Cisco Zero Trust

Architecture Guide

January, 2023

© 2023 Cisco and/or its affiliates. All rights reserved.

Contents

Introduction 3

Cisco Zero Trust Framework 3

Zero Trust Security Frameworks 4

- User and Device Security 4
- Network and Cloud Security 5
- Application and Data Security 6

Cisco SAFE Capabilities 8

- Zero Trust Common Capabilities 8
- Security Capability Groups 9
  - Endpoint Security 9
  - Secure Internet Gateway 10
  - Application Workload Security 11
- Internet Edge Capabilities 12

Cisco SAFE Business Flows 14

- Zero Trust Business Flows 14
- Zero Trust Business Flows - Threat Vectors 14
- Zero Trust Business Flows - Capability Mapping 15
- Zero Trust Business Flows - Capability Mapping by Zero Trust Pillar 16

Cisco Zero Trust Reference Architecture 17

Appendix 19

- Appendix A - Cisco Zero Trust Reference Architecture - Security Capabilities 19
- Appendix B - Cisco Zero Trust Reference Design 23
- Appendix C - Zero Trust Detailed Business Flows with Capabilities 24
- Appendix D - Acronyms Defined 31
- Appendix E - References 32
- Appendix F - Feedback 32

© 2023 Cisco and/or its affiliates. All rights reserved.

Introduction

Zero trust is a strategic approach to security that centers on the concept of eliminating trust from an organization's network architecture. Trust is neither binary nor permanent. It can no longer be assumed that internal entities are trustworthy, that they can be directly managed to reduce security risk, or that checking them one time is enough. The zero-trust model of security prompts you to question your assumptions of trust at every access attempt.

Traditional security approaches assume that anything inside the corporate network can be trusted. The reality is that this assumption no longer holds true, thanks to mobility, BYOD (Bring Your Own Device), IoT (Internet of Things), cloud adoption, increased collaboration, and a focus on business resiliency. A zero-trust model considers all resources to be external and continuously verifies trust before granting only the required access.

The key to comprehensive Zero Trust is extending security throughout the entire network environment with examples such as:

- Employees accessing sensitive applications, both on and off the enterprise network
- Contractors and guests using the network infrastructure
- Application to application communications
- Communication between industrial control systems

Cisco Zero Trust Framework

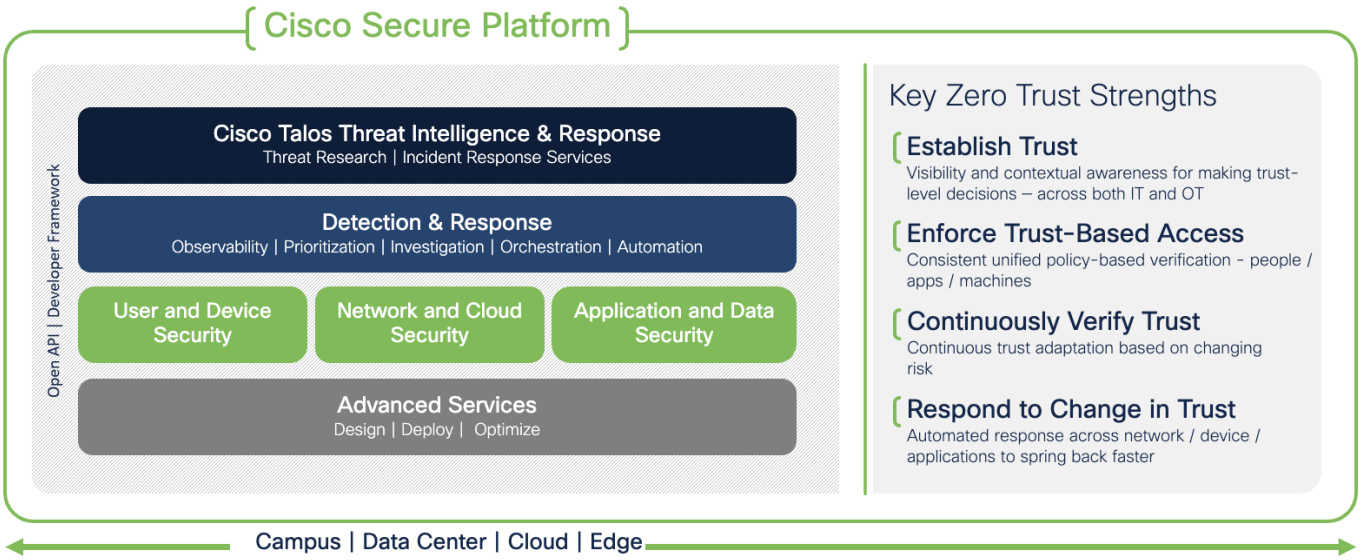


Figure 1. Cisco Zero Trust Framework

Security is not a one-size-fits-all and Zero Trust is more than network segmentation. 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

© 2023 Cisco and/or its affiliates. All rights reserved.

- **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

Zero Trust Security Frameworks

The following table shows how Zero Trust Frameworks map to the Cisco Zero Trust Framework.

Cisco	NIST Cyber Security Framework	CISA	Common
User and Device Security	Users	Identity	Visibility & Analytics Automation & Orchestration Governance
	Devices	Device	
Network and Cloud Security	Networks/Hybrid Multi-Cloud	Network/ Environment	
Application and Data Security	Applications	Application Workload	
	Data	Data	

This architecture guide is focused on the Cisco Zero Trust Framework with the User and Device Security, Application and Data Security, and Network and Cloud Security pillars. If interested in how Cisco products map to other Zero Trust Frameworks, refer to Zero Trust Frameworks.

User and Device Security

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.

With a zero-trust approach to securing users and devices, you can help prevent or mitigate against several different types of attacks that target users and devices in this new perimeter-less world:

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.

© 2023 Cisco and/or its affiliates. All rights reserved.

The ideal end state of your zero trust for user and device security would allow your enterprise to answer the following:

- **Are my users really who they say they are?** Verify the identity of every user, regardless of type (contractors, vendors, third-party providers, partners, remote users, employees, temporary workers, etc.)
- **What devices are connecting to my applications and data** Get visibility into every type of device, both managed or unmanaged (mobile, laptops, and desktops; company-issued, -owned, or -managed; user-owned)
- **Who or what is allowed to access my applications and data?** By enforcing adaptive access policies, you can limit access to enterprise applications and data based on user role, type of device, security health of user devices, user group, application type, and much more
- **How can I enable remote, frictionless access for all users?** With a remote-access proxy, you can enable access to multi-cloud environments, web applications, servers, VPNs, and more for employees, remote workers, and contractors. With Single Sign-On (SSO), you can allow users to securely access their cloud and on-premises applications seamlessly by logging in just once

Network and Cloud Security

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.

With a zero-trust approach to securing the workplace, you can help prevent or mitigate against several different types of attacks that target the network:

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.
	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.

In an enterprise architecture, the network may span multiple domains, locations, or sites such as main campuses and remote branches, each with multiple devices, services, and policies. A Zero Trust solution should demand an end-to-end architecture that ensures consistency in terms of connectivity, segmentation, and policy across the full spectrum of the network.

Zero Trust for the network and application security enables network administrators to:

- **Know who is on the network.** To truly secure the network, you need to know what is connecting to it. For managed devices, such as laptops and smartphones, mobile device management (MDM) can be used to determine what the connecting device is what it says it is. For unmanaged devices, such as

© 2023 Cisco and/or its affiliates. All rights reserved.

BYOD or IoT devices, network-based machine learning can be used to identity attributes for categorization, while sensitive workloads can be limited to managed devices controlled by the enterprise

- **Define what endpoints can access.** Segmentation and access policies should be easily defined for individual devices as well as groups of similar devices. These policies should be defined with least privilege access to help ensure that the devices have only the minimal level of access to minimize the potential for lateral movement of threats
- **Provide always-on analysis and enforcement.** Security threats are always evolving, so a continuous loop of analysis and enforcement must be administered to stay atop intrusions and vulnerabilities. It is important to understand traffic norms and identity the out-of-policy traffic, enabling device isolation in the case of an event

Application and Data Security

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. With a zero-trust approach to securing applications and data, you can help prevent or mitigate against several different types of attacks that target applications:

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.

The need for comprehensive visibility of all network traffic down to the individual workload level for effective security policy management and enforcement has never been more important than now. The ideal end state of your zero trust for the workloads solution would allow your enterprise to answer the following:

© 2023 Cisco and/or its affiliates. All rights reserved.

- **Do I have complete visibility of application communication?** Achieving comprehensive zero trust and true end-to-end visibility across on-premises and multi-cloud environments requires robust network-based detection and response. It is critical to understand who and what are on the network before any segmentation policies can be applied
- **Can I control workloads moving laterally throughout the network?** When you have visibility across how the digital business operates, you can create smart segmentation policies to control access to critical resources. This ability is very important to prevent threats from spreading and creating a significant impact.
- **Do I understand the posture of my applications and are they compliant with industry best practices?** Organizations that have moved resources and workloads to public cloud environments like AWS, Azure, and Google Cloud Platform face a multitude of new security, policy, and compliance-related challenges. Developing robust cloud security posture management (CSPM) capabilities such as monitoring risk exposure levels related to configuration, network segmentation, user, and system events helps guarantee sound policy management and protect against data leakage

© 2023 Cisco and/or its affiliates. All rights reserved.

Cisco SAFE Capabilities

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

Zero Trust Common Capabilities

The following common capabilities are included in Cisco Zero Trust.

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.
	Device Posture Assessment	The device posture assessment analyzes the device and assesses its security posture, and reports it to the policy decision management system.
	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.
	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	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.
	Security Assertion Markup Language (SAML) & Single Sign on (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.
	Security Orchestration Automation and Response (SOAR)	SOAR is a set of technologies that enable organizations to collect information monitored by the security operations team.

© 2023 Cisco and/or its affiliates. All rights reserved.

Capability Icon	Capability Name	Capability Description
	Threat Intelligence	Knowledge of emerging threats from active adversaries is shared with solutions that will utilize the information to protect the organization.

Security Capability Groups

A security capability group is made up of multiple security capabilities.

The security capability groups are:

- Endpoint Security
- Secure Internet Gateway
- Application Workload Security

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.

© 2023 Cisco and/or its affiliates. All rights reserved.

Capability Icon	Capability Name	Capability Description
	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	Mobile device management (MDM) 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.
	Web Security Connector	The Web security connector redirects all web traffic to a full web proxy that provides secure web gateway security services.

Secure Internet Gateway

A Secure Internet Gateway (SIG) unifies multiple functions in a single solution that traditionally required a set of on-premises security appliances (firewalls, proxies, gateways) or single function cloud-based security solutions.

Capability Icon	Capability Name	Capability Description
	Application Visibility & Control	Visibility and access control to approved web applications.
	Cloud Access Security Broker (CASB)	An intermediary between cloud providers, cloud-based applications, and cloud consumers to enforce an organization's security policies and usage.
	Data Loss Prevention	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 Security	DNS security enforces security at the DNS layer to block malware, phishing, and command and control callbacks over any port.
	Firewall	Macro segmentation is the process of separating a network topology into smaller sub-networks, often known as zones. A firewall is typically the enforcement point between zones in a network.

© 2023 Cisco and/or its affiliates. All rights reserved.

Capability Icon	Capability Name	Capability Description
	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.
	Remote Browser Isolation	Provides an added layer of protection against browser-based security threats for high-risk users. RBI moves the most dangerous part of browsing the internet away from the end user's machine and into the cloud.
	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.

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.

© 2023 Cisco and/or its affiliates. All rights reserved.

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 and Change Management	The output of application dependency mapping provide 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 Self-Protection (RASP)	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/Grouping for Software Defined Policy	Segmentation using Endpoint Groups (EPG), TrustSec Security Group Tag (SGT), or VLANs.

Internet Edge Capabilities

The following Internet edge capabilities are included in Cisco Zero Trust.

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.

© 2023 Cisco and/or its affiliates. All rights reserved.

Capability Icon	Capability Name	Capability Description
	Remote Access VPN	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.
	Reverse Proxy	Allows users to securely access to on-premises websites, web applications, and SSH servers using any browser, from anywhere in the world without having to install, configure remote access software on their device.
	Software Defined-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.
	Web Application Firewall	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.

© 2023 Cisco and/or its affiliates. All rights reserved.

Cisco SAFE Business Flows

Zero Trust 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 B.

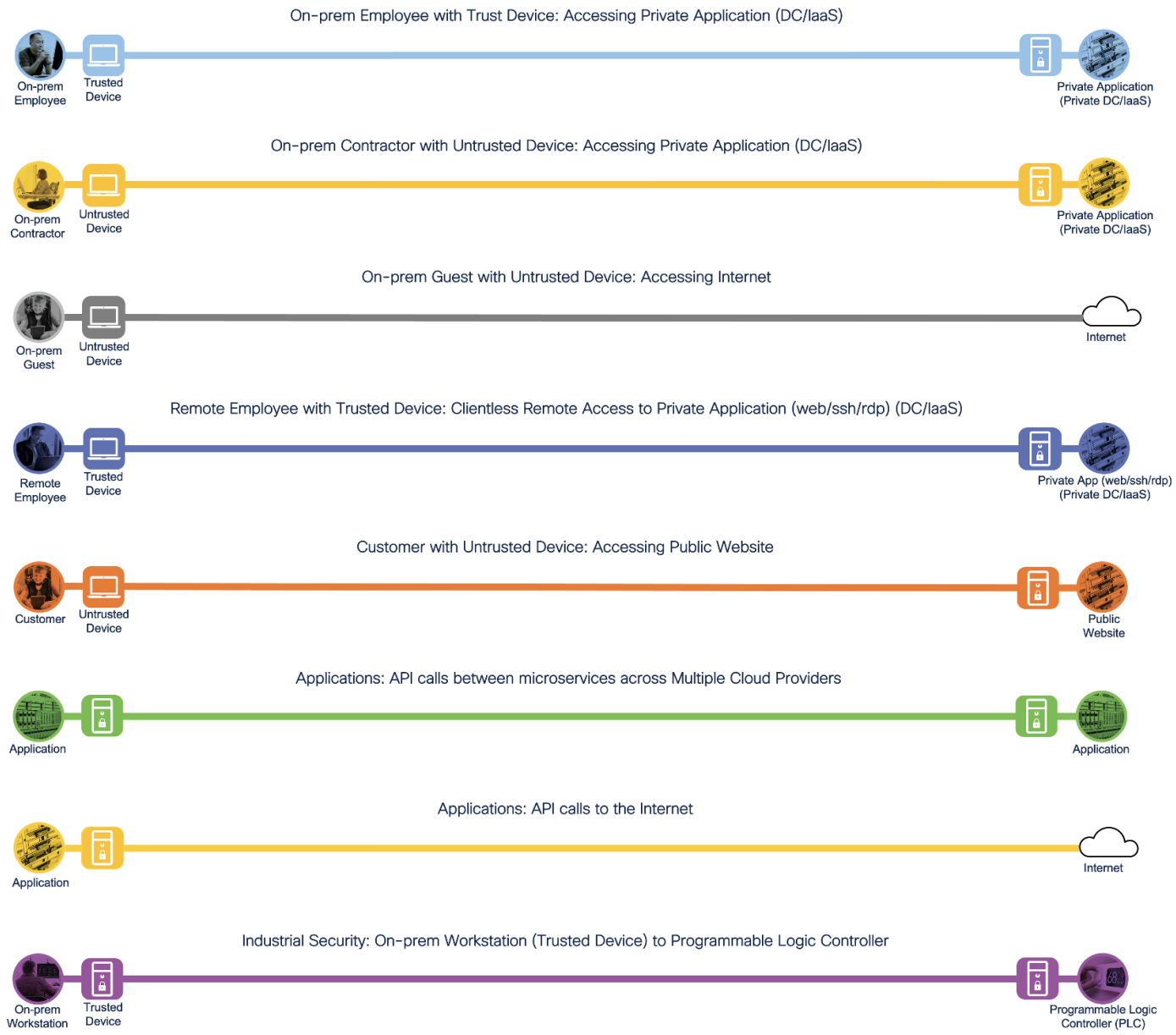


Figure 2. Zero Trust Business Flows

Zero Trust Business Flows - Threat Vectors

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.

© 2023 Cisco and/or its affiliates. All rights reserved.

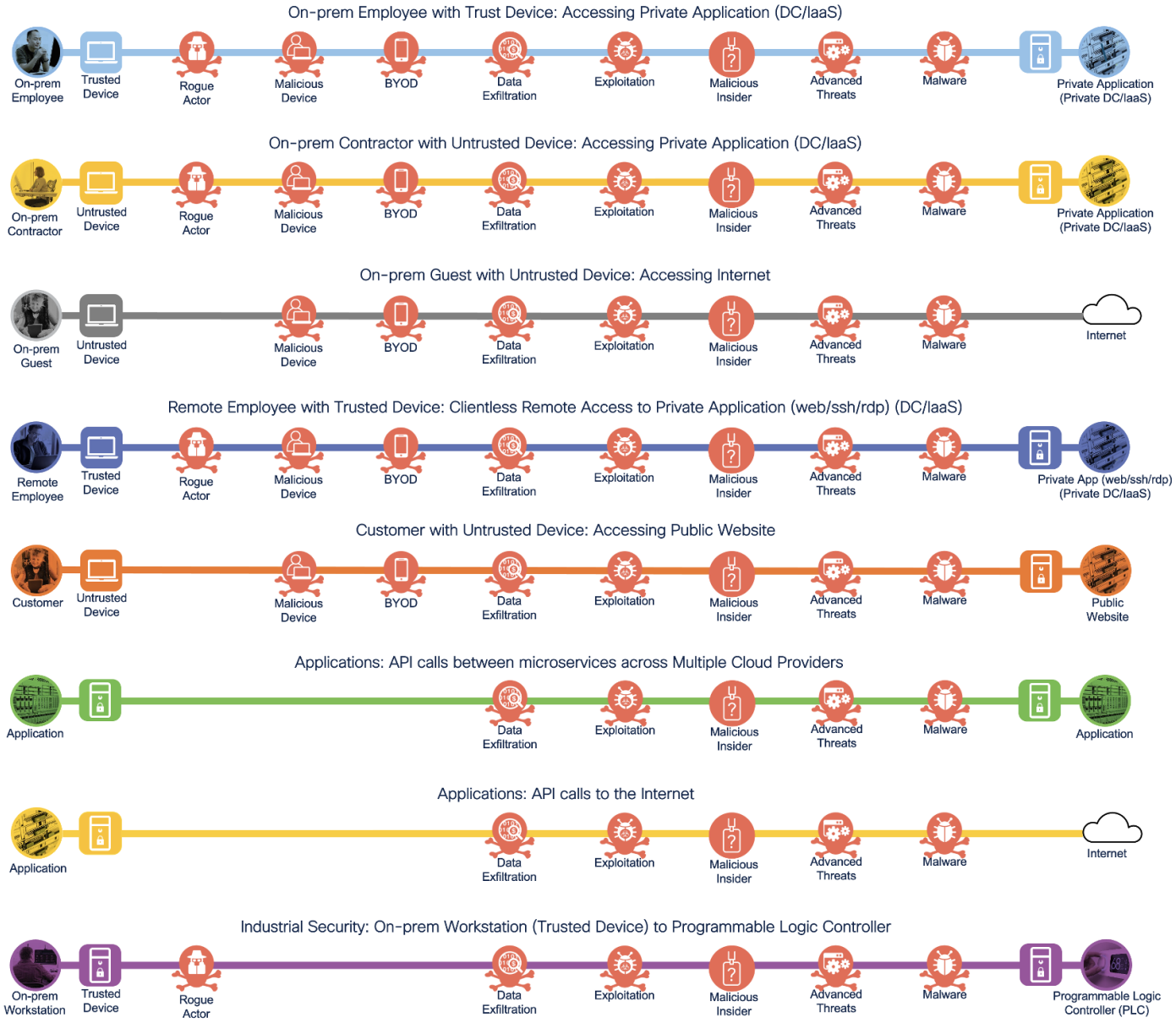


Figure 3. Zero Trust Business Flows with Threat Vectors

Zero Trust Business Flows - Capability Mapping

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 thus, 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.

© 2023 Cisco and/or its affiliates. All rights reserved.

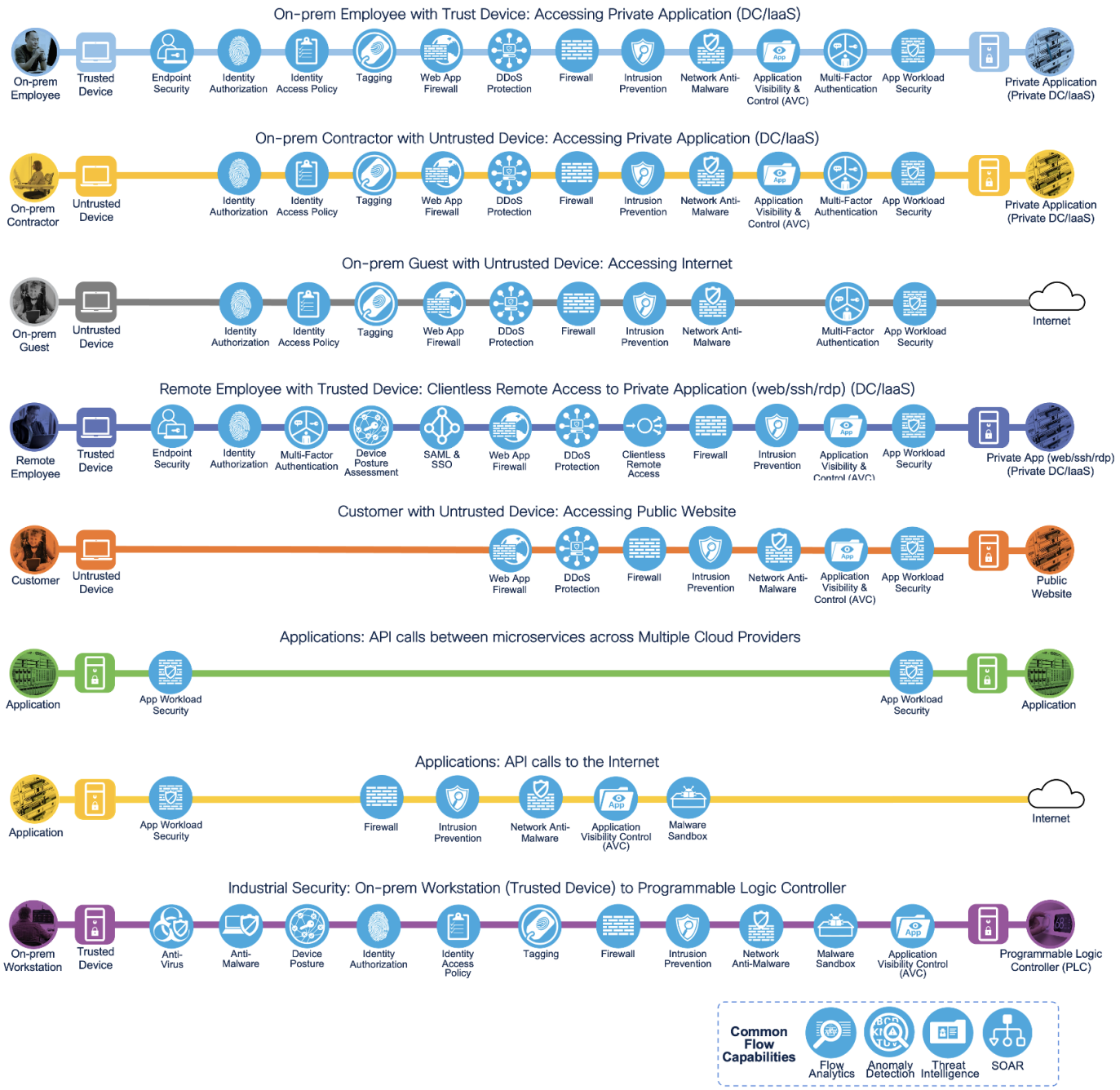


Figure 4. Zero Trust Business Flows with Capabilities

The capabilities required to protect the business flow are represented above. This is a consolidated view of the business flows with capabilities. The detail business flows with the security capability groups expanded out can be found in the Appendix C.

The Common Flow Capabilities grouping is a common set of capabilities that applies to all flows.

Zero Trust Business Flows - Capability Mapping by Zero Trust Pillar

The mapping of security capabilities to zero trust pillar are represented below for each of the zero trust business flows.

© 2023 Cisco and/or its affiliates. All rights reserved.

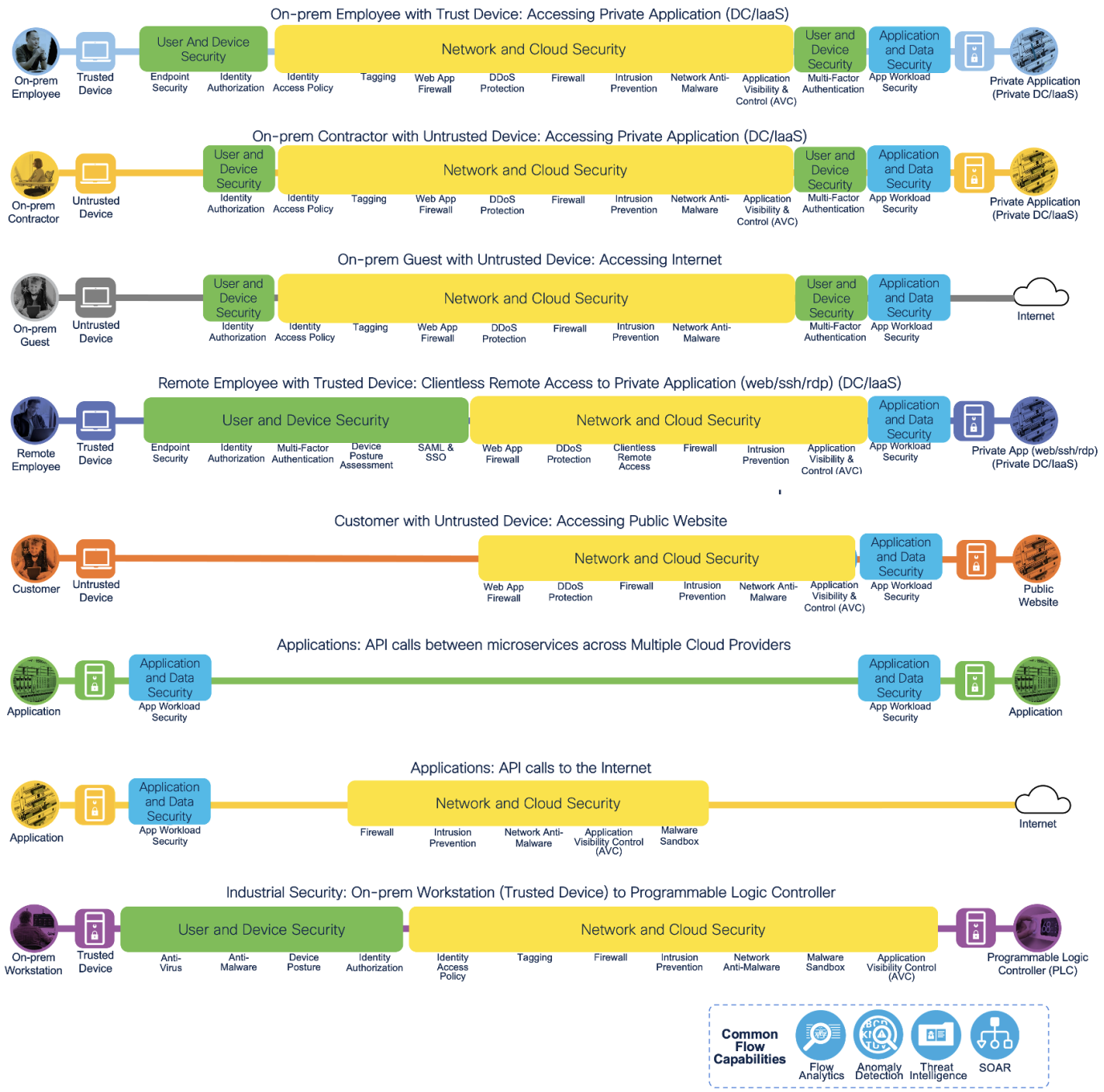


Figure 5. Zero Trust Business Flows with Capabilities by Zero Trust Pillar

Cisco Zero Trust Reference Architecture

The Cisco Zero Trust Reference Architecture below includes the architectural components needed to deliver the security capabilities by zero trust pillar. The Cisco Zero Trust Reference Architecture is included in the Cisco Security Reference Architecture and is presented below in that format and merging it with the SAFE methodology.

© 2023 Cisco and/or its affiliates. All rights reserved.

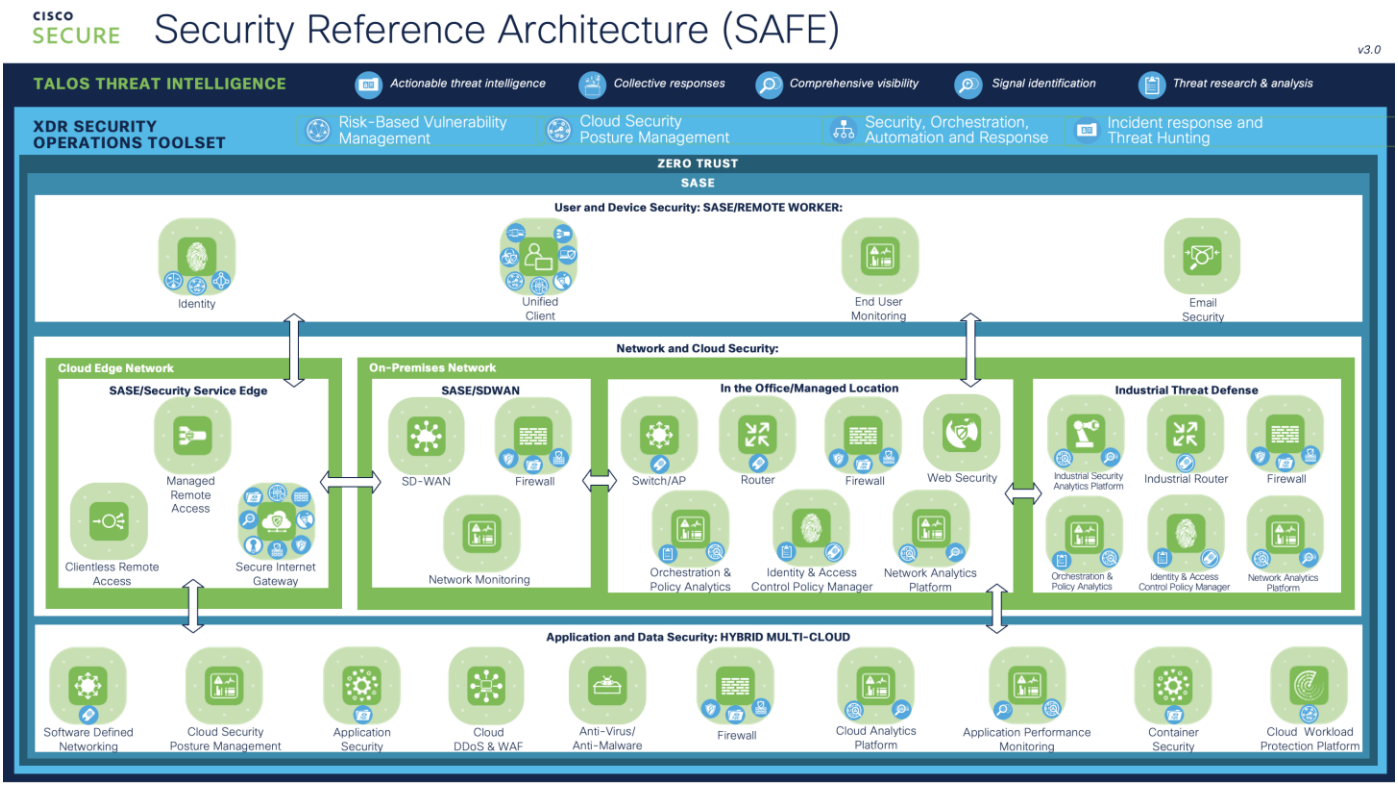


Figure 6. **Cisco Zero Trust Reference Architecture**

© 2023 Cisco and/or its affiliates. All rights reserved.

Appendix

Appendix A - Cisco Zero Trust Reference Architecture - Security Capabilities

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

Capability Icon	Capability Name	Security Solution
	Anomaly Detection	Cisco Secure Network Analytics Cisco Cyber Vision Cisco Secure Cloud Analytics Cisco Secure Access by Duo
	Anti-Virus	Cisco Secure Endpoint
	Anti-Malware	Cisco Secure Endpoint (integrated with Umbrella, Firewall & SD-WAN) Cisco Secure Malware Analytics
	Application Dependency Mapping	Cisco Secure Workload
	Application Visibility & Control	Cisco Umbrella Cisco Secure Firewall Cisco Secure Workload Cisco AppDynamics Cisco Secure Application Cisco Secure Web Appliance Cisco Cloudlock Cisco Meraki
	Asset Management	Cisco Secure Cloud Insights
	Cloud Access Security Broker (CASB)	Cisco Umbrella Cisco Cloudlock
	Cloud Security Posture Management (CSPM)	Cisco Secure Cloud Insights
	Endpoint Security	Cisco Secure Endpoint Cisco Secure Access by Duo Device Health Application

© 2023 Cisco and/or its affiliates. All rights reserved.

Capability Icon	Capability Name	Security Solution
	Data Loss Prevention	Cisco Cloudlock Cisco Umbrella
	Device Health Connector	Cisco Duo Device Health
	Device Posture Assessment	Cisco Secure Access by Duo
	Distributed Denial of Service (DDoS) Mitigation	Radware DDoS
	DNS Security	Cisco Umbrella
	DNS Security Connector	Cisco Secure Client (AnyConnect) Cisco Umbrella Virtual Appliance
	Firewall	Cisco Secure Firewall Cisco Umbrella Cisco Secure Workload Cisco Meraki MX
	Flow Analytics	Cisco Secure Network Analytics Cisco Secure Cloud Analytics Cisco Cyber Vision Cisco Secure Workload
	Identity Authorization	Cisco Secure Access by Duo Cisco Identity Services Engine
	Intrusion Prevention	Cisco Secure Firewall Cisco Umbrella
	Malware Sandbox	Cisco Secure Malware Analytics

© 2023 Cisco and/or its affiliates. All rights reserved.

Capability Icon	Capability Name	Security Solution
	Mobile Device Management	Cisco Meraki Mobile Device Manager
	Micro-Segmentation	Cisco Identity Services Engine Cisco Secure Workload Cisco Secure Application
	Multi-Factor Authentication	Cisco Secure Access by Duo
	Network Anti-Malware	Cisco Secure Firewall Cisco Umbrella Cisco Meraki MX Cisco Secure Email Appliance Cisco Secure Web Appliance
	Policy Generation, Audit and 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 Choice
	Remote Browser Isolation	Cisco Umbrella
	Reverse Proxy	Cisco Duo Network Gateway
	Runtime Application Self-Protection (RASP)	Cisco Secure Application
	Security Assertion Markup Language (SAML) & Single Sign on (SSO)	Cisco Secure Access by Duo

© 2023 Cisco and/or its affiliates. All rights reserved.

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

© 2023 Cisco and/or its affiliates. All rights reserved.

Appendix B – Cisco Zero Trust Reference Design

The following is the Cisco Zero Trust Reference Design which identifies the products that deliver the security capabilities required in the Cisco Zero Trust Reference Architecture.

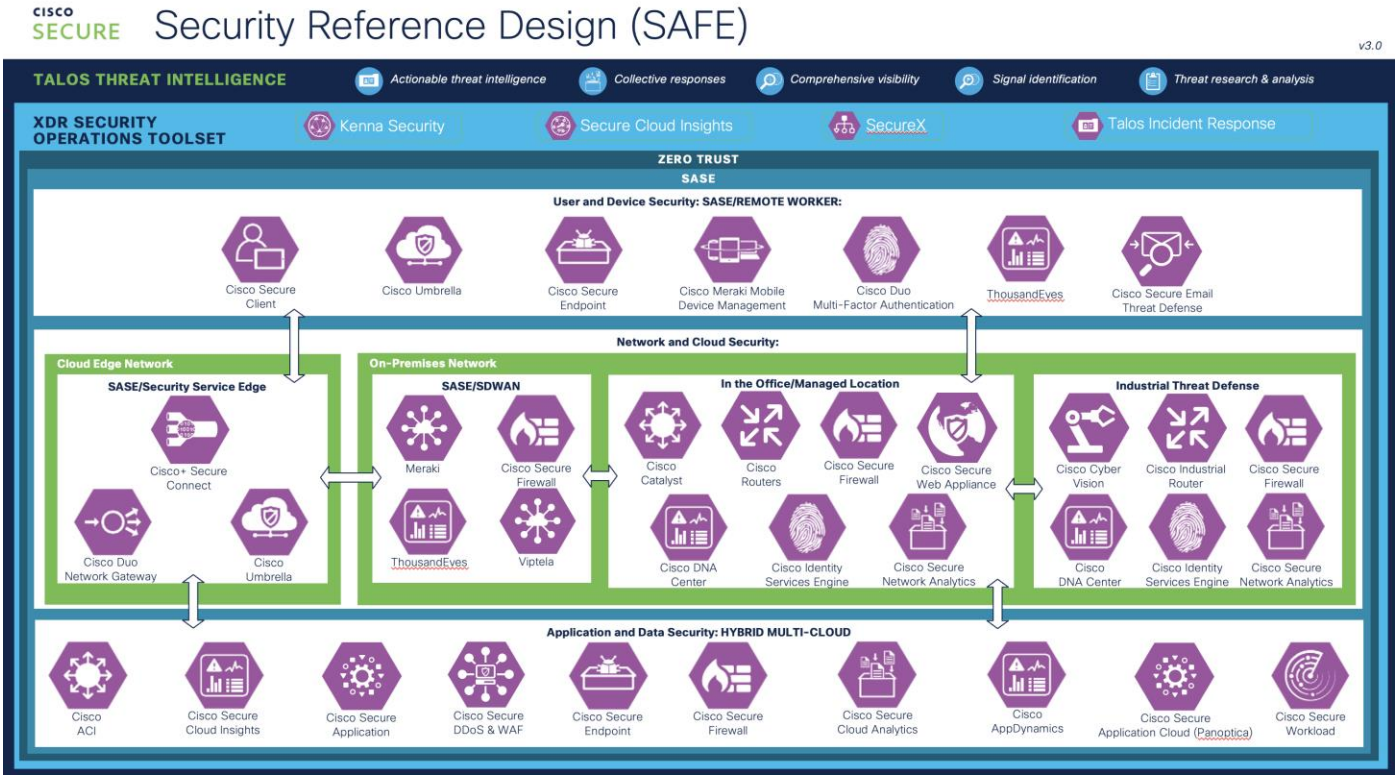
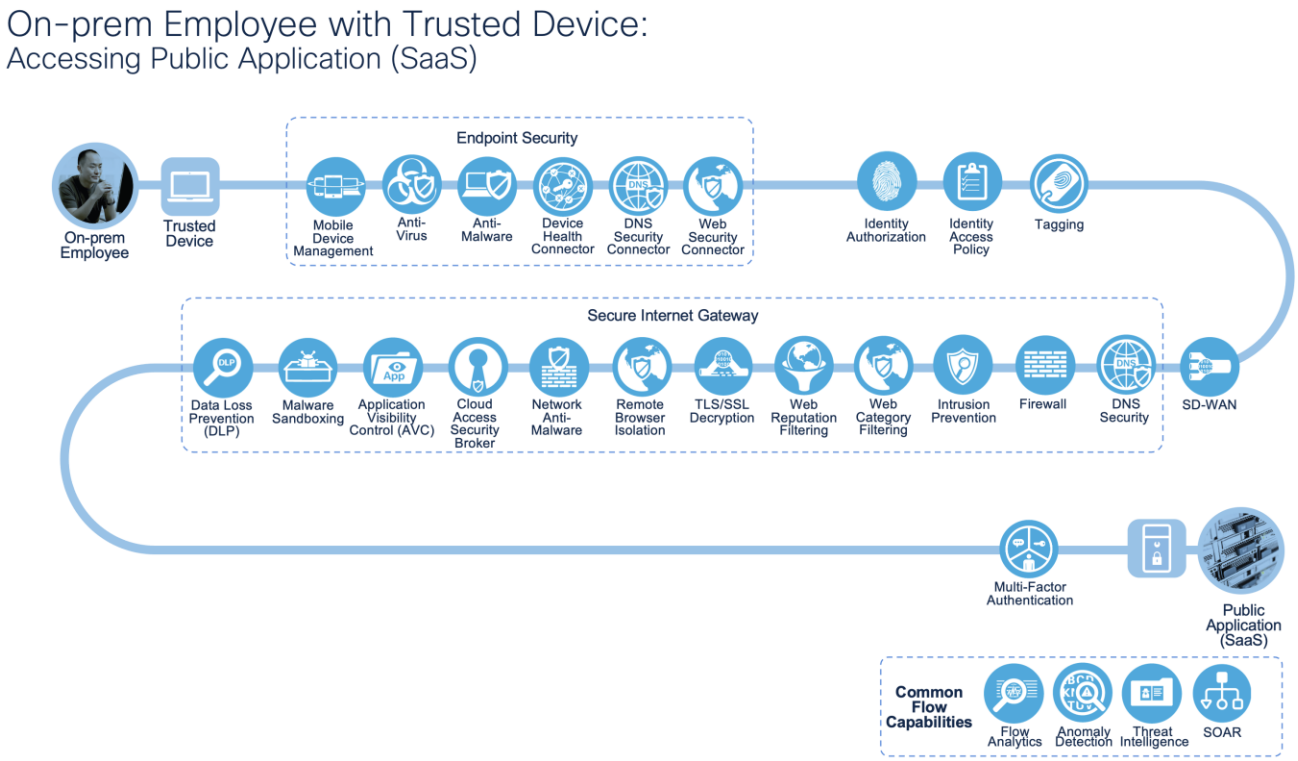


Figure 7. Cisco Zero Trust Reference Design

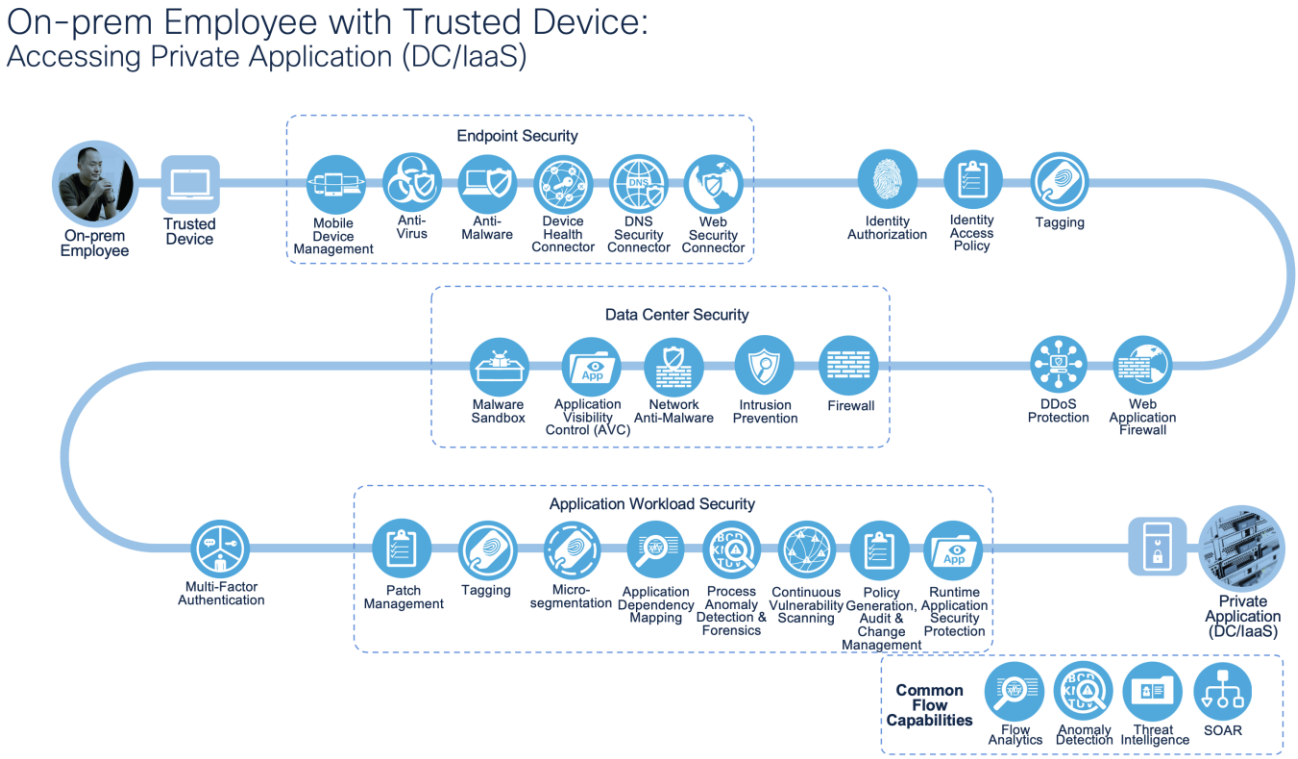
© 2023 Cisco and/or its affiliates. All rights reserved.

Appendix C – Zero Trust Detailed Business Flows with Capabilities

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

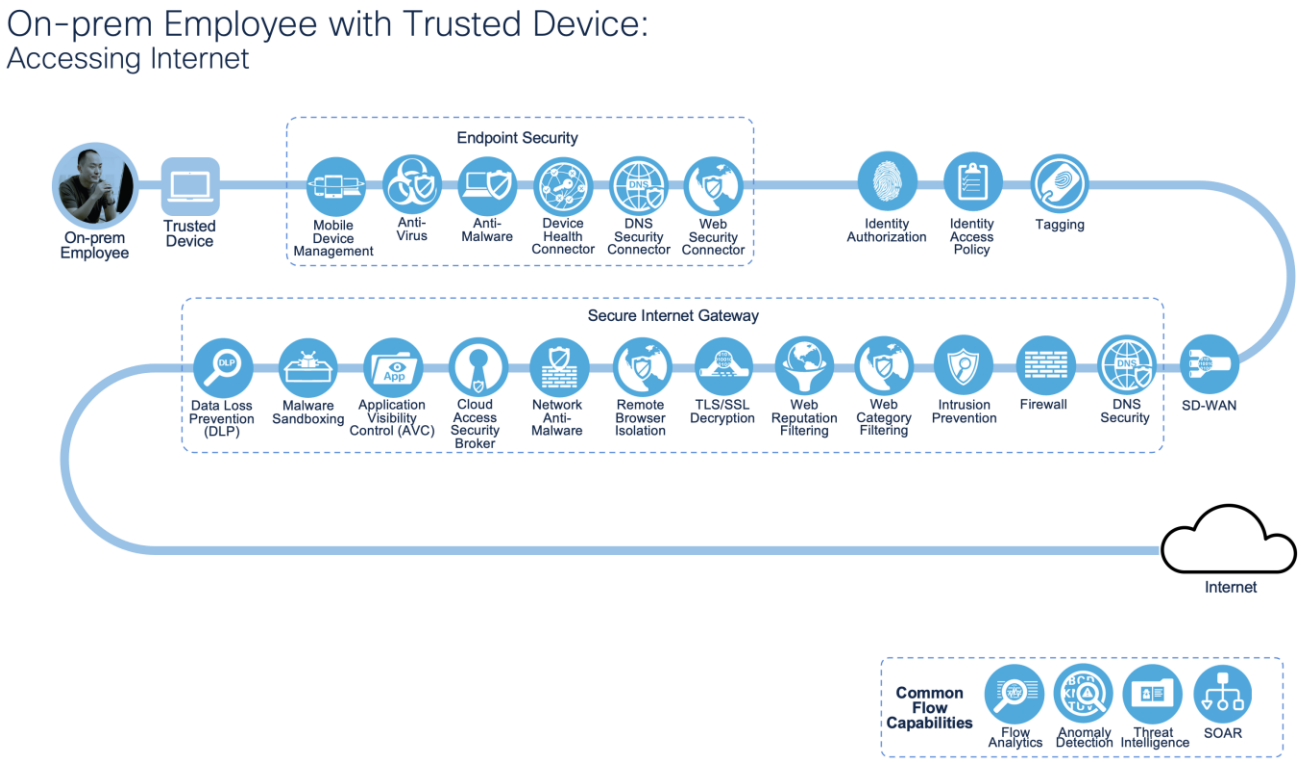


On-prem employee: Accessing Private Application (DC/IaaS)

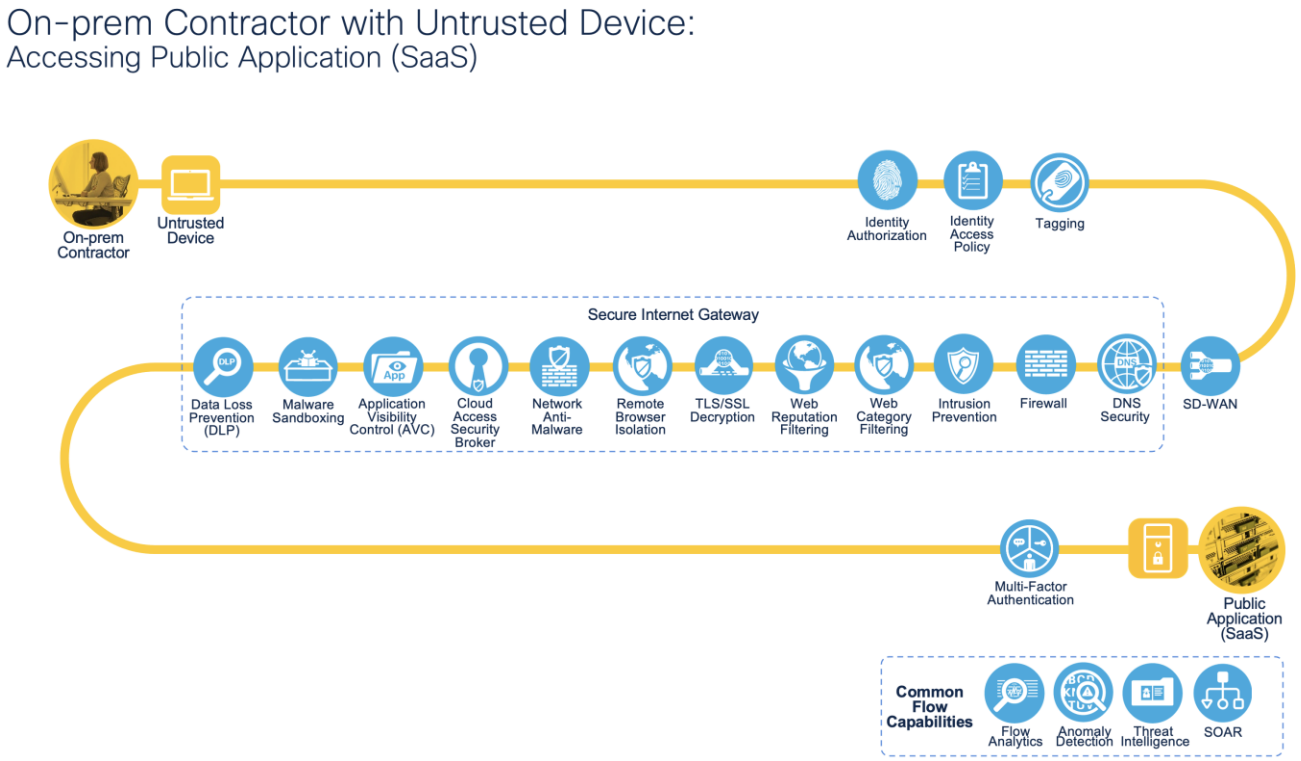


© 2023 Cisco and/or its affiliates. All rights reserved.

On-prem Employee with Trusted Device: Accessing Internet

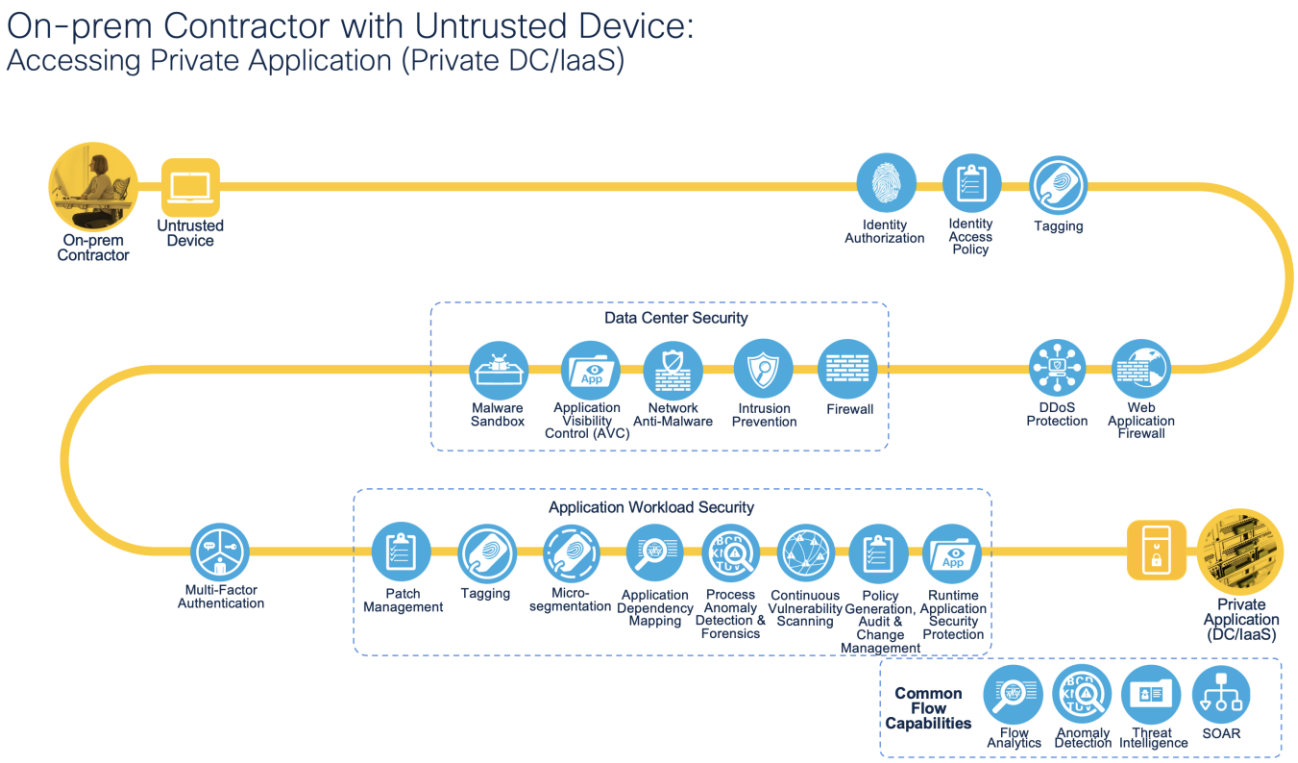


On-prem Contractor with Untrusted Device: Accessing Public Application (SaaS)

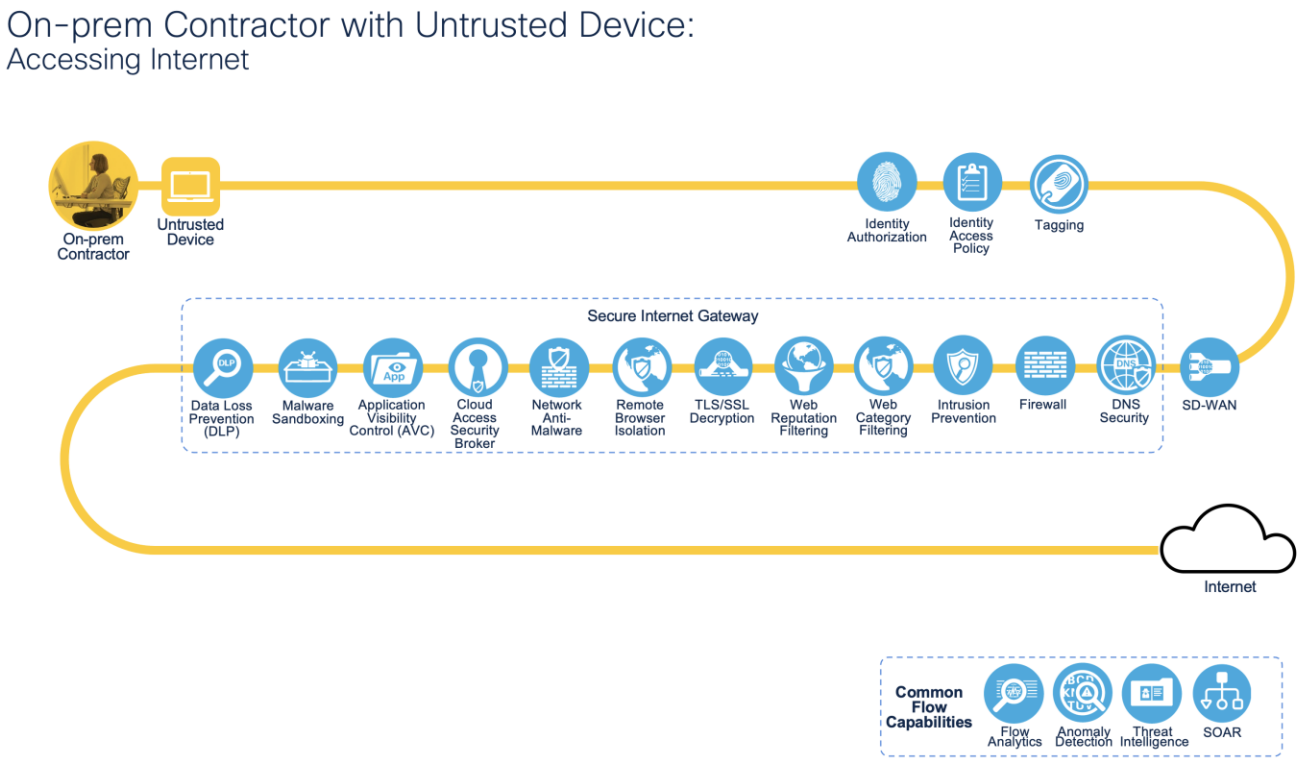


© 2023 Cisco and/or its affiliates. All rights reserved.

On-prem Contractor with Untrusted Device: Accessing Private Application (DC/IaaS)

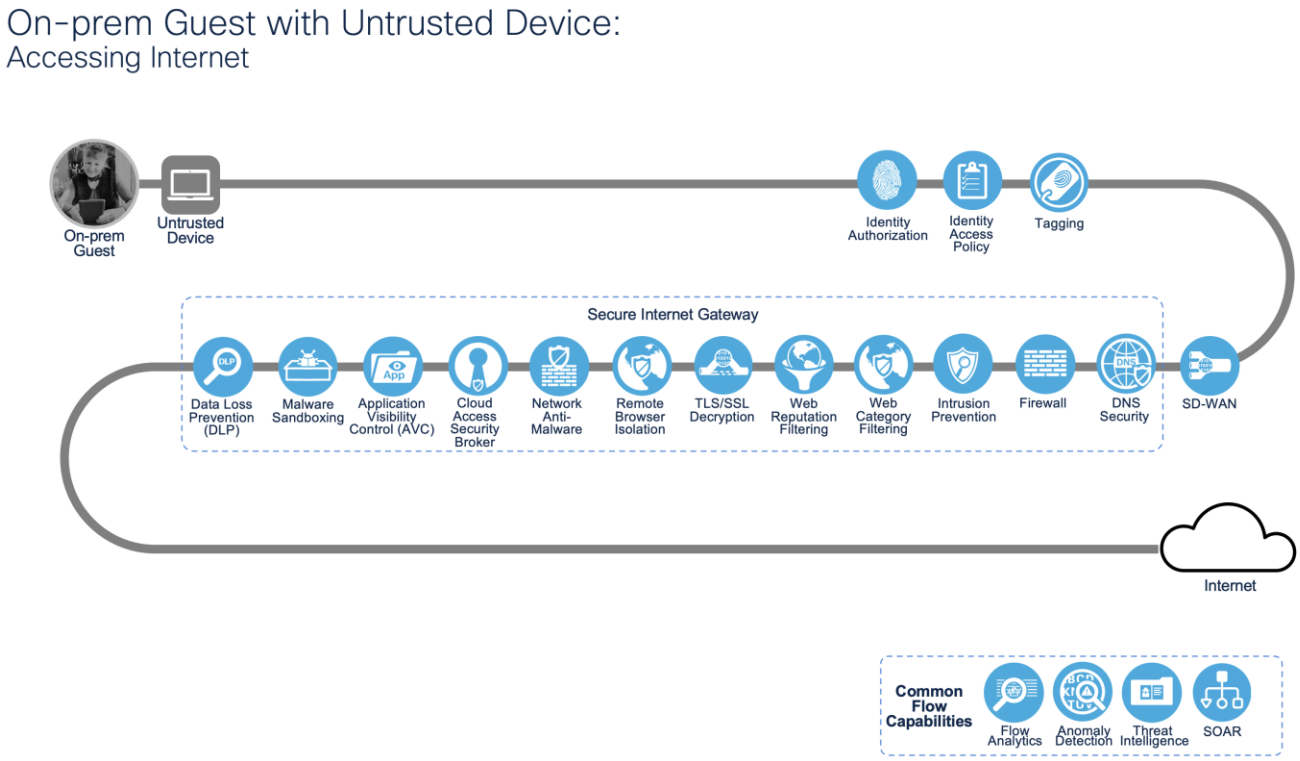


On-prem Contractor with Untrusted Device: Accessing Internet

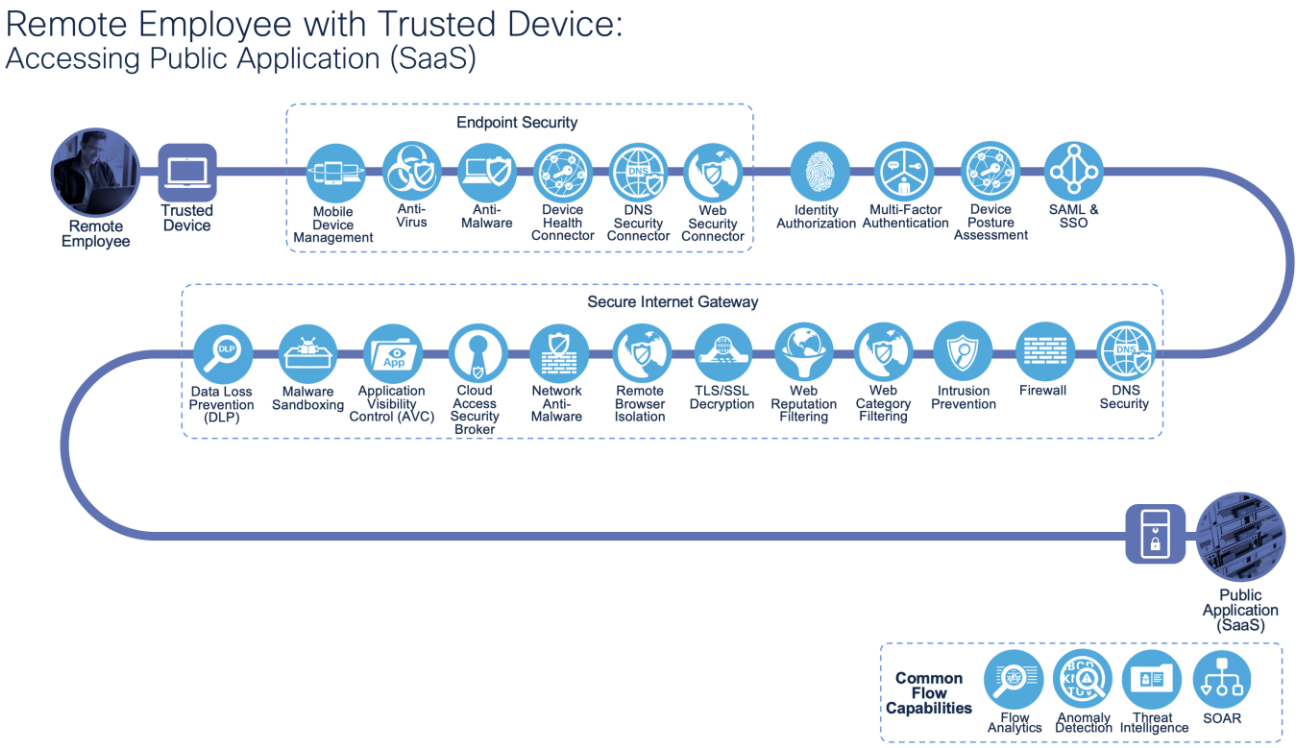


© 2023 Cisco and/or its affiliates. All rights reserved.

On-prem Guest with Untrusted Device: Accessing Internet

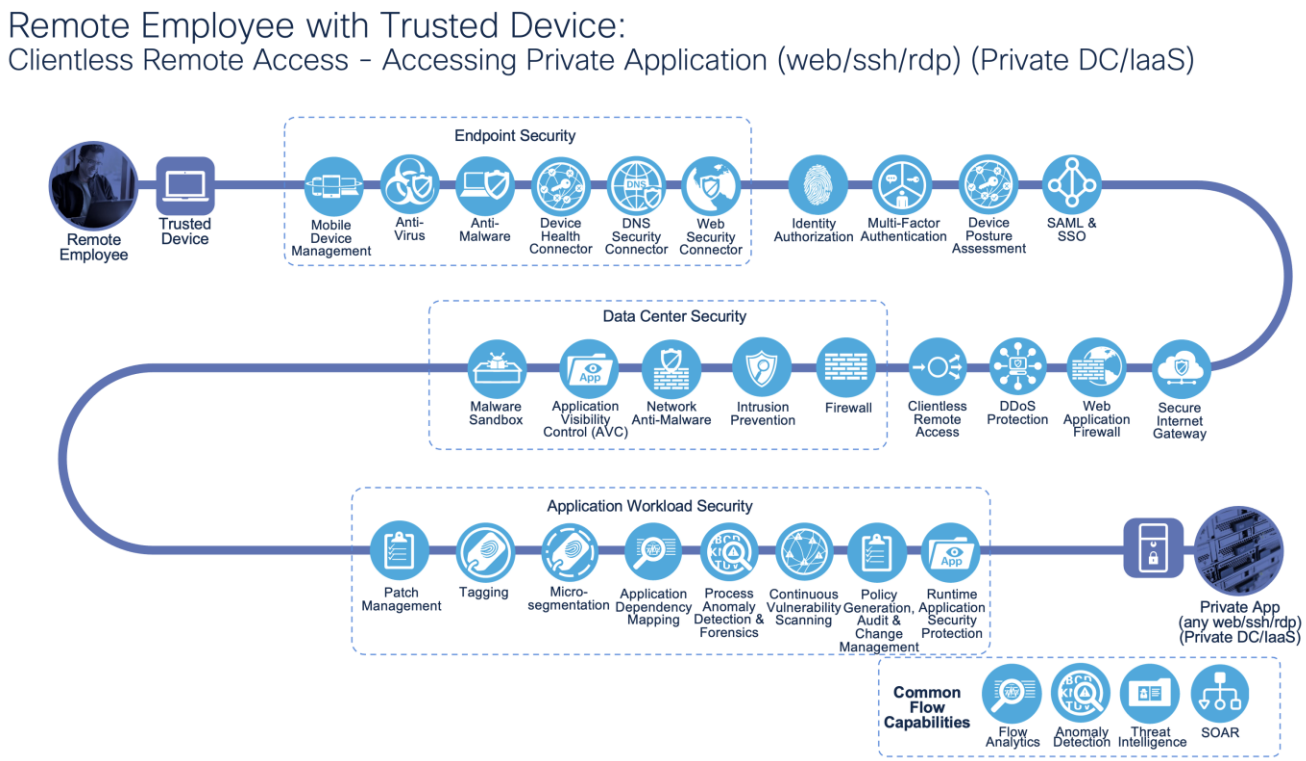


Remote Employee with Trusted Device: Accessing Public Application (SaaS)

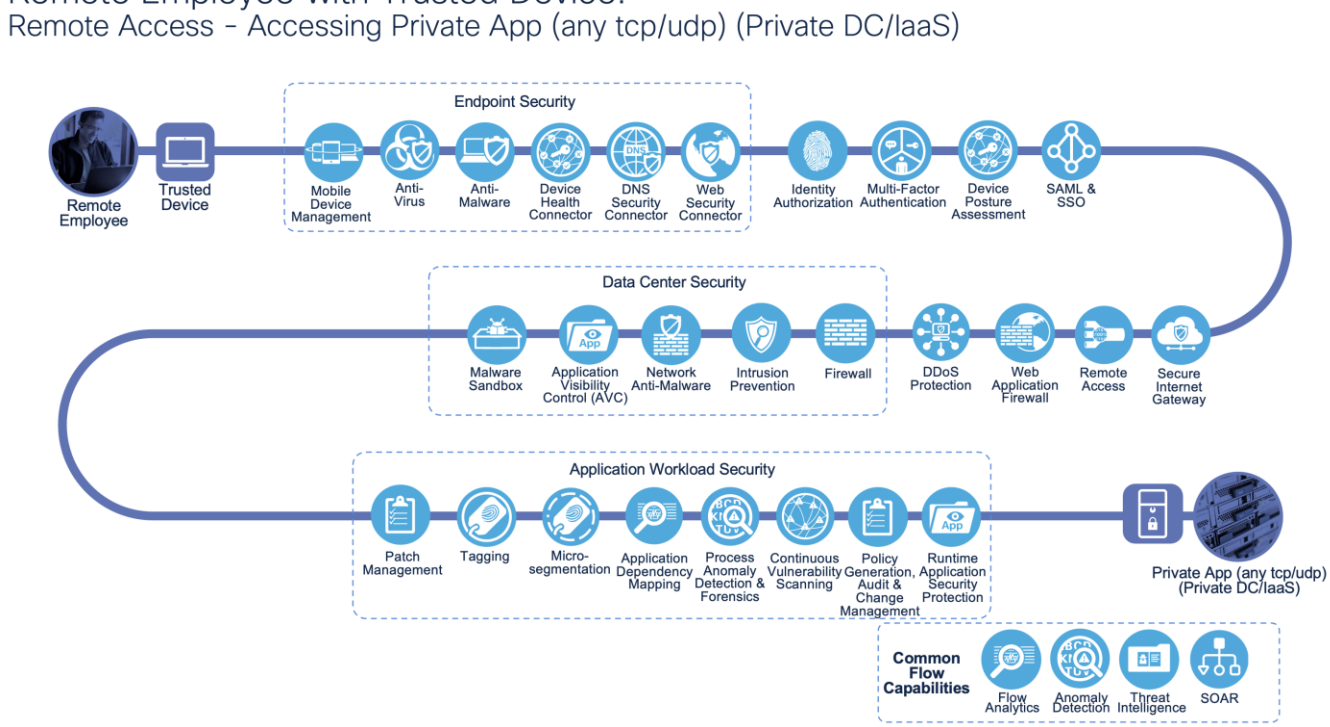


© 2023 Cisco and/or its affiliates. All rights reserved.

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

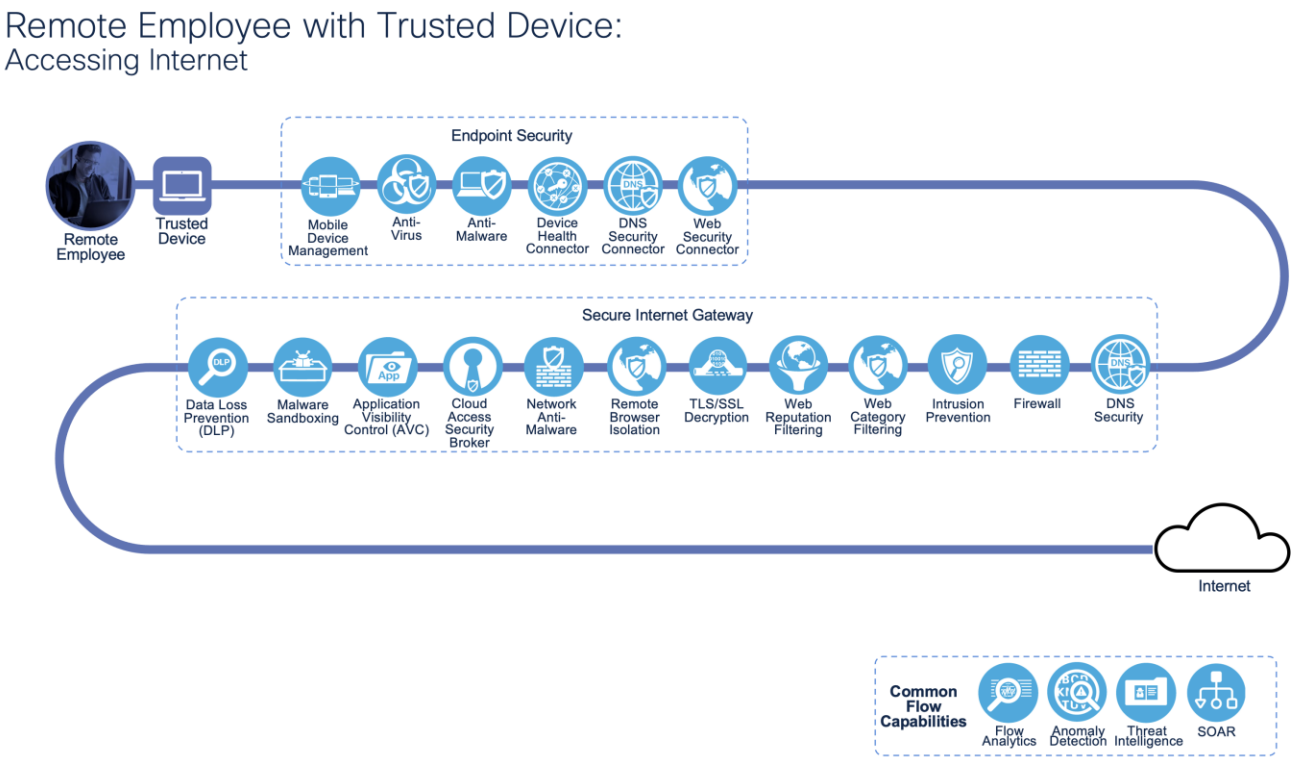


Remote Employee with Trusted Device: Accessing Private Application (any tcp/udp) (Private DC/IaaS)

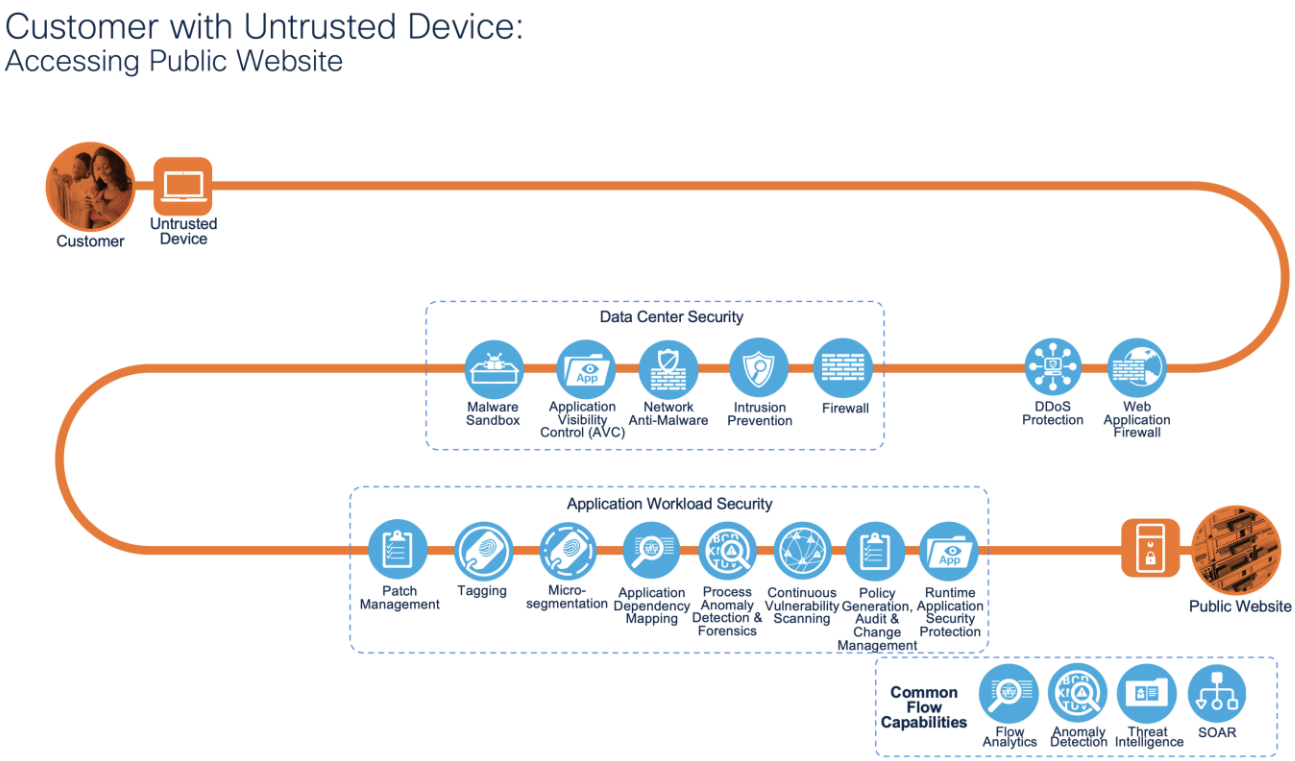


© 2023 Cisco and/or its affiliates. All rights reserved.

Remote Employee with Trusted Device: Accessing Internet

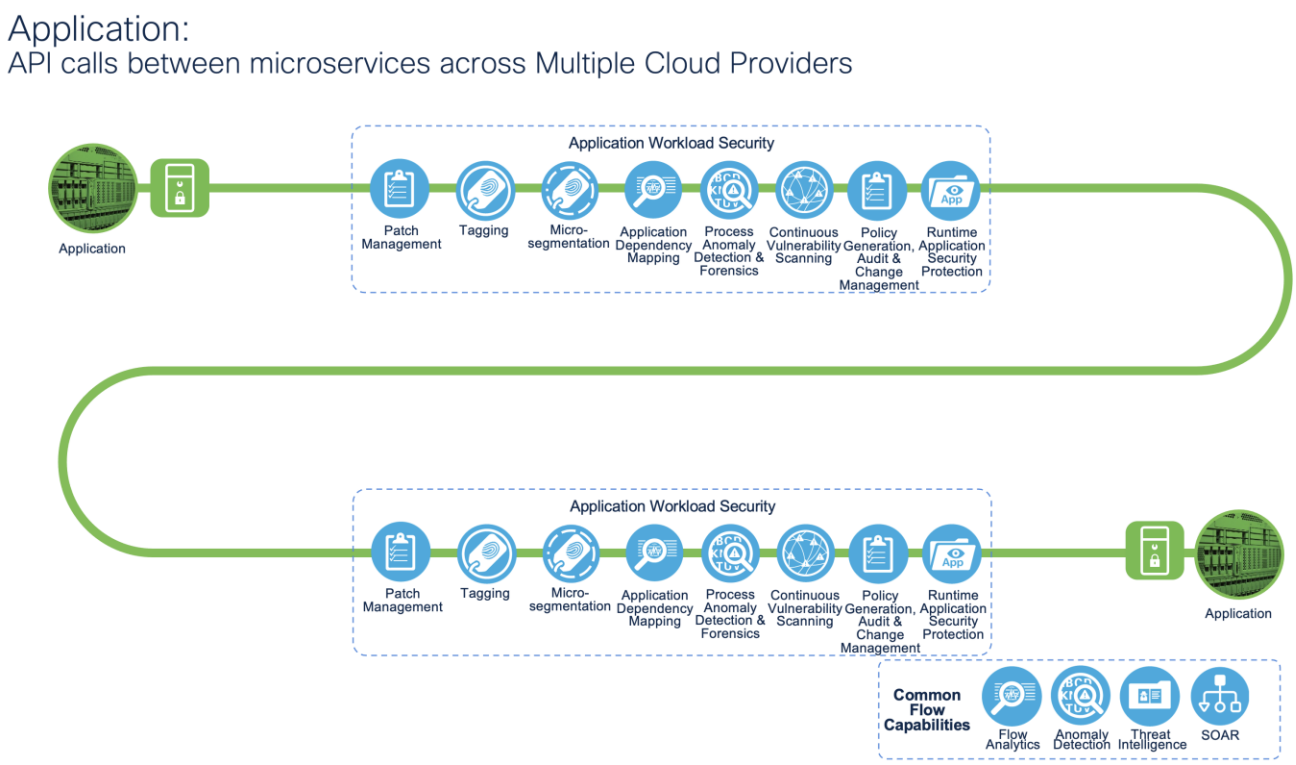


Customer with Untrusted Device: Accessing Public Website

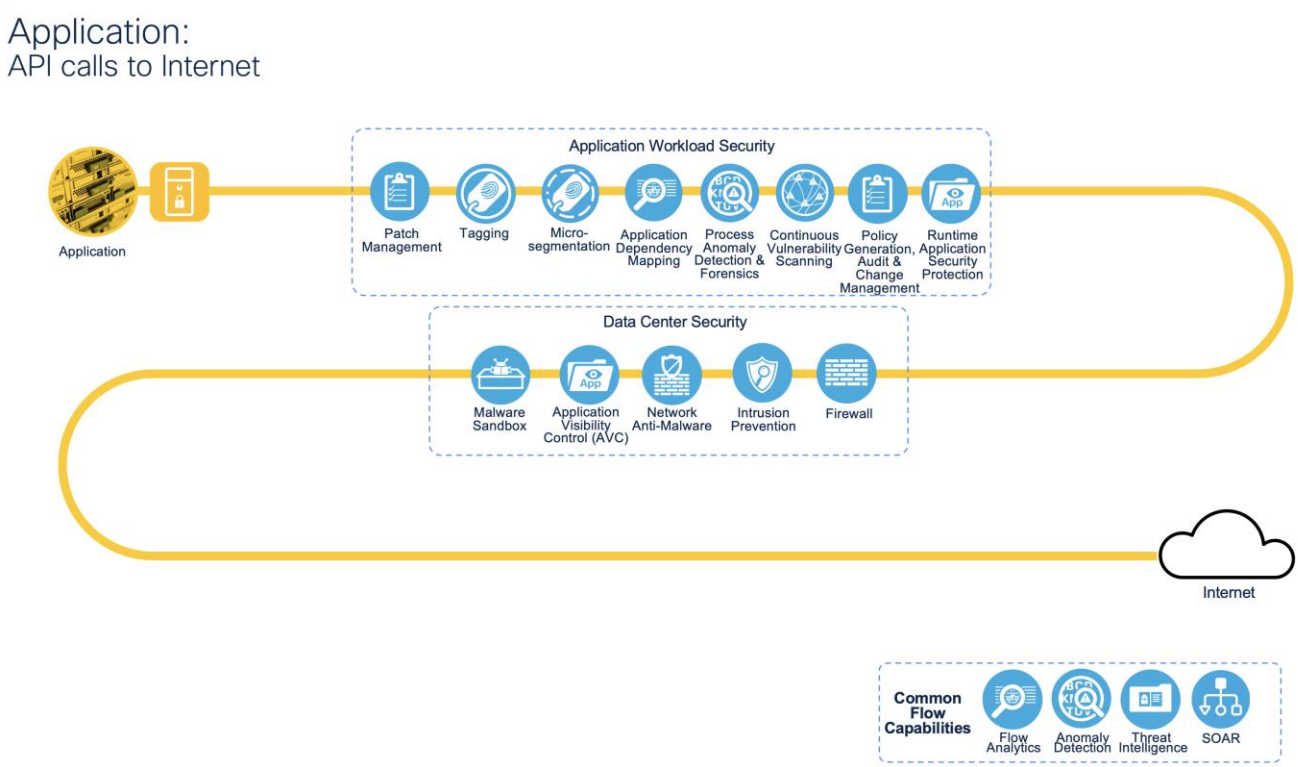


© 2023 Cisco and/or its affiliates. All rights reserved.

Application: API calls between microservices in the Data Center

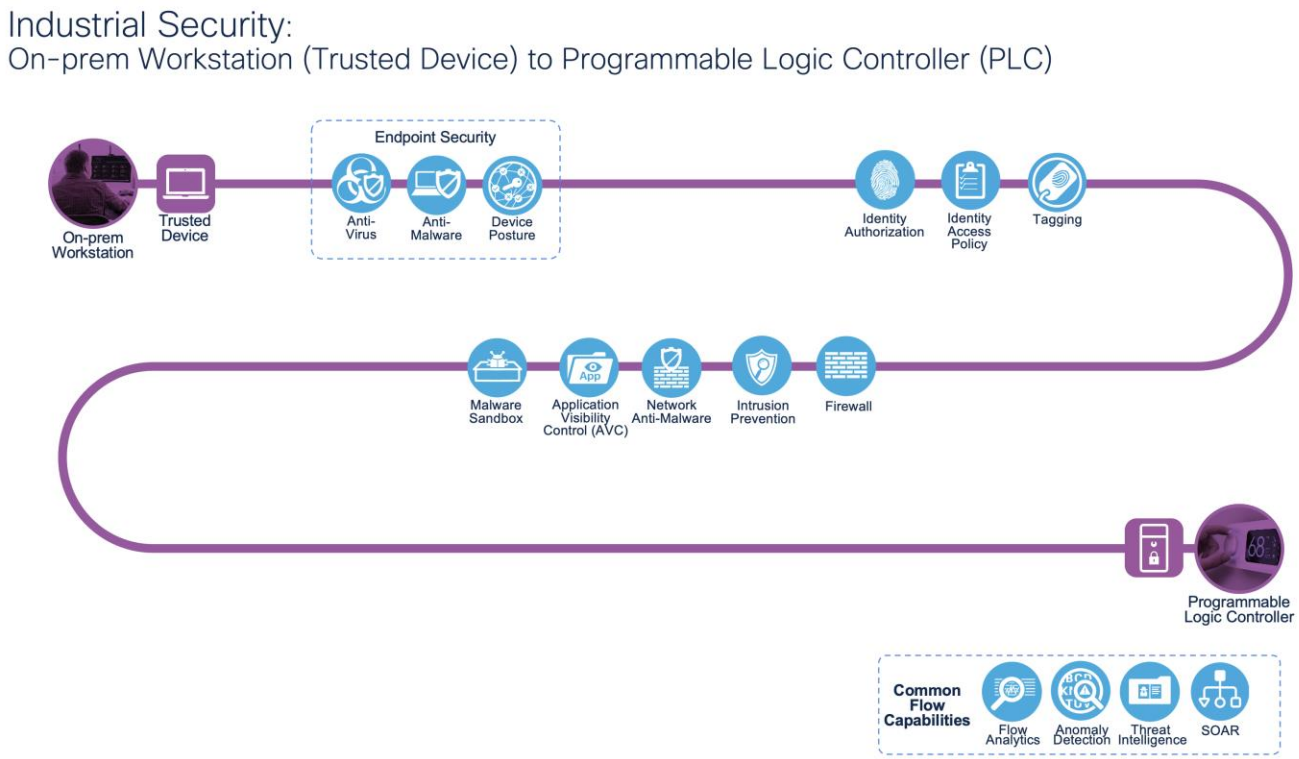


Application: API calls to Internet



© 2023 Cisco and/or its affiliates. All rights reserved.

Industrial Security: On-prem Workstation (Trusted Device) to Programmable Logic Controller (PLC)



Appendix D - Acronyms Defined

Acronym	Definition
BYOD	Bring Your Own Device
CSPM	Cloud Security Posture Management
DLP	Data Loss Prevention
DNS	Domain Name System
IoT	Internet of Things
IPS	Intrusion Prevention System
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
NDR	Network Detection & Response
SNMP	Simple Network Management Protocol
SSO	Single Sign-On
WAF	Web Application Firewall
WAN	Wide Area Network
XSS	Cross Site Scripting

© 2023 Cisco and/or its affiliates. All rights reserved.

Appendix E - References

- Cisco Zero Trust Security
- Zero Trust Frameworks
- Zero Trust: User and Device Security Design Guide
- Zero Trust: Going Beyond the Perimeter
- Cisco Secure Workload
- Software-Defined Access
- Cisco SAFE
- Cisco Security Reference Architecture

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**.

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)

© 2023 Cisco and/or its affiliates. All rights reserved.