Cisco Secure Access Service Edge (SASE) and Security Service Edge (SSE)

Architecture Guide

September, 2023

Contents

Introduction 3

SASE 5

Security Service Edge 6

Software Defined WAN 12

Digital Experience Monitoring 14

Cisco SASE/SSE Architecture 15

Cisco SAFE Business Flows 16

Attack Surfaces 17

Cisco SAFE Capabilities 20

Cisco SAFE Business Flows - Capability Mappings 29

SASE/SSE Reference Architecture 30

Appendix 37

Appendix A – SASE/SSE Reference Architecture Security Capabilities 37

Appendix B – SASE/SSE Reference Design 42

Appendix C – SASE/SSE Detailed Business Flows with Capabilities 46

Appendix D – Acronyms Defined 51

Appendix E - References 53

Appendix F - Feedback 53

Introduction

Today’s workforce expects seamless access to applications wherever they are, on any device. With the rise of remote work, the growing push of company data and infrastructure into the cloud, and the increasing number of cloud applications such as Office 365 and Salesforce utilized by the workforce, the amount of traffic directed to the Internet has increased significantly. The need for cloud-enabled security services expands daily as contractors, partners, IoT devices and more each require network access no matter where they are. IT needs to protect and ensure optimal application performance for users and devices as if they were located at a corporate office or branch. Each requires secure access to applications and must now be treated as a ‘branch of one.’

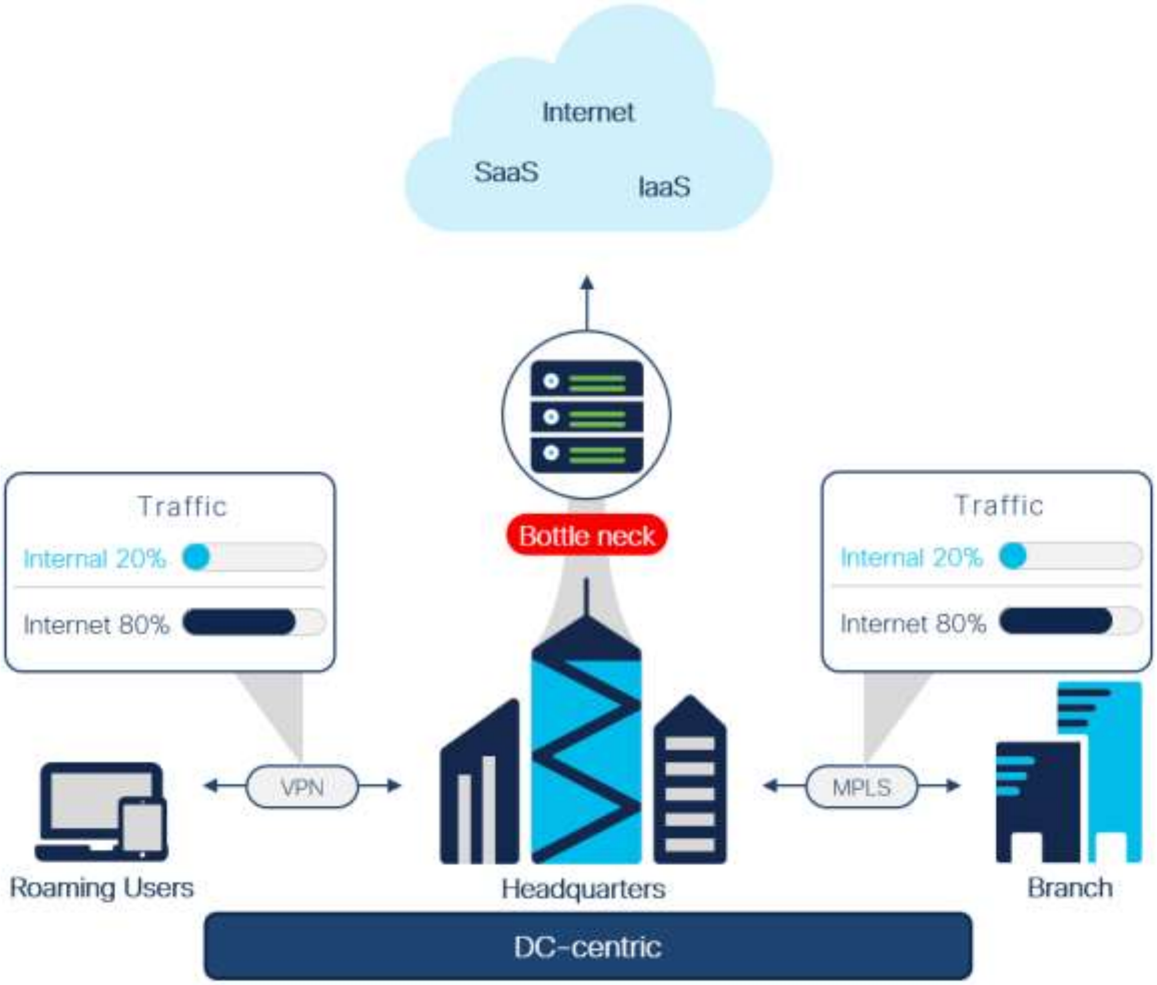


Figure 1.
High level DC-Centric Architecture

Because of these changes, the DC-centric model has become costly and inefficient for handling this traffic. Consider the following:

- Remote work and hybrid work are here to stay as people work from anywhere on a continuous basis. This makes user mobility is a paramount capability for modern enterprises
- Distributed users and applications are hard to manage and increase security risk due to a larger attack surface
- There are significant problems with application performance and user experience using traditional networking architectures with modern cloud applications

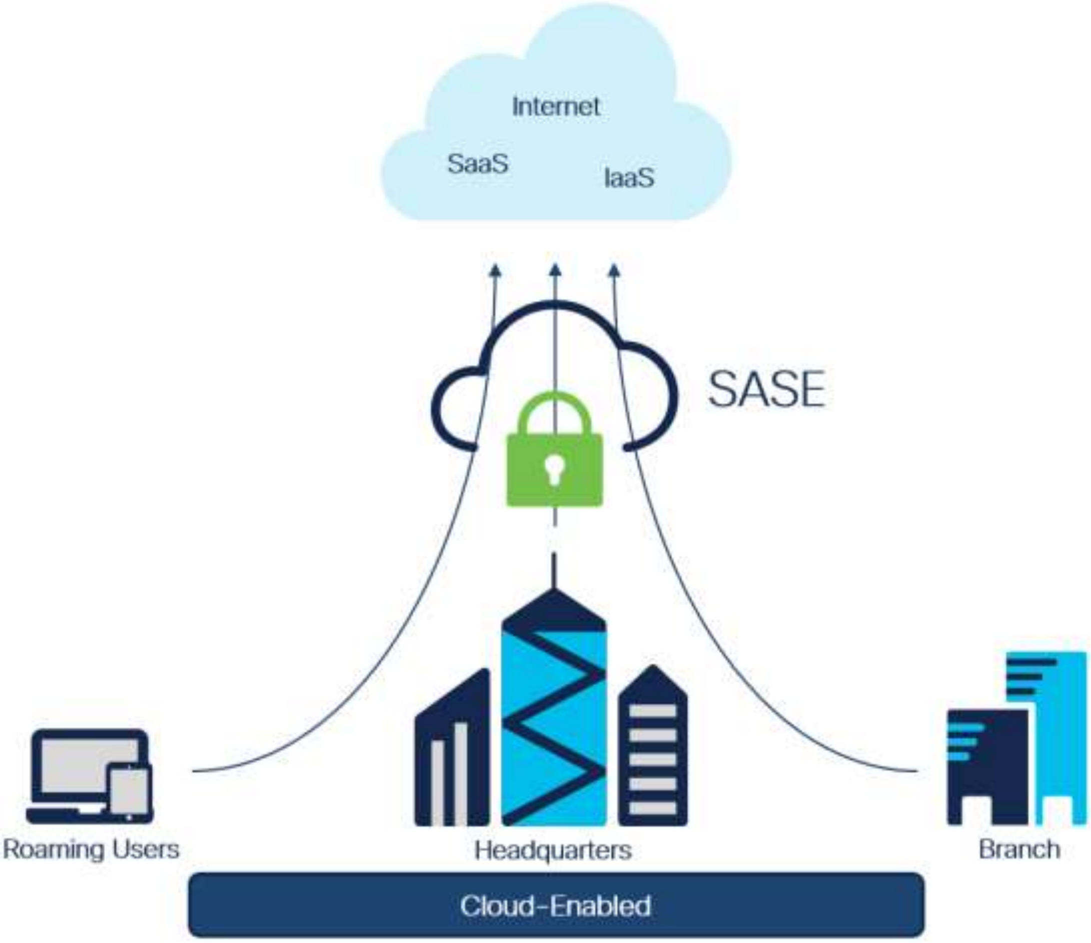


Figure 2.
High level SASE Architecture

In this new paradigm, IT requires a simple and reliable approach to protect and connect with agility. This is forcing a convergence of network and security functions closer to users and devices, at the edge—and is best delivered as a cloud-enabled model called secure access service edge (SASE).

SASE

In 2019, Gartner published a report called The Future of Network Security Is in the Cloud. In this report, Gartner introduced the SASE concept. Back in 2017, several vendors and analysts in the industry defined a new concept – the secure Internet gateway (SIG). This cloud native solution offers multiple functions including domain name system (DNS) security, secure web gateway (SWG), firewall as a service (FWaaS), and cloud access security broker (CASB) to improve security and performance while reducing costs and maintenance tasks. The SASE concept goes beyond the capabilities found within SIG and includes the convergence of networking functionality as well.

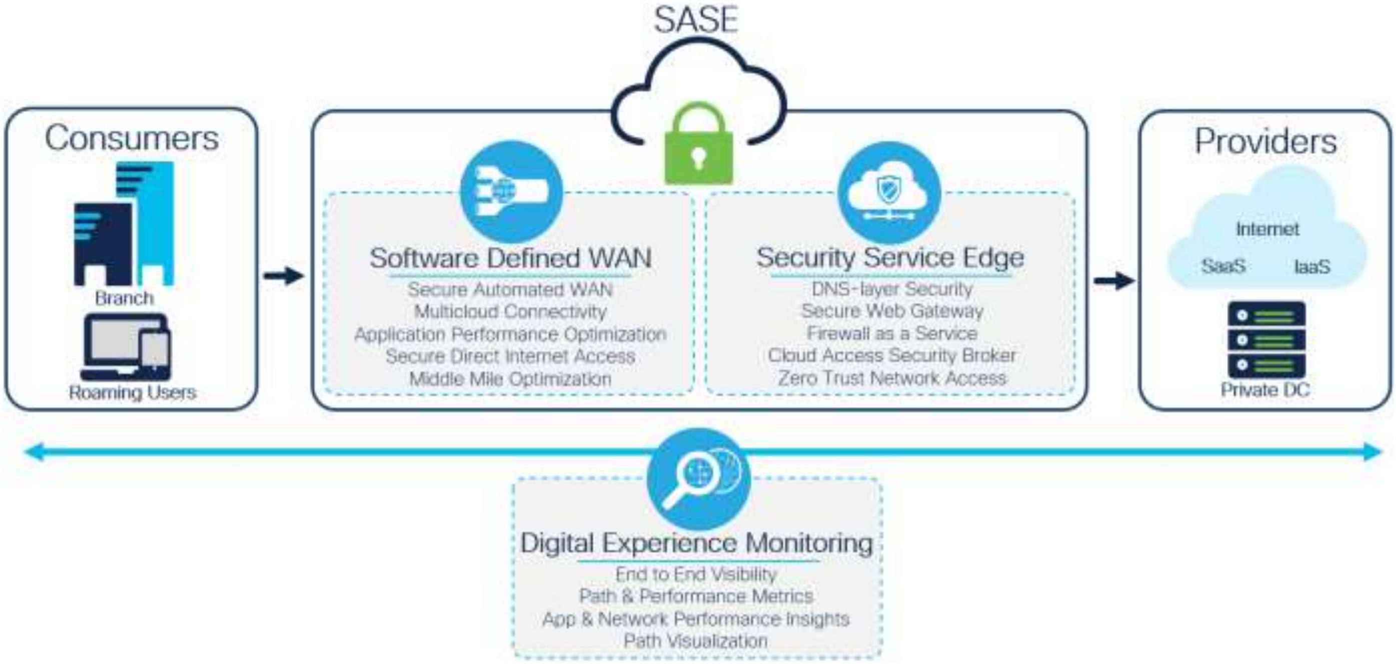


Figure 3.
SASE Capability Overview

Cloud computing services offer convenient, pay-as-you-go models that eliminate costly expenditures and maintenance. Cloud providers host a choice of infrastructure, platform, and software offerings on-site that you “rent”, giving your organization the flexibility to turn cloud computing services up and down according to changing requirements. There are three main cloud computing service options:

- **Infrastructure-as-a-Service (IaaS)**: In this model, a cloud provider hosts infrastructure components that are traditionally located in on-premise data centers. With IaaS, your organization can choose when and how you want to administer workloads, without needing to buy, manage, and support the underlying infrastructure
- **Platform-as-a-Service (PaaS)**: This model is one layer of abstraction above IaaS. Cloud providers, in addition to providing infrastructure components, also host and manage operating systems and middleware that your developers need to create and run applications
- **Software-as-a-Service (SaaS)**: With SaaS, cloud providers host and manage an entire infrastructure, as well as end-user applications. When your company chooses a SaaS model, you do not need to install anything; your users will be able to log in and begin immediately using the cloud provider’s application running on their infrastructure

The goal of SASE is to provide secure access to applications and data from your data center or cloud platforms like Azure, AWS, Google Cloud, and SaaS providers based on:

- **Identity**: limiting application access to specified users and devices
- **Context**: risk-based assessment to prevent questionable users or compromised/insecure devices from accessing the network
- **Least Privilege**: limit user and device access to only services that have been defined for their usage

Service edge refers to global point of presence (PoP), IaaS, or colocation facilities where local traffic from branches and endpoints is secured and forwarded to the appropriate destination without first traveling to data center focal points.

The Software Defined WAN (SD-WAN) and Security Service Edge (SSE) components of SASE are primarily delivered as Networking-as-a-Service (NaaS) and Security-as-a-Service (SECaaS) models. This refers to the ability to offer these services as SaaS. By delivering security and networking services together from the cloud, organizations will be able to securely connect any user or device to any application without having to install and maintain the network management and security infrastructure.

Security Service Edge

Cloud adoption, distributed workforces, and threats have been on the rise for years. As more users connect to company networks from anywhere that has an internet connection, more data is being routed outside of traditional on-premises data centers, creating security gaps that traditional DC-centric network architectures aren't built to handle.

In 2021, Gartner coined a new concept for businesses who may be ready to transition to cloud security without a complete overhaul of their network architectures SASE requires. This concept is known as Security Service Edge. The SSE architecture is a collection of security functions that can reduce complexity and improve user experience by consolidating multiple disparate security capabilities and delivering them from the cloud. These security functions include, but are not limited to, DNS-layer security, secure web gateway, firewall as a service, cloud access security broker, and zero trust network access.

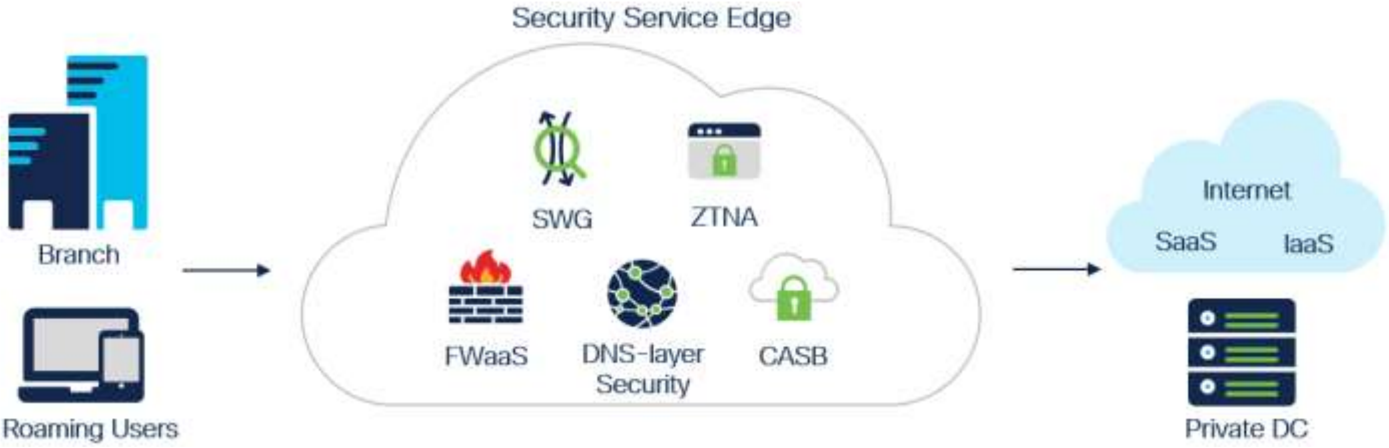


Figure 4.
Security Service Edge Capability Overview

Because of this, organizations have flexibility in determining whether to deploy SSE or move towards a full SASE deployment. The answer may vary by each organization's own unique needs. For organizations with a hybrid workforce, however, when the additional security features of SSE are paired with the enhanced connectivity features of SASE, the organization gets a holistic solution that protects uses and devices from threats while boosting network performance. A full SASE solution makes it easier than ever to scale up or down an increasingly distributed workforce. While moving towards SSE may be a first step, journeying beyond SSE to include the network component may be in the best interest of organizations in a hybrid world.

Whether included in an SASE architecture or deployed standalone, a Security Service Edge architecture should:

- Provide secure seamless access for users
- Provide security with consistent policy
- Update threat protection and policies without hardware and software upgrades
- Restrict access based on identity and context
- Increase security staff effectiveness with centralized policy management

DNS-layer Security

DNS resolution is the first step when a user attempts to access a website or other service on the Internet. DNS-layer Security logs and categorizes DNS activity by type of security threat or web content and the action taken, whether it was blocked or allowed.

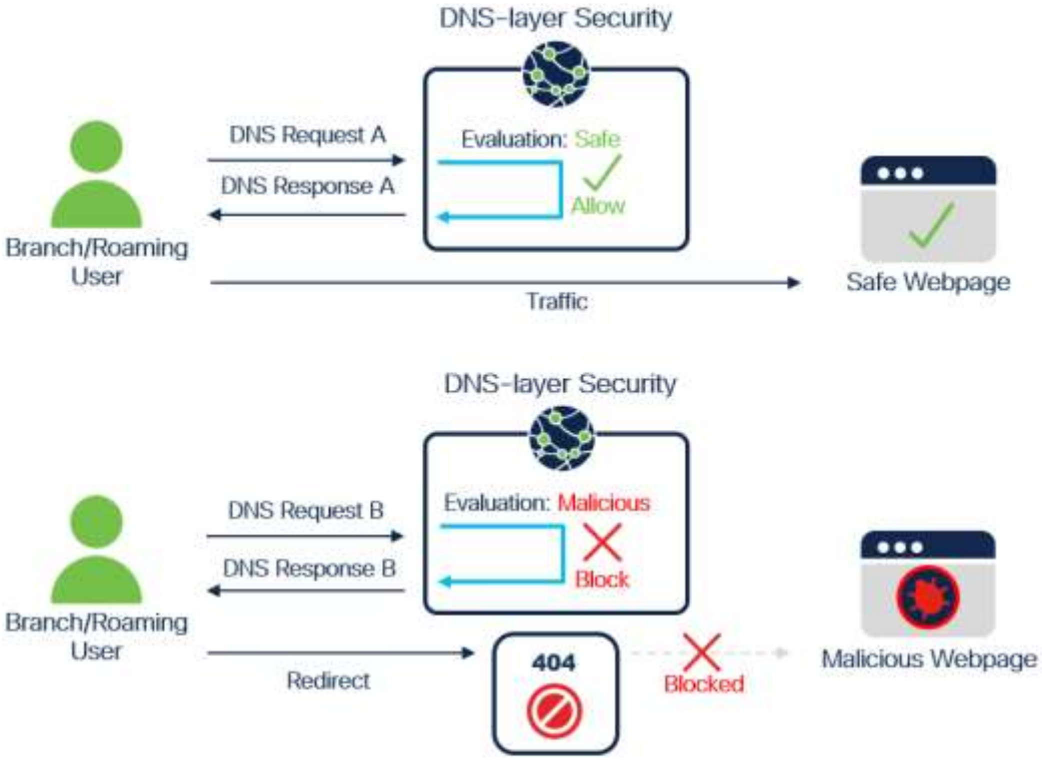


Figure 5.
DNS-layer Security Overview

It is critical that the DNS-layer security is underpinned by excellent threat intelligence sources. Threat intelligence itself is not a solution but is a crucial security architecture component. A threat intelligence platform centralizes the collection of threat data from numerous sources and formats and most importantly presents the data in a usable format.

Secure Web Gateway

A cloud-based web proxy or SWG provides security functions such as URL and category filtering and real-time inspection of inbound files for malware and other threats. SSL/TLS decryption is necessary to inspect encrypted web traffic before other certain SWG security capabilities can enforced. Content filtering by category or specific uniform resource locators (URLs) is used to block destinations that violate policies or compliance rules. Remote browser isolation protects users from potential malware and other threats by redirecting browsing to a cloud-based host. This isolation is achieved by serving the web content to users via a remotely spun up surrogate browser located in the cloud.

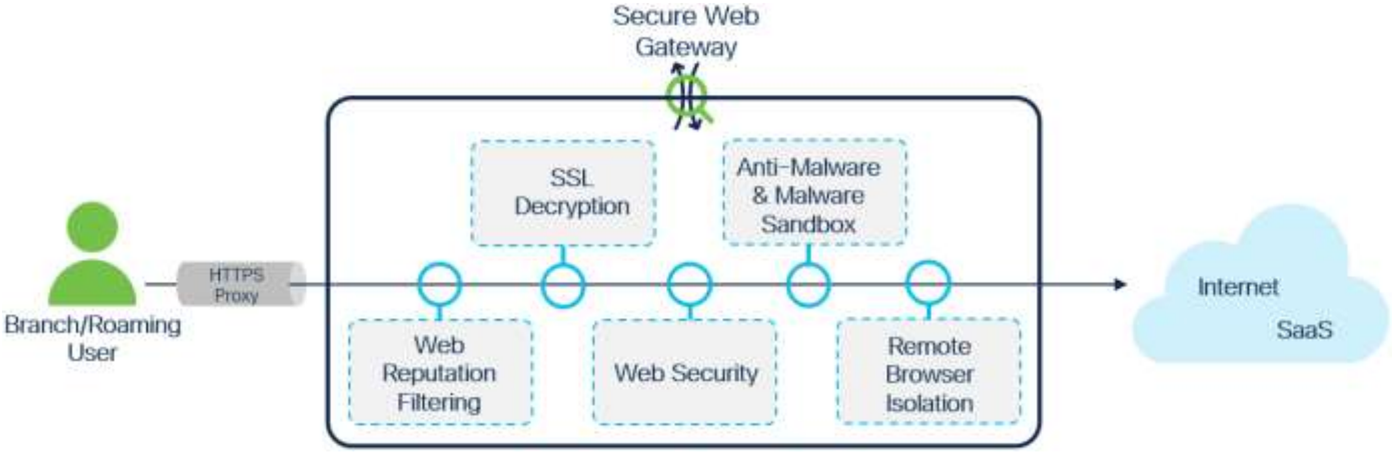


Figure 6.
Secure Web Gateway Overview

Network anti-malware inspects files as they traverse the network, using dynamic threat intelligence to check the disposition of files before they reach the device. File sandboxing is used to open and inspect untrusted files which could compromise an endpoint.

Firewall As a Service

Firewall as a Service (FWaaS) is the cloud-based delivery of firewall functionality to protect non-web Internet traffic. In addition to layer 3-4 filtering, FWaaS typically includes features for intrusion prevention and application-level visibility and control.

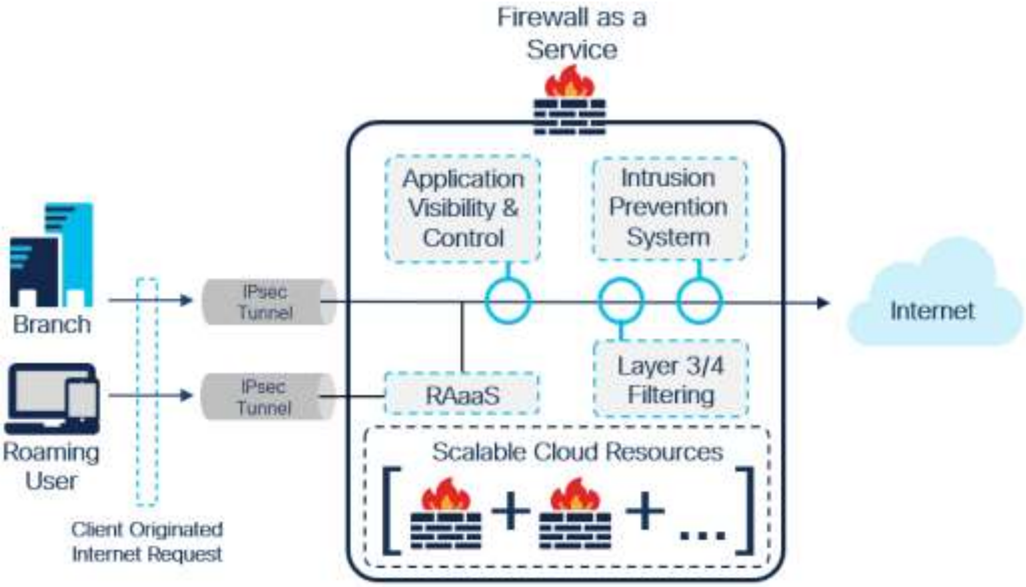


Figure 7.
Firewall as a Service Overview

Some of the benefits provided by FWaaS when compared to on-premises firewalls include:

- Scalable due to the pool of resources available to cloud-delivered firewalls allowing easy growth or contraction based on an organization's need
- Centralized policy management for multiple remote locations
- Easier to deploy and maintain

Remote Access as a Service (RAaaS) provides cloud-delivered VPN services for roaming users covering use cases for applications or services that ZTNA solutions do not support. Like FWaaS, RAaaS provides a scalable alternative to on-premises VPN solutions and in addition to private application access, enables roaming users to receive security capabilities provided by through the FWaaS such as Layer 3-4 traffic filtering and intrusion prevention. RAaaS should still follow zero trust principles, incorporating multi factor authentication (MFA), context checks, and least privilege access to private applications.

Cloud Access Security Broker

Cloud access security brokers help control and secure the use of SaaS applications. The value of CASBs stems from their capability to give insight into cloud application usage across cloud platforms and to identify unsanctioned use. CASBs use auto discovery to expose shadow IT, detecting and reporting on the cloud applications that are in use across the network.

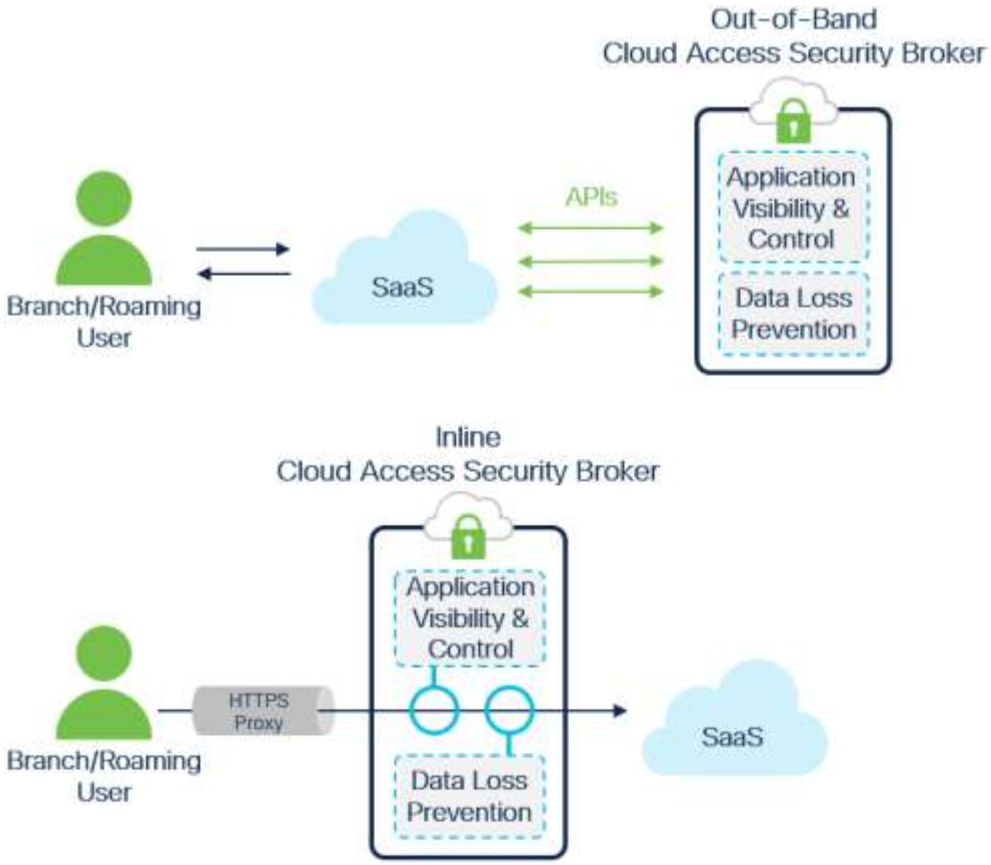

Out-of-Band
Cloud Access Security Broker
APIs
Branch/Roaming User
SaaS
Application Visibility & Control
Data Loss Prevention
Inline
Cloud Access Security Broker
Application Visibility & Control
HTTPS Proxy
Branch/Roaming User
SaaS
Data Loss Prevention

Figure 8.
Cloud Access Security Broker Overview

A vital ability of CASB is data loss prevention (DLP) - the capability to detect and provide alerts when abnormal user activity occurs to help stop both internal and external threats.

Although included as part of CASB, inline DLP warrants its own mention and provides data security for user traffic traversing the Internet or traversing data centers to utilize private applications. A common CASB deployment is to install out of band and to provide API based DLP functionality. For increased security, DLP should be implemented as a standalone inline feature of the SASE security stack to catch sensitive information as it passes through the network. This can then be supplemented with DLP capabilities built into a CASB.

Zero Trust Network Access

In a DC-centric model roaming users are provided remote access to resources using full tunnel VPN, redirecting all traffic, internal and internet destined, to the data center. Scalability issues can arise as users shift between on-premises and remote work and VPN appliances are starved for resources. User experience suffers as backhauled traffic causes high latency and users must enter credentials numerous times during the workday creates password exhaustion. In a cloud-enabled model, access can be provided to private or public applications leveraging a clientless or client based zero trust network access solution.

Zero Trust security takes a “never trust, always verify” approach to security. To do this, it is essential to verify identity and context. Identity is determining who a user is. Traditional identity checks use passwords, but these can be stolen, or brute forced making password-only identity checks unreliable forms of identity verification. Context is the use of supplemental information to improve security decisions at the time they are made according to Gartner. This supplemental information may include, but is not limited to, OS version, browser version, firewall status, and location. An assessment is done based on this information to determine if access should be allowed to the application based on the calculated risk. For example, the security policy for a restricted application could require the user to use an updated browser not susceptible to certain vulnerabilities. ZTNA verifies a user’s identity and context before granting least privilege access to permitted applications using a trust broker, which is a system that facilitates identity and context checks against users and restricts visibility and access to applications based on a configured policy.

After identity and context are verified, least privilege access is given based on granular policy rules and the user only has visibility and access to applications they are authorized to. This access is segmented on a per-application basis at layer 7 in the OSI model, limiting a potential attacker’s lateral movement within the network and containing breaches. Because only traffic specific to the authorized application traverses the ZTNA solution rather than all client traffic, the overall remote user experience is improved.

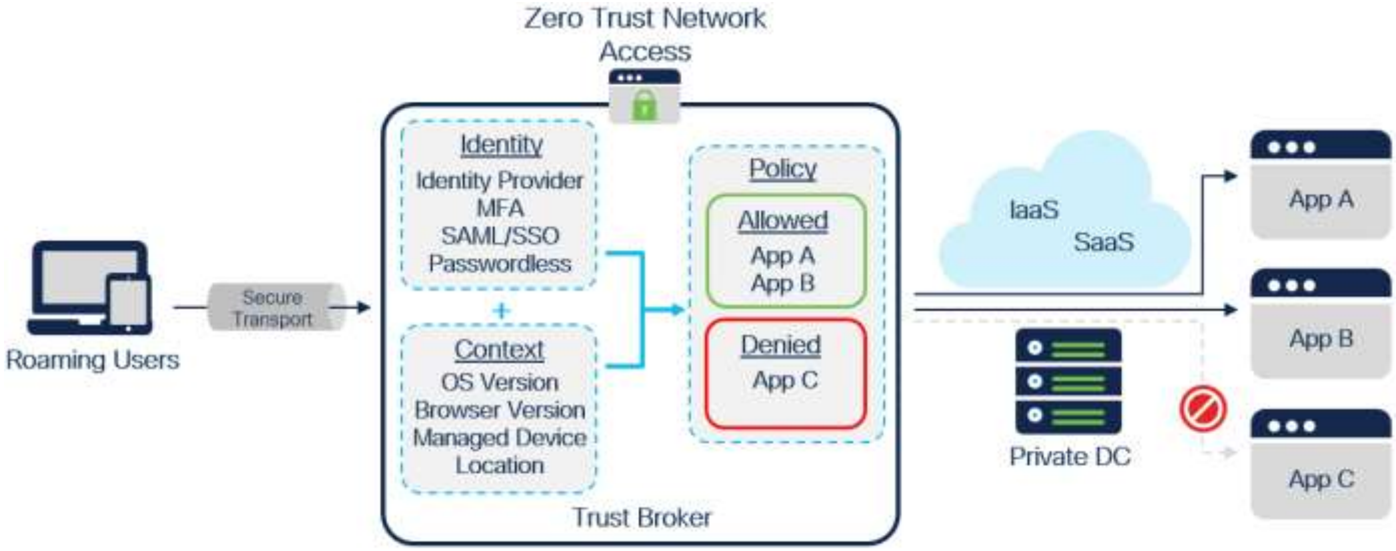


Figure 9.
Zero Trust Network Access Overview

As mentioned earlier, traditional identity checking may only use passwords can be unreliable. ZTNA requires a strong, cloud-based, multi-factor authentication solution that ensures users are verified before granted access to specified resources. User experience can be further improved using SAML/SSO or passwordless authentication capabilities helping mitigate password exhaustion and poor security habits. ZTNA solutions typically take the form of a reverse proxy for clientless ZTNA access via a browser or a software agent for client based ZTNA access. While clientless ZTNA solutions can provide seamless access to users with managed and unmanaged devices, client based ZTNA solutions offer enhanced security using additional device and policy checks available with software agents.

Software Defined WAN

A traditional DC-centric network model made sense when the enterprise data center was the primary destination for users to access applications and data across the network, however, the wide-scale use of cloud applications has become fundamental to business operations at all locations. The centralized security approach has also become impractical because of the high cost of backhauling traffic and the resulting performance issues at remote locations.

To overcome these costs and performance issues, many organizations are adopting a more decentralized networking approach to optimize performance, otherwise known as direct Internet access (DIA). DIA is an architecture component in which certain Internet-bound traffic or public cloud traffic from the branch can be routed directly to the Internet, thereby bypassing the latency of tunneling Internet-bound traffic to a central site. The goal of SASE is to connect users and devices, regardless of location, to any application across any cloud. A secure automated WAN is used to optimize performance by ensuring the fastest, most reliable and secure path to the cloud.

Configuring multiple routers connected to different circuits (for example, an MPLS link and a broadband Internet link) to route network traffic efficiently and optimally can be challenging. Beyond simple load balancing, available bandwidth capacity may go unused during periods of congestion. For example, your broadband Internet connection may be running slowly during a given period of time, while your costly MPLS link is relatively uncongested and may actually be able to provide faster Internet connectivity. The inability to aggregate disparate links means wasted bandwidth capacity and lower employee satisfaction.

SD-WAN combines and optimizes traditional WAN technologies, such as MPLS and broadband Internet connections. This allows organizations to efficiently route network traffic to multiple remote branch locations while providing enhanced monitoring and management capabilities. SD-WAN monitors network traffic across all available links in real-time and dynamically selects the best route for each data packet traversing the network. Additionally, through direct peering relationships to cloud providers middle mile optimization reduces overall hop counts, which reduces latency and improves the overall user experience when accessing applications.

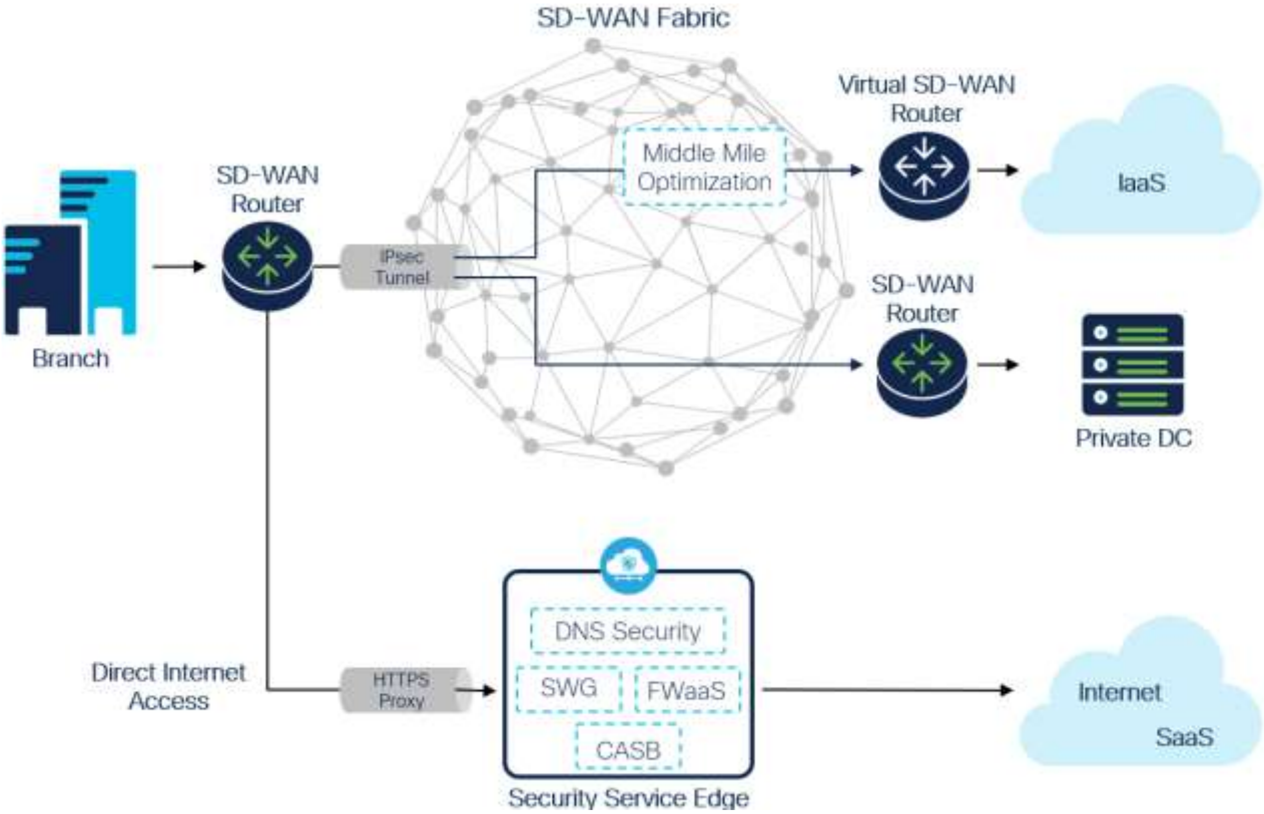


Figure 10.
SD-WAN Overview

The SD-WAN component of a SASE architecture should have the following qualities:

- Flexible, as a service WAN management for on-premises, cloud, and multitenant environments
- Route traffic across different links (MPLS, Internet, 5G, etc.) based on destination
- Route traffic across different links based on cost
- Aggregate multiple links to provide greater total bandwidth
- Rerouting traffic across an alternate link when a link is congested, unstable, or down
- Prioritizing certain application traffic to ensure quality of service

Digital Experience Monitoring

With the rise of remote work, employees are now connecting to enterprise services, applications, and networks from distributed locations both within and outside of the corporate perimeter. Moving from a DC-centric architecture using legacy WANs and security architectures to a cloud-enabled SASE or SSE architecture increases agility, resilience, and performance. But with this change, organizations are challenged to deliver reliable application performance because of the increased external dependencies in the new enterprise ecosystem that they don't own or control. When something goes wrong, network teams often carry the burden of proving the network innocent with no visibility into end-to-end dependencies, such as ISP networks or SaaS application performance. This leads to wasted resources, higher mean time to identify (MTTI) and mean time to repair (MTTR), and negative impacts to the digital experience.

Digital experience from a SASE perspective is how end users experience any application, from wherever they're sitting whether that is from their home office or an on-premises branch site. Digital Experience Monitoring (DEM) is a Gartner IT category that emerged in 2019 to address user experience, human or machine, across every dependency, whether network or service, inside or outside your organization. DEM is used to ensure the reachability and availability of business-critical SaaS, internally hosted applications, and cloud-based services over any network, including the Internet and the corporate network.

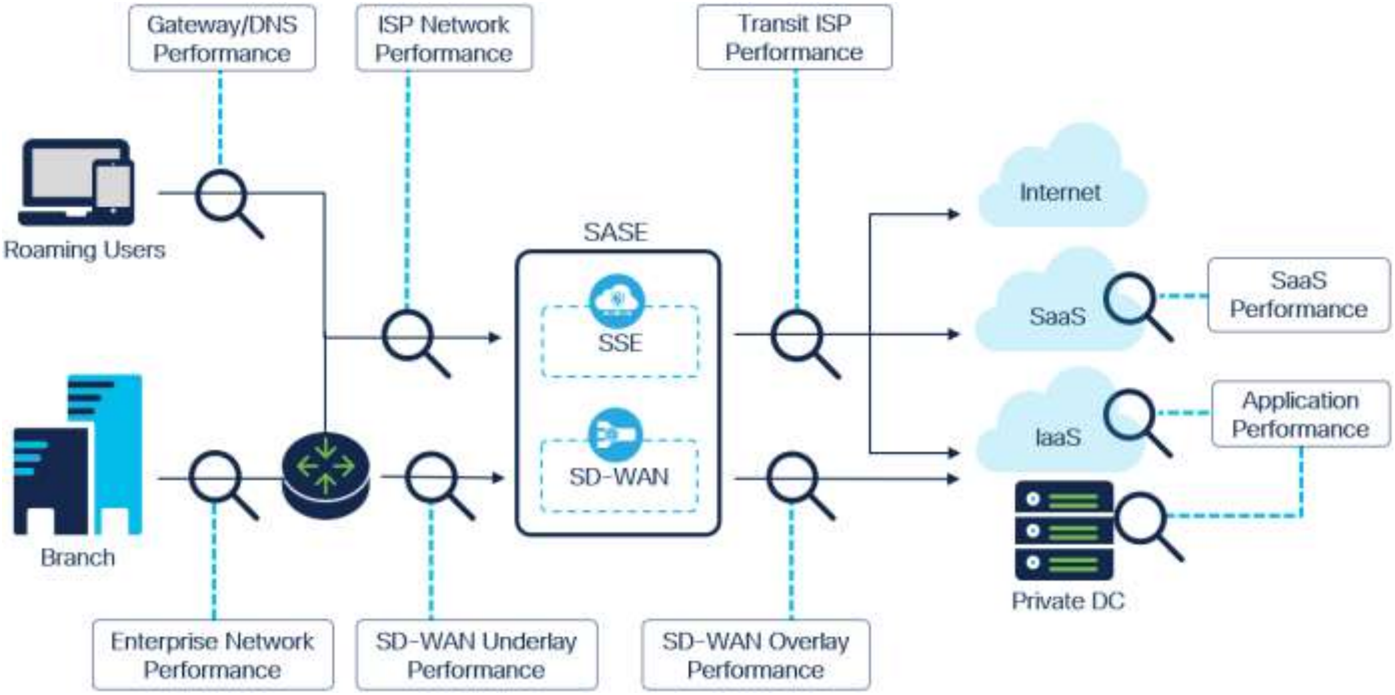


Figure 11.
Digital Experience Monitoring Overview

The Digital Experience Monitoring component of a SASE or SSE architecture should have the following qualities:

- Provide metrics to improve the Digital Experience for users no matter where they are or what application they are using
- Provide lower Mean Time to Identification (MTTI) of issues
- Eliminate wasteful finger-pointing between teams
- Hold providers accountable and get swift resolutions

Cisco SASE/SSE Architecture

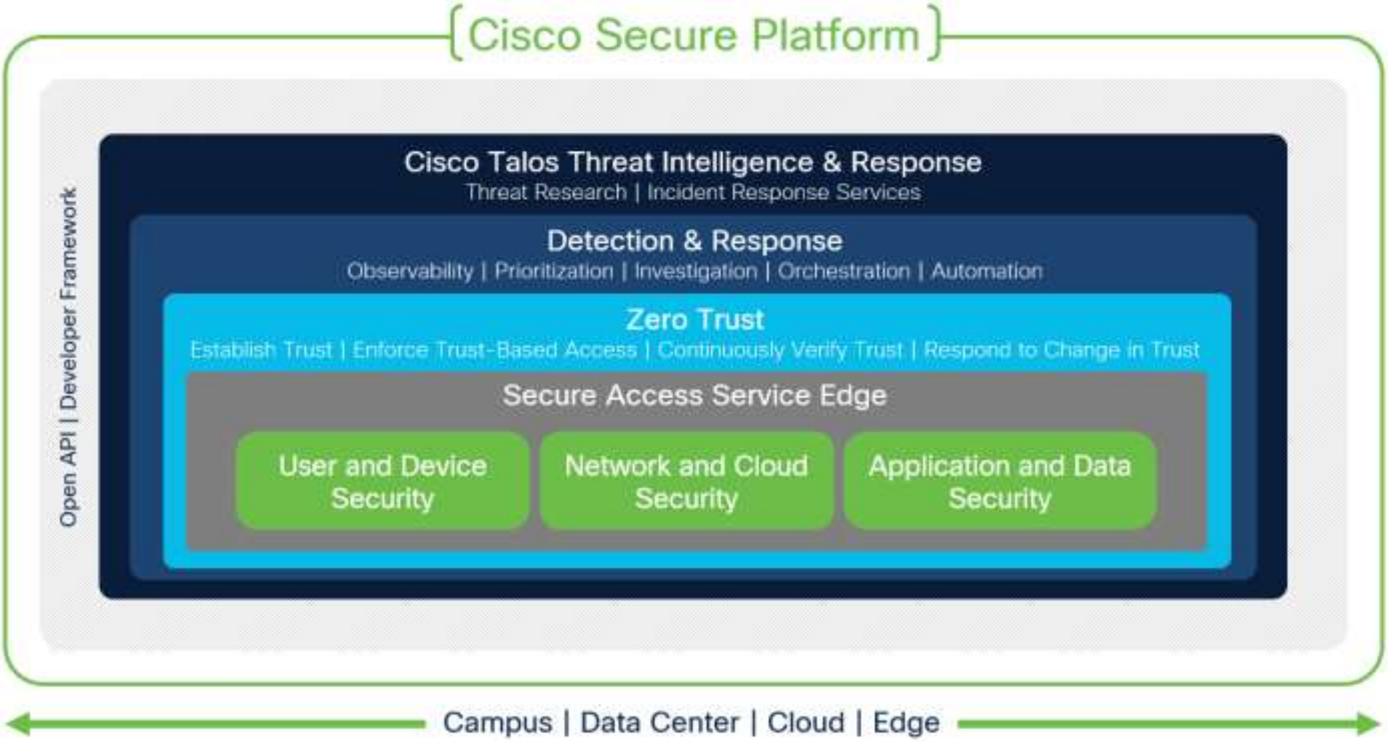

Cisco Secure Platform
Cisco Talos Threat Intelligence & Response
Threat Research | Incident Response Services
Detection & Response
Observability | Prioritization | Investigation | Orchestration | Automation
Zero Trust
Establish Trust | Enforce Trust-Based Access | Continuously Verify Trust | Respond to Change in Trust
Secure Access Service Edge
User and Device Security
Network and Cloud Security
Application and Data Security
Open API | Developer Framework
Campus | Data Center | Cloud | Edge

Figure 12.
Cisco Secure Framework

Security is not a one-size-fits-all solution. To help understand the architecture, Cisco has broken it down into three pillars:

- **User and Device Security**: making sure users and devices can be trusted as they access systems, regardless of location
- **Network and Cloud Security**: protect all network resources on-prem and in the cloud, and ensure secure access for all connecting users
- **Application and Data Security**: preventing unauthorized access within application environments irrespective of where they are hosted

The Cisco SASE/SSE Architecture incorporates the principles of zero trust to create a comprehensive solution to secure all access to applications from any user, device, and location. Furthermore, the architecture is enhanced by extended detection and response (XDR) and Threat Intelligence technologies.

This architecture guide primarily focuses on securing these three pillars from a SASE/SSE perspective using SAFE. For more information on Cisco Zero Trust security, refer to the Cisco Zero Trust Architecture Guide.

Cisco SAFE Business Flows

SAFE uses the concept of business flows to simplify the analysis and identification of threats, risks, and policy requirements for effective security. This enables the selection of very specific capabilities necessary to secure them. This is a sample set of business flows. Additional detailed business flows can be found in Appendix C.

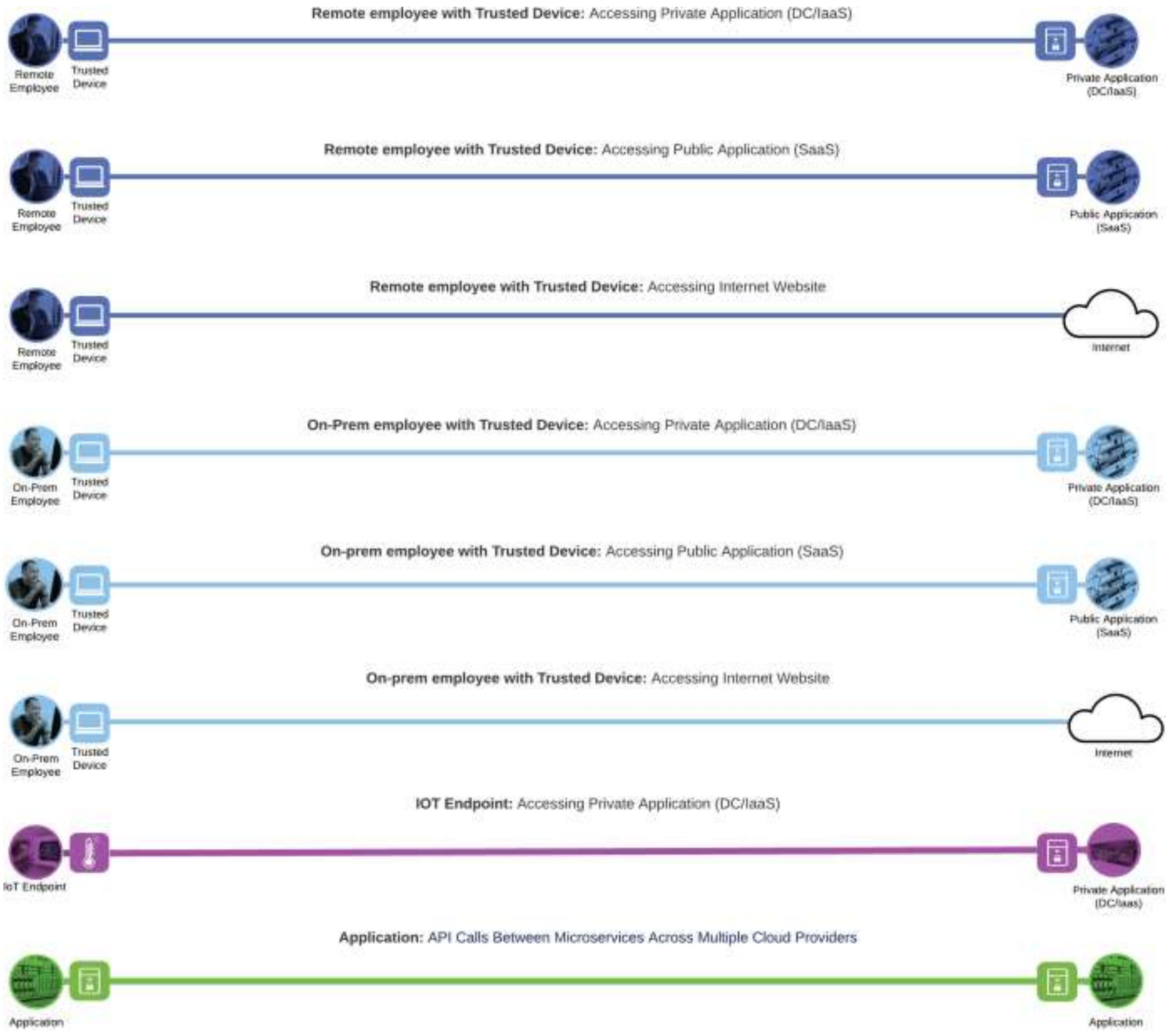

Remote employee with Trusted Device: Accessing Private Application (DC/IaaS)
Remote Employee
Trusted Device
Private Application (DC/IaaS)
Remote employee with Trusted Device: Accessing Public Application (SaaS)
Remote Employee
Trusted Device
Public Application (SaaS)
Remote employee with Trusted Device: Accessing Internet Website
Remote Employee
Trusted Device
Internet
On-Prem employee with Trusted Device: Accessing Private Application (DC/IaaS)
On-Prem Employee
Trusted Device
Private Application (DC/IaaS)
On-prem employee with Trusted Device: Accessing Public Application (SaaS)
On-Prem Employee
Trusted Device
Public Application (SaaS)
On-prem employee with Trusted Device: Accessing Internet Website
On-Prem Employee
Trusted Device
Internet
IOT Endpoint: Accessing Private Application (DC/IaaS)
IoT Endpoint
Private Application (DC/Iaas)
Application: API Calls Between Microservices Across Multiple Cloud Providers
Application
Application

Figure 13.
SASE/SSE Business Flows

Attack Surfaces

The next step in the SAFE methodology is to identify the threats for each business flow. This is the attack surface, and the mitigation of these threats is the business problem to be solved.

User and Device

User and Device Security provides solutions that establish trust in users and devices through authentication and continuous monitoring of each access attempt, with custom security policies that protect every application.

Threat Icon	Threat Name	Threat Description
☠	Rogue Actor	Attackers can easily steal or compromise passwords via phishing emails sent to users. With stolen credentials, they can log in to work applications or systems undetected and access data. Brute-force attacks involve programmatically trying different credential pairs until they work, another attack that can be launched remotely. Once inside, attackers can move laterally to get access to more sensitive applications and data.
☠	Malicious Device	Devices running older versions of software – such as operating systems, browsers, plugins, etc. – can be susceptible to vulnerabilities not patched by software vendors. Without those security patches, devices that access work applications and data can introduce risks by increasing the overall attack surface.
☠	Insecure Unmanaged Device (BYOD)	Often, devices that are not owned or managed by your IT team can have out-of-date software and lax security. Devices that do not have certain security features enabled – such as encryption, firewalls, passwords, etc. – are considered riskier or potentially out of compliance with data regulation standards that require encryption, like healthcare industry compliance standards.

Network and Cloud

Network and Cloud Security enables users to securely connect to your network from any devices, anywhere while restricting access from non-compliant devices. Automated network-segmentation capabilities enable administrators to set policy for users, devices, and application traffic without requiring network redesign.

Threat Icon	Threat Name	Threat Description
☠	Data Exfiltration	Suspect data loss occurs when an abnormal amount of data has been transferred out of the network. Suspect data hoarding occurs when an inside host is found downloading an abnormal amount of data from other inside hosts.
☠	Exploitation	Hosts attempting to compromise each other, such as through worm propagation and brute force password cracking.

Threat Icon	Threat Name	Threat Description
☠	Malicious Insider	An unknown host on the network, or a host that has been compromised and has attempted deviant communication, such as reaching out to a command-and-control server.

Application and Data

Application and Data Security secures connections for all APIs, microservices, and containers that access applications, whether in the cloud, data center, or other virtualized environment. Enterprise networks are increasingly becoming more complex as applications move to multi-cloud and leverage containers and microservices, effectively creating new security, reporting, and compliance challenges.

Threat Icon	Threat Name	Threat Description
☠	Advanced Threats	For example, a malicious actor, on the public network, exploits a PHP Code Injection vulnerability on the web application and gains access to the details of the underlying operating system and installed packages. The attacker then exploits a known vulnerability in the underlying operating system or the installed package to perform privilege escalation and then goes on to establish a command-and-control channel to a malicious server running on attacker’s network by remotely executing a piece of code. The attacker then starts profiling the application environment and exfiltrates sensitive data out through the established command-and-control channel over an outbound UDP 53 port (DNS protocol).
☠	Malware	Zero-day malware attacks, poorly developed applications or unpatched applications are all attack vectors that can be exploited by threat actors. If not protected, the attacker can push malicious code in the source repository resulting in infected software and potential propagation.
☠	Malicious Insider	Without appropriate network visibility and segmentation policies, unknown users / applications may exist in the network or known applications may deviate from characteristic behavior. Malicious actors can take advantage of a flat network with little to no visibility and infiltrate the network without triggering suspicion.

Cisco SAFE Business Flows – Threat Vectors

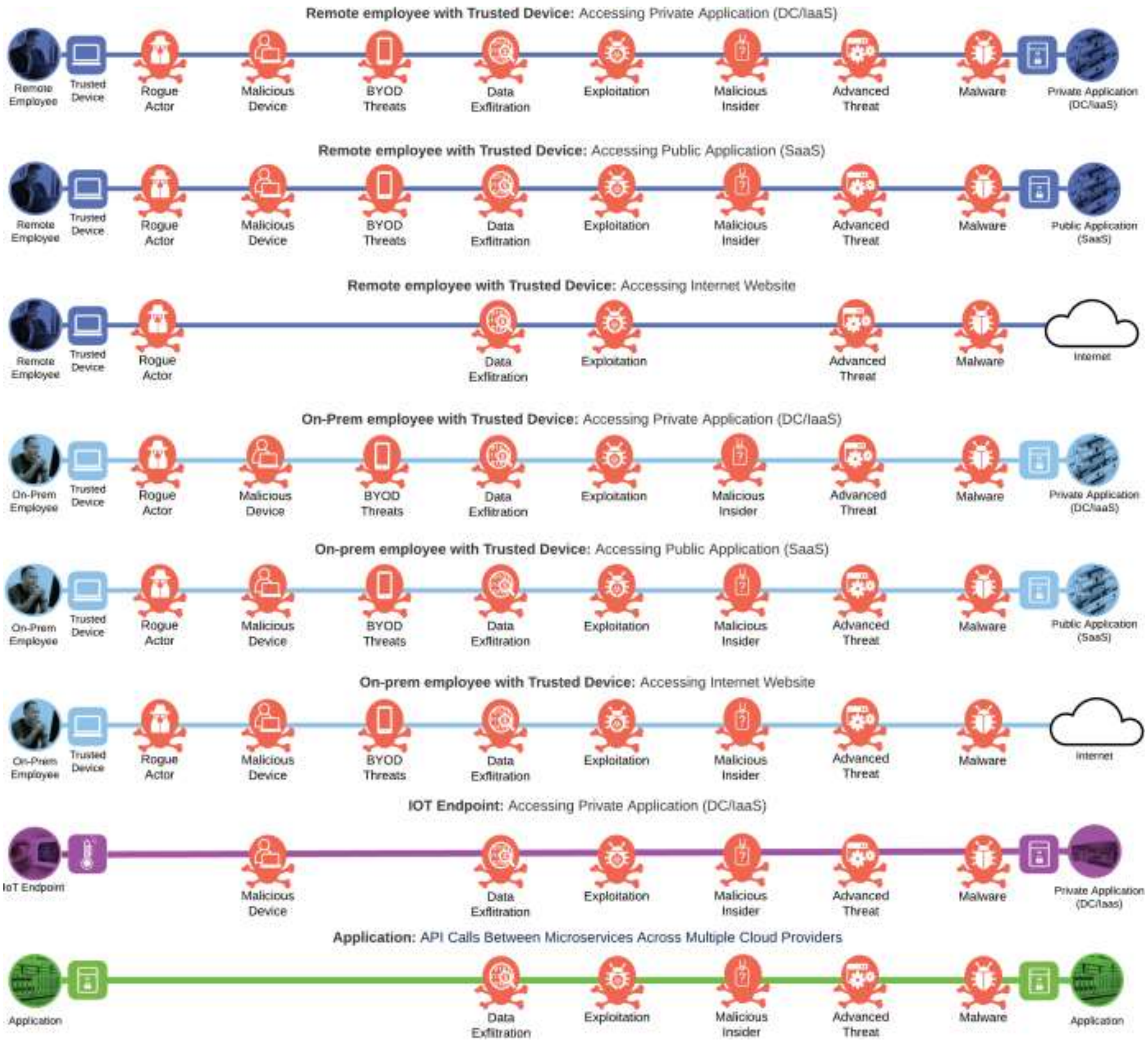


Figure 14.
SASE/SSE Business Flows with threats

Cisco SAFE Capabilities

The Cisco SASE/SSE Architecture is defined using the Cisco SAFE methodology. For more information on SAFE please go to cisco.com/go/safe.

Common Capabilities

The following common capabilities are included in Cisco SASE and SSE.

Capability Icon	Capability Name	Capability Description
	Anomaly Detection	Anomaly detection maintains complex models of what is normal, and, in contrast, what is anomalous. Not all anomalous traffic is malicious, and therefore deviations in the network are classified into event categories to assign severity to the anomalies.
	DNS, DHCP, and IP Address Management (DDI)	DDI is a unified service or solution that centralizes management of DNS and DHCP services and has an IP address management component. Some benefits include visibility and control of these components from a single pane of glass while improving security, resiliency, and support.
	Flow Analytics	Network Detection and Response (NDR) solutions leverage pre-existing infrastructure to offer enterprise-wide, contextual visibility of network traffic. Flow information can be used to conduct forensic analysis to aid in lateral threat movement investigations, ensure ongoing zero trust verification is provided, and modern tools can even detect threats in encrypted traffic.
	Security Orchestration Automation & Response (SOAR)	SOAR is a set of technologies that enable organizations to collect information monitored by the security operations team.
	Threat Intelligence	Knowledge of emerging threats from active adversaries is shared with solutions that will utilize the information to protect the organization.

Secure Access Service Edge

The SASE Security Capability group includes the Digital Experience Monitoring and SD-WAN capabilities, and the Secure Service Edge security capability group.

Digital Experience Monitoring

Digital Experience Monitoring (DEM) addresses user experience, human or machine, across every dependency, whether network or service, inside or outside your organization. DEM looks at the entire digital journey and how every part of it drives successful user actions. By focusing on visibility into digital experience as a whole, DEM helps bridge IT initiatives to business outcomes.

SD-WAN

Provides a replacement for traditional WAN routers and are agnostic to WAN transport technologies. SD-WAN provides dynamic, policy-based, application path selection across multiple WAN connections and supports service chaining for additional services such as WAN optimization and firewalls.

Security Service Edge

The Security Service Edge security capability group includes the DNS-layer security capabilities and the following security capability groups:

- Cloud Access Security Broker
- Firewall as a Service
- Secure Web Gateway
- Zero Trust Network Access

Cloud Access Security Broker

An intermediary between cloud providers, cloud-based applications, and cloud consumers to enforce an organization’s security policies and usage.

Capability Icon	Capability Name	Capability Description
App	Application Visibility & Control (AVC)	Visibility and access control to approved web applications.
DLP	Data Loss Prevention (DLP)	Data Loss Prevention (DLP) is 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.

DNS-layer Security

DNS security enforces security at the DNS layer to block malware, phishing, and command and control callbacks over any port.

Firewall as a Service

Organizations are embracing direct internet access instead of backhauling traffic to the data center. FWaaS provides cloud delivered firewall services without the need to deploy, maintain, and upgrade physical or virtual appliances at a site.

Capability Icon	Capability Name	Capability Description
	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.
	Remote Access as a Service	Enables users who are working remotely to securely access and use applications and data that reside in the enterprise data center and headquarters, encrypting all traffic the users send and receive.

Secure Web Gateway

Secure Web Gateway protects your network against unwanted software or malware users may encounter on the web. It does this by granting your IT or SecOps team granular control over what users on the company network can do while online.

Capability Icon	Capability Name	Capability Description
	Malware Sandbox	Inspects and analyzes suspicious files and URLs and their associated artifacts.
	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.
	Remote Browser Isolation (RBI)	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.
	TLS/SSL Decryption	Ability to decrypt and inspect encrypted web traffic and block hidden attacks.
	Web Reputation Filtering	Compares each new website visited against known sites and then blocks access to sites that launch malicious code.
	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.

Zero Trust Network Access

Zero Trust Network Access allows organizations to provide granular and adaptive access controls to public and private applications. Lateral movement is prevented through application layer segmentation while user experience is improved due to traffic not being backhauled through a data center.

Capability Icon	Capability Name	Capability Description
	Application Segmentation	Least privilege access involves giving users and devices access to only the resource required. Often, network segmentation stops at layer 2 or 3 (Data link and Network layers, respectfully) of the OSI model. Application segmentation involves segmenting and preventing lateral movement at layer 7 of the OSI model or the Application Layer.
	Device Posture Assessment	The device posture assessment analyzes the device and assesses its security posture, and reports it to the policy decision management system.
	Identity Authorization	Establish trust by verifying user and device identity at every access attempt. Least privilege access should be assigned to every user and device on the network, meaning only the applications, network resources and workload communications that are required should be permitted.
	Multi-Factor Authentication (MFA)	Authentication based on usernames and passwords alone is unreliable since users may have trouble storing, remembering, and managing them across multiple accounts, and many reuse passwords across services and create passwords that lack complexity. Passwords also offer weak security because of the ease of acquiring them through hacking, phishing, and malware. Multi-factor authentication (MFA) requires extra means of verification that unauthorized users will not have. Even if a threat actor can impersonate a user with one piece of evidence, they will not be able to provide two or more.
	SAML & SSO	Security Assertion Markup Language (SAML) is an open standard that simplifies the login experience for users. It lets them access multiple applications with one set of credentials, usually entered just once. SAML is the underlying technology that links applications with trusted identity providers.

Endpoint Security

Endpoint security solutions protect endpoints such as mobile devices, desktops, laptops, and even medical and IoT devices. Endpoints are a popular attack vector, and the goal of an attacker is to not only compromise the endpoint but also to gain access to the network and the valuable assets within.

Security practices such as turning on disk encryption, disabling automatic login, and installing anti-virus help ensure an endpoint is “healthy” when joining the network or accessing an application.

Capability Icon	Capability Name	Capability Description
	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 endpoint anti-malware.
	Anti-Virus	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. Anti-Malware solutions typically also include Anti-Virus capabilities.
	Device Health Connector	The device health connector analyzes a device and assesses its security posture, and reports it to the policy decision management system.
DNS	DNS Security Connector	The DNS security connector enforces security at the DNS layer to block malware, phishing, and command and control callbacks over any port.
	Mobile Device Management (MDM)	Mobile device management includes software that provides the following functions: software distribution, policy management, inventory management, security management, and service management for smartphones and media tablets. MDM provides endpoint access control based on policies.
	Telemetry Connector	In a cloud-enabled SASE/SSE architecture, internet traffic is not backhauled through a data center. This can create gaps in visibility due to traditional network monitoring solutions being bypassed. The telemetry connector gathers rich flow context directly from an endpoint on or off premises and provides visibility into network connected devices and user behaviors by exporting flow records to a telemetry collector.
	Web Security Connector	The Web security connector redirects all web traffic to a full web proxy that provides secure web gateway security services.

Zero Trust Network Segmentation

Zero Trust Network Segmentation is a security solution that enforces network segmentation policies on user and device traffic that access the network after verifying their identity and context.

Capability Icon	Capability Name	Capability Description
	Device Posture Assessment	The device posture assessment analyzes the device and assesses its security posture, and reports it to the policy decision management system.
	Identity Access Policy	Policies that control tag assignment and allowed communication between tagged traffic on network devices such as switches and firewalls. For example, Security Group Access Control List (SGACL).
	Identity Authorization	Establish trust by verifying user and device identity at every access attempt. Least privilege access should be assigned to every user and device on the network, meaning only the applications, network resources and workload communications that are required should be permitted.
	Tagging	Segmentation using Endpoint Groups (EPG), TrustSec Security Group Tag (SGT), or VLANs.

WAN/Internet Edge

The following WAN and Internet edge capabilities are included within the Cisco SASE/SSE Architecture.

Capability Icon	Capability Name	Capability Description
	Distributed Denial of Service (DDoS) Mitigation	Provides protection against a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.
	Web Application Firewall (WAF)	A Web Application Firewall (WAF) protects websites from application vulnerability exploits like SQL injection, cross-site scripting (XSS), cross-site request forgery, session hijacking, and other web attacks.

Data Center Security

Data center security is the practice of applying security controls to the data center with the goal of protecting it from threats that could compromise the confidentiality, integrity, or availability of business information assets or intellectual property. Data center security follows the workload across physical data centers and multi-cloud environments to protect applications, infrastructure, data, and users. The practice applies to traditional data centers as well data centers in the public cloud.

Because the focus of this guide is on SASE/SSE, details regarding securing the data center are limited in scope. More detail information about securing the data center can be found in the Secure Data Center Design Guide.

Capability Icon	Capability Name	Capability Description
App	Application Visibility & Control (AVC)	Visibility and access control to approved web applications.
DLP	Data Loss Prevention (DLP)	Data Loss Prevention (DLP) is 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.
	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.
	Malware Sandbox	Inspects and analyzes suspicious files and URLs and their associated artifacts.
	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.

Application Workload Security

Application Workload Security includes measures at the application level that aim to prevent data or code within the application from being stolen or hijacked. It encompasses the security considerations that happen during application development and design, but it also involves systems and approaches to protect applications after they get deployed.

All application servers should be hardened and follow security practices such as disabling root access, using SNMPv3 instead of SNMPv2, enabling certificate-based authentication for web clients, etc.

Capability Icon	Capability Name	Capability Description
	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 load balancer configs.
	Continuous Vulnerability Scanning	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunities for attackers.
	Micro-Segmentation	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.
	Patch Management	The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.
	Policy Generation, Audit & Change Management	The output of application dependency mapping provides an allowed access list policy. This policy will need to be audited and changed as required.
	Process Anomaly Detection & Forensics	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.
	Runtime Application Security Protection	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.
	Tagging	Segmentation using Endpoint Groups (EPG), TrustSec Security Group Tag (SGT), or VLANs.

Cisco SAFE Business Flows - Capability Mappings

Not all business flows have the same requirements. Some use cases are subject to a smaller attack vector and therefore require less security to be applied. Some have larger and multiple vectors and require more. Evaluating the business flow by analyzing the attack surfaces provides the information needed to determine and apply the correct capabilities for flow specific and effective security. This process also allows for the application of capabilities to address risk and administrative policy requirements.

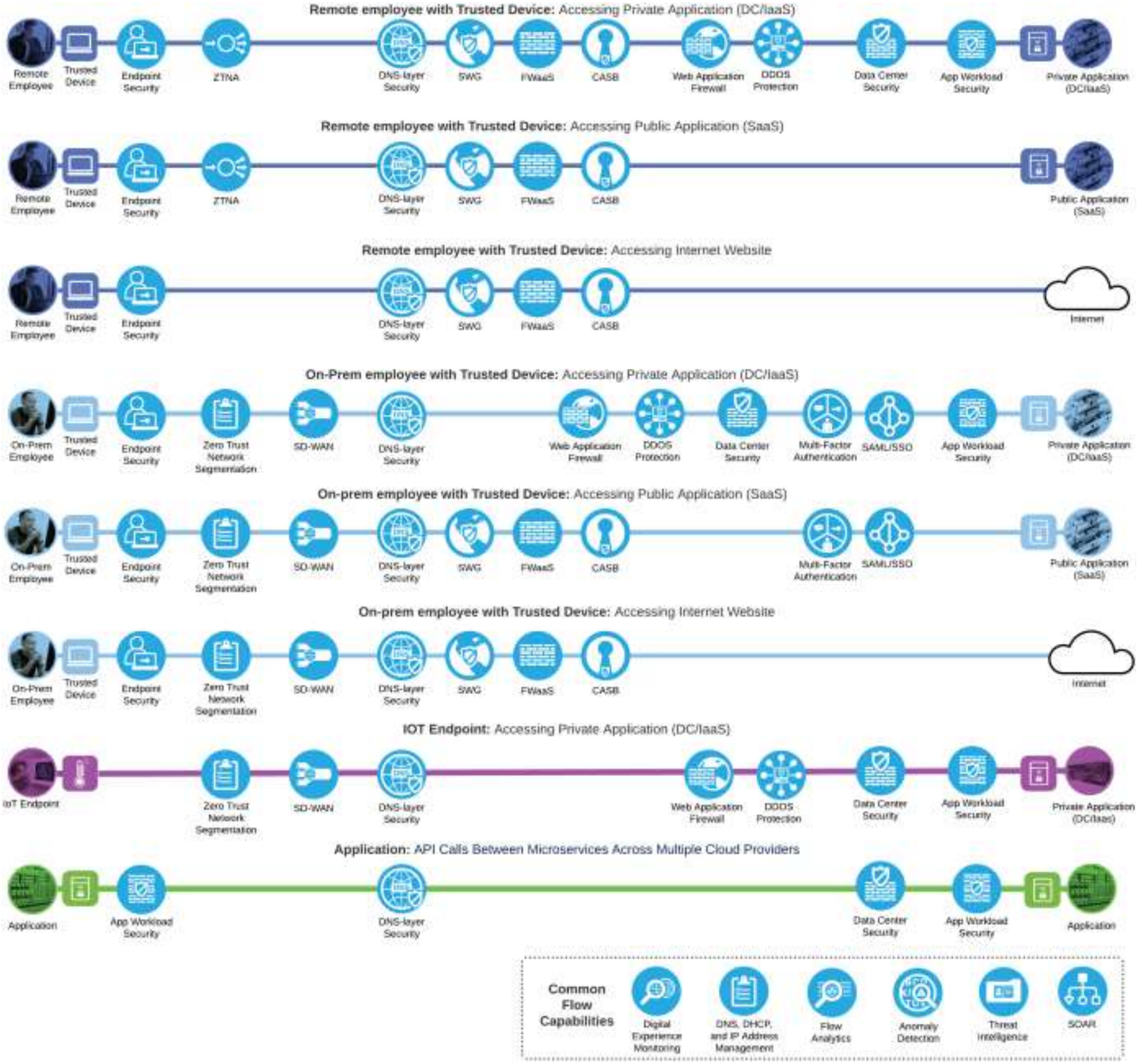


Figure 15.
SASE/SSE Business Flows with SAFE Capabilities

SASE/SSE Reference Architecture

The Cisco SAFE Security Reference Architecture below includes the main architectural components needed to deliver the security capabilities for each pillar. The Cisco SAFE Reference Architecture is included in the Cisco Security Reference Architecture and is presented below in that format and merged with the SAFE methodology.

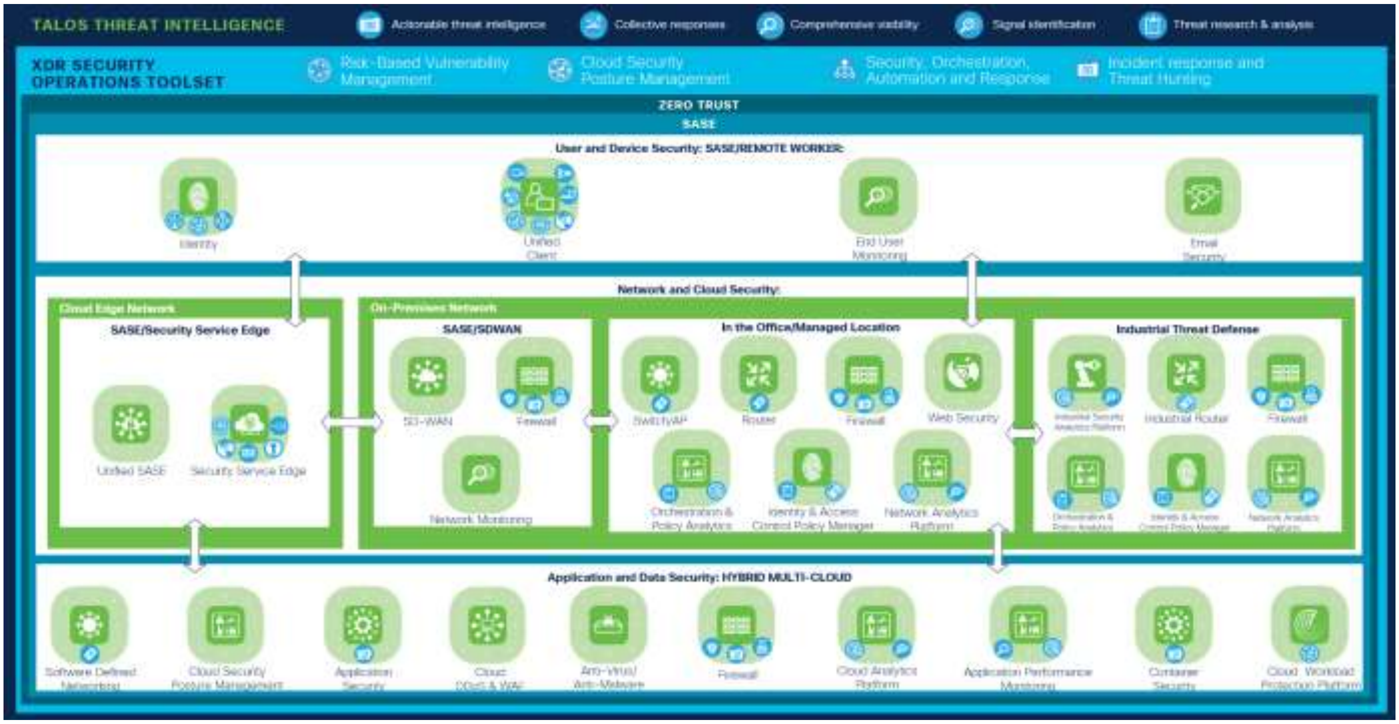

TALOS THREAT INTELLIGENCE
Actionable threat intelligence
Collective responses
Comprehensive visibility
Signal identification
Threat research & analysis
XDR SECURITY OPERATIONS TOOLSET
Risk-Based Vulnerability Management
Cloud Security Posture Management
Security, Orchestration, Automation and Response
Incident response and Threat Hunting
ZERO TRUST
SASE
User and Device Security: SASE/REMOTE WORKER:
Identity
Unified Client
End User Monitoring
Email Security
Network and Cloud Security:
Cloud Edge Network
SASE/Security Service Edge
Unified SASE
Security Service Edge
On-Premises Network
SASE/SDWAN
SD-WAN
Firewall
Network Monitoring
In the Office/Managed Location
Switch/AP
Router
Firewall
Web Security
Orchestration & Policy Analytics
Identity & Access Control Policy Manager
Network Analytics Platform
Industrial Threat Defense
Industrial Security Analytics Platform
Industrial Router
Firewall
Orchestration & Policy Analytics
Identity & Access Control Policy Manager
Network Analytics Platform
Application and Data Security: HYBRID MULTI-CLOUD
Software Defined Networking
Cloud Security Posture Management
Application Security
Cloud DDoS & WAF
Anti-Virus/ Anti-Malware
Firewall
Cloud Analytics Platform
Application Performance Monitoring
Container Security
Cloud Workload Protection Platform

Figure 16.
Cisco SAFE Security Reference Architecture

The Cisco SASE/SSE Architecture below includes the architectural components needed location-by-location to deliver the security capabilities for each pillar and is structured as follows:

- SASE (SD-WAN + SSE + DEM) and Cloud Security (Top)
- Consumers (Left)
    - On-prem employees and IoT devices located at a Campus
    - Remote Employees located at their Home Office or Public Location
    - On-prem employees and IoT devices located at a Small Branch
- Providers (Right)
    - Private applications located in Cloud Workloads (IaaS)
    - Private applications located in a private Data Center
    - Internet Website
    - Public Application (SaaS)

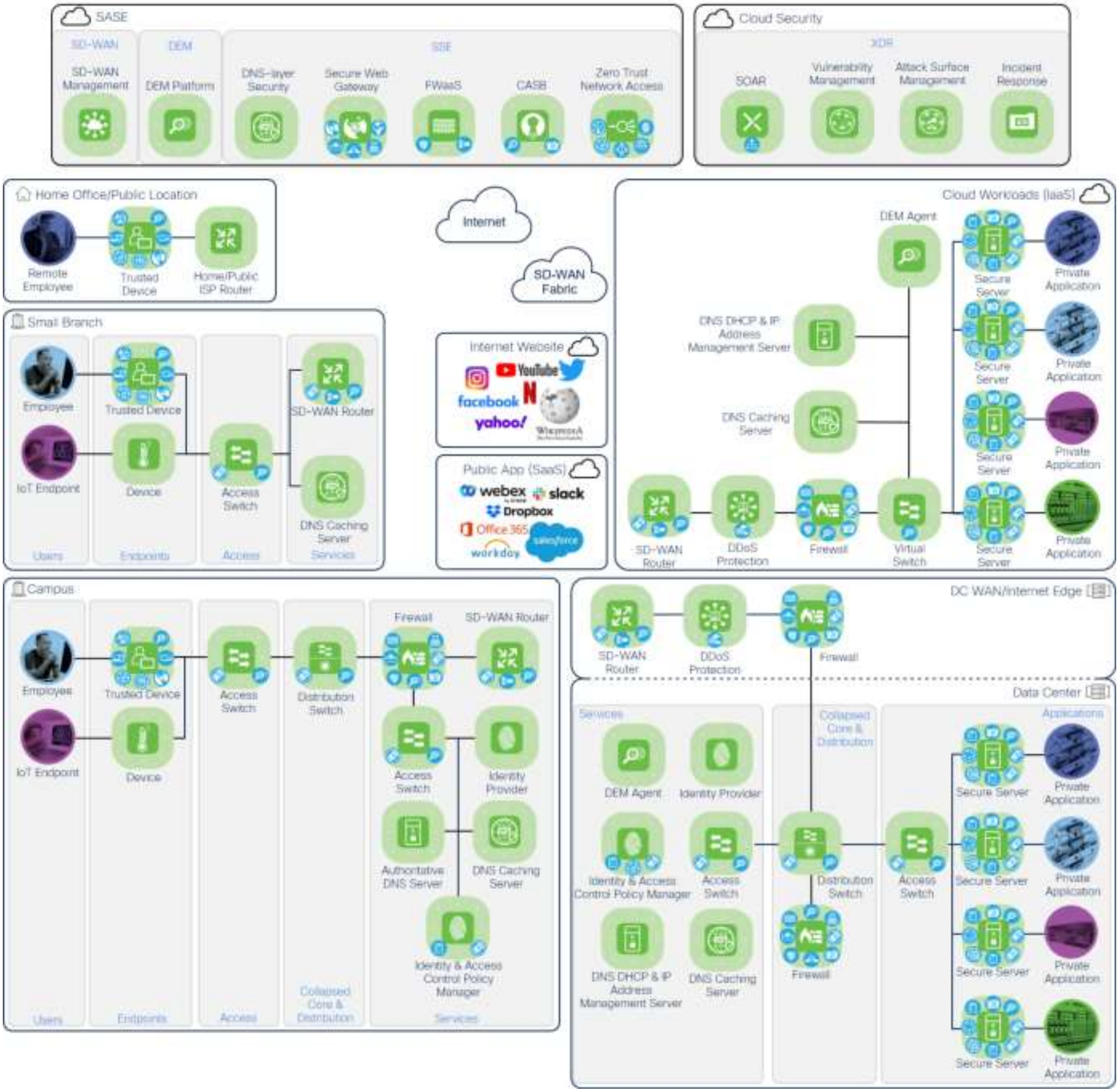
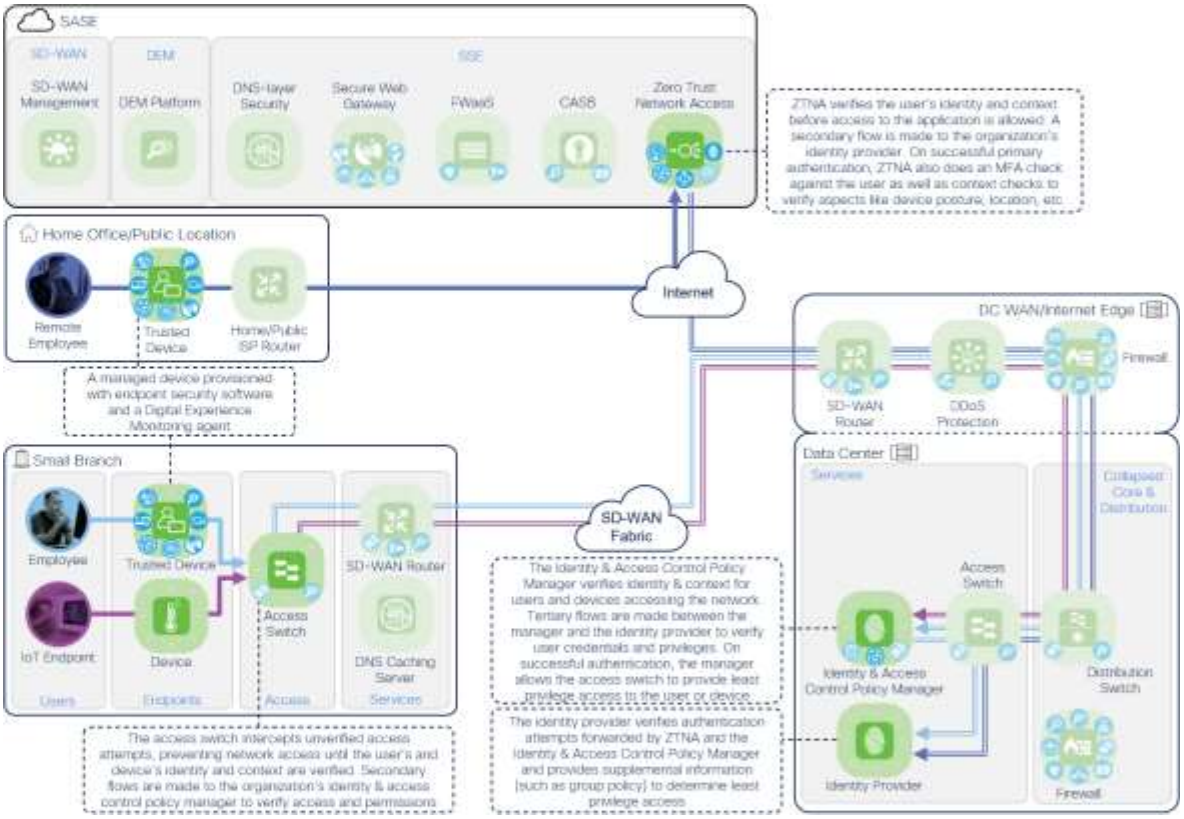


Figure 17.
Cisco SASE/SSE Reference Architecture

User and Device Security

Security in this pillar involves making sure users and devices can be trusted as they access applications, workloads, and data, regardless of location. With a hybrid workforce, users may be located on-premises at a branch, at home, or a coffee shop. Regardless of their location, it is imperative that they are identified and have the appropriate context before accessing company resources.

Identity involves the authentication, authorization, and accounting of entities accessing resources to confirm they are who they say they are, they will only have access to the resources they need, and their access attempt is logged in case there is a breach. For roaming users, this is done using ZTNA or RAaaS with the primary factor of authentication using an identity provider such as Microsoft Active Directory but should be enhanced through mechanisms such as MFA. On-prem users are identified with 802.1x before they are allowed to access the network. User experience for both roaming and on-prem users can be improved by enabling SAML and SSO for private and public applications, minimizing password exhaustion for users who have the option of signing into multiple services using a single set of credentials. Along with identity, context is also important before access is allowed. Device posture and other risk-based assessment checks against the device such as if the browser or anti-virus definitions are out-of-date can prevent risker devices from accessing the network.



ZTNA verifies the user's identity and context before access to the application is allowed. A secondary flow is made to the organization's identity provider. On successful primary authentication, ZTNA also does an MFA check against the user as well as context checks to verify aspects like device posture, location, etc.

A managed device provisioned with endpoint security software and a Digital Experience Monitoring agent

The access switch intercepts unverified access attempts, preventing network access until the user's and device's identity and context are verified. Secondary flows are made to the organization's identity & access control policy manager to verify access and permissions

The Identity & Access Control Policy Manager verifies identity & context for users and devices accessing the network. Tertiary flows are made between the manager and the identity provider to verify user credentials and privileges. On successful authentication, the manager allows the access switch to provide least privilege access to the user or device

The identity provider verifies authentication attempts forwarded by ZTNA and the Identity & Access Control Policy Manager and provides supplemental information (such as group policy) to determine least privilege access

Figure 18.
SASE/SSE User & Device Security Business Flows with SAFE Capabilities

With managed devices, there is option to install endpoint security software to lower the risk of compromise to devices connecting to trusted and untrusted networks. This software adds anti-malware security capabilities to prevent and remove threats, connectors needed to forward traffic to the SASE or SSE cloud for inspection and policy enforcement, and more. For visibility into the user's digital experience, an agent is installed onto the managed device to monitor application performance from the user's perspective, providing additional assistance to IT teams troubleshooting connectivity issues that user may experience. A cloud-based mobile device management (MDM) solution can be used to distribute software, including endpoint security software, and manage security policies on the device no matter where they are located.

When using an unmanaged device, such as a personal smartphone or PC, the user can verify their identity using MFA and simpler context checks can be done, however, there is no insight into what services are running on the device. Network controls must be put in place to limit network access and to detect suspicious traffic patterns.

Users are not the only endpoints connected to the network. IOT Endpoints such as lighting, heating and air conditioning have changed the way security must be enforced on the network. These devices are not only absent a user, but many do not have the capability to leverage an 802.1X supplicant or a Certificate. In this case, context checks such as posture and device profiling assessments can be used to control devices as they connect to the network. Typically, the device MAC address is used to uniquely identity the device, and a profile is built using information such as:

- Is the device secured using a strong method of authentication?
- What are the services it is trying to connect to?
- What ports is the device communicating on?

All of which allows us to build control policies and assign identifying tags to the devices traffic as it communicates across the network.

Network and Cloud Security

After successful identity and context verification, user or device traffic must be routed to a public SaaS application, private application within a datacenter or IaaS environment, or public Internet website. The Network and Cloud security pillar handles providing secure transport for user, device, and application traffic as it is routed over insecure underlay networks while enforcing the organization's security policy to prevent unauthorized access to protected applications and sensitive data. Traffic destined to public SaaS applications or internet websites is routed through the SASE/SSE cloud where cloud security services are performed. Traffic destined to private applications is routed through on-premises access where traditional on-premises security services are applied.

For roaming users accessing public or private applications, least privileged access is provided by a ZTNA solution after identity and context verification. As an initial step to accessing the application, the DNS request for the application is verified using DNS security protecting the user from phishing attempts using similar looking URLs. Traffic is proxied through the SASE/SSE cloud to provide security and enforce company policies for web-based traffic (SWG), non-web traffic (FWaaS), and provide data loss prevention (CASB). ZTNA does per application segmentation, preventing lateral movement by the user. For private applications in the data center or IaaS environment, traffic is appropriately tagged and monitored as it passes through the network. Firewalls enforce the security policy set by the identity & access control policy manager. For public SaaS applications, access is monitored for any abnormal behavior by the CASB. Public

Internet websites accessed by the user, such as YouTube, don’t require identity checks controlled by the organization, however for managed devices DNS security and SWG can be used to restrict access to insecure or inappropriate websites. Inline DLP can prevent data loss and FWaaS can filter non-web traffic and provide intrusion prevention for inbound traffic.

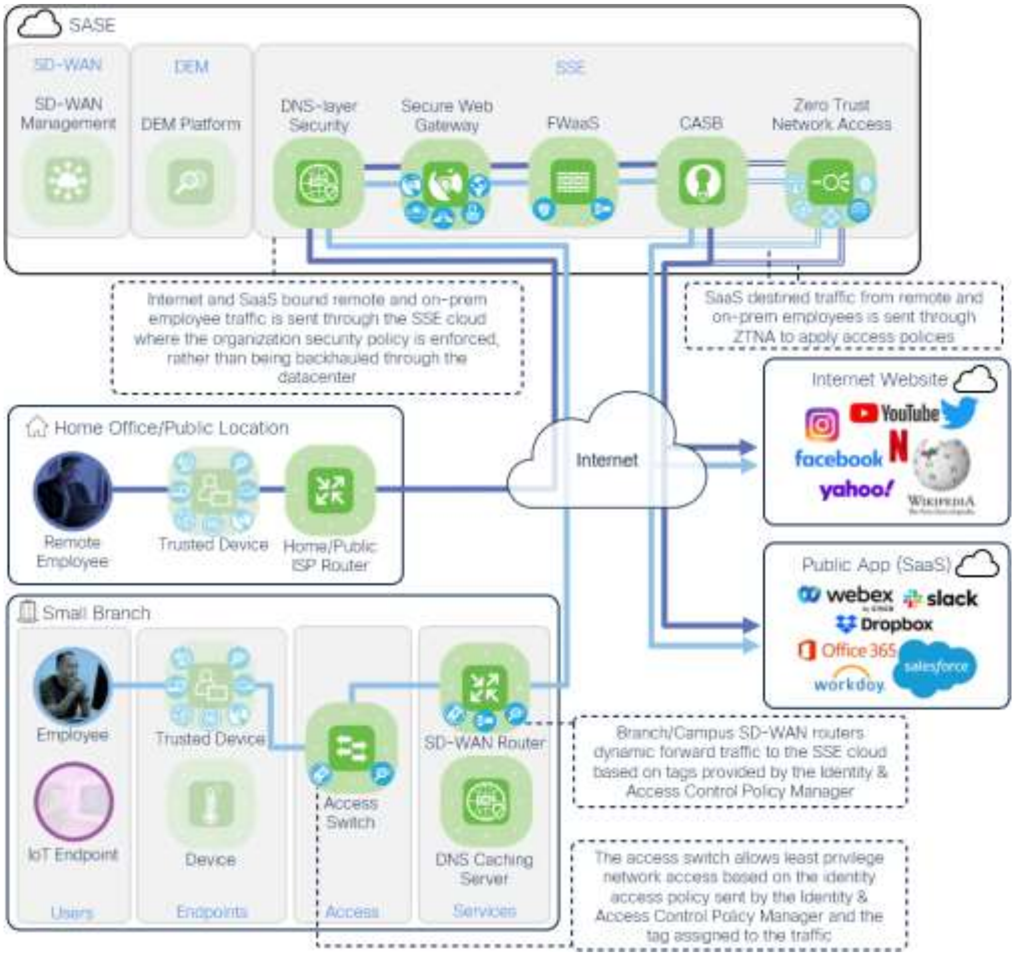
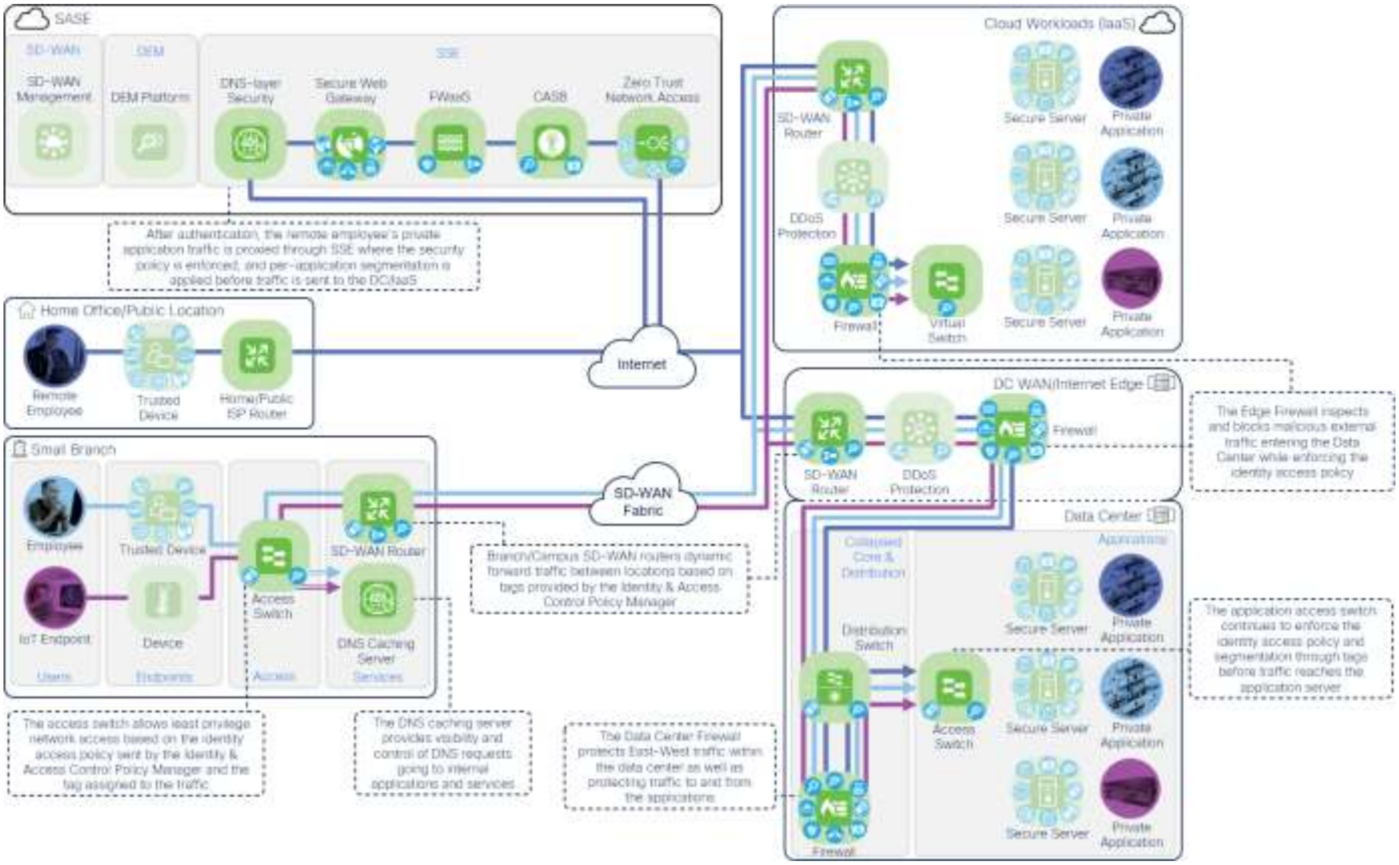

SASE
SD-WAN
SD-WAN Management
DEM
DEM Platform
SSE
DNS-layer Security
Secure Web Gateway
FWaaS
CASB
Zero Trust Network Access
Internet and SaaS bound remote and on-prem employee traffic is sent through the SSE cloud where the organization security policy is enforced, rather than being backhauled through the datacenter
SaaS destined traffic from remote and on-prem employees is sent through ZTNA to apply access policies
Internet Website
YouTube
facebook
yahoo!
Wikipedia
Home Office/Public Location
Remote Employee
Trusted Device
Home/Public ISP Router
Internet
Public App (SaaS)
webex
slack
Dropbox
Office 365
salesforce
workday
Small Branch
Employee
IoT Endpoint
Trusted Device
Device
Access Switch
SD-WAN Router
DNS Caching Server
Users
Endpoints
Access
Services
Branch/Campus SD-WAN routers dynamic forward traffic to the SSE cloud based on tags provided by the Identity &amp; Access Control Policy Manager
The access switch allows least privilege network access based on the identity access policy sent by the Identity &amp; Access Control Policy Manager and the tag assigned to the traffic

Figure 19.
SASE/SSE Network & Cloud Security (Internet/SaaS) Business Flows with SAFE Capabilities

Alternatively, roaming users can connect to private applications using RAaaS services within SSE. This could be for accessing legacy apps, or ones difficult to re-architect for SSO or Zero Trust model compatibility. Managed devices (or unmanaged devices with an installed VPN client) may access the network over an encrypted tunnel as if they were sitting on the corporate network. While some applications suit a ZTNA implementation, more sensitive applications may require the extra layer of protection an IPsec tunnel would provide. Access could, through the security policy, be limited to managed devices, where endpoint security software can be installed to protect sensitive data from compromised devices. Like ZTNA, identity and context should still be verified and least privilege access should be implemented through mechanisms like split tunneling and tagging. Split tunneling will route only IP traffic associated with the specified application over the tunnel while enforcing tagging will limit lateral movement.

For on-prem users and IOT devices, least privileged access is enforced by network devices in the branch and data center (SD-WAN routers, switches, and firewalls) after identity and context verification. After verification of the DNS requests, traffic from these users and devices is tagged and segmentation is applied based on the identity access policy distributed by the identity and access policy manager. For private applications in the data center or IaaS environment, SD-WAN routers securely route traffic to remote locations over underlay networks using IPsec tunnels while maintaining tags and segmentation. Firewalls within the data center environment enforce the security policy, blocking unauthorized access and checking for malware or intrusion attempts. For internet bound traffic (SaaS or public website), like roaming users, DNS requests initiated by on-prem employees is verified by DNS security as an initial step. After DNS security verifies the domain is safe, a DNS reply is sent, and the Internet bound traffic is forwarded to the SASE/SSE cloud by the SD-WAN router. The SASE/SSE service provides security and enforces security policies for web-based traffic (SWG), non-web traffic (FWaaS), and provides data loss prevention (CASB).



After authentication, the remote employee's private application traffic is proxied through SSE where the security policy is enforced, and per-application segmentation is applied before traffic is sent to the DC/IaaS

Branch/Campus SD-WAN routers dynamic forward traffic between locations based on tags provided by the Identity & Access Control Policy Manager

The access switch allows least privilege network access based on the identity access policy sent by the Identity & Access Control Policy Manager and the tag assigned to the traffic

The DNS caching server provides visibility and control of DNS requests going to internal applications and services

The Data Center Firewall protects East-West traffic within the data center as well as protecting traffic to and from the applications

The Edge Firewall inspects and blocks malicious external traffic entering the Data Center while enforcing the identity access policy

The application access switch continues to enforce the identity access policy and segmentation through tags before traffic reaches the application server

Figure 20.
SASE/SSE Network & Cloud Security (Private Application) Business Flows with SAFE Capabilities

Finally, a digital monitoring experience agent is installed at the branch, data center, and IaaS environment to monitor ISP and SD-WAN performance close to the users and close to the hosted private applications used by employees.

Application and Data Security

While organizations can benefit from the scale and agility offered by hosting applications within hybrid and multi-cloud environments, difficulties arise with managing the security of these distributed applications. For example, with applications running across multiple infrastructures comes an increased attack surface. The Application and Data Security pillar focuses on the security capabilities needed to prevent unauthorized access whether those applications or workloads are hosted in the data center or in the cloud. Along with user-to-application traffic, Application and Data Security must also be enforced for application-to-application traffic where there may be API calls and other communications between microservices or containers.

Traffic to these applications initially passes a web application firewall which monitors and filters web-based traffic for exploits and malicious connection attempts. DDoS protection blocks attempts to overwhelm the application server and disrupt service availability. Successful DDoS attacks can cause productivity loss as well as revenue loss for applications necessary for sales while successful exploits against the application servers can allow exfiltration of sensitive customer data or software code.

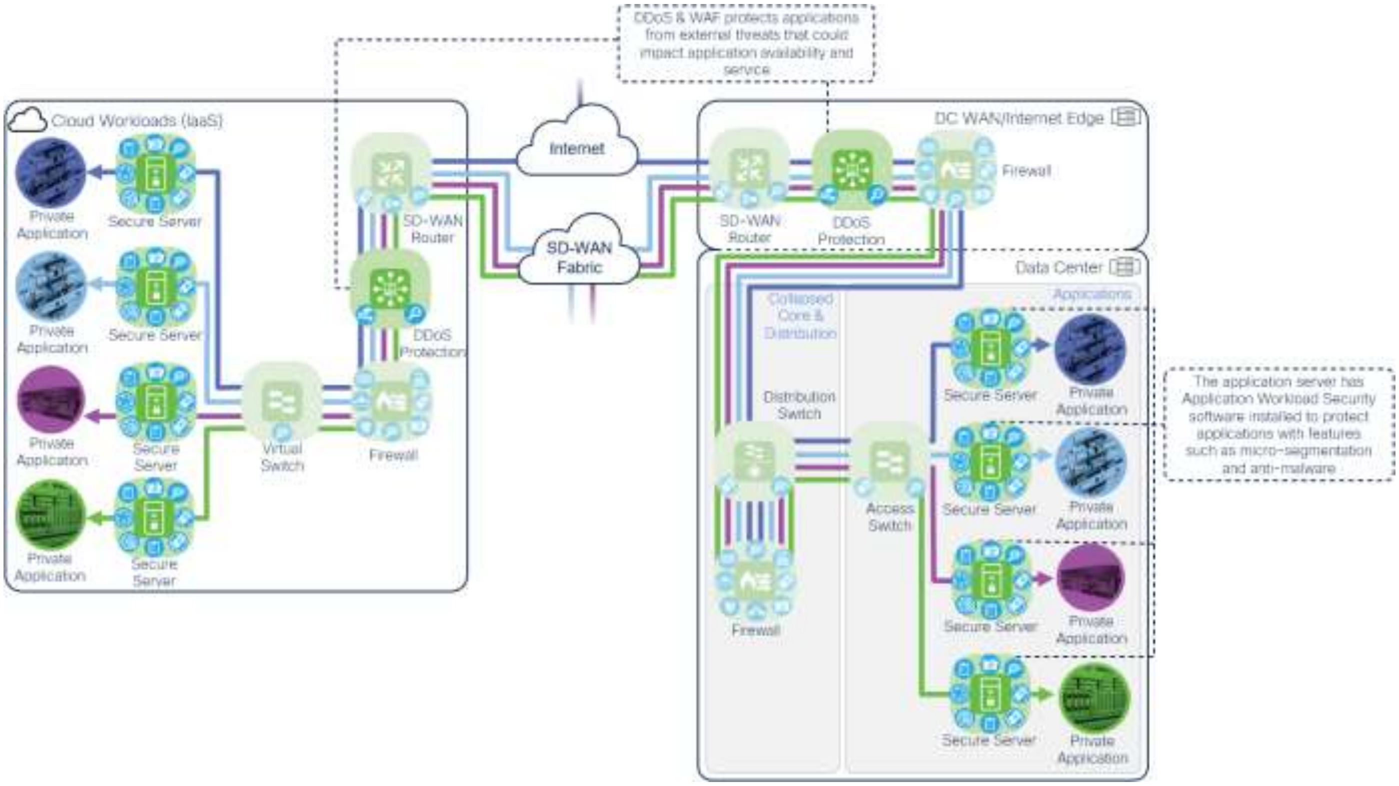


Figure 21.
SASE/SSE Application & Data Security Business Flows with SAFE Capabilities

On the application server, an anti-malware software agent is deployed to provide defense in depth, preventing and removing malicious threats not detected by endpoint security software, SASE/SSE, or network firewalls. For comprehensive security, workload protection software should be deployed to on the server including features such as:

- Micro-segmentation to reduce the attack surface for application traffic and only allowing known and required communications

- Visibility into application behaviors, dependencies, and vulnerabilities as this is important for baselining normal behavior to quickly identify abnormal or suspicious behavior
- Continuous vulnerability scanning to allow for quick detection and quarantining of workloads affected by risky vulnerabilities

Through these features, the attack surface of distributed applications is reduced, lateral movement is minimized in the event of a security incident, and the identification of anomalies and suspicious behavior is accelerated.

Appendix

Appendix A – SASE/SSE Reference Architecture Security Capabilities

Considering the architecture discussed in the previous section of this document, all the capabilities and Cisco/Cisco Partner solutions can be mapped as below.

Capability Icon	Capability Name	Cisco/Cisco Partner Security Solution
	Anomaly Detection	Cisco Secure Network Analytics Cisco Cyber Vision Cisco Secure Cloud Analytics Cisco Duo
	Anti-Malware	Cisco Secure Endpoint (integrated with Secure Connect, Umbrella, Firewall & SD-WAN) Cisco Secure Malware Analytics
	Anti-Virus	Cisco Secure Endpoint (integrated with Secure Connect, Umbrella, Firewall & SD-WAN) Cisco Secure Malware Analytics
	Application Dependency Mapping	Cisco Secure Workload
	Application Segmentation	Cisco Secure Connect Duo Network Gateway
App	Application Visibility & Control (AVC)	Cisco Umbrella Cisco Secure Firewall Cisco Secure Workload Cisco AppDynamics Cisco Secure Application Cisco Secure Web Appliance

Capability Icon	Capability Name	Cisco/Cisco Partner Security Solution
		Cisco Cloudlock Cisco Meraki Cisco Secure Connect
	Asset Management	Cisco Secure Cloud Insights
	Cloud Access Security Broker (CASB)	Cisco Umbrella Cisco Cloudlock Cisco Secure Connect
	Continuous Vulnerability Scanning	Cisco Secure Workload
DLP	Data Loss Prevention (DLP)	Cisco Cloudlock Cisco Umbrella Cisco Secure Connect
	Distributed Denial of Service (DDoS) Mitigation	Radware DDoS
	Device Health Connector	Cisco Duo Device Health
	Device Posture Assessment	Cisco Identity Services Engine Cisco Duo Cisco Secure Firewall Cisco Secure Connect
	Digital Experience Monitoring (DEM)	ThousandEyes
	DNS, DHCP, and IP Address Management (DDI)	BlueCat Integrity
DNS	DNS Security	Cisco Umbrella Cisco Secure Connect

Capability Icon	Capability Name	Cisco/Cisco Partner Security Solution
		BlueCat Edge
DNS	DNS Security Connector	Cisco Secure Client (AnyConnect) Cisco Umbrella Virtual Appliance
	Firewall	Cisco Secure Firewall Cisco Umbrella Cisco Secure Workload Cisco Meraki MX Cisco Secure Connect
	Flow Analytics	Cisco Cyber Vision Cisco Secure Network Analytics Cisco Secure Cloud Analytics Cisco Secure Workload
	Identity Access Policy	Cisco Identity Services Engine
	Identity Authorization	Cisco Duo Cisco Identity Services Engine Cisco Secure Connect
	Intrusion Prevention	Cisco Secure Firewall Cisco Umbrella Cisco Secure Connect
	Malware Sandbox	Cisco Secure Malware Analytics
	Micro-Segmentation	Cisco Identity Services Engine Cisco Secure Workload Cisco Secure Application
	Mobile Device Management (MDM)	Cisco Meraki Systems Manager

Capability Icon	Capability Name	Cisco/Cisco Partner Security Solution
	Multi-Factor Authentication (MFA)	Cisco Duo
	Network Anti-Malware	Cisco Secure Firewall Cisco Umbrella Cisco Meraki MX Cisco Secure Email Appliance Cisco Secure Web Appliance Cisco Secure Connect
	Patch Management	Cisco Secure Workload
	Policy Generation, Audit & Change Management	Cisco Secure Workload
	Process Anomaly Detection & Forensics	Cisco Secure Workload
	Remote Access VPN	Cisco Secure Firewall (ASA (Adaptive Security Appliance)) Cisco Secure Firewall (FTD (Firepower Threat Defense)) Cisco Meraki MX Cisco Secure Connect
	Remote Browser Isolation (RBI)	Cisco Umbrella
	Runtime Application Security Protection	Cisco Secure Application
	SAML & SSO	Cisco Duo Cisco Secure Connect

Capability Icon	Capability Name	Cisco/Cisco Partner Security Solution
	SD-WAN	Cisco Meraki Cisco Viptela
	Security Orchestration Automation & Response (SOAR)	Cisco SecureX
	Tagging	Cisco Secure Workload
	Telemetry Connector	Cisco Secure Client (AnyConnect)
	Threat Intelligence	Cisco Talos
	TLS/SSL Decryption	Cisco Secure Firewall Cisco Umbrella Cisco Secure Connect Radware Alteon
	Vulnerability Management	Cisco Kenna Cisco Secure Workload
	Web Application Firewall (WAF)	Radware WAF Radware kWAF
	Web Reputation Filtering	Cisco Umbrella Cisco Secure Web Appliance Cisco Secure Connect
	Web Security	Cisco Umbrella Cisco Secure Web Appliance Cisco Secure Connect

Capability Icon	Capability Name	Cisco/Cisco Partner Security Solution
	Web Security Connector	Cisco Secure Client (AnyConnect)

Appendix B – SASE/SSE Reference Design

The following is the Cisco SAFE Security Reference Design which identifies the products that deliver the security capabilities required in the Cisco SASE/SSE Reference Architecture.

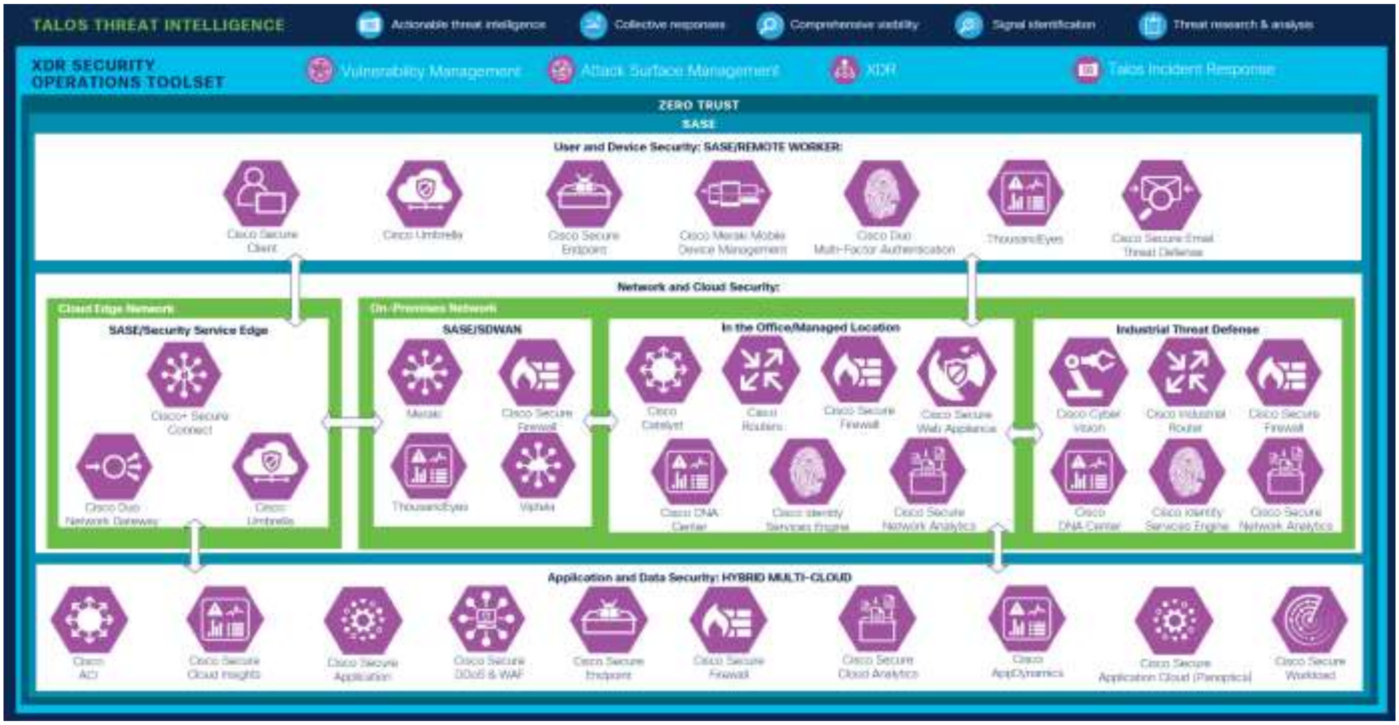
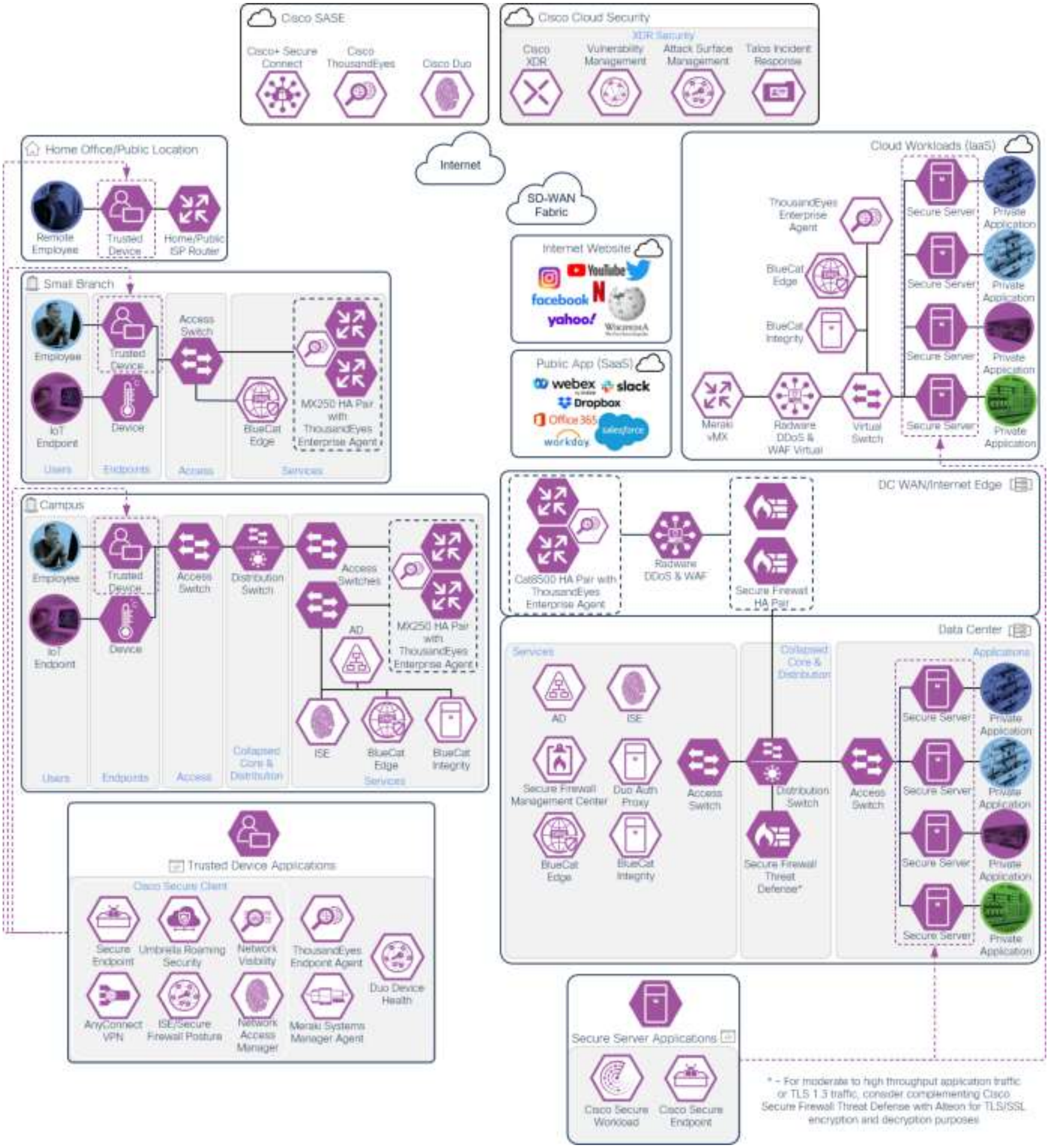

TALOS THREAT INTELLIGENCE
Actionable threat intelligence
Collective responses
Comprehensive visibility
Signal identification
Threat research & analysis
XDR SECURITY OPERATIONS TOOLSET
Vulnerability Management
Attack Surface Management
XDR
Talos Incident Response
ZERO TRUST
SASE
User and Device Security: SASE/REMOTE WORKER:
Cisco Secure Client
Cisco Umbrella
Cisco Secure Endpoint
Cisco Meraki Mobile Device Management
Cisco Duo Multi-Factor Authentication
ThousandEyes
Cisco Secure Email Threat Defense
Network and Cloud Security:
Cloud Edge Network
SASE/Security Service Edge
Cisco+ Secure Connect
Cisco Duo Network Gateway
Cisco Umbrella
On-Premises Network
SASE/SDWAN
Meraki
Cisco Secure Firewall
ThousandEyes
Viptela
In the Office/Managed Location
Cisco Catalyst
Cisco Routers
Cisco Secure Firewall
Cisco Secure Web Appliance
Cisco DNA Center
Cisco Identity Services Engine
Cisco Secure Network Analytics
Industrial Threat Defense
Cisco Cyber Vision
Cisco Industrial Router
Cisco Secure Firewall
Cisco DNA Center
Cisco Identity Services Engine
Cisco Secure Network Analytics
Application and Data Security: HYBRID MULTI-CLOUD
Cisco ACI
Cisco Secure Cloud Insights
Cisco Secure Application
Cisco Secure DDoS & WAF
Cisco Secure Endpoint
Cisco Secure Firewall
Cisco Secure Cloud Analytics
Cisco AppDynamics
Cisco Secure Application Cloud (Panoptica)
Cisco Secure Workload

Figure 22.
Cisco SAFE Security Reference Design

The Cisco Unified SASE Design below identifies the products that deliver the security capabilities required location-by-location in the Cisco SASE/SSE Reference Architecture. A unified SASE solution is more than just a SaaS service provided by a single vendor that provides all SASE network (SD-WAN) and security (DNS-layer security, SWG, FWaaS, CASB, ZTNA) capabilities within a single product. A unified SASE design must also be highly integrated and provide ease of management. Some of the benefits of a unified SASE design are:

- Unified management allowing for efficient creation and deployment of network and security policies
- Improved user experience through consistent security policy enforcement regardless of the user's location
- Improved visibility with integrated SASE components due to unified data

This unified SASE design uses Cisco Secure Connect for the primary SASE security capabilities and is complemented by Cisco Duo for MFA and Cisco ThousandEyes for DEM. The hardware model numbers for SD-WAN routers are only mentioned for reference. Further analysis is required to determine the correct hardware model for your sites.



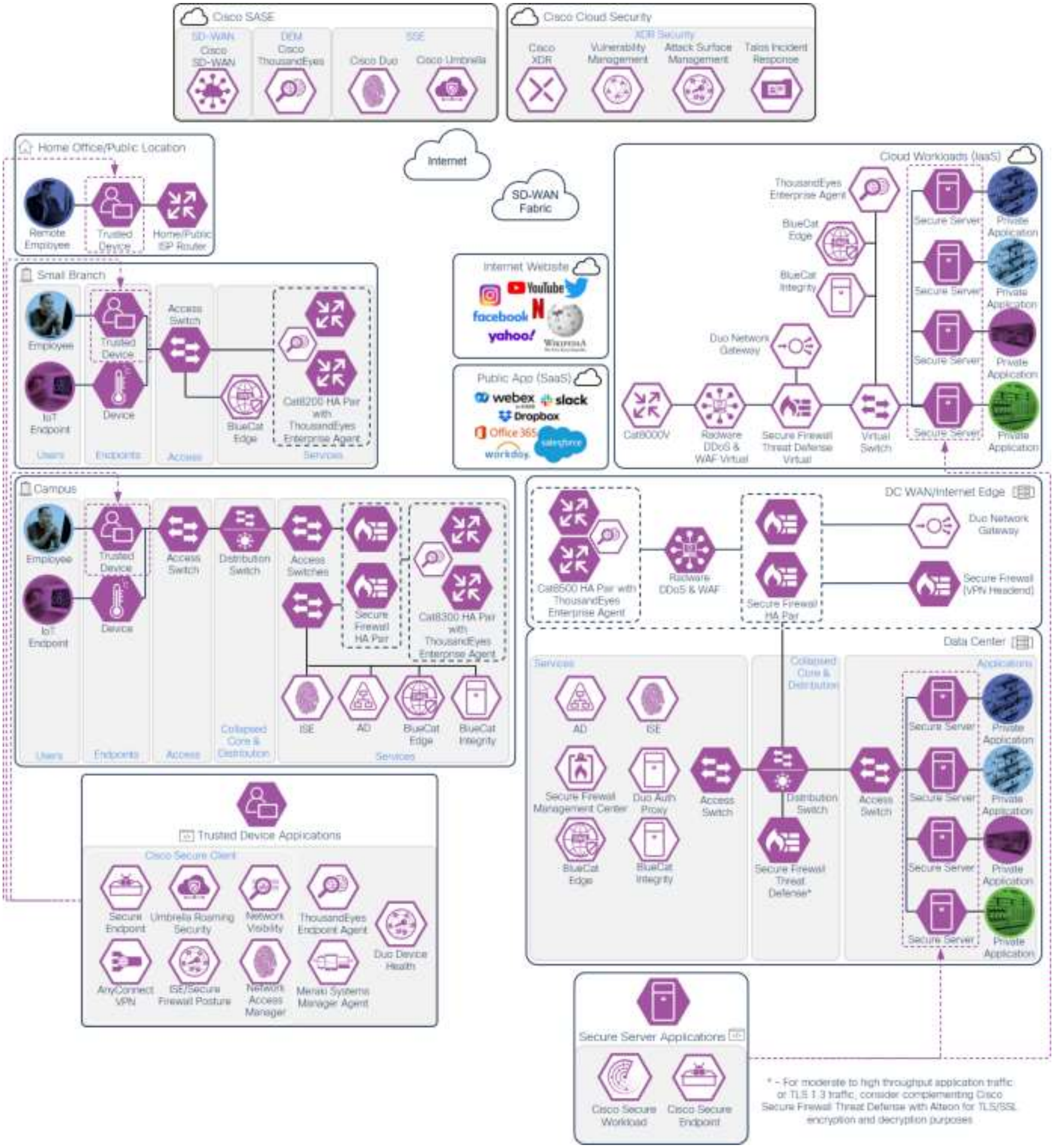
* – For moderate to high throughput application traffic or TLS 1.3 traffic, consider complementing Cisco Secure Firewall Threat Defense with Alteon for TLS/SSL encryption and decryption purposes

Figure 23.
Cisco Unified SASE Design

The Cisco Modular SASE/SSE with Self-Hosted ZTNA & Remote Access Design below also identifies products that deliver the security capabilities required location-by-location in the Cisco SASE/SSE Reference Architecture. Unlike the unified SASE design, this design provides more flexibility for choosing different products for each security capability at the expense of integration and compatibility between products. Still, this design can allow organizations to gradually modify their network rather than moving to a full SASE or SSE architecture all at once. Still, a single vendor unified SSE offers benefits over disparate SSE solutions. These benefits can include:

- Consistent and easier security policy enforcement as all user traffic will get routed through the same SSE cloud for SWG, FWaaS, and CASB functions
- Unified security policy management through a single pane of glass
- Single agent deployment on managed devices, simplifying security software deployment and maintenance

At this time, Cisco's solution for unified SSE uses Umbrella for DNS-layer security, SWG, FWaaS, and CASB security functions but ZTNA and/or Remote Access VPN solutions must be self-hosted. Hardware model numbers for SD-WAN routers are only mentioned for reference. Further analysis is required to determine the correct hardware model for your sites.

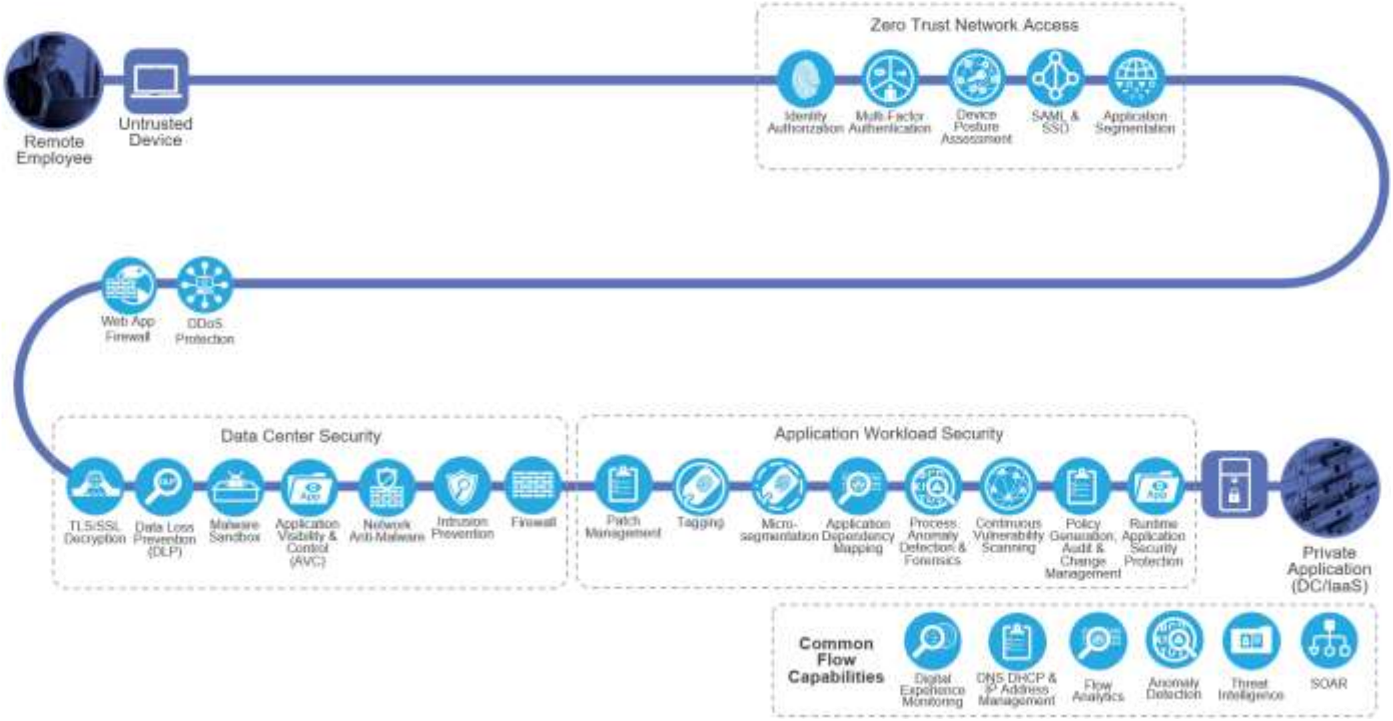


* – For moderate to high throughput application traffic or TLS 1.3 traffic, consider complementing Cisco Secure Firewall Threat Defense with Alteon for TLS/SSL encryption and decryption purposes

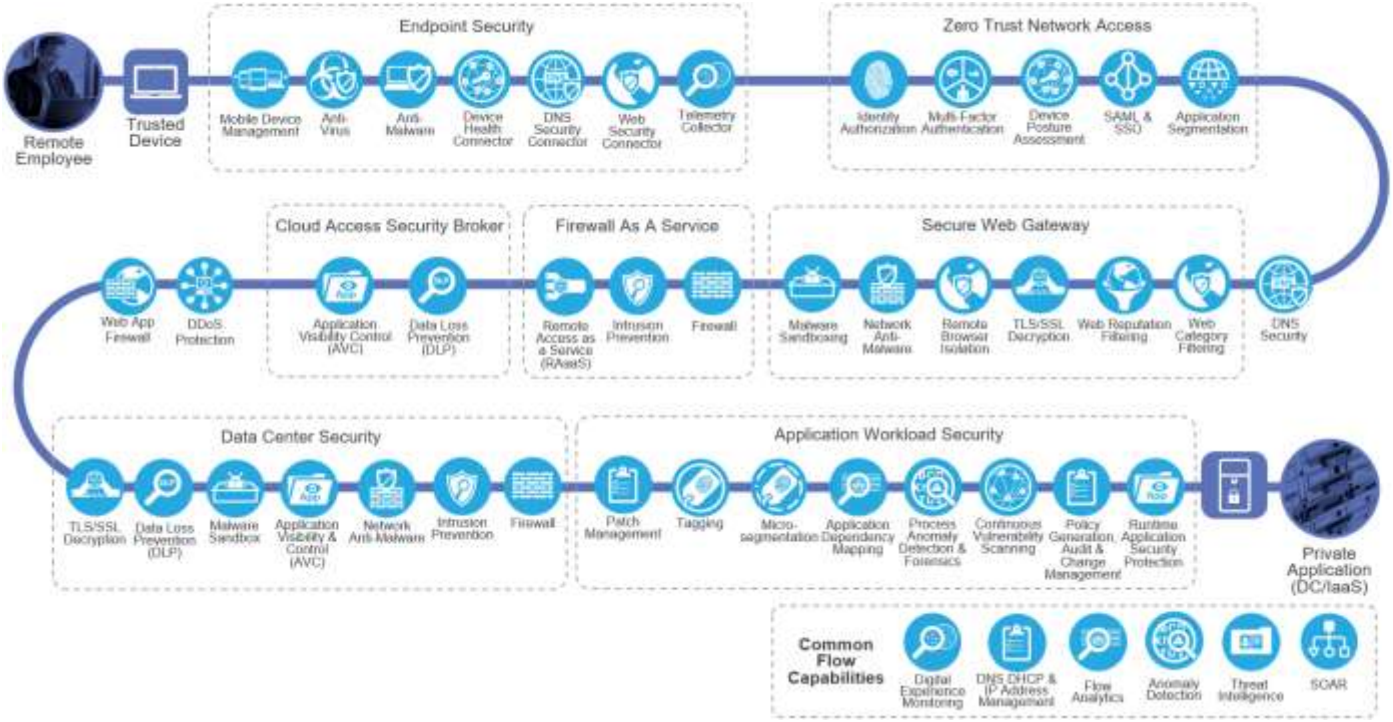
Figure 24.
Cisco Modular SASE/SSE with Self-Hosted ZTNA & Remote Access Design

Appendix C – SASE/SSE Detailed Business Flows with Capabilities

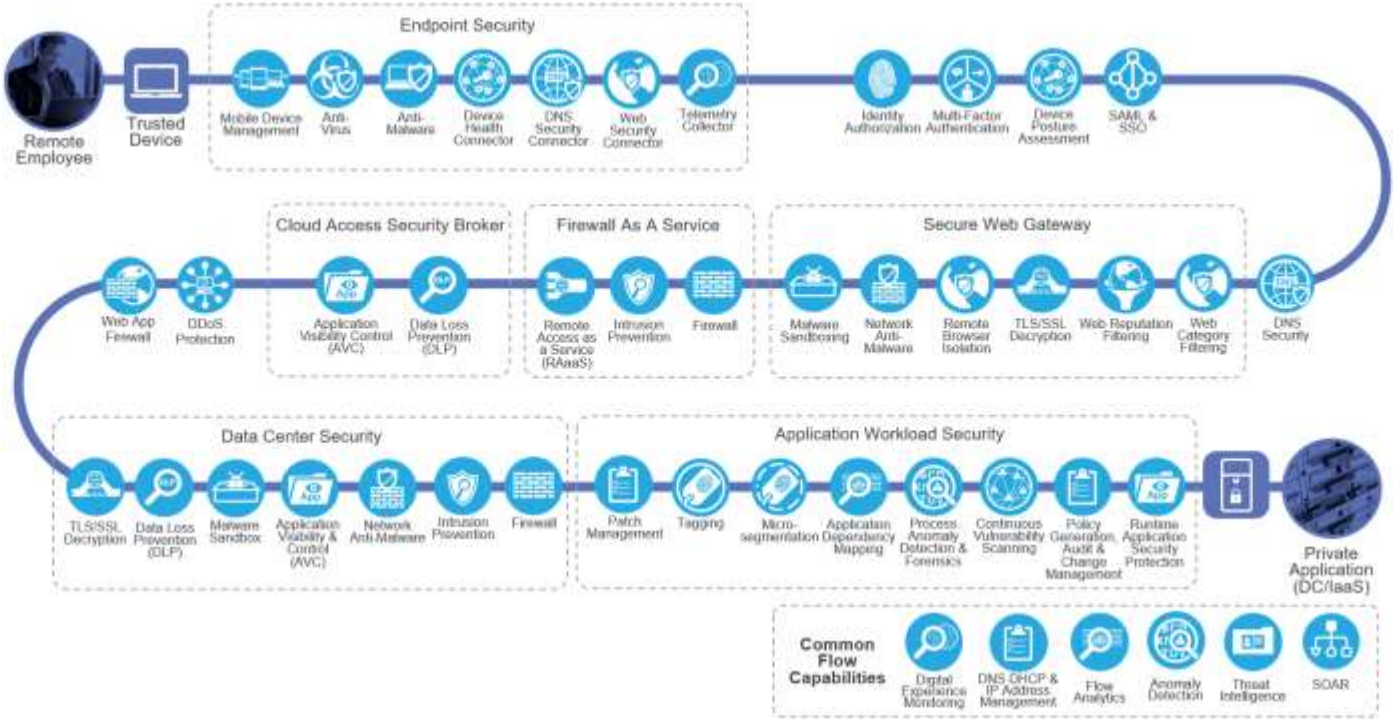
Remote Employee with Untrusted Device: Clientless ZTNA - Accessing Private Application (web/ssh/rdp) (DC/IaaS)


Remote Employee
Untrusted Device
Zero Trust Network Access
Identity Authorization
Multi-Factor Authentication
Device Posture Assessment
SAML & SSO
Application Segmentation
Web App Firewall
DDoS Protection
Data Center Security
TLS/SSL Decryption
Data Loss Prevention (DLP)
Malware Sandbox
Application Visibility & Control (AVC)
Network Anti-Malware
Intrusion Prevention
Firewall
Application Workload Security
Patch Management
Tagging
Micro-segmentation
Application Dependency Mapping
Process Anomaly Detection & Forensics
Continuous Vulnerability Scanning
Policy Generation, Audit & Change Management
Runtime Application Security Protection
Private Application (DC/IaaS)
Common Flow Capabilities
Digital Experience Monitoring
DNS DHCP & IP Address Management
Flow Analytics
Anomaly Detection
Threat Intelligence
SOAR

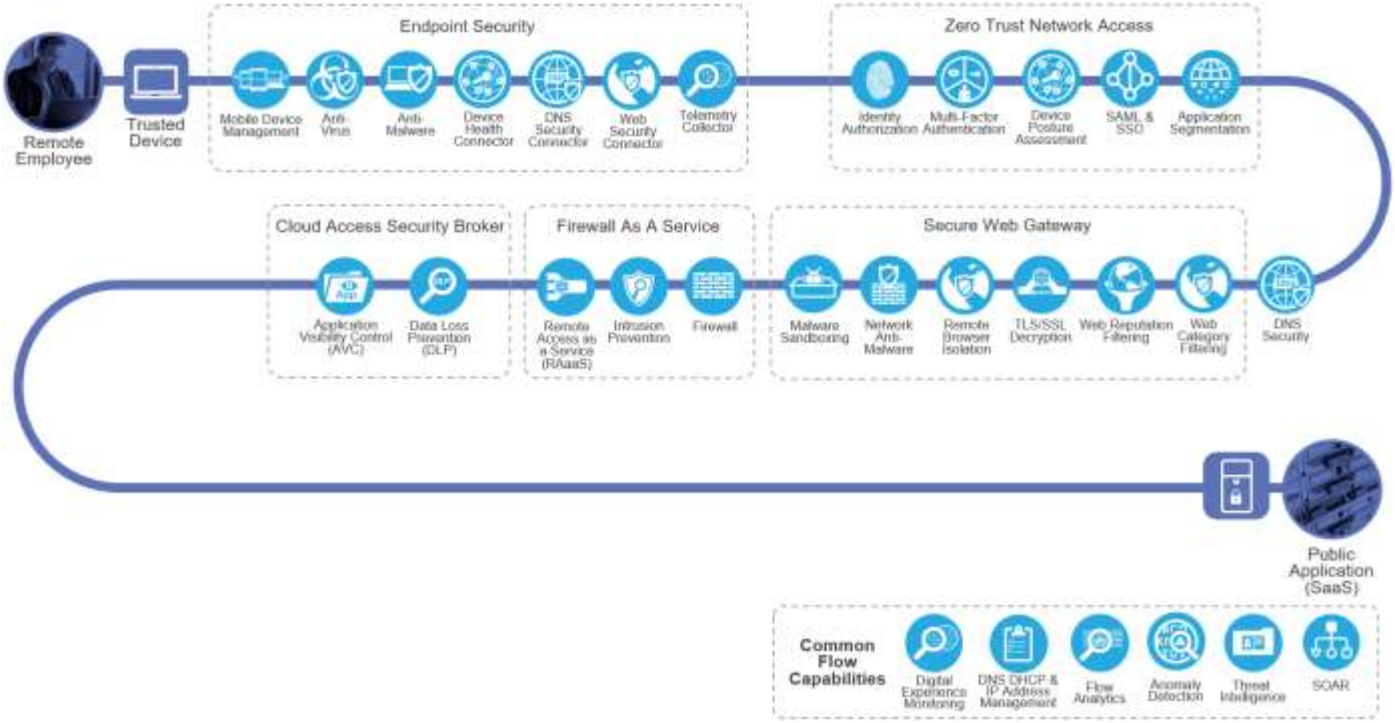
Remote Employee with Trusted Device: Clientless ZTNA - Accessing Private Application (web/ssh/rdp) (DC/IaaS)



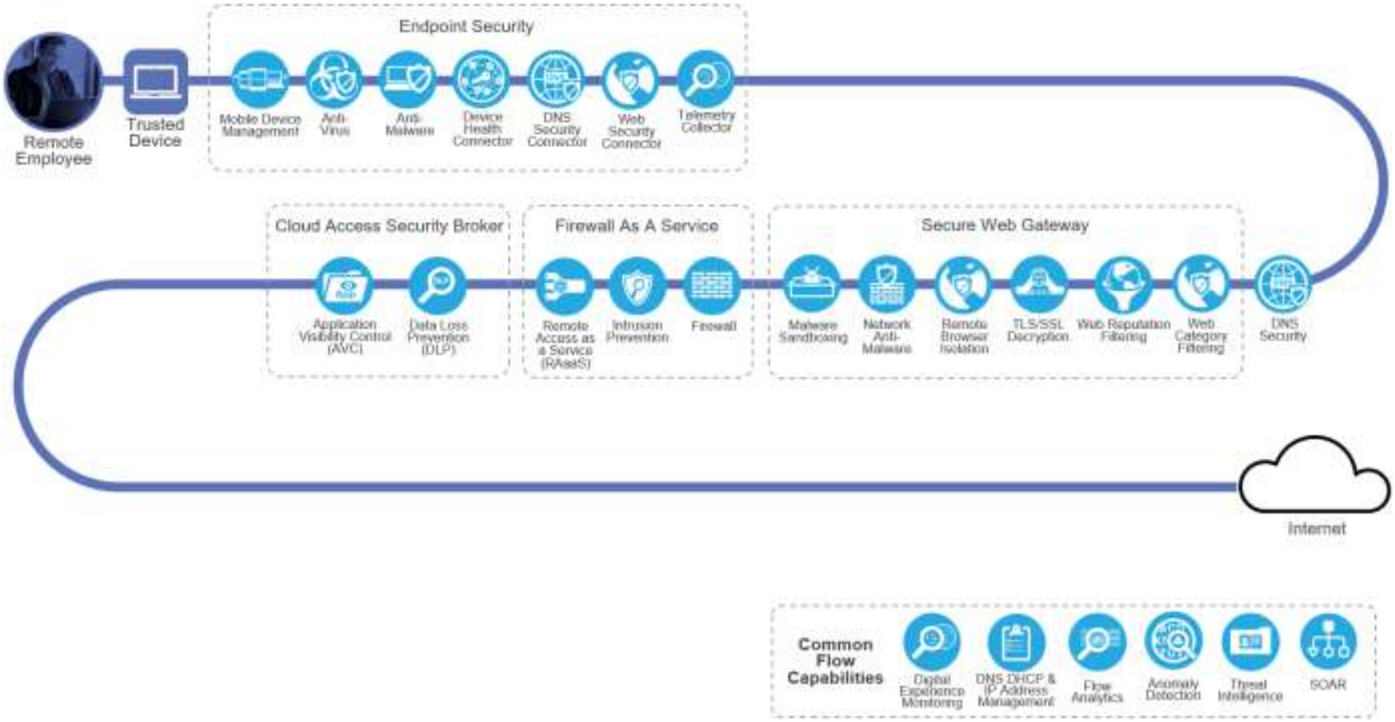
Remote Employee with Trusted Device: Remote Access - Accessing Private Application (any tcp/udp) (DC/IaaS)



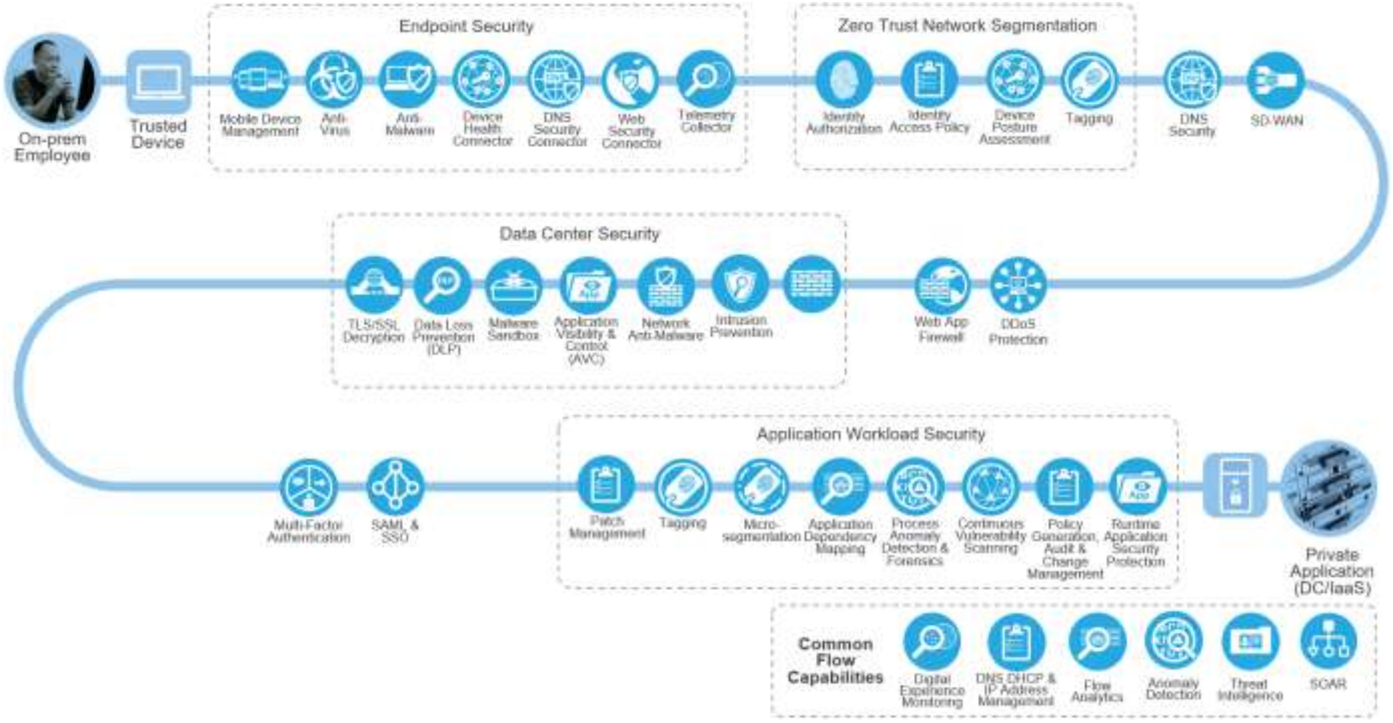
Remote Employee with Trusted Device: Accessing Public Application (SaaS)



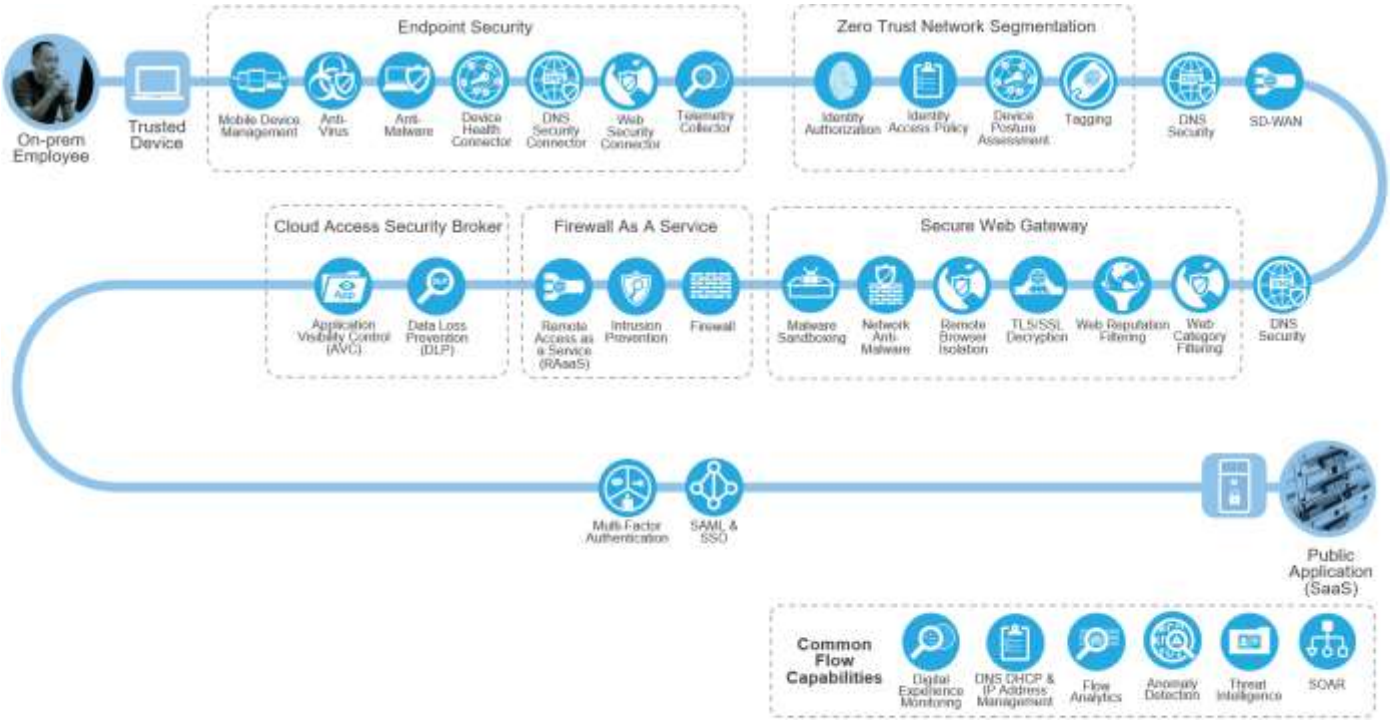
Remote Employee with Trusted Device: Accessing Internet Website



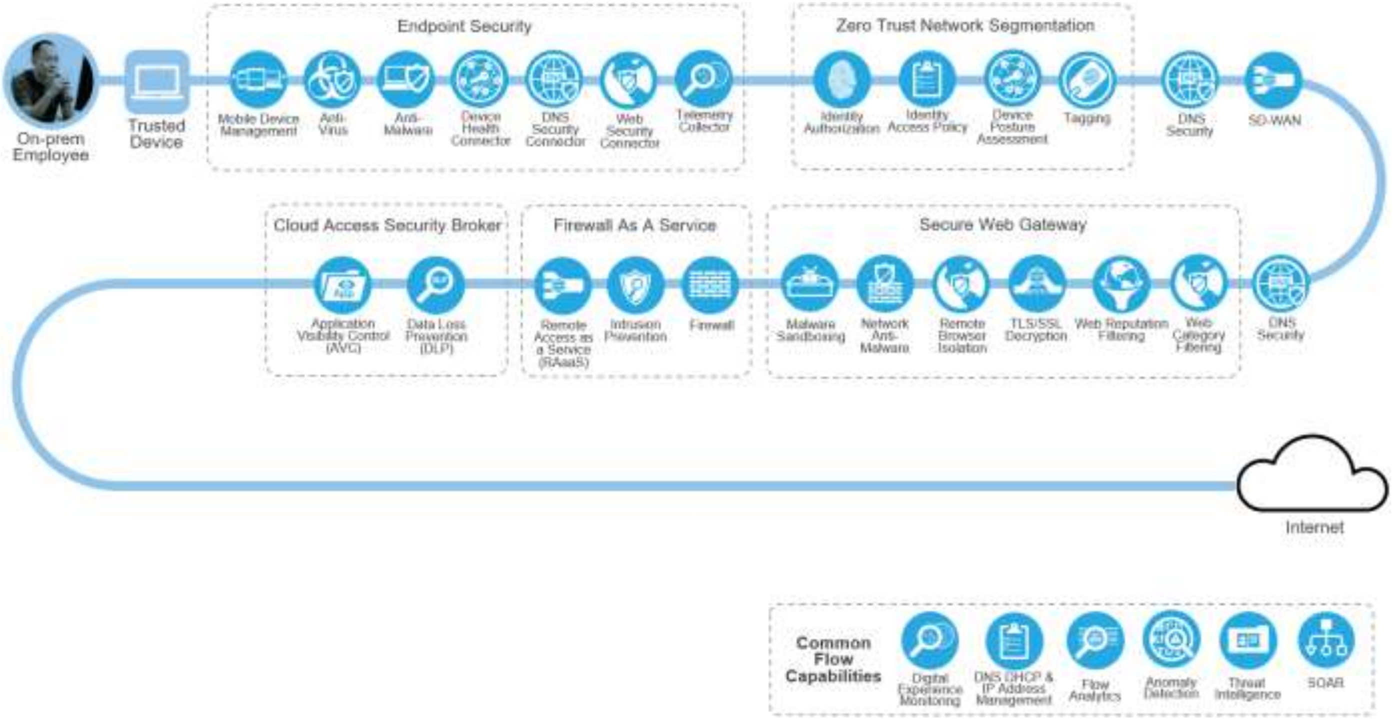
On-prem Employee with Trusted Device: Accessing Private Application (DC/IaaS)



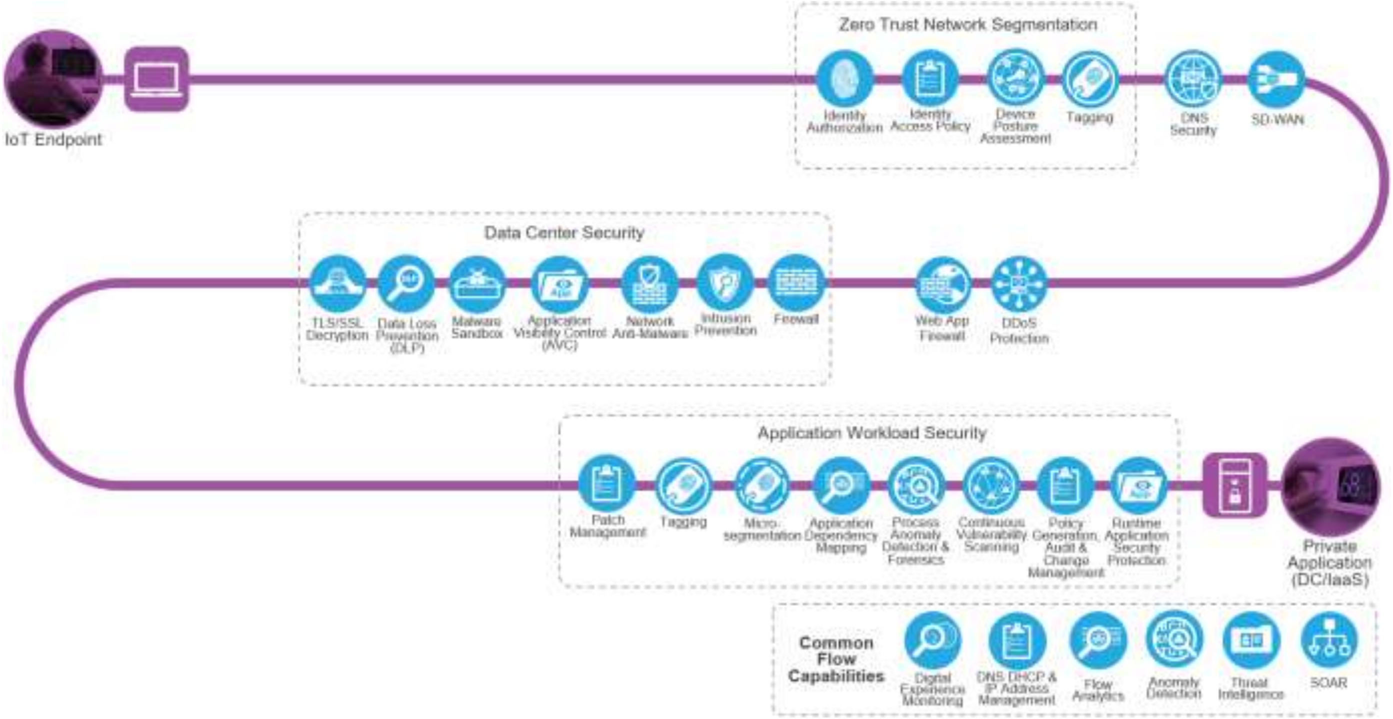
On-prem Employee with Trusted Device: Accessing Public Application (SaaS)



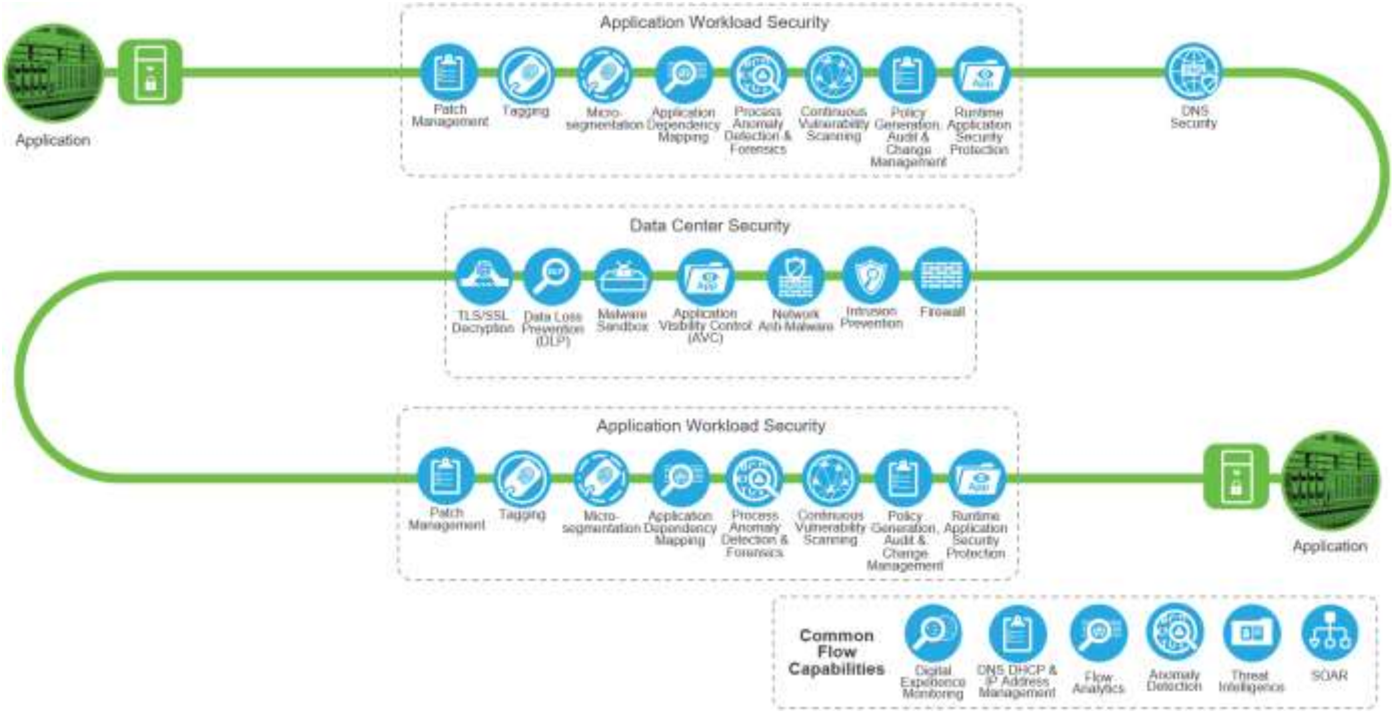
On-prem Employee with Trusted Device: Accessing Internet Website



IoT Endpoint: Accessing Private Application (DC/IaaS)


IoT Endpoint
Zero Trust Network Segmentation
Identity Authorization
Identity Access Policy
Device Posture Assessment
Tagging
DNS Security
SD-WAN
Data Center Security
TLS/SSL Decryption
Data Loss Prevention (DLP)
Malware Sandbox
Application Visibility Control (AVC)
Network Anti-Malware
Intrusion Prevention
Firewall
Web App Firewall
DDoS Protection
Application Workload Security
Patch Management
Tagging
Micro-segmentation
Application Dependency Mapping
Process Anomaly Detection & Forensics
Continuous Vulnerability Scanning
Policy Generation, Audit & Change Management
Runtime Application Security Protection
Private Application (DC/IaaS)
Common Flow Capabilities
Digital Experience Monitoring
DNS DHCP & IP Address Management
Flow Analytics
Anomaly Detection
Threat Intelligence
SOAR

Application: API calls between microservices across Multiple Cloud Providers


Application
Application Workload Security
Patch Management
Tagging
Micro-segmentation
Application Dependency Mapping
Process Anomaly Detection & Forensics
Continuous Vulnerability Scanning
Policy Generation, Audit & Change Management
Runtime Application Security Protection
DNS Security
Data Center Security
TLS/SSL Decryption
Data Loss Prevention (DLP)
Malware Sandbox
Application Visibility Control (AVC)
Network Anti-Malware
Intrusion Prevention
Firewall
Application Workload Security
Patch Management
Tagging
Micro-segmentation
Application Dependency Mapping
Process Anomaly Detection & Forensics
Continuous Vulnerability Scanning
Policy Generation, Audit & Change Management
Runtime Application Security Protection
Application
Common Flow Capabilities
Digital Experience Monitoring
DNS DHCP & IP Address Management
Flow Analytics
Anomaly Detection
Threat Intelligence
SOAR

Appendix D – Acronyms Defined

Considering the design discussed in previous sections of this document, all the capabilities and Cisco solutions corresponding to each capability can be mapped as below.

Acronym	Definition
AD	Active Directory
API	Application programming interface
ASA	Adaptive Security Appliance
AVC	Application Visibility and Control
AWS	Amazon Web Services
BYOD	Bring Your Own Device
DC	Data Center
DDI	DNS, DHCP, and IP Address Management
DDoS	Distributed Denial of Service
DEM	Digital Experience Monitoring
DIA	Direct Internet Access
DLP	Data Loss Prevention
DMZ	Demilitarization Zone
DNS	Domain Name System
EPG	Endpoint Groups
FMC	Firepower Management Center
FQDN	Fully Qualified Domain Name
FTD	Firepower Threat Defense
FWaaS	Firewall as A Service
IaaS	Infrastructure as a Service
IoT	Internet of Things
IPS	Intrusion Prevention System
ISE	Identity Services Engine
ISP	Internet Service Provider
MDM	Mobile Device Management

Acronym	Definition
MFA	Multi-Factor Authentication
MPLS	Multiprotocol Label Switching
MTTR	Mean Time to Repair
MTTI	Mean Time to Identify
MX	Meraki Security
NaaS	Networking as a Service
NDR	Network Detection and Response
OS	Operating System
OSI	Open Systems Interconnection
PaaS	Network Time Protocol
PAC	Network Visibility Module
PoP	Point of Presence
RAaaS	Remote Access as a Service
RBI	Remote Browser Isolation
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SASE	Secure Access Service Edge
SD-WAN	Software Defined Wide Area Network
SECaaS	Security as a Service
SGACL	Security Group Access Control List
SGT	Security Group Tag
SIG	Security Information and Event Management
SQL	Structured Query Language
SSE	Security Service Edge
SSL	Secure Sockets Layer
SSO	Single Sign On
SWG	Secure Web Gateway

Acronym	Definition
TLS	Transport Layer Security
URL	Uniform Resource Locators
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide Area Network
XDR	Extended detection and response
XSS	Cross site scripting
ZTNA	Zero Trust Network Access

Appendix E - References

- Cisco SAFE
- Cisco SASE
- Cisco SD-WAN powered by Meraki
- Cisco SD-WAN powered by Viptela
- Cisco Security Refence Architecture
- Cisco ThousandEyes
- Cisco Umbrella
- BlueCat
- Cisco Secure Data Center Architecture Guide
- Cisco Zero Trust Architecture Guide
- Cisco Secure Connect
- SASE for Dummies

Appendix F - 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.

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**.