Cisco Private 5G Security

Design Principles and Capabilities

Contents

Introduction

Cisco's Private 5G solution, offered as a service, is designed to fit seamlessly into existing enterprise networks and provide private cellular networking capabilities for that enterprise. The solution builds on Cisco's enterprise networking best practices and a clear understanding of enterprises' understanding and expectations of private networks. The private 5G solution was designed with careful consideration of enterprise IT and Local Area Network (LAN) requirements, as well as security and operational needs. End-to-end security has been integrated into the solution from its inception. This document provides a high-level view of the security capabilities of the Cisco® Private 5G solution and addresses both inherent security features within the solution as well as leveraging security capabilities from the wider Cisco enterprise solutions portfolio. This document is not intended to be a comprehensive security design document for Private 5G given that end-to-end security design of any deployment relies on underlying architectures, technologies, platforms, and security features of the enterprise network that Private 5G is being deployed into.

This document is divided into three sections:

1. **Security of the Cisco Private 5G architecture:** Private 5G offered as a service is a distributed multicloud-hosted solution with several components. This section describes the Private 5G architecture and covers the security of the individual components and security of the connectivity between these components.
2. **Device-to-enterprise network security:** The security of the connectivity of the device to the Private 5G edge in the enterprise is covered. Also highlighted is how Cisco's Private 5G solution provides tight integration with an enterprise's existing security solutions.
3. **Secure enterprise design:** We discuss Cisco enterprise security design fundamentals and best practices that provide a foundation for Private 5G security design.

Security of Cisco's Private 5G architecture

Cisco Private 5G solution

Private 5G offered as a service is an end-to-end offering that enables devices on enterprise premises to connect via cellular radios to the enterprise network through a combination of cloud-hosted as well as on-premises platforms. Figure 1 briefly describes the Cisco Private 5G solution layout and components, which include:

- Cisco Control Center, enhanced with Cisco 5G/4G converged packet core, operated on Cisco and/or public clouds. The Control Center platform enables end-to-end management and visibility of the solution including secure multitenant enterprise edge configuration and tenant-specific secure device lifecycle management. The Control Center can be accessed through cloud-based UX as well as APIs enabling easy integration into existing enterprise IT operations and applications. Control Center is operated on Cisco Cloud, which already has extensive geographic presence, and can extend the geographic footprint by using public clouds such as AWS.
- Cisco Edge Appliance on the enterprise premises hosting a private version of the converged packet core with features that enable close integration with existing enterprise policies and networking. The Cisco Edge appliance is designed to securely connect to the cloud.
- Private 5G/4G radio on enterprise premises with spectrum allocated to the enterprise.
- Enterprise endpoints enabled through an SIM provided by Cisco that can connect to the dedicated private radio and packet core.

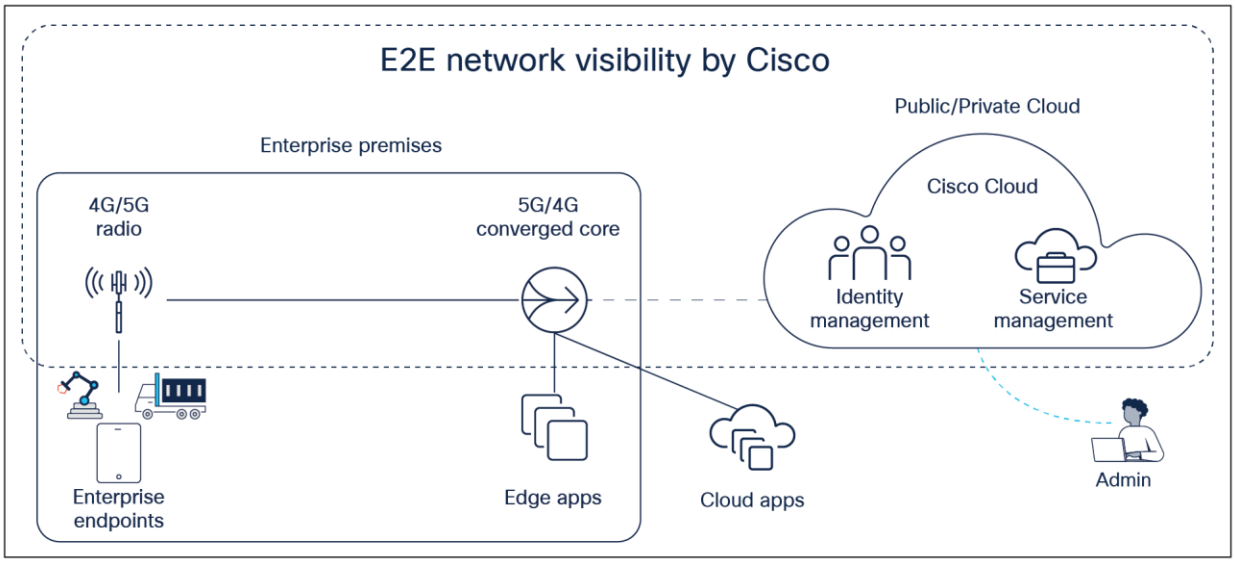

Figure 1.
Cisco Private 5G as-a-service solution

There are three main groupings of components in the solution that are relevant to security architecture. These groupings are depicted in Figure 2 and include:

- **Enterprise premises:** Cisco edge node and radio components are housed on enterprise premises. The edge node hosts packet core components, as well as agents that enable secure connectivity to the cloud. Radio components include remote radio heads as well as centralized and distributed units depending on the model of radio being deployed. Enterprise premises components are responsible for the following capabilities:
  - Data connectivity from device to the enterprise network
  - Interface to the radio access network
  - Interface to the enterprise access network
  - Access management and session management functionality of the 5G core
- **Cisco Control Center:** Housed on a Cisco managed cloud platform, Control Center is responsible for subscriber management, secure device lifecycle management, and management/operations user interfaces and APIs. Specific capabilities include:
  - Enterprise ID and policy registered during onboarding, unique Enterprise ID generated to tag all enterprise-related info
  - Multitenant environment, Enterprise ID used to identify tenancy
  - Subscriber data – device and SIM info
  - Authentication credentials
  - Management access
  - Key Performance Indicators (KPIs) and metrics
  - Usage records

- Location information
- Deployment configuration data per enterprise

- **Edge orchestration:** Offered through Cisco Control Center with functions hosted either on the Cisco private cloud or on the public cloud to expand the geographic footprint of the Control Center. Capabilities that are hosted on the public cloud include:
  - Multitenant environment, Enterprise ID used to identify tenancy
  - Management access
  - KPIs and metrics
  - Software images
  - Deployment configuration
  - Configuration backups

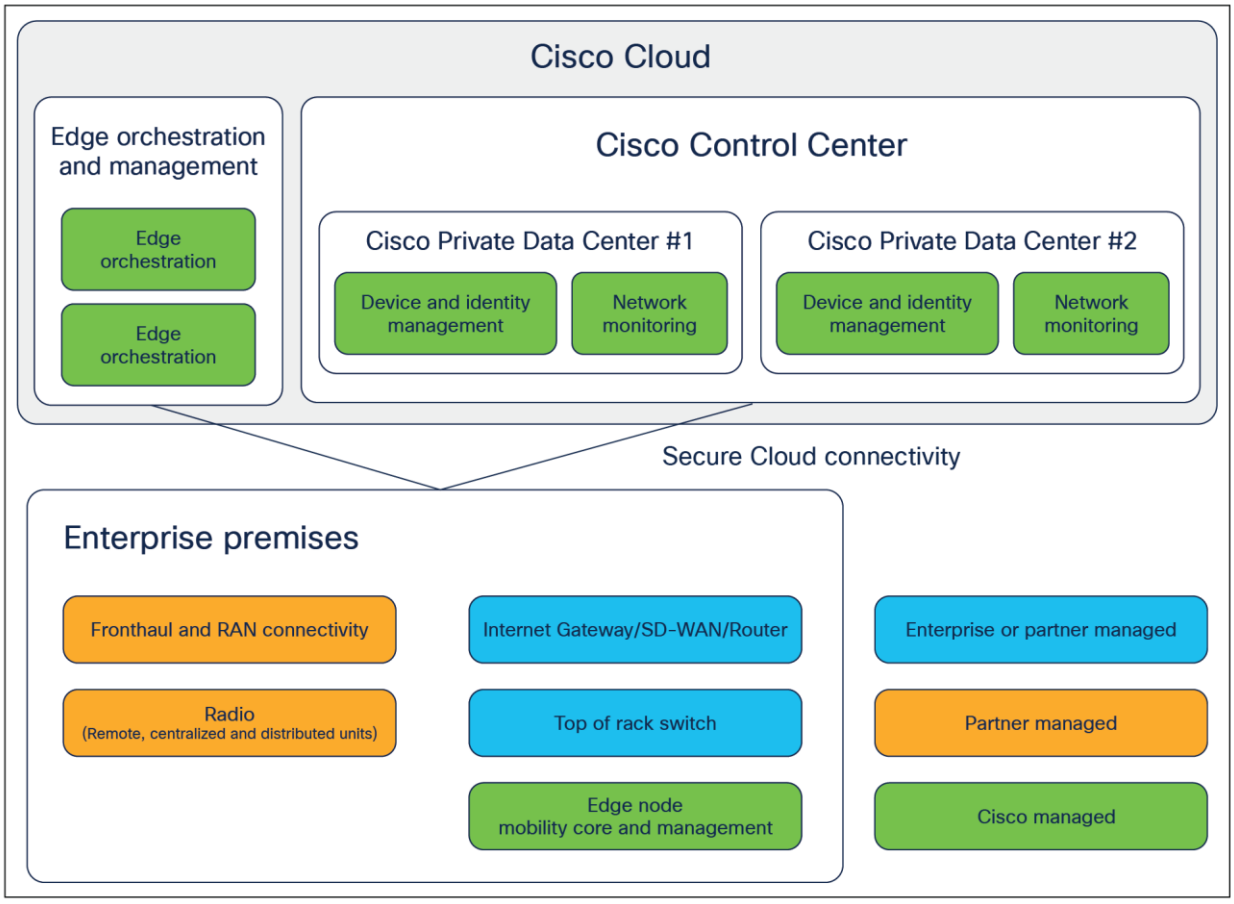

Figure 2.
High-level component view of Cisco Private 5G

Encrypted and fully monitored tunnels provide secure connectivity between all components, enabling them to communicate safely in a multicloud distributed environment. The service leverages a combination of proven centralized cloud capabilities with essential components deployed within the enterprise sites to distribute the user plane, which is the key function responsible for all data exchange. Management capabilities of the solution are offered to the enterprise via a secure user interface and APIs and are protected with complete role-based access control that maps each enterprise to its unique tenancy with secure separation of all operational data and exchange. User data doesn't leave enterprise premises and is protected through enterprise security mechanisms.

Enterprise premises security

Physical security

Within the enterprise facility, the edge node from Cisco should be deployed within a secure access facility, as defined by the enterprise, and controlled with existing enterprise access control protocols. Given that the facility itself is likely owned and operated by the enterprise or a specific partner, Cisco only offers guidance on how to physically secure the edge node, but the responsibility of physically securing the equipment lies with the enterprise.

It is highly recommended that edge nodes are either deployed in locked cages to prevent unauthorized access, environmental threats/damage, and interference, or at the very least protected by restricted access to avoid service disruption and loss of property.

The following capabilities are required as minimum Best Current Practice (BCP):

1. Physical barriers for installation
2. Badged access to the facility and room hosting the edge node
3. Logging of access to facilities

Integrating with on-premises enterprise LAN

Enterprise premises security architectures vary depending on the specific enterprise deployment venue and characteristics. The Cisco Private 5G solution is designed to be easily integrated into enterprise security architectures.

Key considerations for integration into existing enterprise security designs include:

- Network connectivity to Top-of-Rack (TOR) switches: Cisco edge node and Radio Access Network (RAN) components need to be connected to the TOR switch.
- Placement of firewalls and traffic inspection engines: It's assumed that Cisco components are placed in a secure and firewall-protected zone. Design of the zone and multiple zones of security is the responsibility of the customer or partner.
- Traffic segmentation policies and assignment of segments (VLANs) to Cisco Private 5G components: Separate segments are required for the packet core management and control and data plane, as well as radio network connectivity. These segments must be allocated and configured by the customer or operating partner.

Cisco recommendations for a secure enterprise design are covered later in this document.

Cisco edge node components

Cisco edge node hosts 5G packet core components. These include User Plane Function (UPF), Session Management Function (SMF), and Access Management Function (AMF)/Mobility Management Entity (MME) that are responsible for 5G core protocol implementations and control agents that monitor functioning and health of the edge node. All data communication between on-premises network functions and cloud-hosted network functions are encrypted through HTTPS (transport layer security [TLS] 1.2). To ensure enterprise data protection, only a unique auto-generated account ID is used for tagging and storing enterprise-specific information.

Secure operation of the Cisco edge node can be organized into three main categories:

- Secure management plane, consisting of configuration and monitoring of the various components, and collection and secure storage of enterprise-specific configuration data
- Secure control plane, consisting of device authentication and authorization, session connectivity, and mobility control
- Secure user plane, consisting of user data exchange between device, radio, and enterprise LAN and protection of enterprise-specific data within the enterprise security domain

In addition to the Cisco edge node, on-premises components of the Private 5G service include radio and other devices, each of which has their own unique security requirements.

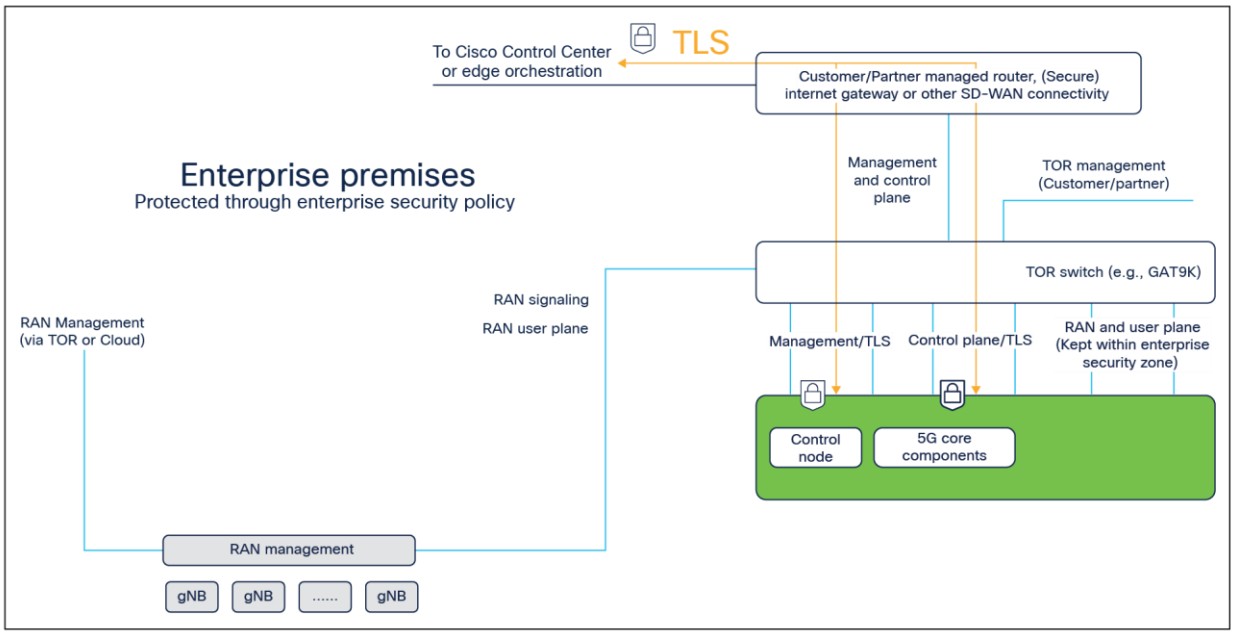

Figure 3.
Secure connectivity toward the cloud from the edge using TLS tunnels

Management plane security

Management of the Private 5G components is accomplished by the Private 5G Edge Orchestration function, which may use agents deployed on the Cisco private cloud or on the public cloud such as AWS.

The interface between the on-premises edge node and the Edge Orchestration function is for delivery of lifecycle management information of the network functions. It also provides visibility of the on-premises components' network health and enables secure and consistent Continuous Integration/Continuous Deployment (CI/CD) experience for the enterprise use of the network functions. Cisco operation will ensure version control and new feature deployment of the converged 4G/5G edge node easily and securely.

After initial bootup, the on-premises agent initiates connection to the cloud via a well-known URL and establishes a TLS connection. Once the TLS connection is established, a session is created using the device's credentials that were established during the device onboarding phase. Upon establishment of a session, local agents at the edge securely communicate with services running in the cloud using keys created during session establishment. Agents on the edge use this connection to download edge configuration data and operational actions and to upload metrics.

The communication toward the cloud leverages HTTPS (TLS 1.2 using REST APIs), and the connection supports well-known HTTP proxy configurations.

Control plane security

The Cisco edge node allows the network functions on the edge to communicate with those on the Control Center cloud in a secure manner. Once a secure connection is established, session(s) keys are exchanged and used to validate the session and create a session ID that can be used by NFs to communicate. All control plane messaging is initiated from the packet core on-premises and secured via HTTPS. Cloud-initiated messages are retrieved by the edge node using a pull mechanism to avoid inbound connections from the cloud.

User plane security

Inherent to the 3rd Generation Partnership Project (3GPP) architecture, the User Plane Function (UPF) terminates and anchors the private 4G/5G user plane traffic, ensuring that only devices that have been authenticated, authorized, and allocated an IP address are able to transmit the data through the network. Any traffic that's identified as malformed or contains flows initiated from the network side without corresponding device-initiated flows are dropped.

Firewall placement and user plane

It's highly recommended that an external firewall is deployed to ensure protection of the private 5G network when possible. While the firewall is not part of the preintegrated solution, Cisco does offer optional firewall capabilities that could be integrated by the managed service provider based on specific enterprise requirements.

In addition, optional security gateways could be deployed to terminate traffic originating from the RAN.

DDoS protection of the user plane

It is recommended to deploy an external Distributed-Denial-of-Service (DDoS) protection mechanism when required and feasible. Like the firewall, this optional capability can be provided by Cisco and integrated by the managed service provider. Various DDoS protection mechanisms exist, including on-premises (for application layer protection and volumetric attacks), always on in the case of a high-risk environment, on demand for scenarios where enterprises may want to deploy once a potential attack is detected and could sustain a brief outage, or a hybrid solution for a combination of the above scenarios.

Given that 5G could open a higher threat surface due to the inherent nature of higher bandwidth toward the device, it's recommended to deploy DDoS protection in conjunction with a secure Domain Name System (DNS) mechanism.

Data encryption of the user plane

It is assumed that the device and the user plane are within a trusted network domain, but if needed, additional data encryption capabilities could be deployed inline. Traditionally, this capability is not leveraged due to the high volume of the user plane transmitted, but for a controlled set of environments, it's possible to deploy a security gateway between the radio network and user plane as an optional capability. Note that data plane traffic between the device and RAN is encrypted and its integrity is protected. The keys used for data plane encryption and integrity protection are different from those used for the signaling plane for added security.

Radio subsystem security

Security design of the radio subsystem is the responsibility of the partner or customer. These designs vary based on the radio model being used, because traditional radio units need to be secured differently than disaggregated models. It's generally assumed that the RAN system is operated within the physically secure perimeters of the enterprise premises. As such, only secure access to the radio operations is needed, which can be provided with TLS or IPsec tunnels to the radio operation unit. In the case of disaggregated radio models where Radio Units (RU), Centralized Units (CU), and Distributed Units (DU) need to be secured separately, one must consider placement of firewalls and traffic monitoring agents on the connectivity path of the distributed components.

Edge orchestration function security

Data and software in the edge orchestration function is secured following Cisco's cloud requirement and best practices and Cisco Control Center security best practices. These include:

- Encrypting data at rest
- Leveraging industry standards for secure key management practices
- Secure multitenancy schemes
- Stringent access control
- Least-privilege principle applied to all systems and processes

Cisco Control Center security – Role-based access control

This solution supports cloud management for all exposed capabilities including software Lifecycle Management (LCM) for the service, device onboarding, SIM configuration, and policy management. All the access is controlled via robust Role-Based Access Control (RBAC), which is completely in control of the enterprise administrator and managed service provider administrator. Enterprises can enable services across multiple sites and manage site-to-site variations with full RBAC for IT managers. Managed service providers will receive visibility into a single enterprise persona or a dashboard for a view across all enterprise customers onboarded by the service provider.

Several roles can be assigned for an enterprise administrator, each with their specific levels of access control (for example, one role enabling the master administrator to provision and modify devices, while another one to only enable the enterprise user to view devices and their usage). Similar levels of roles can be assigned for managed service provider partners. The ability to customize the roles and privileges is also provided.

Access monitoring

The Control Center production network is segregated from the Cisco corporate network and requires a separate set of credentials for logical access. Approved Control Center personnel then connect to the production network through a set of bastion hosts that restrict access to network devices and other components, logging all activity for security review.

Control Center developers and administrators on the corporate network, who need to access production components to maintain them, must explicitly request access through the proprietary ticketing system. All requests are reviewed and approved by the applicable service owner and Control Center security.

Account review and audit

Accounts are reviewed every 90 days; explicit reapproval is required or access to the resource is automatically revoked. Access is also automatically revoked when an employee's record is terminated in Cisco's human resources system. Windows, UNIX, and other systems accounts are disabled, and the user is removed from all additional systems.

Requests for changes in access are captured in the Control Center ticketing system. When changes in an employee's job function occur, continued access must be explicitly approved to the resource, or it is revoked.

Background checks

Cisco has established formal policies and procedures to delineate the minimum standards for logical access to the Control Center platform and infrastructure hosts. Cisco conducts criminal background checks, as permitted by law, as part of pre-employment screening practices for employees and commensurate with the employee's position and level of access. The policies also identify functional responsibilities for the administration of logical access and security.

Credentials policy

Cisco security has established a credentials policy with required configurations and expiration intervals. Passwords are required to be complex and are forced to be changed every 90 days.

Data separation (Multitenant)

The solution is inherently designed to be multitenant with clear separation of profile information for subscriber identity, enterprise data, and procedures in place to ensure safeguarding of enterprise identity. API and user interface access restrict visibility of one enterprise's data being spilled over to another by using internal mechanisms that segregate all configuration, metrics, and usage data based on an enterprise ID and a corresponding Public Land Mobile Network (PLMN) ID.

The managed service provider has the visibility within the account for multiple enterprises, and each enterprise will only have visibility to the specific enterprise data.

Data encryption

The solution protects enterprise data by using disk encryption hardware. This type of data encryption provides the best protection and performance for Control Center operations. Data encryption is applied at the data center level and is defined based on case-by-case and formal agreements. Cisco's export compliance policy restricts the sale of any products containing strong encryption capabilities to entities or end users from certain countries. The purpose of this policy is to prevent bad actors from stealing powerful encryption algorithms. The list of users and countries changes over time based on geopolitical developments.

API security

All the Control Center APIs are available via TLS/HTTPS protected endpoints that provide server authentication. We encourage users to leverage TLS/HTTPS for all interactions with Control Center. Users with REST API access are allocated an API key that the user could generate for themselves through the web interface if the corresponding role allocated to the user allows API access. In some cases, API keys can be generated for additional users—especially for users that don't have web access based on role-based access control.

To ensure secure access:

- If a user has both web interface and API access, they must generate their own API key. A user with web interface access, but no API access, cannot generate an API key for themselves.
- If a user has API access, but no web interface access, they must rely on the managed service provider or account administrator user with appropriate privileges to generate an API key for them.
- An administrator user can generate an API key for another user if that user has API access only and cannot log in to the web interface to perform the task for themselves.

A mechanism for resetting the API key is available, and for security reasons, users are encouraged to change the key on a regular basis or whenever the user has reason to believe the key may have been compromised.

Additional details on key generation and REST API access will be shared as part of the onboarding process.

DDoS protection

Control Center utilizes a wide variety of automated monitoring systems to provide an elevated level of service performance and availability. Monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts.

Control Center security monitoring tools help identify several types of Denial-of-Service (DoS) attacks, including distributed, flooding, and software/logic attacks. When DoS attacks are identified, the Control Center incident response process is initiated. In addition to the DoS prevention tools, redundant telecommunication providers at each location as well as additional capacity protection against the possibility of DoS attacks are leveraged.

To tackle DDoS attacks, proprietary DDoS mitigation techniques are used. Additionally, Control Center's networks are multihomed across several providers to achieve internet access diversity. Unauthorized port scans by customers are a violation of the Control Center Acceptable Use Policy. Violations of this policy are taken seriously, and every reported violation is investigated. Unauthorized port scanning is stopped and blocked.

Network devices, including firewall and other peripheral monitoring devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, Access Control Lists (ACLs), and configurations to enforce the flow of information to specific information system services.

Secure device LCM

For SIM profile and ordering, bulk order of SIMs based on a profile defined by Cisco are procured via secure mechanisms with mutual agreement and industry best practices for SIM procurement from leading SIM and identity providers. In the case of physical SIMs or Universal Integrated Circuit Cards (UICCs), once physical SIMs are received via a secure mechanism, the SIM output file is uploaded into Control Center to create a database record of all SIMs and inventory (ability to transfer into specific managed service provider accounts or uploaded from specific accounts).

Once the SIMs are migrated to specific enterprise accounts, the enterprise is responsible for securely managing the lifecycle of the device based on specific roles created for enterprise accounts. Only users with approved roles can perform SIM actions (for example, activate, deactivate, retire, purge, and so on) depending on enterprise needs.

Any activity related to SIM and device lifecycle management is logged and tracked for auditing purposes.

In addition, the solution offers the ability to block any stolen or misplaced SIMs to ensure they're blocked from connecting to the network and reject any authentication requests.

Beyond all the security mechanisms described above, Control Center's IT infrastructure is designed and managed in alignment with best security practices and a variety of IT security standards, including:

ISO/IEC 27001

SSAE16 SOC 2 Type II (formerly SAS 70 Type II)

GDPR readiness

Control Center protects personal data, erasure, and individual rights by adhering to Cisco's data retention and erasure practices. Simply stated, these practices define what type of data is saved in the Control Center and how long it's stored. Data retention and erasure allows operators to be compliant with local regulations and Cisco contracts, as well as the European Union's General Data Protection Regulation (GDPR). The following are the basic components of Cisco's data retention and erasure practices:

- **Data categories:** Business contact and device information, data/SMS/voice usage, audit trails, invoices, and reports.
- **Data retention:** The continued storage of business and operational data in the Control Center platform for a specific period. The default retention period is 18 months from the date of creation, starting in the next full billing cycle. This time retention period is referred to as the data availability window. Data is purged when it has crossed the retention threshold requirement put in place by either the operator or Cisco.
- **Erasure:** The removal of data from the Control Center platform based on regulatory reasons or for business needs. Erasure requests can be initiated by operators to delete inactive accounts or inactive device-related data.

Note that erasure is permanent. After data has been erased from Control Center, it cannot be retrieved.

Additional details on GDPR readiness can be shared after specific customer agreements and commercial terms.

Device-to-enterprise network security

5G security standards, as defined by the 3GPP, cover the realm between the device and the 5G core network. It's responsible for identity management, authentication, authorization, and subsequently encryption and integrity protection of all traffic between the device and the radio network. Additionally, encryption and identity protection for signaling traffic between the device and the 5G core network is supported. This provides strong security, starting from the radio interface all the way into the 5G core network. Cisco's Private 5G solution couples this security in the 5G network and also seamlessly integrates with the security policies in the enterprise using Cisco Identity Services Engine (ISE).

Per 5G standards, all devices accessing the 5G network perform mutual authentication and authorization with the authentication server in the 5G network.

The device has two identities. One is the identity in the SIM card used to access the 5G core (this is the permanent identity). The other is the identity of the device itself. This is the secondary or linked identity since a SIM card can be moved from one device to another. Authentication to the 5G network is performed using the identity and credentials stored in the SIM and the 5G network. Subsequent authorization checks are performed based on subscription information stored in Control Center to ensure that only those 5G network features contained in the device profile authorization are allowed.

The Private 5G core through Control Center provides automation rules that can check for a change in permanent identity in the SIM and the identity of the physical device. On detecting such a change, the automation engine takes whatever action is specified. This can be used to effectively tie SIMs to devices as desired, ensuring only authorized devices are allowed access to the 5G network.

After authentication, session keys are derived to encrypt and integrity protect traffic between the device and the private 5G network. The signaling traffic and the data traffic are encrypted over the radio interface. Additionally, signaling traffic between the device and the 5G core is end-to-end encrypted and integrity protected.

Enterprise integration

The security solutions below are optional and extend private 5G security by leveraging existing enterprise tools and/or Cisco security solutions.

Identity Services Engine

Cisco ISE offers a comprehensive approach to network access security and allows enterprises to provide highly secure network access to users and devices. To be able to extend the same security into private 4G/5G networks, Cisco's Private 5G architecture integrates with ISE, enabling the enterprise to define corresponding security and profile policies for each device within ISE when needed. ISE will treat the private 4G/5G networks as a "network device" and extend similar capabilities of an existing access network to create an all-encompassing, contextual identity with attributes such as user, time, location, threat, vulnerability, and access type. IT administrators can centrally define a policy that differentiates guests from registered users and devices or specific IOT devices versus laptops. Regardless of their location, users and endpoints are allowed access to private networks based on role and policy.

When Cisco's Private 5G and ISE integration is available for the specific private network, the solution delivers an enhanced experience where ISE becomes a centralized place in which identity of cellular devices is provisioned as part of device onboarding in ISE. Once onboarded, leveraging existing enterprise infrastructure ISE would be the sole source of policy in the enterprise and provides policy decisions via Radius to Private 5G edge. Also, by linking the identities in ISE to that in the 5G network, it enables coupling of the authentication performed in the 5G network to authorization policies (such as micro-segmentation) that are defined in ISE.

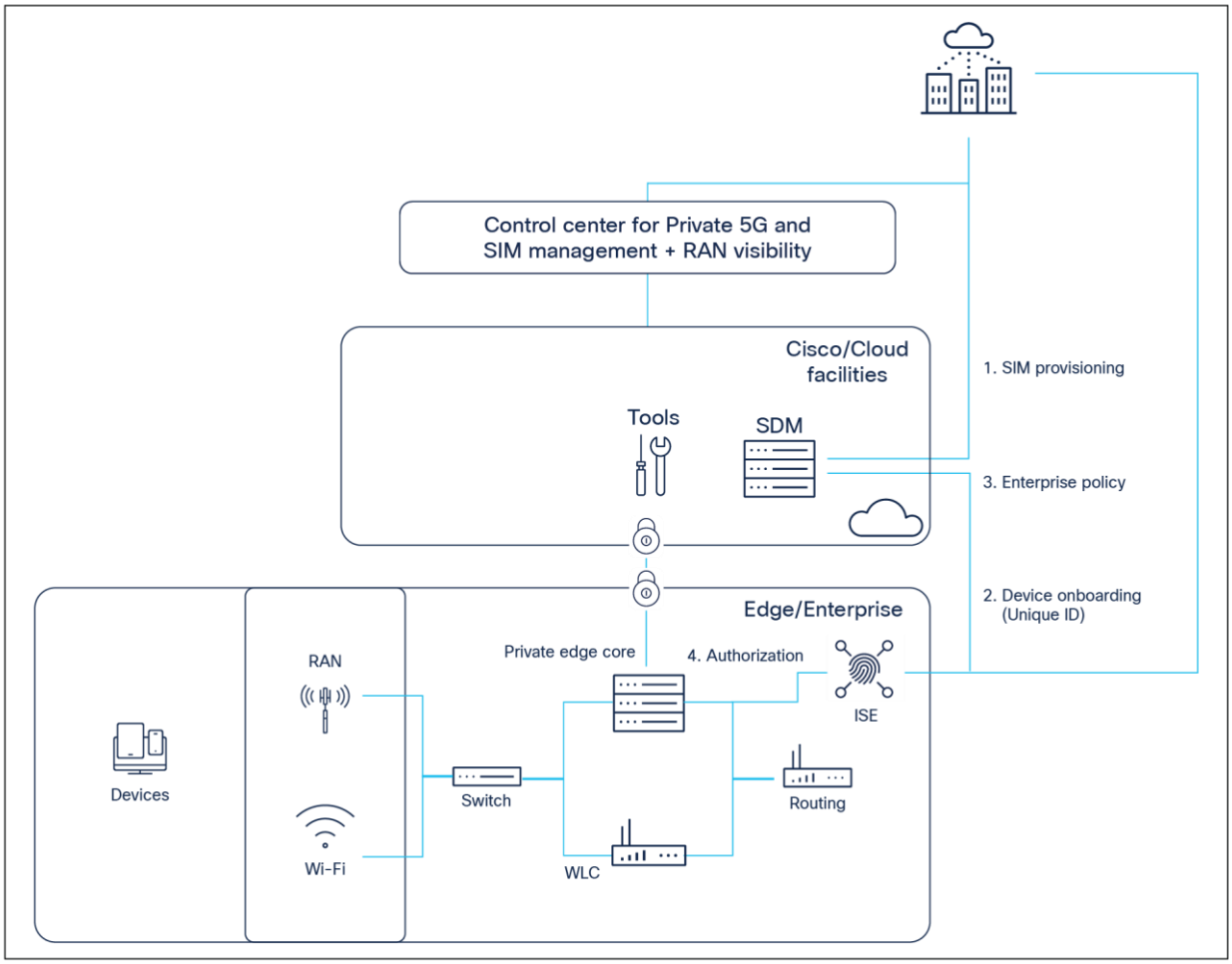

Figure 4.
High-level view of identity services integration from private networks

With ISE integration capabilities and authorization options, enterprises can deploy:

- Macro-segmentation: IP pool and VLANs
- Device-specific QoS policies
- Micro-segmentation: Scalable group tags
- Multiple QoS flow (DSCP-based)
- Downloadable ACLs

The above solution capabilities will be delivered in a phased approach.

Cisco Umbrella and Secure Connect

To help enterprises embrace direct internet access, in addition to DNS-layer security and interactive threat intelligence, Cisco Umbrella® includes secure web gateway, firewall, and Cloud Access Security Broker (CASB) functionality, plus integration with Cisco SD-WAN, delivered from a single cloud security service.

Specifically leveraging DNS, Cisco Umbrella uses the internet's infrastructure to block malicious and unwanted domains, IP addresses, and cloud applications before a connection is ever established. Built 100% in the cloud, Umbrella provides better accuracy and detection of compromised systems for improved security visibility and network protection.

In addition, Umbrella's secure web gateway logs and inspects web traffic for full visibility, URL and application controls, and protection against malware. Leveraging IPsec tunnels, Protected Access Credential (PAC) files, or proxy chaining to forward traffic to Umbrella cloud-based proxy, enterprises can enforce acceptable use policies and block advanced threats.

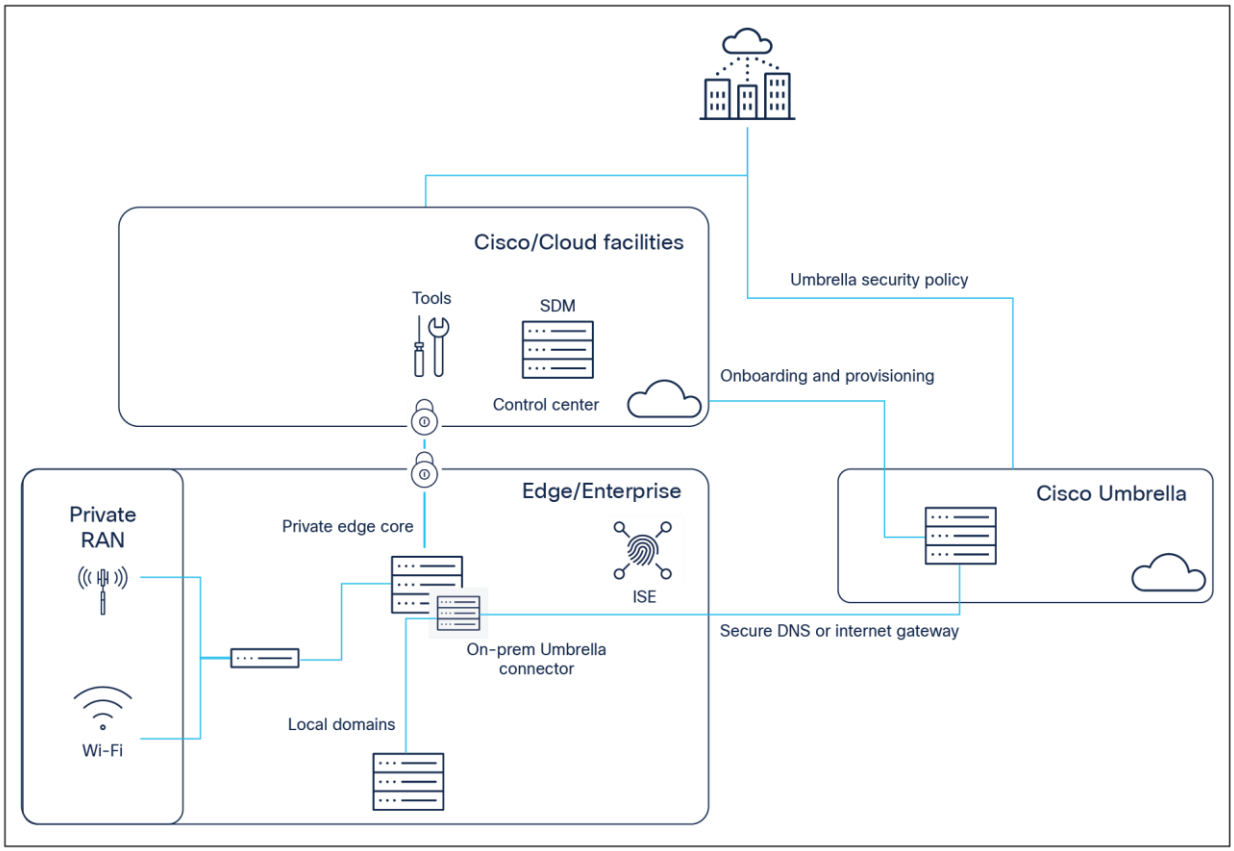

Figure 5.
High-level view of Cisco Umbrella integration into private networks

Leveraging Umbrella and Secure Connect from Cisco's Private 5G solutions, enterprises can achieve:

- **Basic redirect:** Ability to route DNS requests to generic Umbrella and apply standard security policy
- **Enterprise policy:** Ability to specifically tag enterprise ID within the DNS query so Umbrella can apply enterprise-specific policy
- **Automated IP pool provision:** Ability to include enterprise IP pools from the private network to Umbrella when a new IP pool is added within Private 5G network
- **Device identification:** Device-specific tagging along with enterprise ID for device-specific policy
- **Local domain offload:** Ability to offload local domains within enterprise instead of forwarding all DNS queries to Umbrella

The above solution capabilities will be delivered in a phased approach. Refer to the roadmap for additional details.

Cisco ThousandEyes

End-to-end observability is a key capability for both performance and security analysis (e.g., root causing of DDOS attacks). Cisco provides ThousandEyes® as a powerful application that a Managed Service Provider (MSP) can integrate into Cisco's Private 5G solution for enterprises. The following figure shows an example integration of ThousandEyes agents, easily deployable as docker containers, into the Private 5G solution.

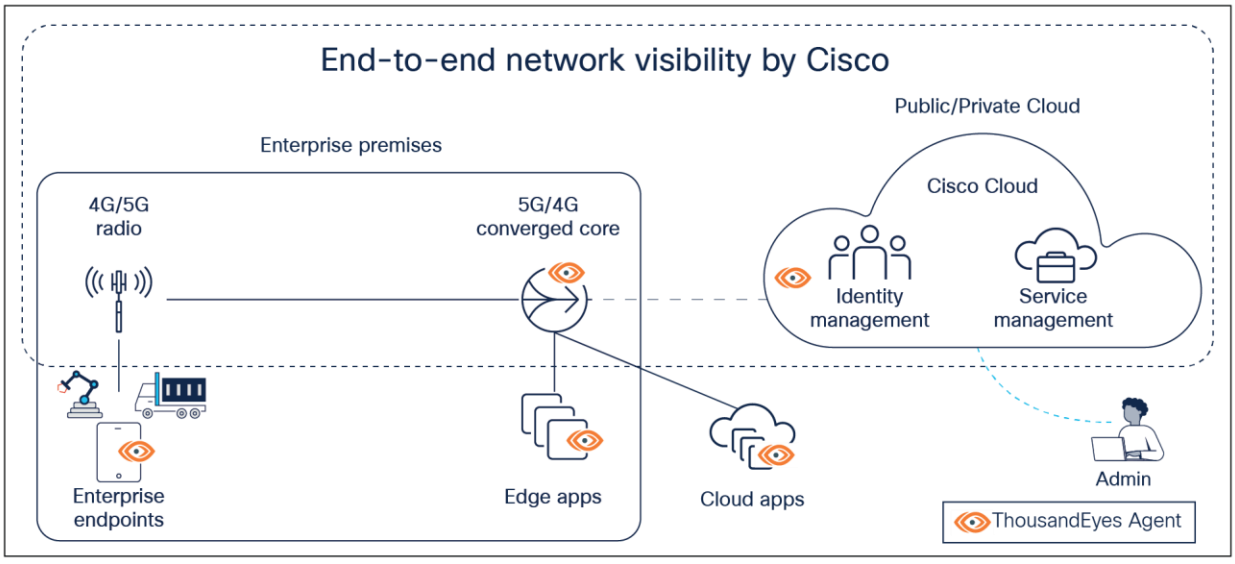

Figure 6.
Integration of Cisco ThousandEyes with Cisco's Private 5G solution

By combining the capabilities of Cisco ThousandEyes, Cisco Private 5G offers customers exceptional network visibility and insights. This empowers them to monitor network health, ensure a reliable service, and scale efficiently across their enterprise locations. The deployment of ThousandEyes agents can enable an enterprise to determine connection quality issues (loss, jitter, latency, throughput, BGP routing, etc.) for the following connections:

- Enterprise endpoints to Edge and Cloud-hosted applications
- Enterprise endpoints to Private 5G converged core on enterprise premise
- Enterprise endpoints and Private 5G enterprise edge to Identity and Service Management services on Cisco Cloud

Secure enterprise design

The Cisco Private 5G solution is designed with security features that enable easy integration into the existing enterprise security framework. In this section we'll cover security topics that relate to enterprise network design, and which need to be considered as Private 5G service is inserted into an existing enterprise network.

Cisco SAFE blueprint

Enterprise security in Cisco is covered through the SAFE blueprint. SAFE is a secure architectural framework example for business networks. SAFE simplifies complexity using a model that focuses on the areas that a company must secure. Using this blueprint, enterprises can design and implement security into their business processes.

SAFE includes:

- Business use cases illustrating the surface that fraudsters can attack
- Security capabilities mapped to common threats within business use cases
- Reference architectures that logically arrange the security capabilities into blueprints
- Designs using reference architectures for common deployment scenarios and solutions

SAFE can be considered a starting point for security design considerations for enterprise. Given that cybersecurity is a topic that increases in complexity every day, there are many other security resources available to an enterprise for establishing solid security practices. The following sections describe some of these resources.

Cisco zero-trust approach to cybersecurity

Cisco's approach to cybersecurity is based on the zero-trust principle promoted by many cybersecurity experts and standard groups such as the National Institute of Standards and Technology (NIST), Defense Information Systems Agency (DISA), International Standardization Office (ISO), Gartner, and Forrester, among others. The effect of zero trust is "ubiquitous least privilege access" (in other words, grant access but make it specific). Foundational assertions to this approach include:

- The network is always assumed to be hostile.
- External and internal threats always exist on the network.
- Network locality is not sufficient for deciding trust in a network.
- Every device, user, and network flow is authenticated and authorized.
- Policies must be dynamic and calculated from as many sources of data as possible.

To understand zero-trust concepts better, let's consider NIST SP 800-207 specifications, as depicted in the following logical diagram:

https://csrc.nist.gov/publications/detail/sp/800-207/final

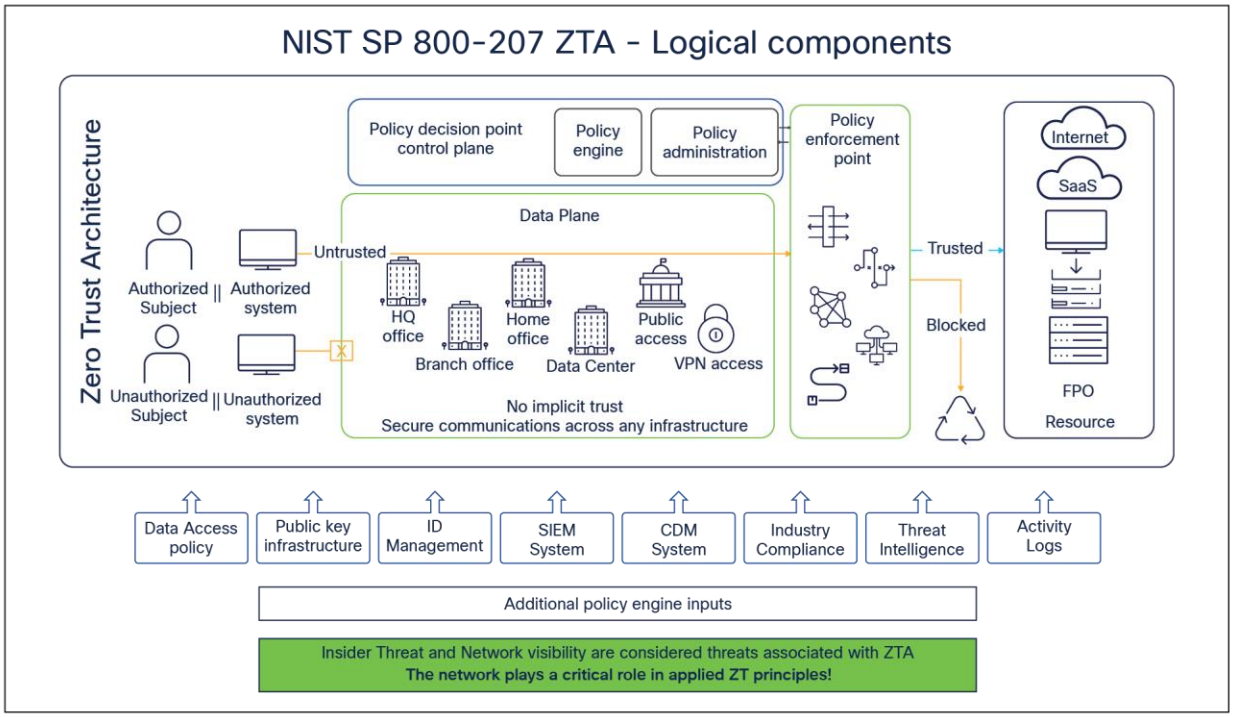

Figure 7.
NIST zero-trust concepts

According to the NIST guidance, any organization that intends to implement zero trust should articulate their access policy rules in a centralized policy engine that orchestrates policy enforcement through various enforcement points throughout the organization. All access will be subject to policy assessment, and there won't be "implicit" trust assigned to any internal access.

The enterprise monitors and measures the integrity and security posture of all owned and associated assets, collects as much information as possible about the current state of assets, network infrastructure, and communications, and uses it to improve its security posture. All data sources and computing services are considered resources. All resource authentication and authorization are dynamic and strictly enforced before access is allowed. Access to individual enterprise resources is granted on a per-connection basis and determined by dynamic policy. All communication is secure regardless of network location.

At Cisco we define and implement zero-trust fundamentals in three large categories, all of which are practiced by our own operational IT across huge global enterprises:

- Trusted workforce: Ensure only the right **users and secure devices** can access applications
- Trusted workplace: Secure all **user and device connections** across your network, including IoT
- Trusted workload: Secure all **connections within your apps**, across multicloud

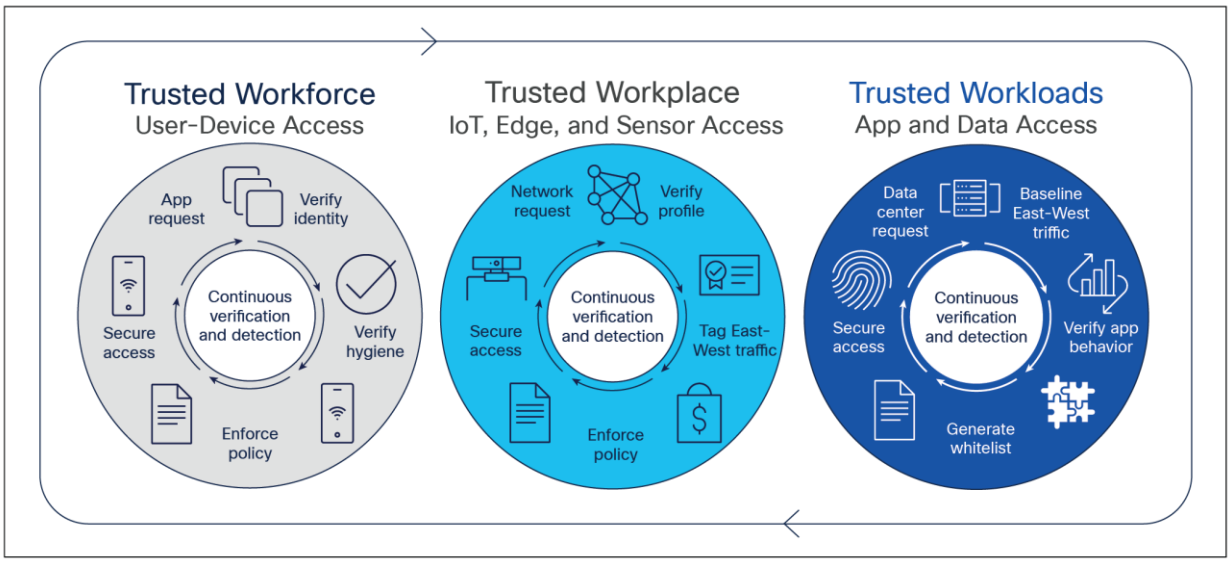

Figure 8.
Cisco zero-trust principles

Other Cisco security components and resources

There are many components to the Cisco security strategy, anywhere from a dynamic knowledge base that grows with world events to innovative product development to ease security tasks, as well as ever-needed discipline for validation and verification. In this section we will go over a few of these foundational components:

Cisco Trust Center: This is a great point of departure for all of our security topics. This site provides a single point through which you can access the latest advisories, guidelines, and documents, because an informed workforce is the most secure and transparency and accurate information sharing are tenets of our security efforts. This and its associated sites are updated on an ongoing basis to reflect the latest security-related news and information for all Cisco customers, partners, and employees.

Secure Standards: We're actively engaged with various national and international private and public bodies that establish cybersecurity standards and requirements (for example, NIST, DISA, and ISO). Cisco is both a driver and a follower of cybersecurity standards worldwide. Our customers rely on our expertise as well as our broad security portfolio to provide them with the most up-to-date cybersecurity information and features. The Cisco security baseline, which is defined and enforced in all our development, enables us to establish and implement a minimum solid set of necessary security features across all products while enabling more advanced and optional features for specific market segments as requested.

Trustworthy Systems Technology: As the largest enterprise cybersecurity company in the world, we lead the way with solutions that are driving the industry in Secure Access Service Edge (SASE), XDR, and zero trust. Integrating it all is Cisco SecureX™, our security platform that provides simplicity, visibility, and efficiency across your security infrastructure.

Cisco Secure Development Lifecycle (CSDL): We infuse security and privacy awareness into the entire development process of all products and services using the CSDL framework. Cisco SDL follows a secure-by-design philosophy from product creation through end of life. Because the security landscape is always evolving, so is CSDL. We constantly review the latest known security and privacy attacks and ensure that our technology can defend against them.

Cloud security

Cisco's Cloud Security Strategy integrates obtaining market access certifications (SOC 2, ISO 27001, FedRAMP, and more) with building secure offers through CSDL. The strategy represents a collaborative effort across engineering and the Security and Trust Organization (S&TO) to co-design deliverables that simultaneously meet security, privacy, and market access expectations. Specifically for our Private 5G solution, we're working with relevant certification providers to complete validation as part of various roadmap releases.

The Cisco Cloud Controls Framework (CCF) is a rationalized framework with comprehensive control requirements taken from numerous, globally accepted security compliance frameworks and certifications. It provides a structured "build-once-use-many" approach for achieving multiple regional and international certifications, enabling market access and scalability, as well as easing compliance strain.

Audits and compliance

At Cisco Control Center operations, we conduct regular reviews of information security systems and compare the results to appropriate security policies. Our technical platforms and information systems are audited for compliance with applicable security implementation standards and documented security controls.

Disaster recovery

Control Center's business-continuity process is designed to minimize the impact of a business interruption and recover information assets through preventive and recovery controls. A business-impact analysis identifies critical processes and integrates the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport, and facilities.

Business continuity plans ensure timely resumption of essential operations. They include controls to identify and reduce risks, limit the consequences of damaging incidents, and ensure that information required for business processes is readily available.

Conclusion

Cisco believes that ensuring security in private cellular networks requires consideration of multiple domains, including network functions, physical on-site infrastructure, transport networks, application layers, and cloud components. Cisco emphasizes that the end-to-end security is a shared responsibility between Cisco, managed service partners, and enterprises.

Cisco has incorporated industry-leading security practices into the private 5G solution at both edge and cloud components. Cisco is committed to deliver an enhanced security experience for enterprises by delivering unified identity and policy through ISE integration as well as common security policies through Umbrella and SASE integration.

Take the complexity out of private 5G and IoT

The next era of digital transformation begins with private 5G and IoT, delivered as a service for simple, intuitive, secure, and trusted modernization of industries. Cisco's Private 5G is a cost-effective, secure, and efficient way for enterprises to deploy cellular services while maintaining IT policy and identity.

To learn more on how Cisco Private 5G simplifies both 5G and IoT operations for enterprise digital transformation, please visit www.cisco.com/go/private5G.

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**.

Printed in USA C11-3180970-02 05/23