

# SAFE Architecture Guide

## Places in the Network: Secure Internet

December 2022

---

# Contents

Overview	3
<b>Cloud Taxonomy</b>	<b>4</b>
<b>Cloud Services</b>	<b>5</b>
<b>Cloud Responsibility</b>	<b>6</b>
Business Flows	6
<b>Functional Controls</b>	<b>8</b>
<b>Capability Groups</b>	<b>9</b>
Threats	10
Security Capabilities	11
<b>Human Attack Surface</b>	<b>11</b>
<b>Devices Attack Surface - Clients</b>	<b>12</b>
<b>Network Attack Surface - Analysis</b>	<b>13</b>
<b>Network Attack Surface - Cloud</b>	<b>14</b>
<b>Applications Attack Surface</b>	<b>15</b>
<b>Management</b>	<b>15</b>
Architecture	17
<b>Internet PIN</b>	<b>18</b>
Attack Surface	20
<b>Humans</b>	<b>20</b>
<b>Devices</b>	<b>20</b>
<b>Network</b>	<b>21</b>
<b>Applications</b>	<b>21</b>
Summary	21
Appendix	21
<b>Appendix A - Suggested Components</b>	<b>22</b>
<b>Appendix B - Feedback</b>	<b>23</b>

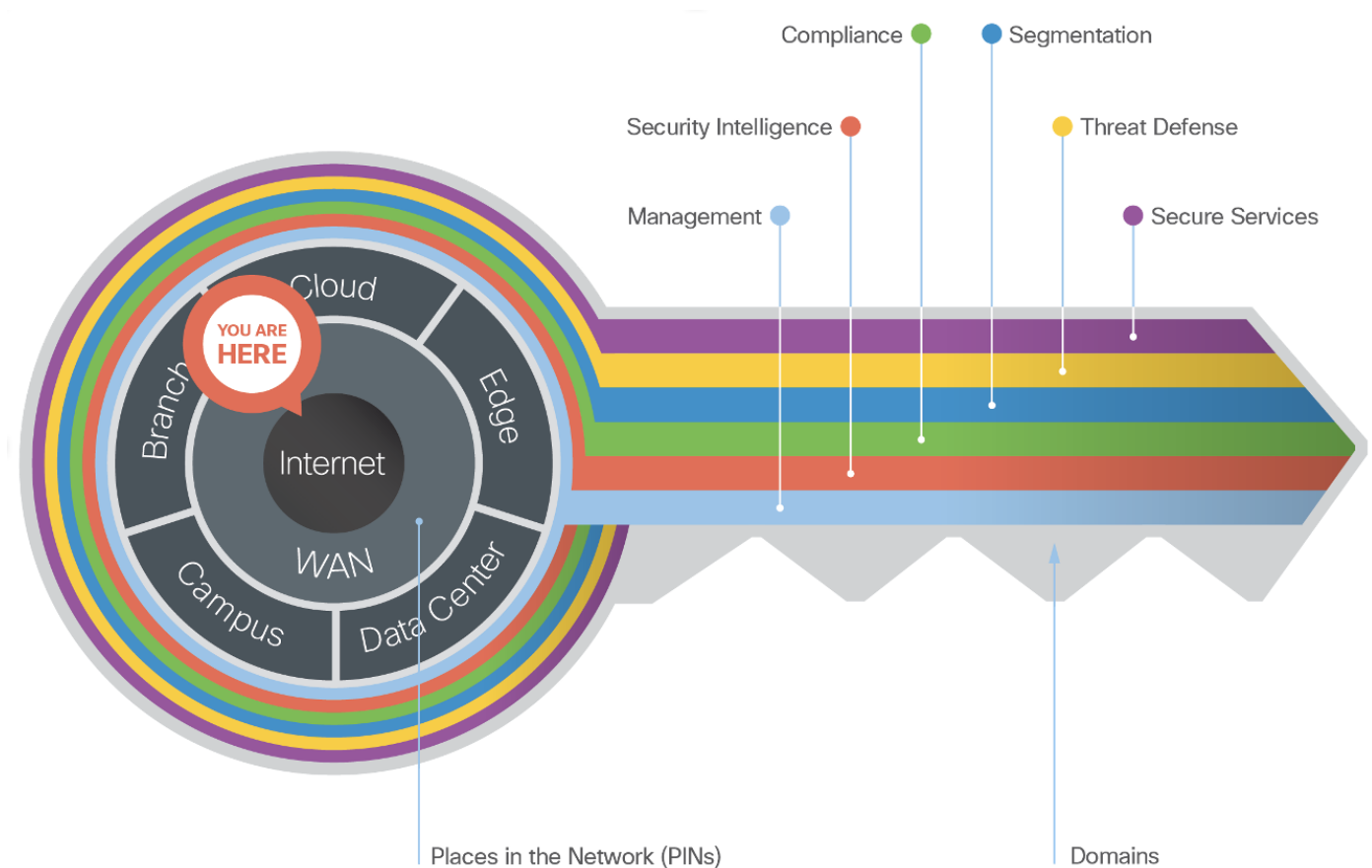
## Overview

The Internet is a place in the network (PIN) that provides access to applications. The applications can be delivered as Software as a Service (SaaS) in the Internet PIN, or delivered as hosted applications in the Cloud or Data Center PINs. This guide addresses Internet business flows and the security used to defend them. The focus of this guide is on the security controls necessary to provide “**security TO the cloud**”.

The Internet is one of the seven 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 Internet architecture guide provides:

- Business flows for the Internet
- Internet threats and security capabilities
- Business flow security architecture



**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.

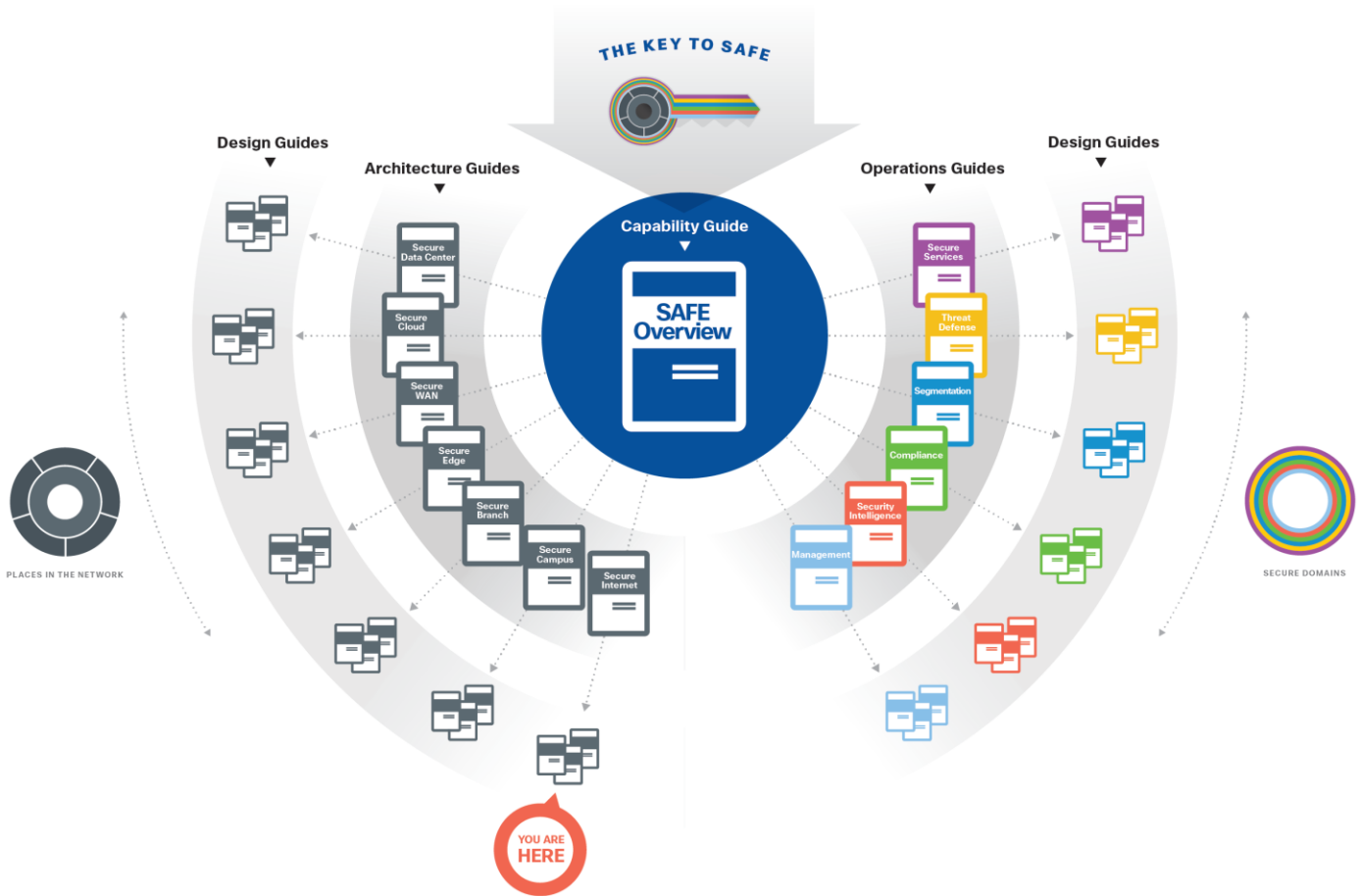


Figure 2. SAFE Guidance Hierarchy

## Cloud Taxonomy

The Internet is a collection of interconnected Information Technology (IT) and clouds. Terms of clouds varies by context, ownership and integration.

Table 1. Common Cloud Terms and Definitions.

Cloud Term	Definition
Cloud	Cloud computing enables convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Public Cloud	A style of computing where scalable and elastic IT-enabled capabilities are provisioned services out of multiple, private cloud and public cloud availability zones. Workloads are not ported between these zones.
Private Cloud	A style of computing where scalable and elastic IT-enabled capabilities are provisioned over IT infrastructure that is on-prem.

Cloud Term	Definition
<b>Hybrid Cloud</b>	A style of computing where scalable and elastic IT-enabled capabilities are provisioned services out of multiple, private and public cloud availability zones. Workloads are actively ported between these zones for reasons including cost, performance and availability.
<b>Multicloud</b>	A style of computing where scalable and elastic IT-enabled capabilities are provisioned services out of multiple, private cloud and public cloud availability zones. Workloads are not ported between these zones.
<b>Hybrid IT</b>	Hybrid IT is when an enterprise adds cloud-based services to complete their entire pool of IT resources. A hybrid IT model enables organizations to lease a portion of their required IT resources from a public/private cloud service provider.

## Cloud Services

Cloud Service Providers (CSP) provide public cloud services. CSPs deliver a variety of cloud services that can provide business application delivery. The following table lists the cloud service types, definitions and the corresponding SAFE PIN Architecture Guide the cloud service is covered under.

**Table 2.** Cloud Service Type, Definition and SAFE PIN coverage

Cloud Service Type	Definition	SAFE PIN Architecture Guide
<b>Software as a Service (SaaS)</b>	Software that is deployed over the internet. A provider licenses an application to customers either as a service on demand, through a subscription, in a “pay-as-you-go” model, or (increasingly) at no charge when there is opportunity to generate revenue from streams other than the user, such as from advertisement or user list sales.	Secure Internet
<b>Functions as a Service (FaaS)</b>	A cloud computing service that provides a platform allowing customers to develop, run, and manage application functionalities without the complexity of building and maintaining the infrastructure typically associated with developing and launching an application. Also referred to as Serverless.	Secure Cloud
<b>Platform as a Service (PaaS)</b>	A computing platform that allows the creation of web applications quickly and easily and without the complexity of buying and maintaining the software and infrastructure underneath it.	Secure Cloud
<b>Container as a Service (CaaS)</b>	A cloud service that allows software developers and IT departments to upload, organize, run, scale, manage and stop containers by using container-based virtualization.	Secure Cloud
<b>Infrastructure as a Service (IaaS)</b>	A way of delivering Cloud Computing infrastructure – servers, storage, network and operating systems – as an on-demand service. Rather than purchasing servers, software, datacenter space or network equipment, clients instead buy those resources as a fully outsourced service on demand.	Secure Cloud
<b>On-Prem</b>	IT services are provisioned over private IT infrastructure for the dedicated use of a single organization. The customer owns all costs for hosting the applications in a location they own.	Secure Data Center

## Cloud Responsibility

The customer selects the cloud service model which best serves the business need. The following figure represents the responsibility model between the Cloud Service Provider and the Customer.

SaaS (Software as a Service)	FaaS (Functions as a Service)	PaaS (Platform as a Service)	CaaS (Container as a Service)	IaaS (Infrastructure as a Service)	On-Prem (private cloud)	
Functions	Functions	Functions	Functions	Functions	Functions	
Applications	Applications	Applications	Applications	Applications	Applications	Cloud Service Provider Responsible
Runtime	Runtime	Runtime	Runtime	Runtime	Runtime	
Middleware or Containers	Middleware or Containers	Middleware or Containers	Middleware or Containers	Middleware or Containers	Middleware or Containers	Customer Responsible
Operating System	Operating System	Operating System	Operating System	Operating System	Operating System	Customer and Cloud Service Provider have Shared Responsibility
Virtualization	Virtualization	Virtualization	Virtualization	Virtualization	Virtualization	
Servers	Servers	Servers	Servers	Servers	Servers	
Storage	Storage	Storage	Storage	Storage	Storage	
Networking	Networking	Networking	Networking	Networking	Networking	

**Figure 3. Cloud Service Shared Responsibility Model**

On the far left, the Software as a Service (SaaS) cloud service has the cloud service provider being responsible for all costs.

On the far right, the On-Prem cloud service (i.e. private cloud) is a traditional data center deployment where the customer is responsible for all costs.

The cloud services between them have varying ownership responsibility. A customer needs to evaluate the service level agreements for all cloud services under consideration.

Runtime is a responsibility highlighted because with an On-Prem or IaaS deployment the customer owns runtime even if the servers sit idle. In a PaaS or FaaS deployment, a customer would only pay for the runtime that they used.

## Business Flows

The SAFE model is based on ten business flows as described in the SAFE Overview Guide. 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.

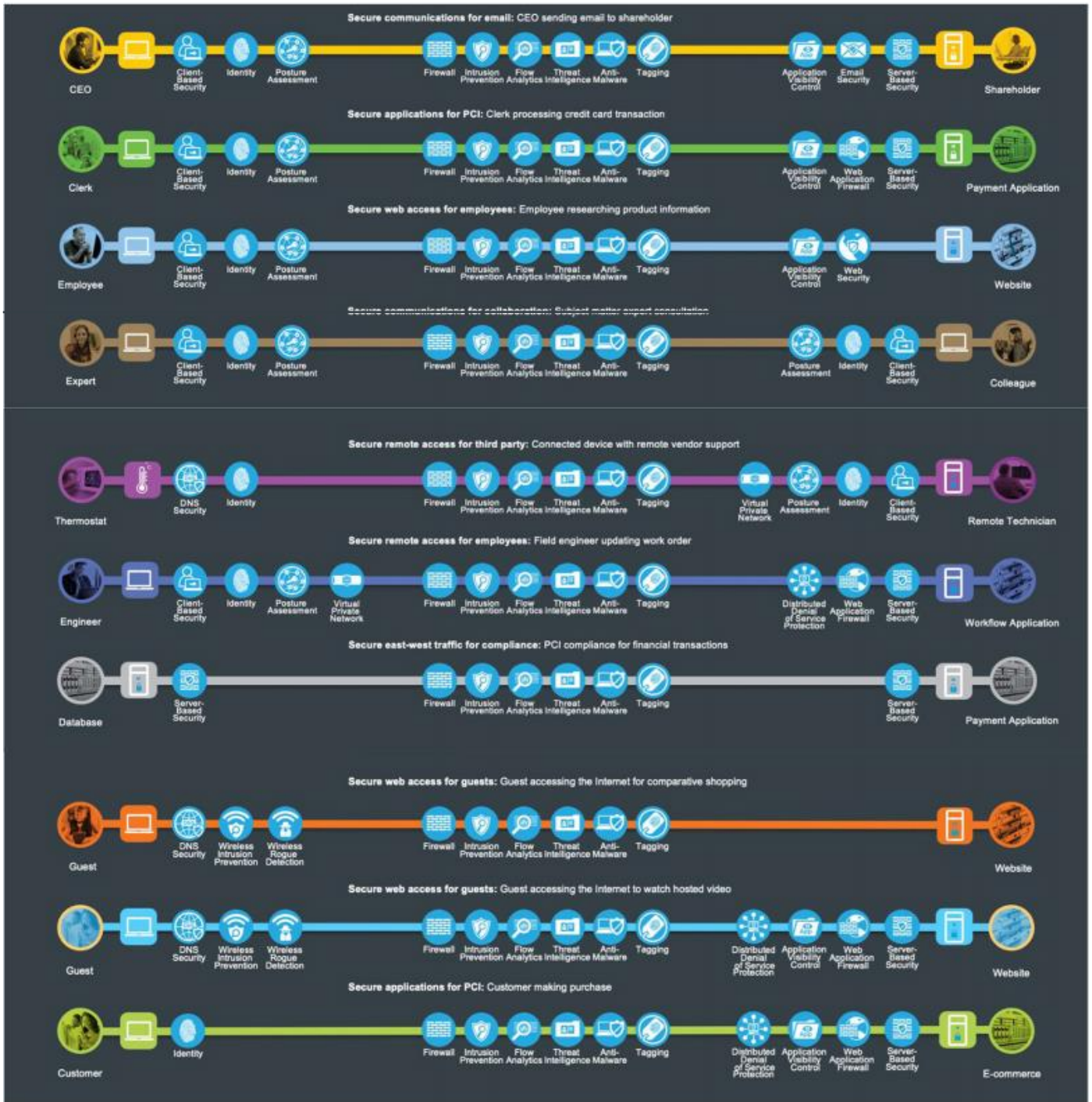
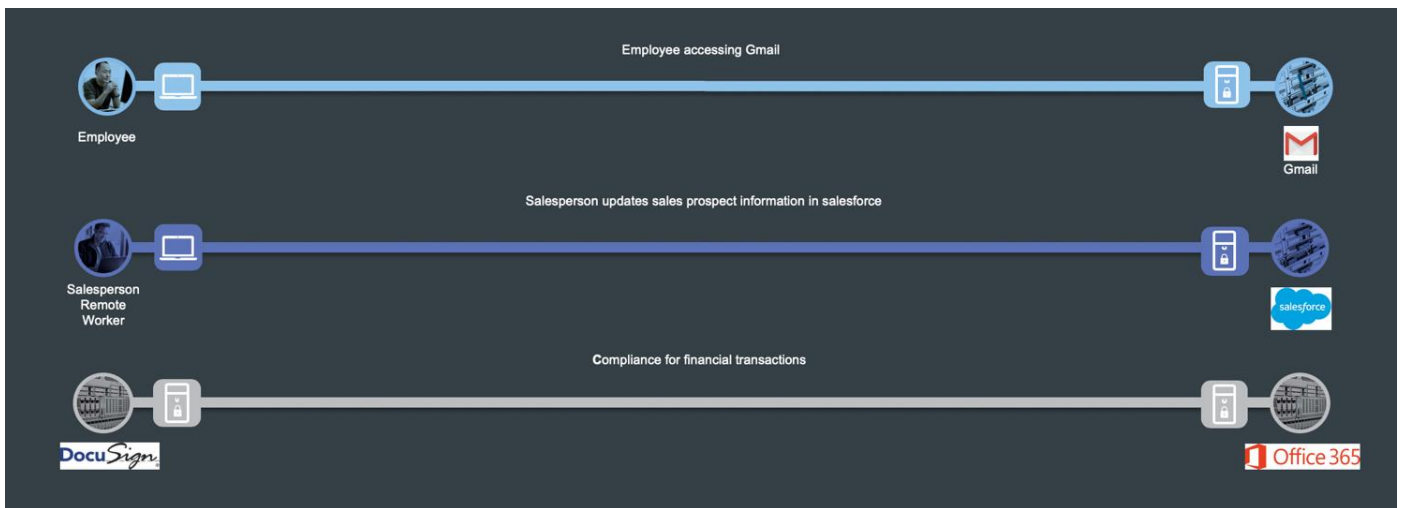


Figure 4. Business use cases are color coded to define where they flow

The Internet provides access to applications. Security “to the cloud” protects access to applications regardless of how the applications are delivered. All of the cloud service types in Table 2 are possible ways to deliver the application. This architecture guide is focused on Software as a Service (SaaS). The following are typical business flow examples for accessing public SaaS applications:

- Secure access to a sanctioned file repository
- Secure access to email
- Managing content within a sanctioned file repository
- Applying appropriate controls for an unsanctioned SaaS application
- Traveling user on a sanctioned application
- External partner collaborating in Office365
- IOT Device living within corporate network accessing public cloud
- Integrated application leveraging Office365 data

The three business flows this architecture guide focuses on to describe the capabilities required to secure the Secure Internet PIN are depicted in Figure 5.



**Figure 5. Internet business use cases are color coded to define where they flow**

The first business flow is an Employee accessing Gmail. In the SAFE model the Employee is located in the branch. The capabilities required in the branch and campus are the same and are documented in the Secure Branch and Secure Campus architecture guides. For simplicity this Employee can be considered in either the branch or campus.

The second business flow is a Salesperson connected directly to the Internet accessing Salesforce. The Salesperson is a remote worker accessing a SaaS application in the Internet.

Lastly, the third business flow represents two SaaS applications (DocuSign and Office365) located in the Internet communicating with each other. The business requires visibility and control capabilities for the traffic between the SaaS applications.

## Functional Controls

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

**Table 3. Functional Controls**



Cloud Term	Definition
Secure Access	Employee on campus or in branch access to the cloud (public, private, SaaS) must be secured.
Secure Remote Access	Secure remote access for employees and third-party partners that are external to the company network.
Secure East/West Traffic	Data moves securely; internally, externally, or to third-party resources.



Figure 6. Internet business flows map to functional controls based on the types of risk they present

## Capability Groups

Internet security is simplified by grouping capabilities into three groups which align to the functional controls: Foundational, Business, and Access. Each flow requires the access and foundational groups. Business activity risks require appropriate capabilities to control or mitigate them.

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

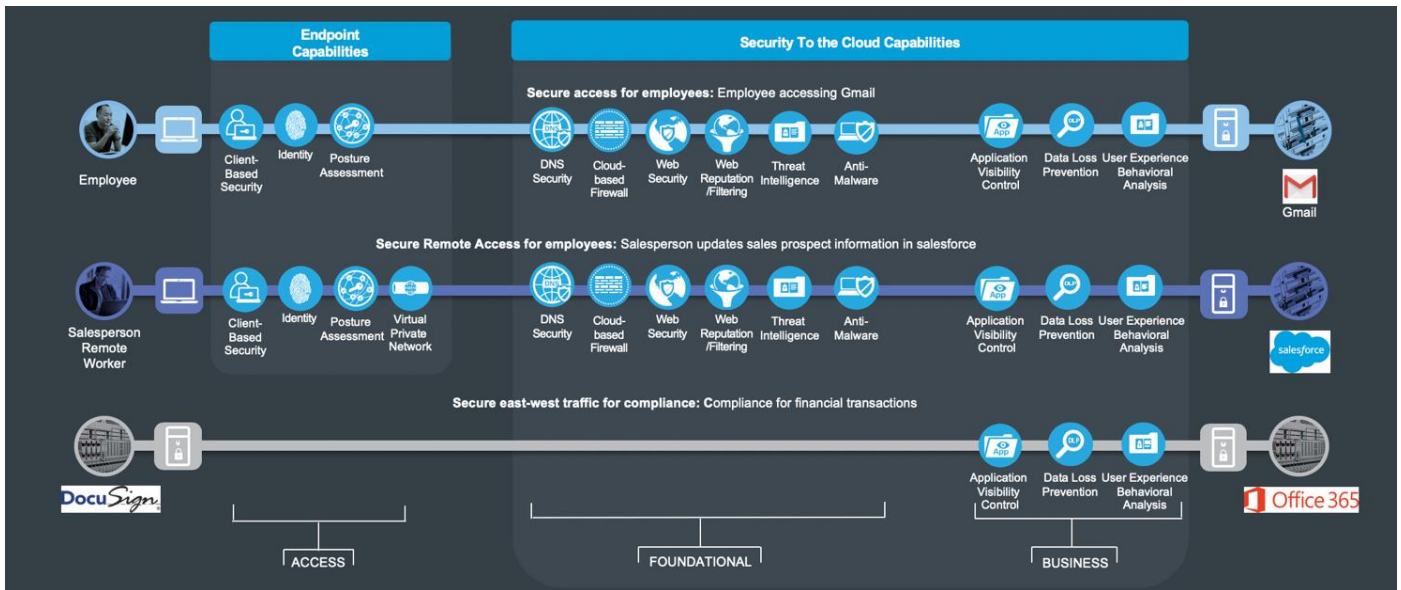


Figure 7. The Internet Business Flow Capability Diagram

Internet threats and capabilities are defined in the following sections.

## Threats

In the Internet, Software as a Service applications contain business information assets and intellectual property. These are the primary goals of targeted attacks and require the highest level of investment to secure.

### Unauthorized application access

Unauthorized access gives attackers the potential to cause damage, such as deleting sensitive files from a host, planting a virus, and hindering performance with a flood of illegitimate information.

### Malware propagation

Data assets in the public cloud SaaS are targets for malware attacks. Applications that process credit card transactions and Internet of Things devices are the most prevalent targets.

### Data extraction (data loss)

The unauthorized ex-filtration or theft of a company’s intellectual property, innovation, and proprietary company data.



# Security Capabilities

The attack surface of the Internet is defined by the business flows, and includes the people and the technology present. The security capabilities that are needed to respond to the threats in the Internet are mapped in Figure 8. The placement of these capabilities is discussed in the architecture section.

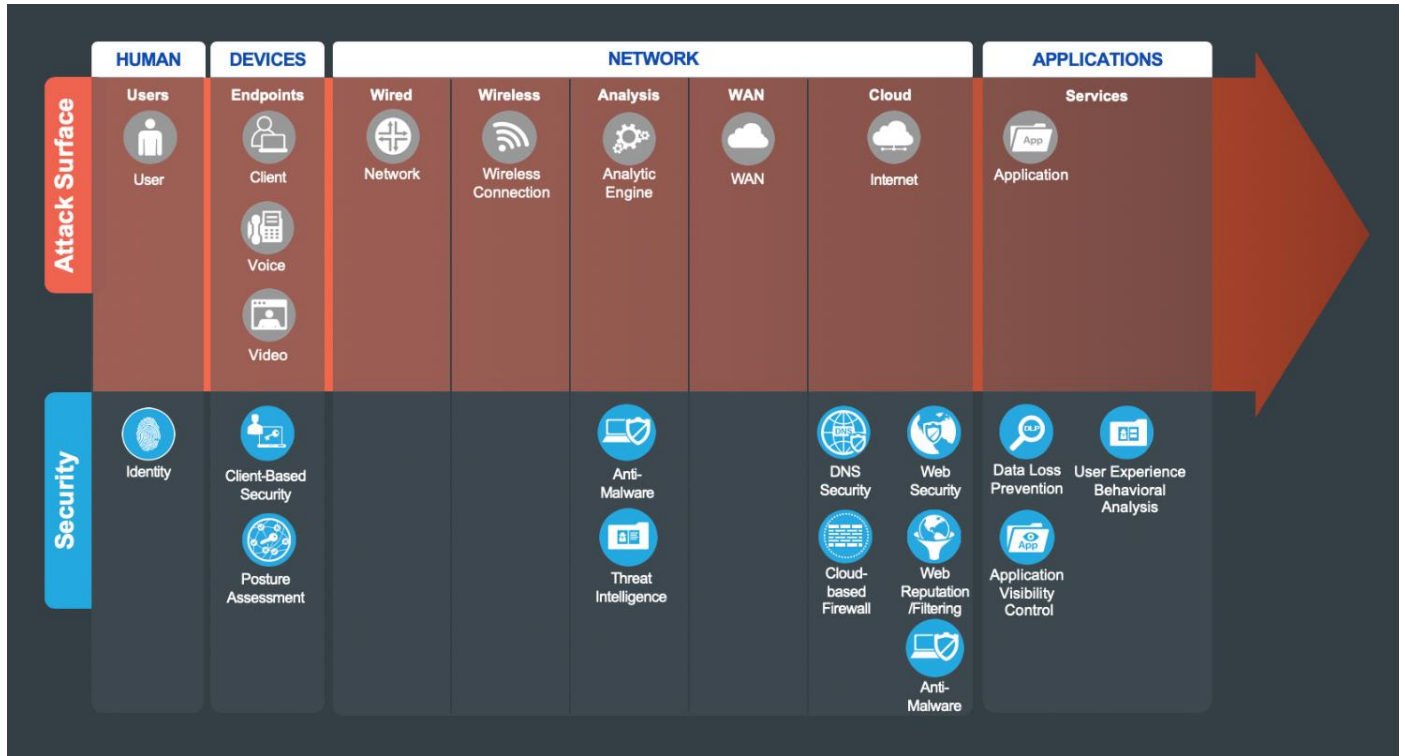


Figure 8. Internet Attack Surface and Security Capabilities – Security to the Cloud

Products that implement these capabilities can be found in Table 4 in the Appendix A.

## 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 - Analysis















Analysis of network traffic within the Internet.

Security Capability		Threat	
	<b>Anti-Malware:</b> Identify, block, and analyze malicious files and transmissions.		Malware distribution across networks or between servers and devices.
	<b>Threat Intelligence:</b> Contextual knowledge of existing and emerging hazards.		Zero-day malware and attacks.







## 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.
	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	
	Application Visibility Control (AVC)		Malicious and risky application usage.
	Data Loss Prevention (DLP)		Sensitive content.
	User Experience Behavioral Analysis (UEBA)		Compromised account.

## Management

### Management, Control, and Monitoring

Security Capability		Threat	
	Anomaly Detection: Identification of infected hosts scanning for other vulnerable hosts.		Malware distribution across services.
	Identity/Authorization: Centralized identity and administration policy.		Viruses compromising systems.
	Logging/Reporting: Centralized event information collection.		Redirection of session to malicious website.
	Monitoring: Network traffic inspection.		Unauthorized access and malformed packets connecting to server.
	Policy/Configuration: Unified infrastructure management and compliance verification.		Targeted attacks taking advantage of known vulnerabilities..
	Vulnerability Management: Continuous scanning, patching, and reporting of infrastructure.		Unauthorized access to system-stored data.

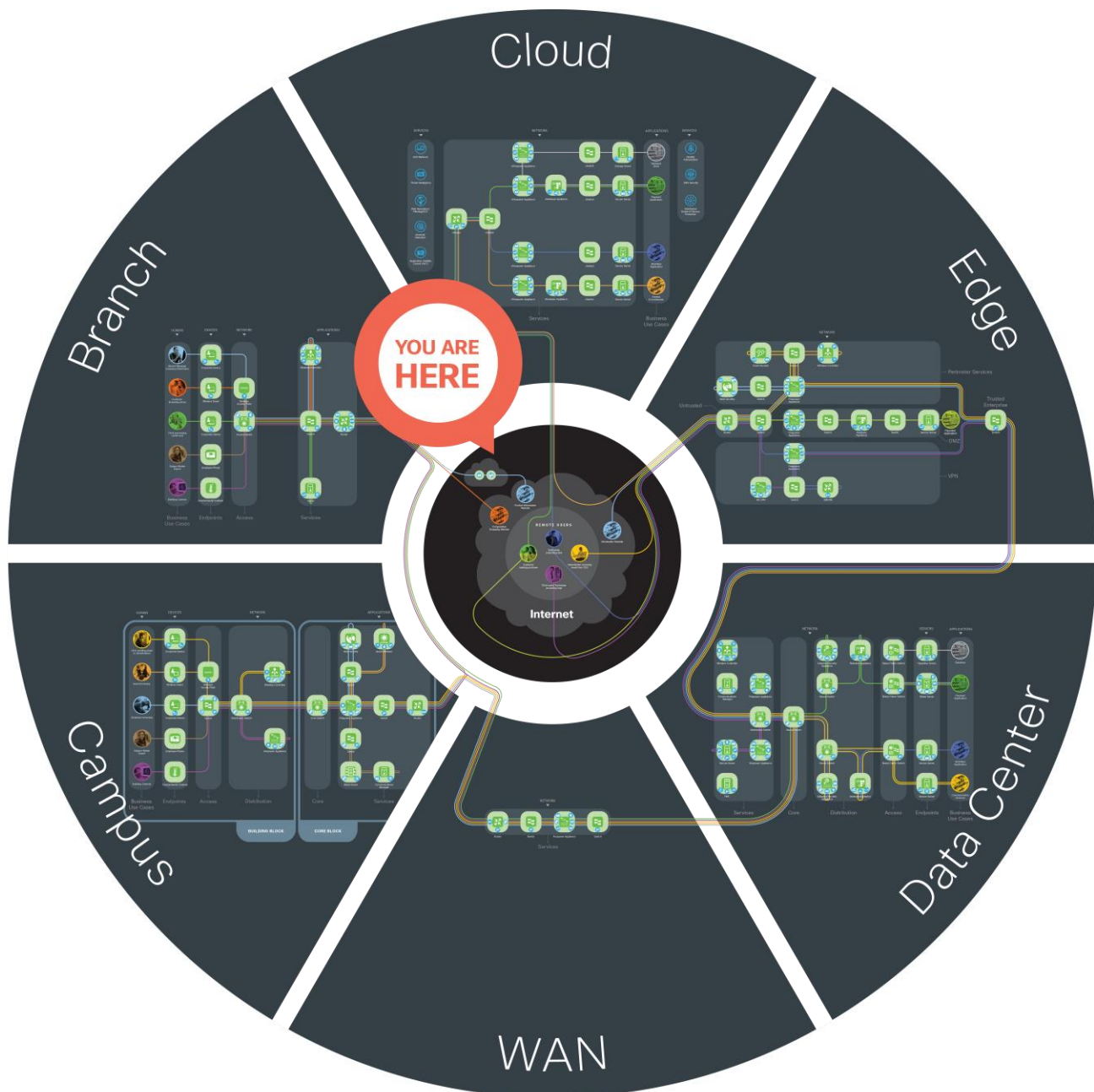




## Architecture

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.

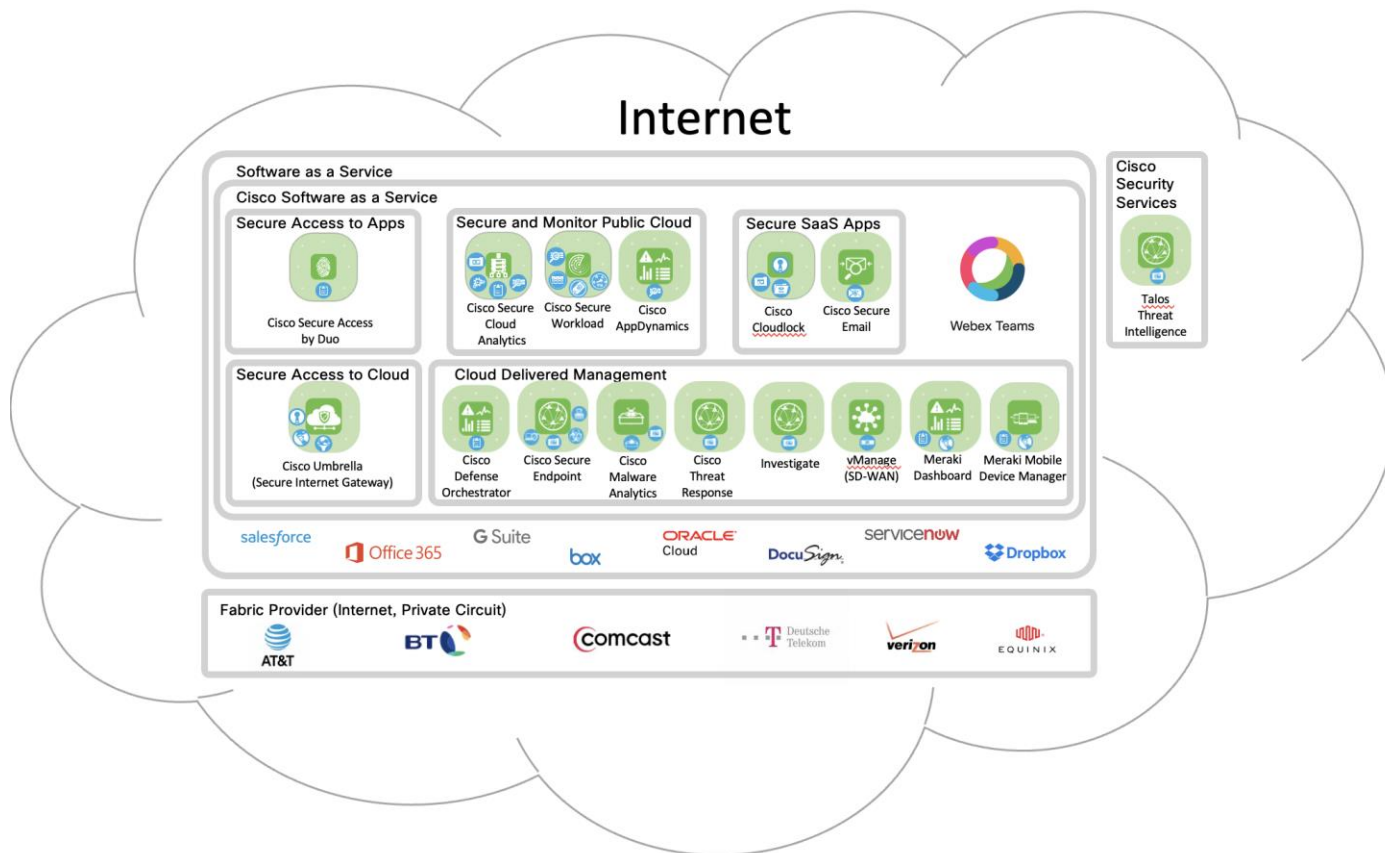
SAFE business flow security architecture depicts a security focus. Traditional design diagrams that depict cabling, redundancy, interface addressing, and specificity are depicted in SAFE design diagrams. Note that a SAFE logical architecture can have many different physical designs.



**Figure 9. SAFE Model. The SAFE Model simplifies complexity across a business by using Places in the Network (PINs) that it must secure.**

## Internet PIN

In the center of the SAFE model (Figure 9) is the Internet PIN. The Internet PIN is described below in Figure 10. At the highest level, Software as a SaaS (SaaS), Cisco Security Services, and Fabric Provider form the Internet PIN.



**Figure 10. Internet PIN.**

**Software as a Service** includes Cisco SaaS solutions as well as other vendor’s SaaS solutions. Cisco SaaS is a group of the security SaaS solutions as well as the Cisco Webex Teams collaboration also delivered with SaaS. There are several non-Cisco SaaS applications depicted above (Salesforce, Office365, G Suite, etc.). This is a sample list of SaaS applications and not a complete list.

The **Cisco Security SaaS** offers are broken up into 4 categories: Secure Access to Apps, Secure Access to Cloud, Secure and Monitor Public Cloud, Cloud Delivered Management, and Secure SaaS Apps.

**Secure Access to Apps** include the Identity solution Cisco Secure Access by Duo. Duo provides a unified access security and multi-factor authentication delivered through the cloud.

**Secure Access to Cloud** includes the Secure Internet Gateway solution Cisco Umbrella. Umbrella delivers complete visibility into internet activity across all locations, devices, and users, and blocks threats before they ever reach your network or endpoints.

---

**Secure and Monitor Public Cloud** solutions are deployed as SaaS but are used to secure applications in the public and private cloud and include:

- **Cisco Secure Cloud Analytics** improves security and incident response across the distributed network, from the private network and branch office to the public cloud
- **Cisco Secure Workload** is designed to secure, manage, and optimize applications and provide analytics on workloads throughout an enterprise (on-prem or public cloud, and is cloud delivered)
- **Cisco AppDynamics** is an Application Performance Management (APM) solution that is cloud delivered

**Cloud Delivered Management** is a collection of SaaS delivered management applications that include:

- **Cisco Defense Orchestrator (CDO)** is a cloud-based solution for managing security policy changes across Cisco security solutions
- **Cisco Secure Endpoint** is a security solution that addresses the full lifecycle of the advanced malware problem and can be cloud delivered
- **Cisco Secure Cloud Analytics** combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware and can be cloud delivered
- **Cisco Threat Response** is a cloud delivered solution that automates integrations across Cisco Security products and threat intelligence sources, accelerating critical security operations functions: detection, investigation and remediation
- **Investigate** provides a complete view of the relationships and evolution of Internet domains, IP addresses, and autonomous systems to pinpoint attackers' infrastructures and predict future threats. Investigate is cloud delivered and a component of Umbrella
- **vManage (SD-WAN)** provides the ability to manage all aspects of the WAN—from provisioning, monitoring, and upgrading routers to application visibility and troubleshooting the WAN, and is delivered from the cloud
- **Meraki Dashboard** is cloud based management that provides centralized visibility & control over Meraki's wired & wireless networking hardware
- **Meraki Mobile Device Manager** provides unified management of mobile devices, Macs, PCs, and the entire network from a centralized dashboard, and is delivered from the cloud

**Secure SaaS Apps** is a collection of Security applications focused on securing other SaaS applications and delivered as SaaS and they include:

- **Cisco Cloudlock** is an API-based Cloud Access Security Broker (CASB) that helps accelerate use of the cloud, and protects your cloud users, data, and applications
- **Cisco Secure Email** provides an infrastructure that is maintained in resilient and geographically diverse Cisco data centers. The service provides email security delivered as SaaS

**Cisco Security Services** are cloud services that are utilized by Cisco security solutions but not delivered as SaaS and they include:

- **Talos** is a Security Intelligence and Research Group made up of leading threat researchers supported by sophisticated systems to create threat intelligence for Cisco products that detects, analyzes and protects against both known and emerging threats

---

The **Fabric Providers** enable the Internet and also provide private circuits. The vendors listed are some of the major players but not a complete list.

Normally in a SAFE architecture guide we would name the architecture icon with a generic name in the green icons. In this case, all production services are deployed today so adding another layer of generic naming is of arguable benefit at this time.

## Attack Surface

The Internet Attack surface (Figure 8) consists of Humans, Devices, Network, and Applications. A successful breach gives an attacker the “keys to the kingdom”.

Security includes these considerations:

- Human administrators can be located anywhere
- Network security requires cloud security to secure access to applications, detect malware, control access to sanctioned applications, and connect the software defined WAN technology.
- Applications and data contain vital company information

The sections below discuss the security capability that defends the threats associated with each part of the attack surface.

### Humans

Typically, humans are administrators for the secure data center, secure cloud and public SaaS applications .

No amount of technology can prevent successful attacks if the administrators themselves are compromised. Administrators that are disgruntled (fired, demoted, bullied, ideology), compromised (blackmail, threats, bribery), or have had their credentials stolen (phishing, key logger, password reuse) are the single biggest risk in the security of a company.

Administrators have a higher level of access than normal users which requires additional controls:

- Multi-factor authentication
- Limited access to job function
- Logging of administrator changes
- Dedicated, restricted workstations
- Removal of old administrator accounts

The primary security capability is Identity. One of the primary threats is “Unauthorized Network Access”. A strong Identity solution is required to mitigate against this threat.

### Devices

The administrator’s device (i.e. laptop, tablet) is used to access tools that administrators use to control and monitor systems that maintain and secure the business applications whether they are secure data center, secure cloud or public SaaS applications. Administrators connect to centralized management systems using secure connectivity with strong encryption (SSH, TLS, VPN) and multi-factor authentication from a variety of devices.

---

The primary security capabilities are Client-Based Security and Posture Assessment for the device. Client-Based Security includes VPN client, Anti-Malware and Secure Internet Gateway capabilities. These are the Access capabilities required for the Internet Attack surface described in Figure 8.

## Network

Cloud security protects the network attack surface for all users accessing applications. The applications can be in various PINs and delivered with varying underlying technologies but the security capabilities required are common. The cloud services SaaS, Serverless, PaaS, CaaS, IaaS and On-Prem are the application deployment possibilities.

Cloud security includes several security capabilities. The primary security capabilities are DNS Security, Cloud-based Firewall, SD-WAN, Web Security, Web Reputation, Cloud Access Security Broker (CASB), Anti-Malware and Threat Intelligence. These are the Foundational capabilities required for the Internet Attack surface described in Figure 8.

One of the primary threats is “Malware propagation”. To mitigate against this threat, the anti-malware solution should operate in-line with the traffic as well as with data at rest in the cloud.

## Applications

To secure access to applications beyond foundational and access capabilities, business capabilities must be deployed to manage business risks introduced by the business practice. The primary security capabilities are Data Loss Prevention, Application Visibility Control, Cloud Access Security Broker (CASB) and User Experience Behavior Analysis (UEBA). These are the Business capabilities required for the Internet Attack surface described in Figure 8.

One of the primary threats is “Data extraction (data loss)”. A data loss prevention solution is required to mitigate against this threat.

## Summary

Today’s companies are threatened by increasingly sophisticated attacks. Public Cloud SaaS services are targeted because they store the company’s data.

Cisco’s Cloud Security architecture and solutions defend the business against corresponding threats using an architectural approach that overcomes the limitations of a point product offering.

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

## Appendix

## Appendix A - Suggested Components

Internet Attack Surface		Security Capability		Suggested Cisco Components
Human	Users		Identity	Cisco Secure Access by Duo Cisco Meraki Mobile Device Management
Devices	Endpoints		Client-based Security	Cisco AnyConnect Secure Mobility Client Cisco Secure Endpoint Cisco Umbrella
			Posture Assessment	Cisco AnyConnect Secure Mobility Client Cisco Identity Services Engine (ISE) Cisco Meraki Mobile Device Management Cisco Secure Access by Duo
Network	Analysis		Anti-Malware	Cisco Secure Endpoint
			Threat Intelligence	Talos Threat Intelligence Cisco Threat Response
	Cloud		Cloud Security	Cisco Umbrella
			DNS Security	Cisco Umbrella
			Cloud-based Firewall	Cisco Umbrella
			Web Security	Cisco Umbrella
			Web Reputation/Filtering	Cisco Umbrella

Internet Attack Surface		Security Capability		Suggested Cisco Components
Applications	Application		Application Visibility Control	Cisco Cloudlock Cisco Umbrella
			Data Loss Prevention	Cisco Cloudlock Cisco Umbrella
			User Experience Behavior Analysis	Cisco Cloudlock

## 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](mailto:ask-security-cvd@cisco.com).

For more information on SAFE, see [www.cisco.com/go/SAFE](http://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)