zone around each workload with consistency across different workload types and environments.</p>	<p>Secure Cloud</p> <p>Secure Data Center</p>	Secure Workload
			<p>Runtime Application Self-Protection (RASP):</p> <p>A security technology that is built or linked into an application or application runtime environment, and is capable of controlling application execution and detecting and preventing real-time attacks.</p>	<p>Secure Cloud</p> <p>Secure Data Center</p>	Panoptica
			<p>Anti-Virus:</p> <p>Anti-Virus typically deals with older established threats such as trojans, viruses and worms. Anti-Virus is generally included in Anti-Malware solutions which also can detect new modern day threats.</p> <p>Anti-Malware</p>	<p>Secure Cloud</p> <p>Secure Data Center</p>	Secure Endpoint

Attack Surface	Attack Surface Examples	Security Capability Icon	Security Capability Description	Places in the Network	Suggested Cisco Components
			solutions typically also include Anti-Virus capabilities.		
			<p>Anti-Malware:</p> <p>Advanced malware's goal, in general, is to penetrate a system and avoid detection. Once loaded onto a computer system, advanced malware can self-replicate and insert itself into other programs or files, infecting them in the process. Anti-malware protection should be implemented in both the network (to prevent initial infection and detect attempts of spread) and in the endpoint (to prevent endpoint infection and remove unwanted threats). This capability represents endpoint anti-malware.</p>	Secure Cloud Secure Data Center	Secure Endpoint
	Storage: Information storage on all media types.		Disk Encryption	Secure Cloud Secure Data Center	Cloud Storage Provider Data Center Provider
	Server-Based Security: Security software to protect hosts.			Secure Cloud Secure Data Center Secure Edge	
			Anti-Malware		Cisco Secure Endpoint
			Anti-Virus		Cisco Secure Endpoint
			Cloud Security		Cisco Umbrella

Attack Surface	Attack Surface Examples	Security Capability Icon	Security Capability Description	Places in the Network	Suggested Cisco Components
			Host-based Firewall		Cisco Secure Workload
			Email Security: Messaging integrity and protections.	Secure Data Center Secure Cloud Secure Edge	Cisco Secure Endpoint Cisco Duo
			Malware Sandbox: Detonation and analysis of file behavior.	Secure Data Center Secure Internet	Secure Malware Analytics
Management	Managment		Logging/Reporting: Centralized event information collection.	All	Secure Cloud Analytics Secure Network Analytics
			Policy/Configuration: Unified infrastructure management and compliance verification.		Firewall Management Center Cisco Defense Orchestrator
			Time Synchronization: Device clock calibration.		All systems and devices
			Vulnerability Management: Continuous scanning and reporting of infrastructure.		Vulnerability Management (Kenna) Firewall Management Center Cisco Defense Orchestrator
			Analysis/ Correlation: Security event management of real-time information.		Secure Cloud Analytics Secure Network Analytics XDR Firewall Management Center
			Anomaly Detection: Identification of infected hosts scanning for other vulnerable hosts.		Secure Cloud Analytics Secure Endpoint Secure Network Analytics XDR Firewall Management


Attack Surface	Attack Surface Examples	Security Capability Icon	Security Capability Description	Places in the Network	Suggested Cisco Components
					Center Cisco Defense Orchestrator
			Monitoring: Network traffic inspection.		Secure Cloud Analytics Secure Network Analytics XDR

Table 9. SAFE Capabilities

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.

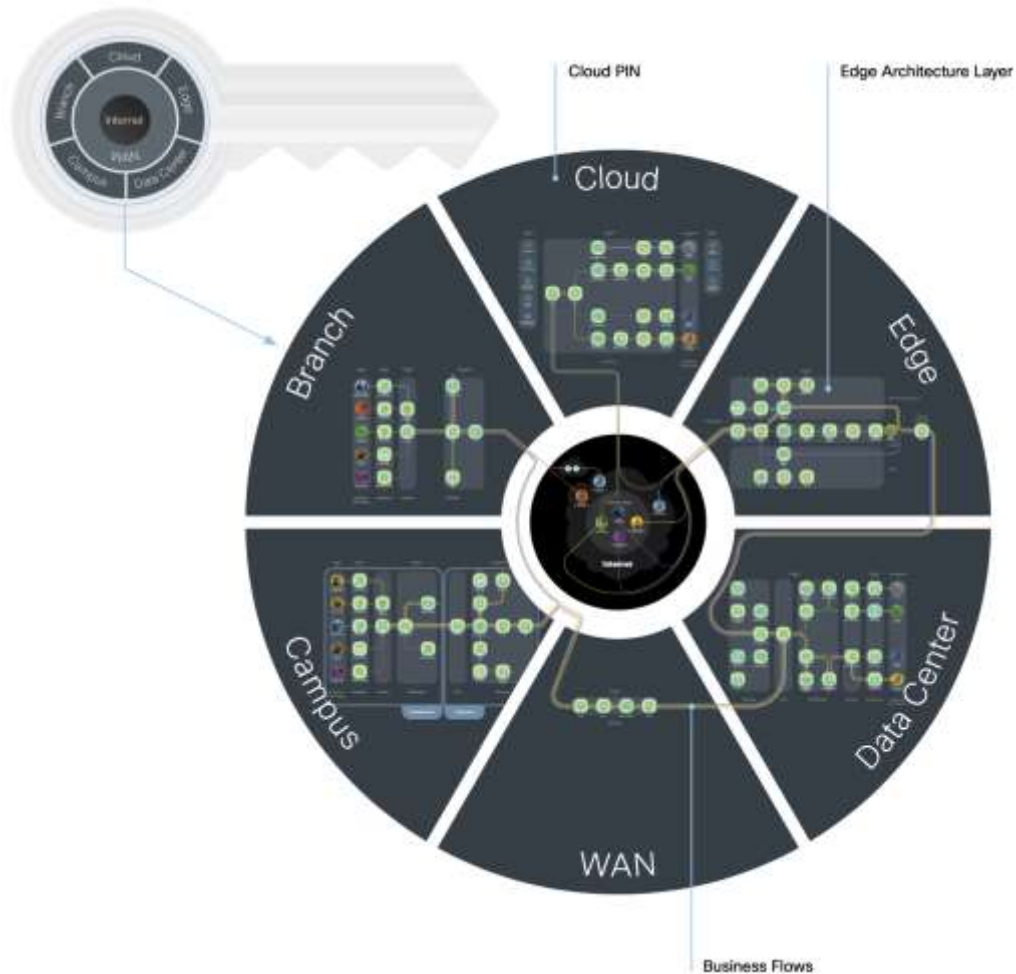


Figure 29. SAFE Model. The SAFE Model simplifies complexity across a business by using Places in the Network (PINs) that it must secure.

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).

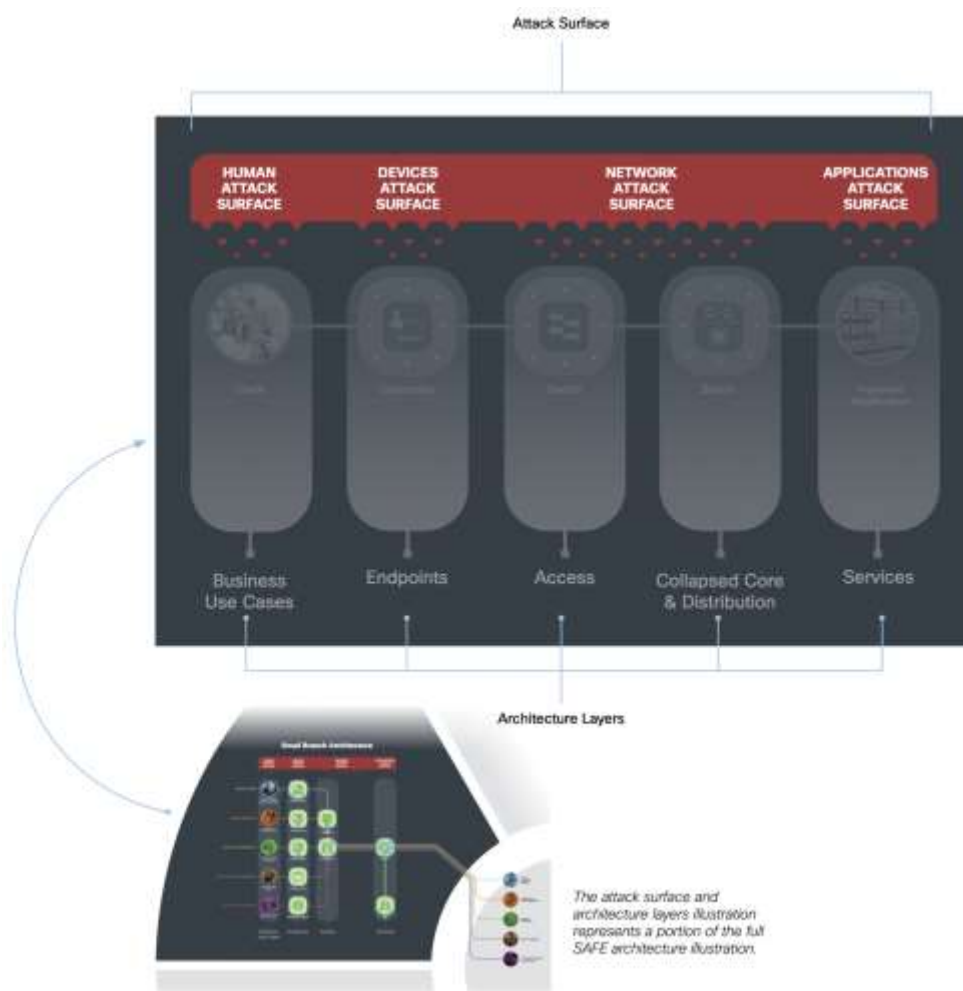


Figure 30. Alignment of attack surface to architecture layers

Attack Surface: Human

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



Figure 31. Human Attack Surface

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.



Figure 32. Identity Capability

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.



Figure 33. Device Attack Surface

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.



Figure 34. Client-Based Security Capabilities

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.



Figure 35. Network Attack Surface

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. This 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.



Figure 36. Network Capabilities

Attack Surface: Applications

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



Figure 37. Application Attack Surface

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.

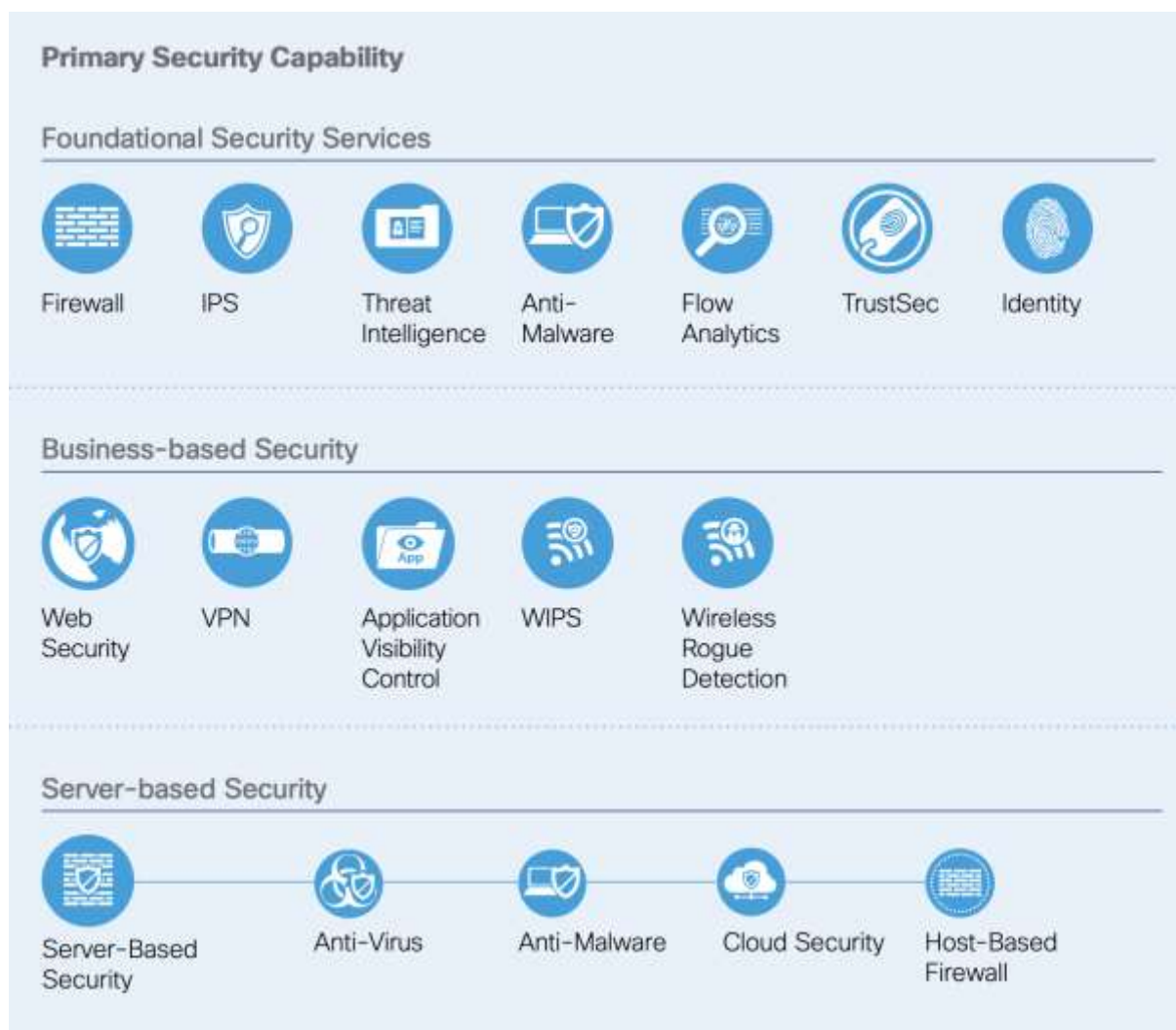


Figure 38. Application Capabilities

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

Appendix A – Business Flows

Internal Business Flows



Figure 39. Internal Business Flows

Third-Party Business Flows



Figure 40. Third-Party Business Flows

Customer Business Flows



Figure 41. Customer Business Flows

Appendix B - 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)