Contact Center Enterprise Solution Security

Last Updated: June 2, 2021 (Release 12.6.1)

Contents

Contact Center Enterprise solution security

The security landscape is ever evolving, with threats emerging on a daily basis. The new threats bring increasing sophistication and innovative mechanisms with substantial potential impact on your business. A security strategy is a necessity to protect the confidentiality, integrity, and availability of your data and system resources.

This white paper discusses the security architecture of **Cisco Contact Center Enterprise** products and solutions, including Cisco® Unified Contact Center Enterprise (Unified CCE), Packaged Contact Center Enterprise (PCCE) and the security controls that are implemented in them. It also discusses how the Contact Center Enterprise security architecture aligns with the Cisco Security Control Framework (SCF).

The audiences for this security white paper include systems architects, senior information security leaders, and business leaders. Readers must understand the core aspects of security in a contact center and the options for mitigation that can enhance the existing security posture of their contact center.

Information assurance and security strategy

Cisco's security strategy is to achieve synergies between security processes, technologies and tools, and security policies for compliance in Contact Center Enterprise solutions. These derive directly from:

- Cisco's product security requirements
- Market-based security and compliance requirements
- Mandatory regulations, security, and compliance requirements
- Collaboration SCF

Contact Center Enterprise security adherence is based on the Cisco Security Control Framework. An internal enterprise security team, as part of the Cisco Secure Development Lifecycle (SDL) processes, verifies our adherence. Figure 1 depicts the SDL.

Figure 1.
Cisco Secure Development Lifecycle

Cisco Security Control Framework (SCF)

The SCF provides design and implementation guidelines for building secure and reliable collaboration infrastructures that are resilient to both well-known and new forms of attacks. The SCF is composed of a model, methodology, control structure, and control sets to support the assessment of technical risk in an infrastructure architecture (Figure 2). It integrates into an ongoing process of continuous improvement. That process incrementally improves the security posture of the infrastructure architecture to address current key threats and to identify, track, and defend against new and evolving threats.

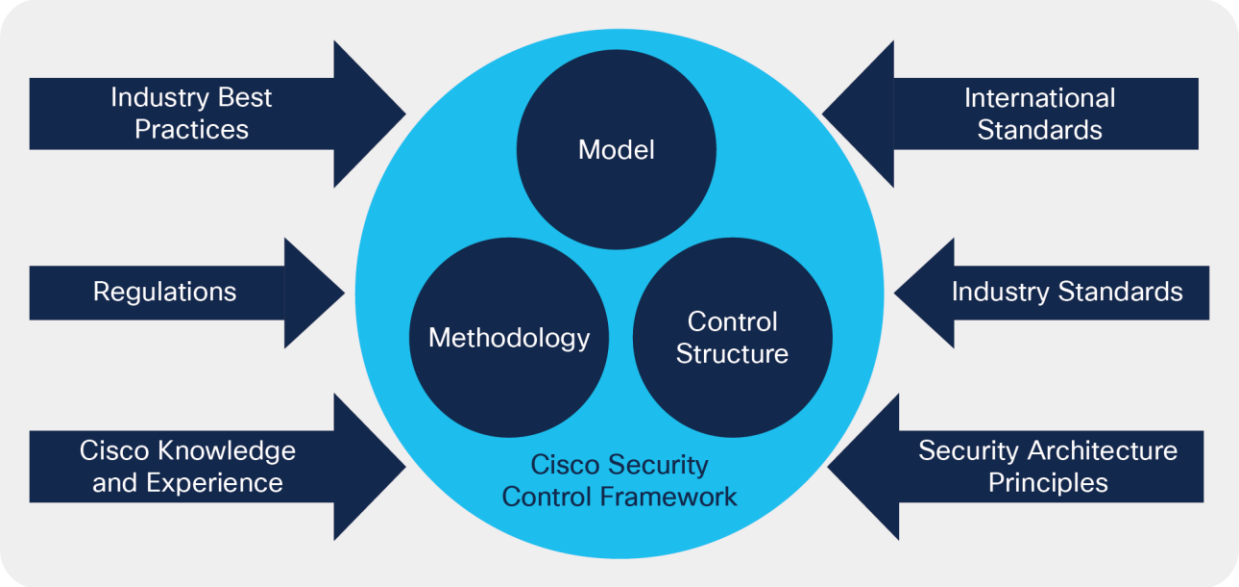

Figure 2.
Cisco Security Control Framework

SCF objectives and architectural resiliency

The SCF defines security actions that help enforce the security policies and improve visibility and control. Visibility is enhanced through the actions of identify, monitor, and correlate. Control is improved through the actions of harden, isolate, and enforce (Figure 3).

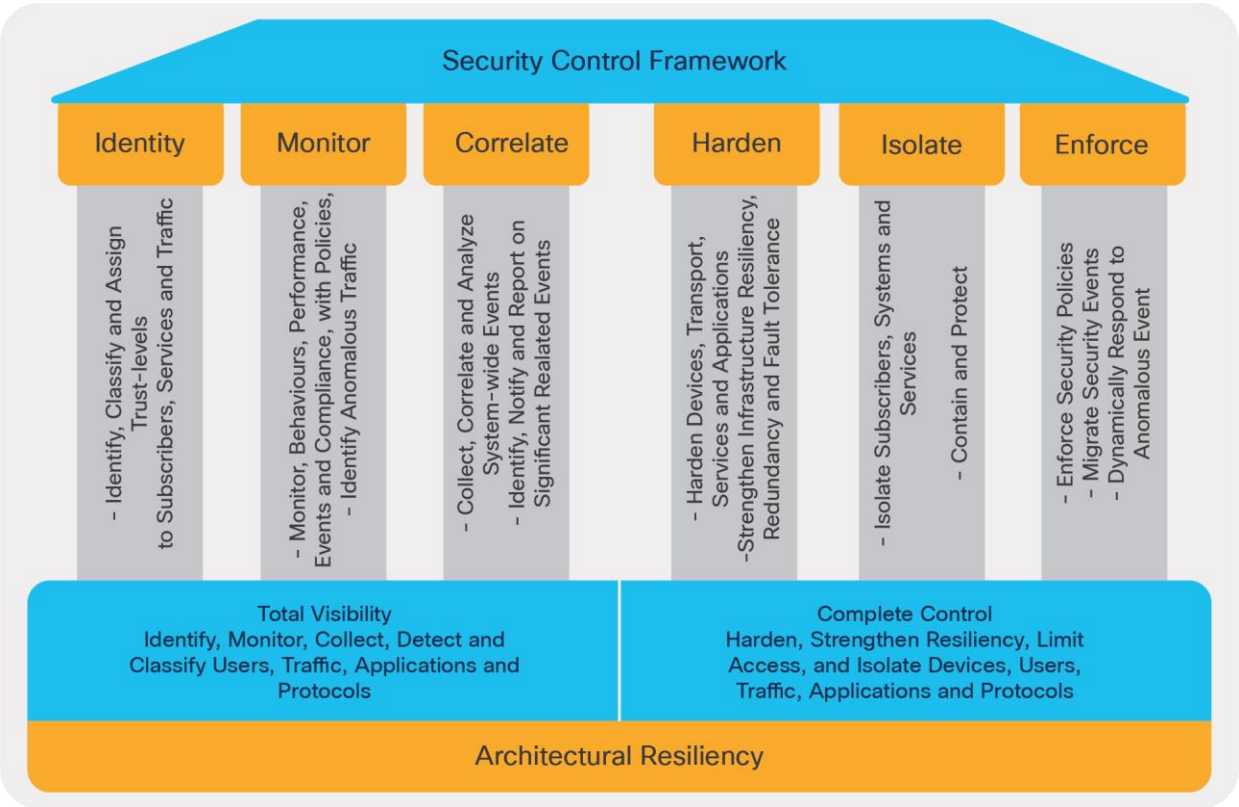

Figure 3.
SCF objectives and architectural resiliency

Security architecture principles

Cisco's SDL aligns with and, in some areas, leads the industry in creating highly secure solution architectures. The SDL principles are designed into every Unified CCE release through the practice of secure coding standards. These standards are designed to prevent vulnerabilities from entering the product. They seek to eliminate undefined behaviors that can lead to unexpected program behavior and known exploitable vulnerabilities.

The security architecture principles mandate that you deploy defensive measures against known security vulnerabilities. These measures include:

- Trust, but verify
- Secure weak entities and significant entities
- Mandate platform hardening
- Fail safe and fail securely
- Defend in depth (each entity verifies inputs)
- Default is always "least privilege" unless approved explicitly
- Segregate privileges (role separation and duty separation)
- Every entity is tri-party-approved before entering the ecosystem (operations, release, and security)
- Protect Personally Identifiable Information (PII) and any data identified as sensitive, at rest, and in transmission
- Log all failures and all create, read, update, and delete actions, and protect the logs

Product security architecture

Cisco Contact Center Enterprise solutions' security architecture comprises multiple, layered security options and controls. You can deploy these security features to meet individual security requirements. You can also combine these features to achieve a robust security posture against attacks.

The Cisco Contact Center Enterprise solutions include some servers that run on Windows Server OS and others that run on the Linux-based Cisco Voice OS (VOS). The security architecture leverages the resources of the OS on which a particular server runs.

On a Windows OS, the servers leverage the Windows Firewall/Defender, Windows NT LAN Manager (NTLM), Windows Hardening Policies, and Active Directory. These servers include:

- The peripheral gateway
- The router
- The logger
- The administration and data server
- Cisco Unified Customer Voice Portal (Unified CVP)
- Cisco Unified Contact Center Management Portal

The Cisco VOS platform is a closed, appliance-based model that runs within a Linux (shell) OS architecture. The servers that run on VOS include:

- Cisco Finesse®
- Cisco Unified Intelligence Center (CUIC)
- Cisco Virtualized Voice Browser (VVB)
- Cisco Unified Communications Manager (CUCM)
- Cisco Unity® Connection
- Cisco Identity Service (IdS)
- Cisco Live Data (LD)
- Cisco Customer Collaboration Platform (formerly SocialMiner®)
- Cisco CloudConnect

The core elements of a Unified CCE instance are shown in Figure 4.

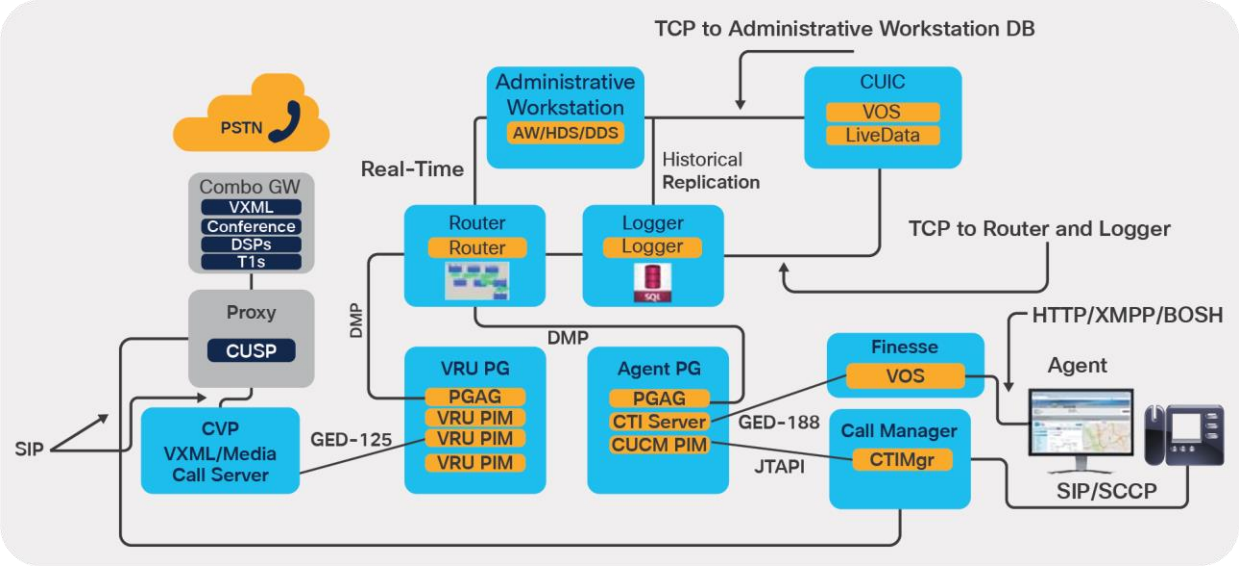

Figure 4.
Cisco Unified CCE

Application endpoints, such as desktops and phones, involve Computer Telephony Interface (CTI), Java Telephony API (JTAPI), and any TAPI applications. These endpoints are secured by leveraging Transport Layer Security (TLS) and Secure Real-Time Transport Protocol (SRTP). The solution also uses a Certificate Trust List (CTL) that you create that establishes signaling authentication between client and server.

Network security architecture

Contact Center Enterprise solutions offer a flexible network security model. There are many areas in the network where you can apply security to the solution, based on your unique needs and compliance requirements. These include firewalls, Access Control Lists (ACLs), private network addressing, Network Address Translation (NAT), setting up a network edge (DMZ), Transport Layer Security (TLS), Secure Real-time Transport Protocol (SRTP), and IP Security (IPsec).

You can secure in-flight data by deploying IPsec. IPsec is an Internet Layer 3 framework made up of open standards designed to ensure private, secure communications over IP networks. Security is provided through the use of cryptographic security services and policies. IPsec helps defend against:

- Network-based attacks from untrusted computers that can result in the denial of service of applications, services, or the network
- Data corruption
- Data theft
- User-credential theft
- Network security attacks (IP spoofing, DNS hijacking) against critical servers, other computers, and the network

You can deploy IPsec in two modes in a Contact Center Enterprise solution. LAN or WAN network endpoints support either transport mode or tunnel mode deployments, while contact center nodes (peripheral gateways, routers, loggers, etc.) support only transport mode IPsec (Figure 5).

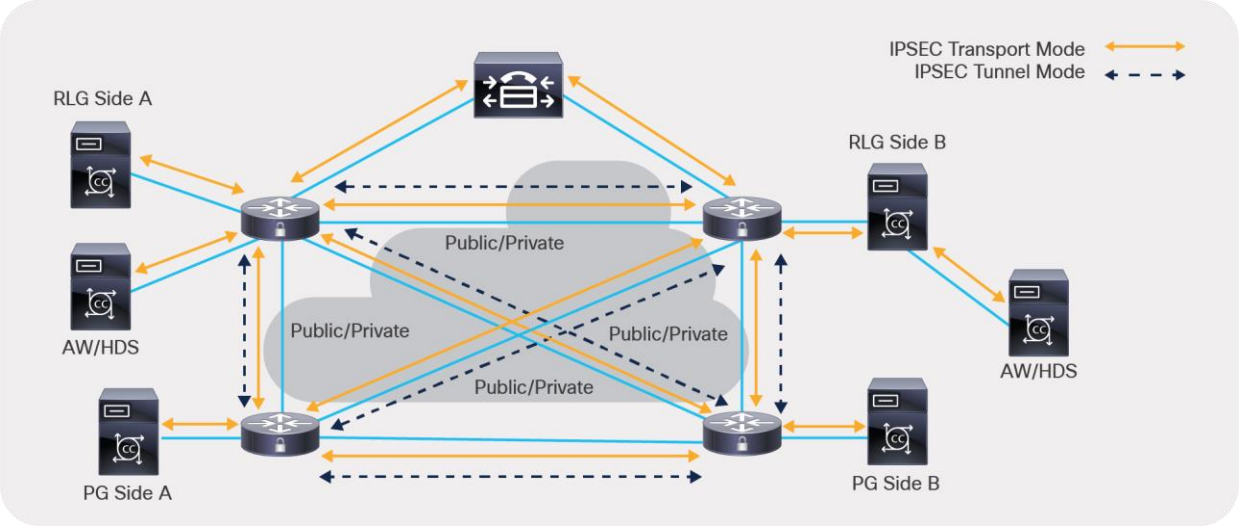

Figure 5.
IPsec transport mode and tunnel mode

TLS could be used in place of IPSec for securing interfaces. Refer to the documentation of each solution component for details on each interface. The documentation specific to the CCE interfaces shown in Figure 4 can be found at:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_12_6_1/configuration/guide/ucce_b_security-guide_12_6_1.html

You secure voice traffic in your solution by applying encryption directly to the Real-time Transport Protocol (RTP), which delivers audio and video streaming. RTP streams are not terminated within the core Contact Center Enterprise solution. Adjunct devices, such as Cisco Unified Communications Manager and voice gateways, supply the media termination within the solution.

SRTP is the method used to secure voice and video traffic (media), whereas SIPS (SIP over TLS) is used to secure the signaling.

Unified CCE web servers use Microsoft Internet Information Services (IIS) for web server responses and Apache Tomcat for client authentication. Solution components such as CVP, VVB, PCCE webconfig frontend UIs, and REST APIs use Apache Tomcat. Finesse, CUIC, and LD front-end use nginx. Communications between web servers and web-based users are trusted and encrypted using HTTPS (TLS).

The servers that make up the Contact Center Enterprise solution reside in a protected data center. They are not typically exposed to open internet traffic. These servers are deployed behind a firewall (Figure 6). The only exceptions are the Cisco Customer Collaboration Platform (CCP) servers, and the Enterprise Chat and Email (ECE) web servers that reside inside a DMZ.

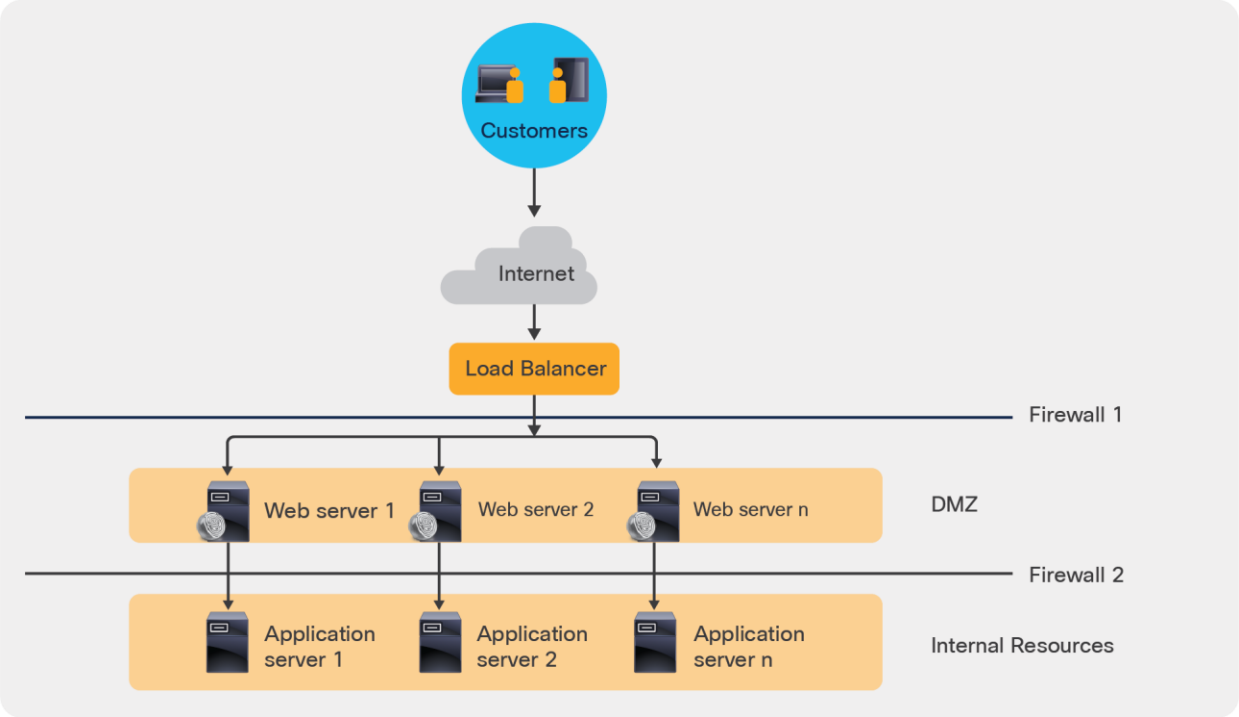

Figure 6.
Using a DMZ to protect the data center

This document focuses primarily on premises-based Contact Center Enterprise solutions. Cisco also offers cloud-based contact center solutions, such as Webex® Contact Center. Our premises solutions also have cloud-based (hybrid) features that enhance Contact Center Enterprise solutions, as mentioned earlier. We are thorough in ensuring compliance with international standards requirements for cloud data handling. Cisco complies with the Binding Corporate Rules (BCR) of the EU, the Privacy Shield, and the Asia-Pacific Economic Cooperation Privacy Framework (APEC Privacy Framework) for cloud data handling and cross-border transfers. Details of these protections are provided on the Cisco Trust Center website at: https://www.cisco.com/c/en/us/about/trust-center.html.

Security Control Framework for total visibility

The Cisco Security Control Framework (SCF) model defines a structure of security objectives and supporting security actions to organize security controls. The model is based on proven industry best practices and security architecture principles, as well as the vast practical experience of Cisco engineers in designing, implementing, assessing, and managing service provider, enterprise, and small and medium-sized business (SMB) infrastructures. Using the Cisco SCF model provides insight into the system's activities through total visibility objectives. The SCF mandates that the system knows:

- Who accesses the system
- What actions are performed
- Whom to inform about any anomalies, functional deviations, or suspicious activities

Key considerations for total visibility include:

- Identifying and classifying users, traffic, applications, protocols, and usage behavior
- Monitoring and recording activity and patterns
- Collecting and correlating data from multiple sources to identify trends and system wide events
- Detecting and identifying anomalous traffic and threats

Identify (identification, authentication, authorization, etc.)

Cisco Contact Center Enterprise solutions leverage two common methods for user authentication and authorization. Unified CCE uses NTLM v2 for server-to-server authentication. Administrative user accounts use Active Directory (AD) for authentication and authorization to perform tasks related to staging, deployment, and operations.

By default, Unified CCE agents authenticate through the Unified CCE configuration SQL database. You can optionally deploy Single Sign-On (SSO) to authenticate agents with a qualified Identity Provider (IdP). The IdP can be internal or external but must provide Security Assertion Markup Language (SAML) v2 assertions for authentication. In an SSO deployment, user passwords are not stored in the application's configuration database. After authentication succeeds, Unified CCE supplies OAuth tokens through Cisco Identity Service for authorization to access protected resources.

Users

Cisco Contact Center Enterprise solutions recognize these classes of users:

- Administrators
- Agents and supervisors
- API users

There are two subclasses of administrators: domain administrators and local administrators. AD holds all administrator identity and authorization. You use domain administrator accounts for setup-related tasks that require domain administrative privileges, such as AD staging. You use local administrator accounts for tasks that require only local administrative privileges in AD, such as binding to an AD root Organization Unit (OU) instance or accessing diagnostic tools.

Agents are the core users of the Contact Center Enterprise solution. You create and authenticate agent accounts through the configuration database.

Supervisors need extra privileges for tasks such as reskilling agents and running reports. Because of this, you create supervisor accounts in AD.

Contact Center Enterprise solutions include several APIs for interfacing with third-party tools. All Unified CCE REST API calls are stateless (not session sticky) but authenticated calls through HTTPS. You define authorized API users during initial system deployment.

Wherever a solution component performs authentication by itself, randomly salted strong hashes generated using recommended hashing functions are supported. This is done to ensure maximum protection from rainbow table and brute-force attacks.

Devices

The Unified CCE solution contains devices that play a central role in user-related data management for authentication and authorization. These devices also provide the capability to perform an “audit-light” change control history.

The Unified CCE administration and data server contains a copy of the Unified CCE configuration schema in an SQL database. This information provides a default (non-SSO) method of authenticating contact center agents. It also provides a mapping of privileges for system administrators to allow for least-privileged access control through the use of Unified CCE’s feature control set.

To support SSO for agents and supervisors, the solution deploys Cisco Identity Service, a VOS-based appliance. Cisco Identity Service is trusted to the IdP and is responsible for internal OAuth token management across protected resources, such as Cisco Finesse and Cisco Unified Intelligence Center. If you enable SSO in your contact center, the relevant agents and supervisor authentication data reside in the customer’s IdP and not within the Unified CCE database. Figure 7 illustrates SSO authentication and authorization.

The Unified CCE logger contains a redundant, primary copy of the entire Unified CCE configuration. The Unified CCE router uses a dynamic key generation method to synchronize and store all configuration transactions and their related history in the logger database. The Unified CCE tools can leverage these configuration and recovery keys to track and revert changes in call routing script history and general Unified CCE configuration transactions.

Active Directory plays a central role in managing security policies across our core Windows-based Unified CCE components and in providing authentication for administrative users. User passwords stored in Active Directory reside in the local Security Accounts Manager (SAM) database. Unified CCE accounts that you create for use with web setup and web administrator authenticate with an Active Directory user account.

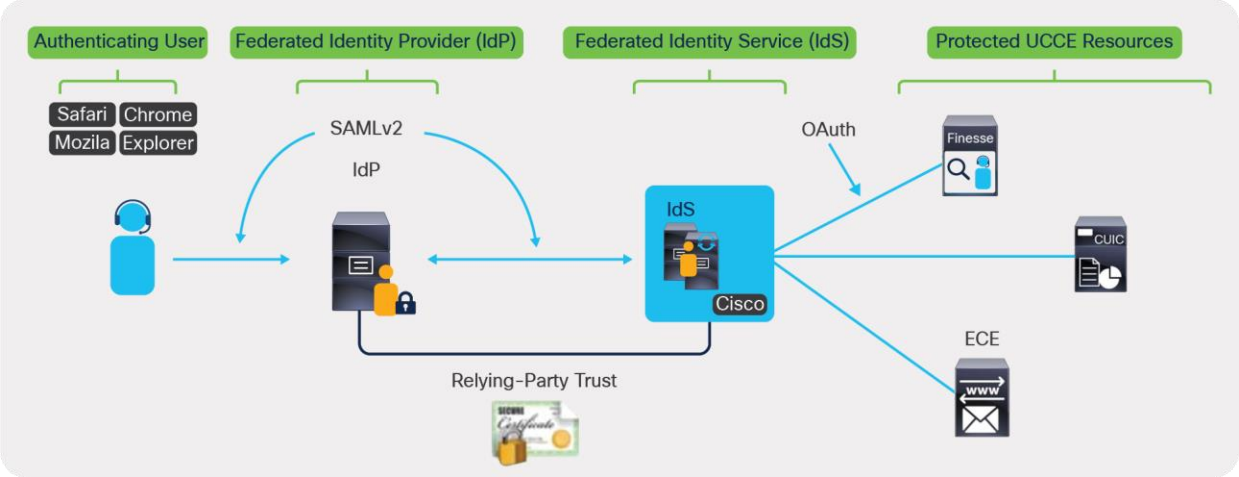

Figure 7.
Single sign-on authentication and authorization

Services and applications

Unified CCE servers operate in a trusted Microsoft Active Directory domain. Before installing any Unified CCE components, you must first perform the required Microsoft Active Directory staging. First create a root OU in the target AD domain where the Unified CCE servers will reside. You can then place the root OU, “Cisco_ICM,” either at the domain root or nested within another OU. Do not nest the root OU more than one layer under the domain root. To create the root OU, you run Unified CCE’s Domain Manager. You must also provide domain administrator rights or delegated (full control) rights to a sub-OU where our root OU is nested. Once the root OU is created by Domain Manager, you no longer require domain administrator rights for the rest of the installation.

After installing the core Unified CCE software, you’ll run WebSetup to create the Active Directory Service accounts required for Unified CCE database services. WebSetup is hard-coded to create these accounts within the AD root OU by default. However, once this is complete, you can run our Service Account Manager (SAM) utility to map our database services to preconfigured AD accounts. If you perform this custom mapping of our service account users, you can delete the default service accounts that Unified CCE WebSetup created.

Unified CCE web servers are configured for secure access (HTTPS). Cisco provides an application, SSL Encryption Utility (SSLUtil.exe), to help configure web servers for use with TLS. This utility simplifies the task of configuring TLS encryption by performing the following functions:

- SSL configuration
- SSL certificate administration

For more details, refer to:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_12_6_1/configuration/guide/ucce_b_security-guide_12_6_1/ucce_b_security-guide_12_6_1_chapter_01000.html?bookSearch=true#concept_EA5EEA5FB4B47361DE014342F213715A

The Cisco Unified Contact Center Security Wizard is a standalone server-hardening deployment tool that simplifies security configuration. With the Security Wizard you can:

- Define Windows Firewall policies
- Apply SQL hardening
- Perform network isolation with IPsec

You may also use OS tools to perform these security tasks, such as those found in Microsoft Internet Information Services (IIS).

Every Cisco Contact Center Enterprise software release is qualified to operate with specific versions of third-party antivirus software.

Hybrid service integrations

Multiple premises solution components, such as CVP, VVB, and Finesse, support optional hybrid features that connect from customer premises to services hosted in public clouds managed and operated by Cisco (except VA-V, which is a direct integration between a premises solution and Google DialogFlow/CCAI).

For each such service, the following measures are common:

- Access tokens for Cisco's WebexCC services are obtained from Webex Control Hub via Cisco CloudConnect, a premises-deployed solution component that acts as mediator.
- gRPC/REST API calls made from premises components to CloudConnect or cloud-hosted services are authenticated, secure (HTTPS), and with limited scope.
- Access tokens are cached in memory and periodically refreshed.
- Access tokens are currently not SSO-based, but tenant-specific.

In addition to these services, you can also use the following security measures specific to each hybrid feature and component.

Cisco Answers:

- The Answers feature and CallType have to be explicitly enabled on CCE for the agent.
- The Answers gadget has to be explicitly enabled for an agent team via Finesse administration.
- CloudConnect has to be explicitly onboarded on Finesse.
- The gadget is cloud-hosted.
- The access token is persisted in browser memory and refreshed periodically.

Cisco Virtual Assistance - Voice (VA-V):

- This feature has to be explicitly enabled and configured via onboarding.
- Enabling secure logging allows masking and disabling of logging of PII data.
- Google is responsible for redacting PII data from transcript storage.

Webex Experience Management (Webex XM):

- Webex XM requires a Cisco partner to set up an auxiliary service to redact PII data and provide storage in compliance with existing standards, such as GDPR, depending on the region of hosting.

Cisco CloudConnect:

- Internal services are containerized and hence, inherit the associated security posture, failure isolation, and ease of upgradability.
- CloudConnect is a VOS-based appliance with limited interfaces.
- Container images are hosted in Docker Hub, protected by credentials that are secured in the Cisco Webex cloud.

Cisco cloud-hosted software repository:

- Software artifacts are stored in a Cisco-hosted JFrog repository and can be accessed only with the required authentication and authorization.
- A unique access token is generated for each customer. The access token is stored encrypted on the CloudConnect instance deployed within the customer's premises.

Monitor

Monitoring plays a vital role in effectively managing the operations that must cover all the critical components of the product architecture. Monitoring helps in detecting any security issues so that those issues can be analyzed and mitigated as soon as possible based on their severity.

Security issues can come from network attacks, network breakages, application security attacks, and transaction failures and can result in denial of services.

Network monitoring

You can monitor your Cisco Contact Center Enterprise solution with the Cisco Unified Communications Manager Real-Time Monitoring Tool (RTMT). The RTMT collects diagnostic information and gathers platform and application configuration data as well. It provides an administrative interface for collecting all diagnostic (health and status) information and requests for all devices in its network topology. Figure 8 shows the solution components that are monitored for their network interactions.

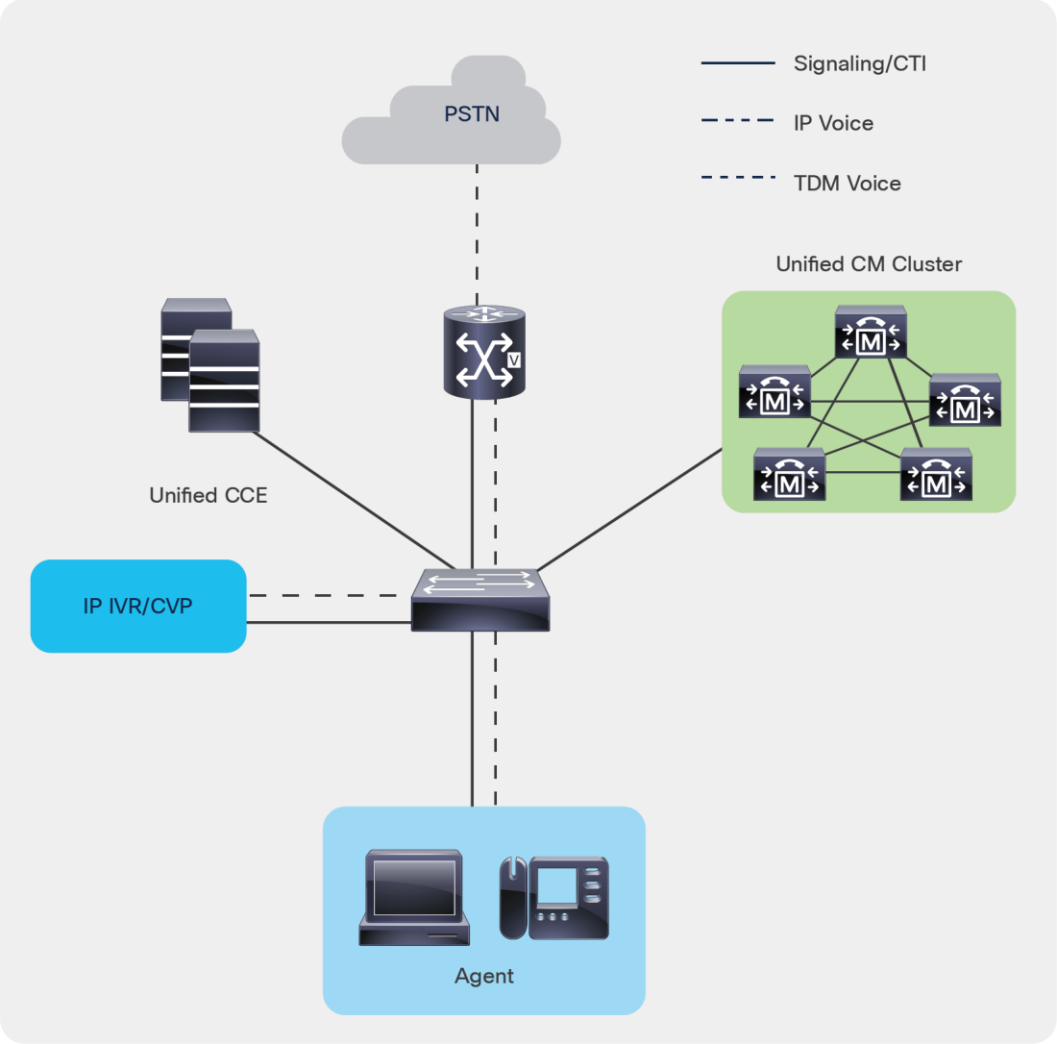

Figure 8.
Unified CCE components that are monitored

Cisco Contact Center Enterprise solutions capture specific network events. They report abnormalities in network requests. By configuring RTMT, which is an option, you can then use other security tools to analyze for security issues such as network-based attacks (slow-TCP attacks, also known as Slow loris, or packet bombardment such as Ping of Death). Each component checks for the heartbeat of the other components with which it interfaces. Network events that are tracked include:

- Host not reachable
- TCP timeouts
- Excessive response delays

Your Cisco Contact Center Enterprise solution provides built-in capabilities to aid in reporting on network abnormalities and for integrating with third-party security intelligence tools, including:

- Real-time performance monitoring of contact center devices
- Device inventory management and discovery
- Prebuilt and custom threshold, syslog, correlation, and system rules
- Link status, device status, device performance, and device 360
- Event alerts in the form of email messages, for user-configured thresholds
- The ability to collect and view traces in default viewers that exist in RTMT

Your security strategy should include security intelligence tools that can integrate with the Contact Center Enterprise solution and analyze this data. You can find third-party tools to fill this role. Cisco also has our own security intelligence tools. They include:

- Cisco Advanced Malware Protection (AMP)

  Cisco AMP provides global threat intelligence, advanced sandboxing, and real-time malware blocking to prevent breaches. And because you can't rely on prevention alone, AMP also continuously analyzes file activity across your extended network, so you can quickly detect, contain, and remove advanced malware.

- Cisco Secure Network Analytics (formerly Stealthwatch®)

  Secure Network Analytics uses industry-leading machine learning and behavioral modeling to help identify and respond quickly to emerging threats. You can monitor your network to see who is on and what they are doing, using telemetry from your network infrastructure. This helps protect your critical data with smarter network segmentation.

- Cisco Prime® Assurance

  Cisco Prime Assurance provides automated, accelerated provisioning, real-time monitoring, proactive troubleshooting, and long-term trending and analytics for Cisco installations.

Data transmissions

The components in Cisco Contact Center Enterprise solutions communicate with other components as part of their business transaction orchestration. The components monitor major data transmission for the segments shown in Figure 9.

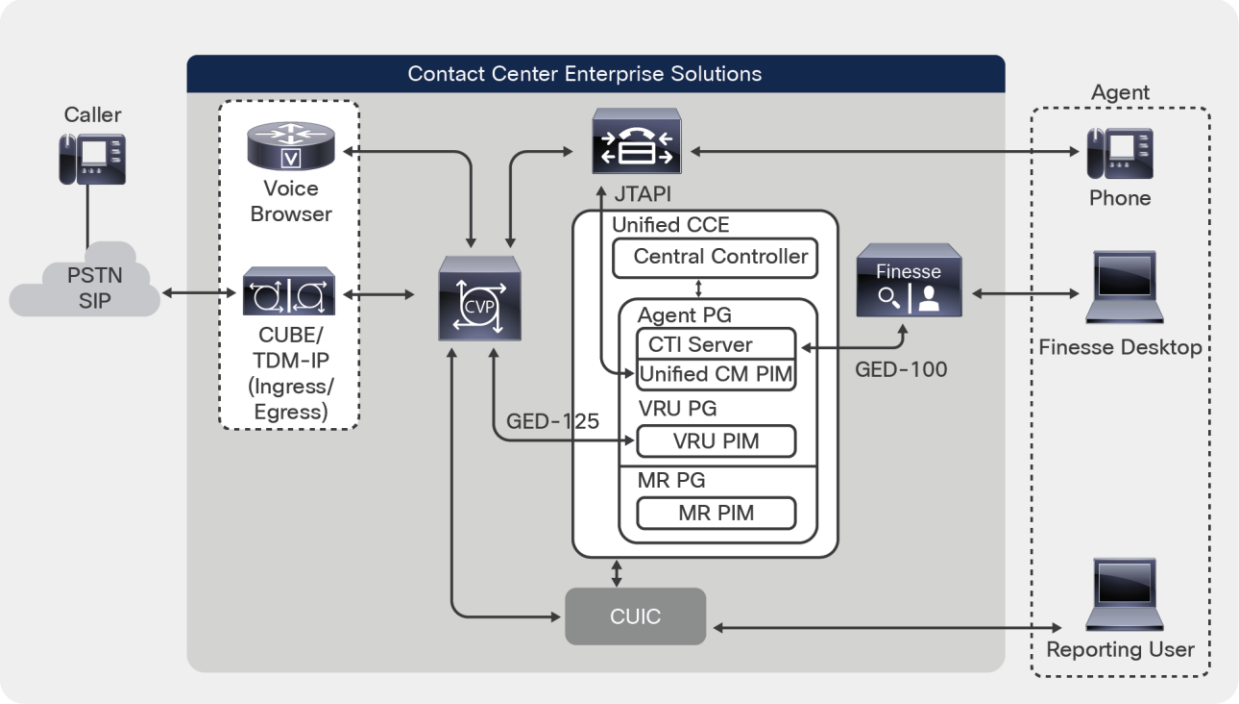

Figure 9.
Monitoring of data transmission components

Incoming calls

Unified CCE receives calls in two primary ways. Inbound calls can come through a Public Switched Telephone Network (PSTN) or an IP-based Session Initiated Protocol (SIP) trunk that uses voice over IP (VoIP) technology to stream media services to a telephony endpoint. In both cases, the physical media traverses between the ingress carrier, voice gateways, and Cisco Unified Communications Manager media termination endpoints. The physical media stream does not terminate within the core Unified CCE components. But Unified CCE and Unified CVP provide critical real-time signaling for call treatment and handling, whereas the Virtualized Voice Browser (VVB) provides for self-service treatment like Interactive Voice Response (IVR) functionality.

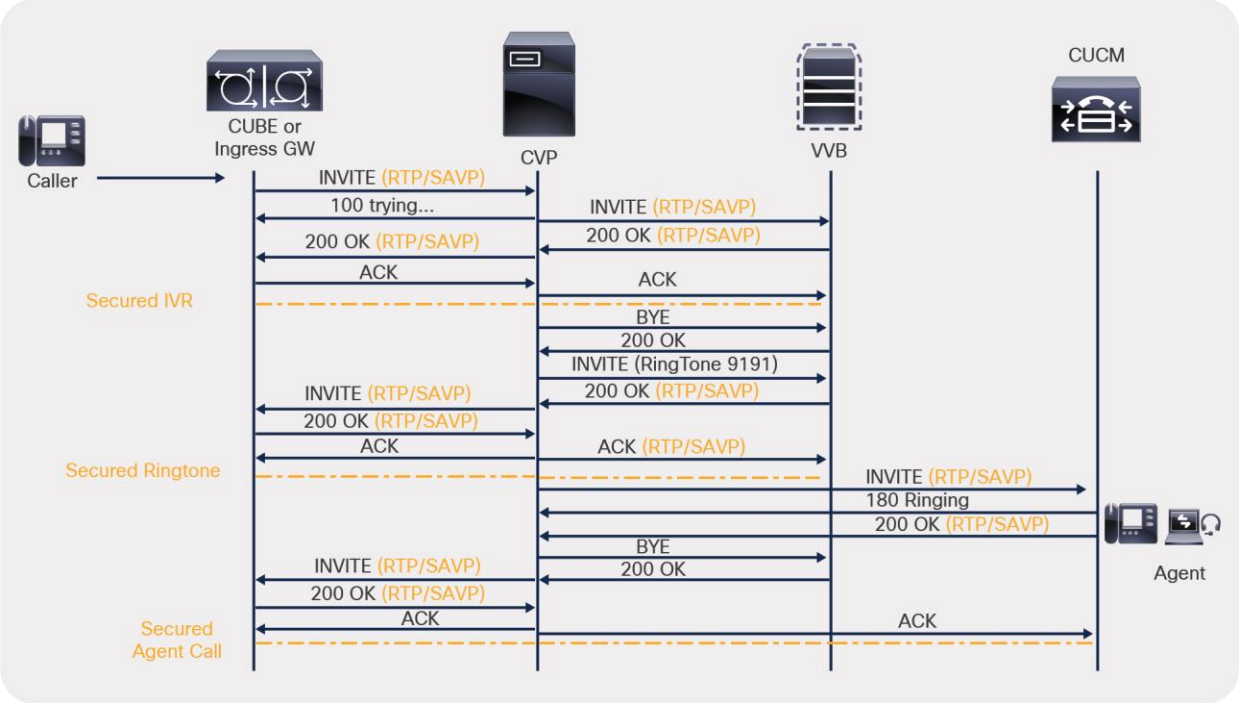

Figure 10.
Handling of incoming calls

The Unified CCE solution includes security features that are designed to actively detect and prevent inbound call attacks related to:

- Toll fraud
- Telephony Denial of Service (TDoS)

Toll fraud is the illicit use of a telephony system to make long-distance (international) calls without any accountability. To prevent toll fraud in a Cisco collaboration network, you can employ various tools, including:

- Cisco Unified Communications Manager Class of Service (CoS)
- Voice gateway toll fraud prevention application
- Voice gateway Class of Restriction (CoR)
- Cisco Unity Connection restriction rules

TDoS attacks generally follow the same model as a data network Denial-of-Service (DoS) attack: unauthorized users flood the system with too many access requests and prevent legitimate users from accessing the system. Unified CCE comes equipped with a Congestion Control capability. You can use Congestion Control to monitor incoming Calls Per Second (CPS) patterns and to alert the contact center and protect it from TDoS attacks.

Business transactions

These are some of the business transactions in which data is captured and monitored for diagnosis and any failure:

- Routing control – Messages that enable a Cisco Unified Communications cluster to request routing instructions
- Device and call monitoring – Messages that enable a cluster to notify Unified CCE of state changes
- Device and call control – Messages that enable a Cisco Unified Communications Manager cluster to receive instructions from Unified CCE

Figure 11 illustrates these business transactions.

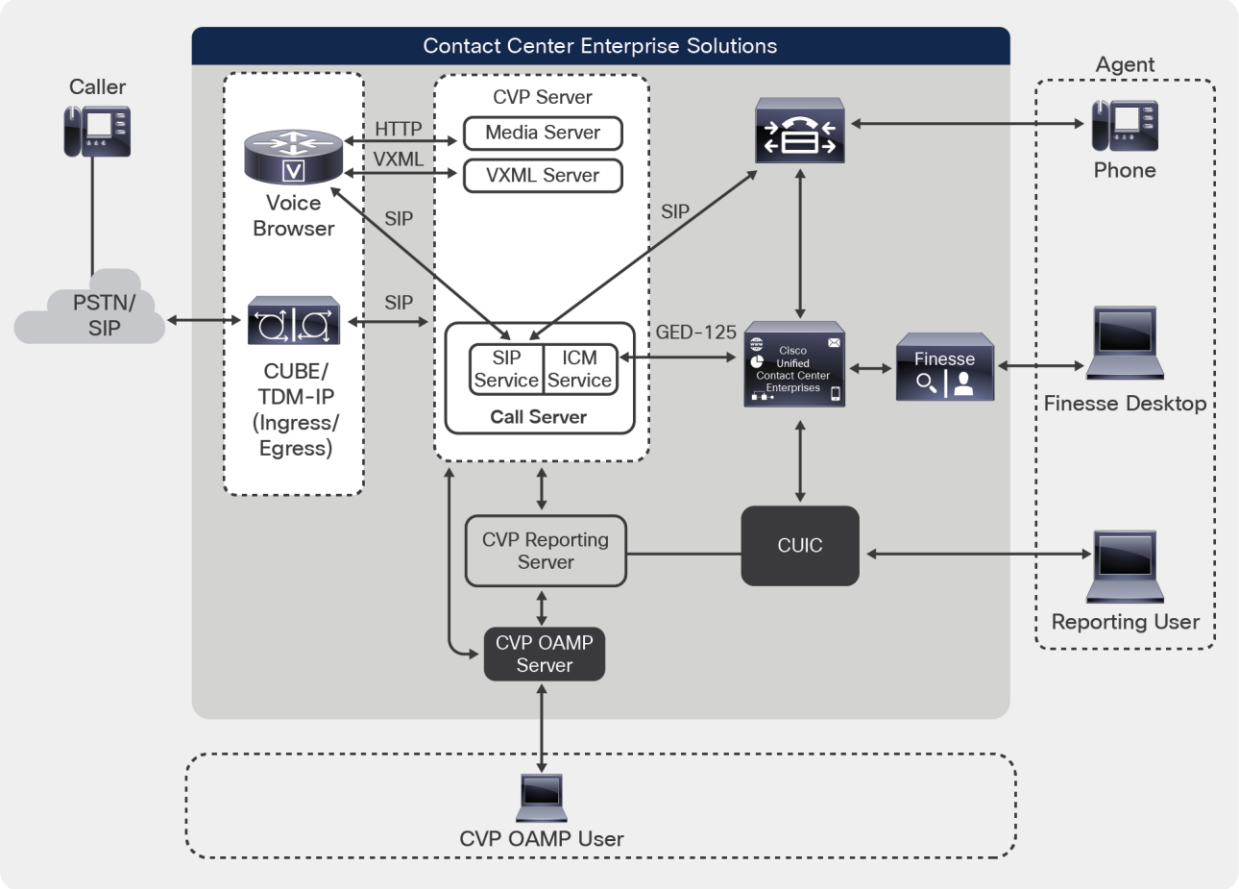

Figure 11.
Unified CCE business transactions (call flows between components)

Logging and auditing

Most application logging frameworks focus on identifying technical faults as they occur. The Unified CCE solution supplies both platform and process logging capabilities through a combination of a custom diagnostic framework API and industry-standard Simple Network Management Protocol (SNMP) and syslog protocols.

Security auditing requires a more tightly integrated method that blends reactive logging with proactive tools and analysis to prevent issues from affecting system health. Unified CCE has built-in auditing features capable of:

- Cradle-to-grave call reporting
- Detailed agent reporting through Unified Intelligence Center and an open database schema
- Audit trails for blended task routing between agents and customers
- Open database schema that enables the tracking of administrative changes by leveraging t_Event and Recovery tables
- Automated alerting through the Cisco Real-Time Remote Monitoring Tool (RTMT)

Business transactions and other data transmissions are logged using syslog and the central repository service. Cisco Unified Intelligence Center provides reporting and analysis capabilities for auditing.

The RTMT sends alerts for any configured violations (incidents) as email messages. It also specifically configures system-critical violations (incidents) with SNMP traps. RTMT can report on the following types of events:

- Device inventory management
- Voice and video endpoint monitoring
- Diagnostics
- Fault management
- Contact center devices' real-time performance monitoring
- Events and alarms along with root-cause analysis
- Contact center device dashboards—prebuilt and custom
- Threshold, syslog, correlation, and system rules—prebuilt and custom
- Multitenancy and logged-in agent licensing information

Correlate

Applying context and meaning to information security requires the correlation of events, incidents, and failures that are recorded between application logging and auditing. Correlation adds critical informational value by evaluating the relationships between what would normally be information silos. Unified CCE offers the ability to correlate real-time and historical events within the solution to increase the value of your security information.

Correlation of events, incidents, and failures helps you identify, understand, and troubleshoot system failures and issues better than finding individual root causes in an isolated manner.

Events and incidents

Any business event can become an incident. Your business also needs to classify some system events as incidents by default. Your operations run book or standard operational procedures will address corrective and preventive actions for those events. Cisco Contact Center Enterprise solutions define the following business events as incidents that require administrative notifications and corrective actions:

- Host not reachable
- TCP timeouts
- Excessive response delays
- Unknown link status
- Unknown device status
- Device, call control, and monitoring message failures
- Routing control message failures

The Contact Center Enterprise solutions provide alert and notification capabilities for these incidents. They send information about such critical failures to administrators for predefined corrective actions.

For more details, refer to the chapter on auditing in the Security Guide for Cisco Unified ICM/Contact Center Enterprise:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_12_6_1/configuration/guide/ucce_b_security-guide_12_6_1.html

Alerts and notifications

Alerts and notifications (alarms) are a system capability that notifies system administrators of an event so they can take any required corrective or preventive actions to maintain smooth business operations. The solution enables you to track significant events, such as account sign-in attempts.

Capturing Contact Center Enterprise real-time alerts

The SNMP Event Translator facility converts Windows events, in real time, into SNMP traps.

Contact Center Enterprise database alerts with Microsoft SQL Server

Microsoft SQL Server includes event capturing and reporting through its audit capabilities. These new capabilities replace SQL Trace, as explained in this Microsoft TechNet article:

https://docs.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-database-engine?view=sql-server-ver15.

Note on Microsoft SQL Server C2 security

Cisco does not support C2 event capturing for audits in Microsoft SQL Server in our Contact Center Enterprise solutions due to degradation in transaction performance.

Contact center user events with Active Directory

The alerting mechanism of the event log monitoring system is a crucial part of Active Directory design. This mechanism helps channel an administrator's attention instantly toward any undesired happenings to help ensure that Active Directory security is not compromised.

For more information on Active Directory security monitoring and alerts, see: https://docs.microsoft.com/enus/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise.

Remote administration events

Contact Center Enterprise solutions allow remote administration of the server with Windows Remote Desktop. All security events are logged for such administration activities. The centralized logging features in Windows Remote Desktop enable you to log events with Windows Server Event Log or SNMP event monitors.

For more details on how system events are captured in Unified CCE, refer to the auditing chapter in the Security Guide for Cisco Unified ICM/Contact Center Enterprise: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_12_6_1/configuration/guide/ucce_b_security-guide_12_6_1.html

Security Control Framework for complete control

The Cisco SCF mandates system resiliency through a complete control objective. It provides enough parameters for the system to be secure and resilient by default to reduce known security vulnerabilities.

Systems hardening

All systems come with a set of default resources enabled. The objective of systems hardening is to disable the unused resources on a system and enable only what is required for your business needs. Systems hardening applies to operating systems, web servers, application servers, database servers, middleware, firewalls, routers, and the hardware that runs them, regardless of vendor and manufacturer.

For more information, see the chapters on hardening and compliance in the Security Guide for Cisco Unified ICM/Contact Center Enterprise: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_12_6_1/configuration/guide/ucce_b_security-guide_12_6_1.html

Cisco Contact Center Enterprise solutions require hardening procedures. Our systems-hardening procedures and guidelines are based on multiple industry standards for secure systems hardening procedures, such as the Center for Internet Security, NIST Security standards SP-800-123, and others. We mandate systems hardening for all product deployments as part of organizational security policies and practices.

Operating system hardening

OS hardening makes an operating system more secure by removing or disabling unwanted services, applications, and ports that the OS includes by default. Hardening properly sets correct and relevant permissions and privileges on applications, the file system, and network settings. It also deletes unused files and applies the latest patches.

For more information, see the Security Guide for Cisco Unified ICM/Contact Center Enterprise.

Database hardening

Database hardening follows the principle of least privilege. It restricts user access by locking down functions that are not required and can be misused. Database hardening also includes segregation of privileges and access restrictions to different schemas and tables for correct and relevant users only. Applying database hardening principles helps ensure greater security through " role separation privileges" for the systems administrator and database administrators.

For protection of data at rest, MSSQL Transparent Data Encryption (TDE) can be enabled in the (P)CCE AW database.

For more information, see the Security Guide for Cisco Unified ICM/Contact Center Enterprise.

Firewall hardening

A firewall defines the perimeter-level security for your enterprise or your internal infrastructure. Firewalls are one of the first defense mechanisms for a network or host to protect its services and applications.

Following industry-standard firewall hardening principles is critical to your security strategy.

For more information, see the Cisco Firewall Best Practices Guide:

https://www.cisco.com/c/en/us/about/security-center/firewall-best-practices.html#1.

Server hardening

Server or infrastructure hardening applies appropriate security to each network component, including web servers, application servers, and any other applications or services. Server hardening starts with a security survey to model the threats that may affect your product or site. You must identify all aspects of your environment (such as components in the web tier) that could be insecure and remove known weaknesses through configuration changes before deploying the product or service.

For more information, see the Center for Internet Security site: https://www.cisecurity.org/cis-benchmarks/.

Middleware, other software, and hardware hardening

SNMP provides a simple architecture with a wealth of information on the health of network devices. However, SNMP offers very little security, because it relies on a community string to protect data exchanged between two computers. This community string is passed in clear text, which effectively voids many security measures. You must properly secure SNMP to protect the confidentiality, integrity, and availability of both the network data and the network devices.

For more information, see the following sources:

- **Cisco Guide to Harden Cisco IOS Devices:** https://www.cisco.com/c/en/us/support/docs/ip/accesslists/13608-21.html#anc54
- **SNMP Guide for Cisco Unified ICM/Contact Center Enterprise:** https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_12_0_1/Configuration/Guide/ucce_b_snmp-guide-for-cisco-unified.html

Active Directory hardening requires a complete investigation into who has elevated privileges throughout the Microsoft Windows environment. You can then reconfigure these settings to ensure that all users have appropriate access. This is a multistep yet straightforward process that covers local users and groups, Active Directory users, Active Directory groups' user rights, Active Directory delegation, group policy delegation, password management, auditing, and monitoring of Active Directory and service accounts.

For more information, see the following Microsoft TechNet article: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory.

Isolate

The focus of isolation is to add additional controls that limit the scope and minimize the impact of attacks and vulnerabilities on users, services, and systems. By creating logical and physical security zones, you can prevent access between the functional blocks in the infrastructure and limit the scope of security breach exploitation.

Systems and architecture isolation

Cisco Contact Center Enterprise solutions follow the defense-in-depth approach (Figure 12). This approach helps ensure that all major functional components are segmented functionally and that firewalls are segmented for tiered, functional security management.

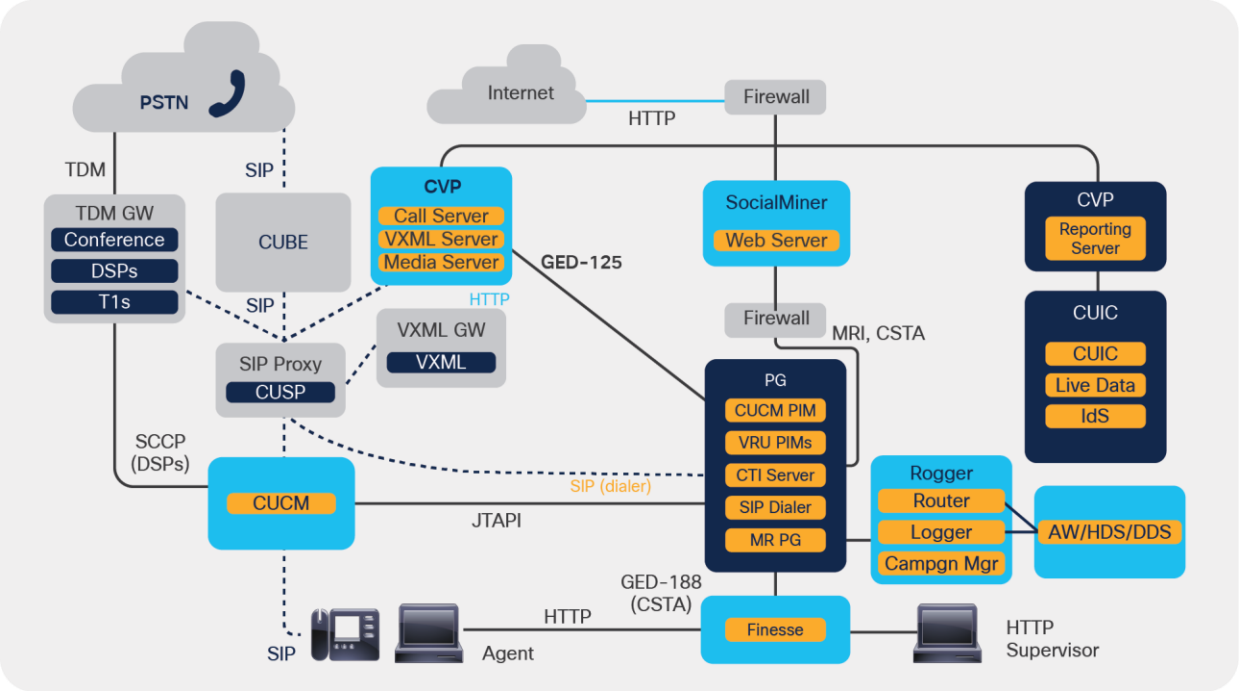

Figure 12.
Contact center defense-in-depth approach

User segmentation

Cisco Contact Center Enterprise solutions separate users into administrators, supervisors, and agents. Each user's role has specific tasks allocated. Agents and administrators are separated through their sign-in capabilities and location restrictions (if applied) and other functional restrictions to agents. Supervisors and administrators can sign in from any terminal or application to monitor and manage the systems.

Application isolation

Cisco Contact Center Enterprise solutions isolate applications based on their functional role. Applications are secured with firewall segmentation and enabled so that only relevant components can connect to them.

The system administrators use Network Address Translation (NAT)-enabled sign-in credentials to manage these individual components remotely with SSH terminals or secure remote desktop-sharing protocols on Windows. Such isolation reduces the risk of an attack being spread further to other system functions.

Read more on systems isolation and segmentation through tiered architecture in the Security Guide for Cisco Unified ICM/Contact Center Enterprise.

Enforce

SCF's main focus is on enhancing visibility and control. The success of the security policies ultimately depends on the degree to which they enhance visibility and control. Smart enterprises take a measured approach to policy enforcement, using a combination of policy awareness, discreet monitoring, and enforcement, which includes:

- Identifying and communicating risk – What's the problem?
- Creating an accepted policy and guidance infrastructure – What do we expect accountable parties to do?
- Developing processes to monitor conformance with policy – How do we know that we are successful?
- Preparing response capabilities for when the controls fail – If there is a breach, who does what to mitigate it?

Effective governance must be directly connected to the consequences of inaction. Policies set expectations and assign accountability. They comply with legal, regulatory, and technical security requirements, spelling out what is and isn't permitted. They define how management governs. They provide direction to security strategy and architecture. But how do you achieve policy compliance?

Cisco's internal security policies and procedures, such as Cisco Secure Development Lifecycle, are enforced on Contact Center Enterprise solutions by default, from their development to their deployment and operations. The next sections discuss policies and procedures that provide enhanced security with optimum product functionality and flexibility.

Processes and technology enforcement

Cisco's Security and Trust Engineering group advocates and accelerates trustworthy processes, policies, and technology across Cisco's products and solutions through:

- Cisco Secure Development Lifecycle (SDL)
- Cisco security engagement managers
- Cisco Security Advocate Program
- Cisco Advanced Security Initiatives Group (ASIG)

These processes, groups, and specialists evaluate Cisco products and services to identify security vulnerabilities and weaknesses. Together, they produce mitigation and improvement plans and perform security analysis on Cisco products and services on a continuous basis. They also define secure development requirements and tools to support Cisco SDL.

Figure 13 illustrates Cisco's security processes, technology, and policies.

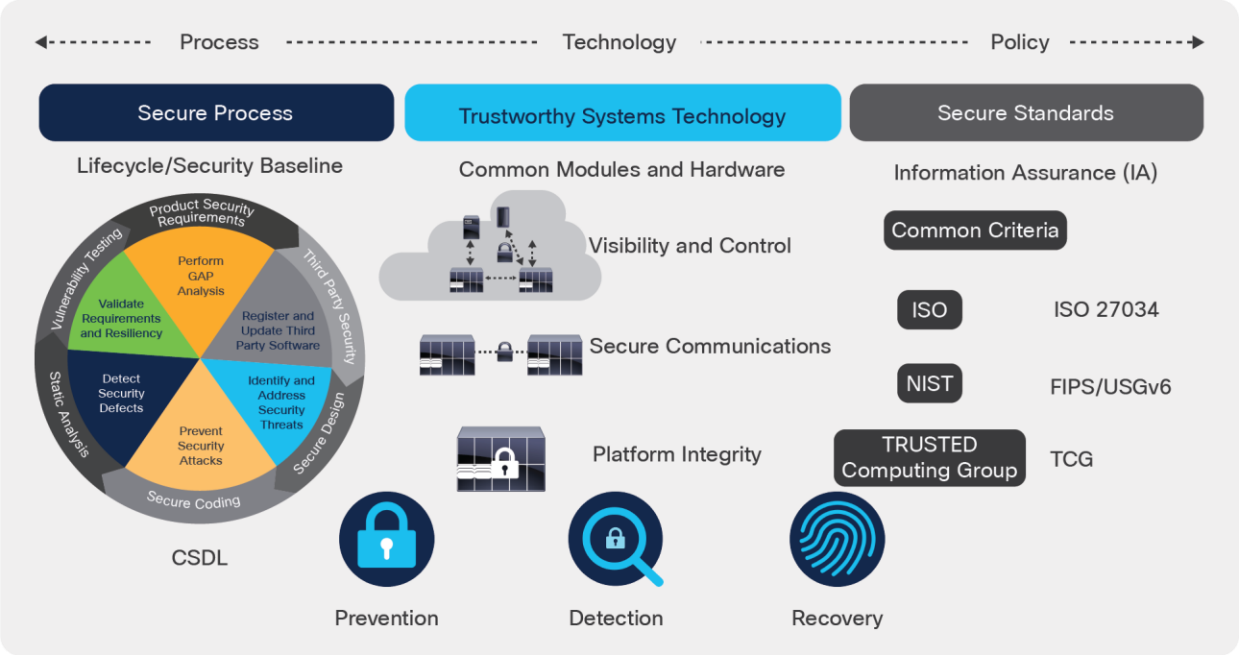

Figure 13.
Security processes, technology, and policies

Cisco Secure Development Lifecycle

Cisco SDL (Figure 14) helps ensure consistent product security through proven techniques and technologies, reducing the number and severity of vulnerabilities in software. SDL conforms to the guidelines of ISO 27034, which is the standard for "Information Technology – Security Techniques – Application Security." Enforcement and mandatory following of SDL is part of Cisco's ISO compliance process, and since 2013, Cisco has used ISO/IEC 27034-1 as a baseline to evaluate SDL. All current, mandatory, application security-related policies, standards, and procedures, along with their supporting people, processes, and tools, meet or exceed guidance in ISO/IEC 270341 as published in 2011.

For more information, see Cisco's SDL processes: https://www.cisco.com/c/en/us/about/security-center/security-programs/securedevelopment-lifecycle.html.

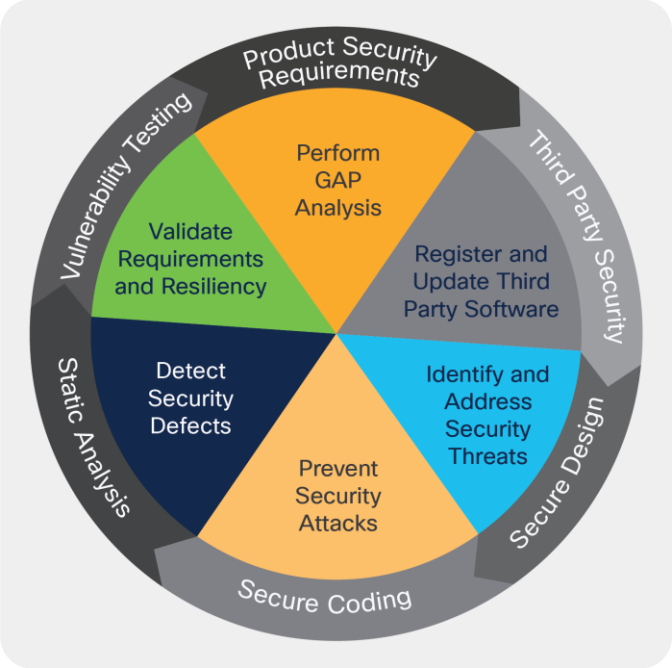

Figure 14.
Cisco Secure Development Lifecycle

Security policies, procedures for deployment, and operations

Cisco's internal security policies are stringent enough to ensure that release staging environments and First Customer-Shipment (FCS) sandbox environments are hardened so that they are identical to production / live deployment security standards and procedures.

Auto-hardening and hardened images

Cisco relies on and enforces auto-hardening scripts along with hardened images of our software stack, such as web servers, application servers, database servers, middleware software, operating systems, and so on. This helps speed up deployment and avoids human error in hardening systems.

Security entry criteria

Internal deployments for release testing and FCS testing must be cleared by all security scanning tools deployed within the development cycle (Figure 15).

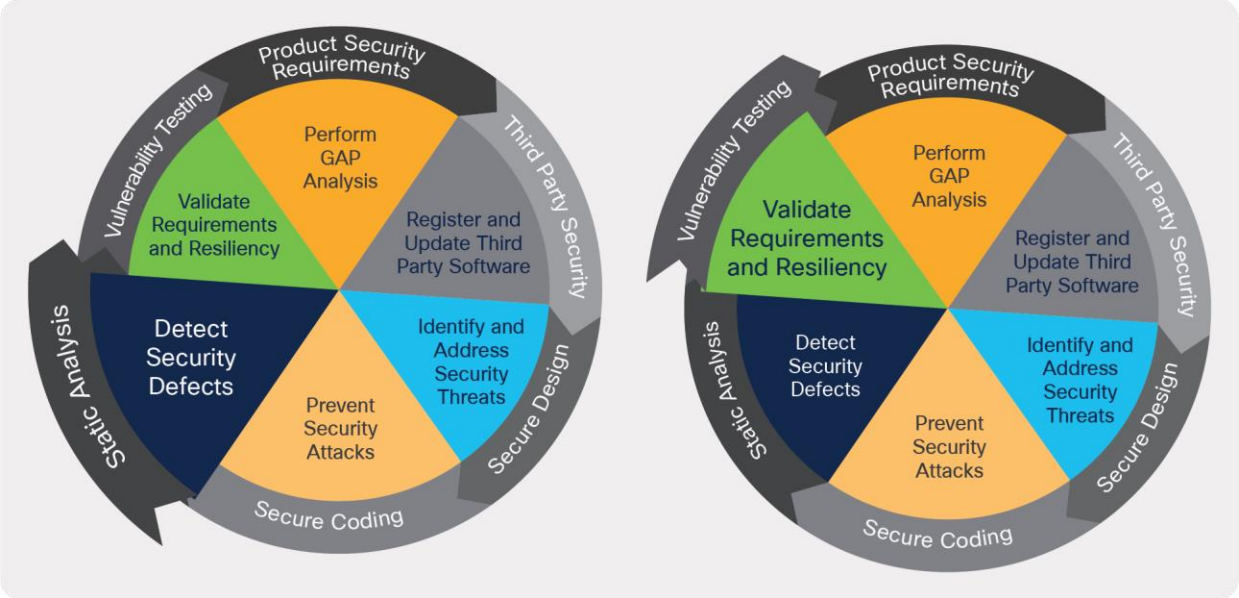

Figure 15.
SDL security testing

CSDL Security Testing		
Network Device Testing		**Application Testing**
Codenomicon Protocol Robustness	**Open Source "Hacker" Tools**	**IBM Rational AppScan**
Test Suites for 50+ Protocols, including DNS, H.323, IKEv2, IPv4, IPv6, HTTP, SIP, SNMP, SSH, TLS and many more	20+ Open Source security tools, including: Amap, Curl, Dsniff, Hydra, Naptha, Nessus, Nikto, Nmap, Xprobe and many more	Family of application attack and test tools, including: risk analysis, security standard compliance testing, vulnerability scan and many more

Deployment and operations security

The Cisco Product Security Incident Response Team (PSIRT) is a dedicated global team that manages receipt, investigation, and public reporting of security vulnerability information for Cisco products and networks (Figure 16).

Figure 16.
Cisco Product Security Incident Response Team

Cisco PSIRT works 24 hours a day, 7 days a week with Cisco customers, Cisco engineering and support, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues with Cisco products and networks (Figure 17).

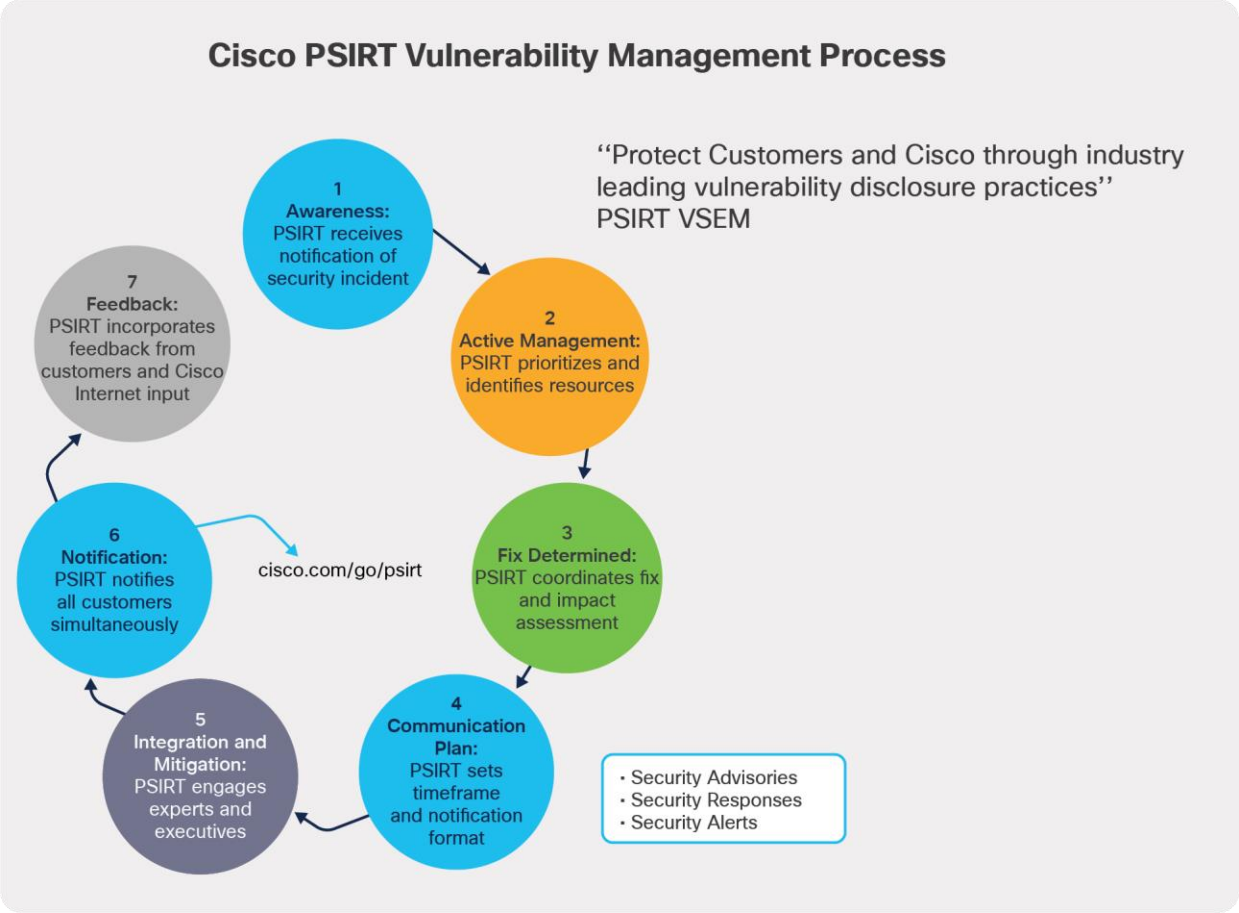

Figure 17.
Cisco PSIRT vulnerability management process

PSIRT announcements are available on Cisco Security Advisories & Alerts at: https://tools.cisco.com/security/center/publicationListing.x.

Compliance, data security, and privacy

Our internal security processes mandate that security compliance is part of our product and services design. Cisco Contact Center Enterprise solutions follow these processes.

Our internal security and compliance processes are rigorous. Since our offerings contain third-party software components, the Contact Center Enterprise solutions iterate through technical, legal, and supply-chain security verification processes to help ensure that security is not compromised. These processes are integral to our product development lifecycle and act as entry criteria for release.

However, our built-in security covers only part of a comprehensive security strategy. You must add your own procedures to ensure compliance with the applicable security, business, and local security requirements while designing your solution's security strategy.

Security standards, practices, and compliance

We define product security requirements for our products as release criteria. We compile these requirements from internal and external sources, based on known risks, customer expectations, and industry practices. Each industry and region has its own unique requirements.

We strive to build products that aid you in complying with these security and privacy requirements. We prioritize those requirements that are common across multiple regions and organizations. Our security requirements for Cisco Contact Center Enterprise solutions reflect the requirements of the standards for the applicable industries:

- The General Data Protection Regulation (EU Regulation 2016/679) PII Data Protection (European Union Personally Identifiable Information)
- The United States Sarbanes-Oxley Act
- The United States Health Insurance Portability and Accountability Act (HIPPA)
- ISO27001
- Common Criteria for Information Technology Security Evaluation
- United States government certifications and standards, including:
  - Federal Information Processing Standards (FIPS)
  - National Institute of Standards and Technology (NIST) SP 800 Series
  - Federal Information Security Management Act (FISMA)
  - Federal Risk and Authorization Management Program (FEDRAMP)
- Other market-demand-based security and compliance requirements, including:
  - SysAdmin, Audit, Network, Security (SANS) Top 20
  - Open Web Application Security Project (OWASP) Top 10
  - Payment Card Industry Data Security Standard (PCI DSS)

Because standards and requirements often overlap, we produce common compliance sheets to help you verify that our products meet your requirements. For an example of these compliance sheets, see the Simplified Crosswalk—HIPAA, PCI, and SOX:

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Compliance/HIPAA/default/HIP_AppD.html.

Data security and privacy

Data security and privacy are of the utmost priority in your contact center (Figure 18). Cisco Contact Center Enterprise products enforce data classification standards and policies to secure the identified sensitive data, including Personally Identifiable Information (PII) within your contact center solution.

Most organizations simply choose not to store PII or credit card data on any local system unless absolutely necessary. For the Unified CCE solution, the measures taken specifically use Extended Call Context (ECC) variables for PII data within the call script applications. These variables are not written to the historical database or otherwise stored.

If audio recording is part of your customer care policy, do not record credit card information. Many organizations choose to have the agent pause the recording when credit card information is spoken. Others take a more automated approach by using desktop analytics or integration with third-party applications that provide automatic pause and resume functionality. If the path to the data source traverses "open, public networks," such as the internet, ensure that you encrypt the data while in transit.

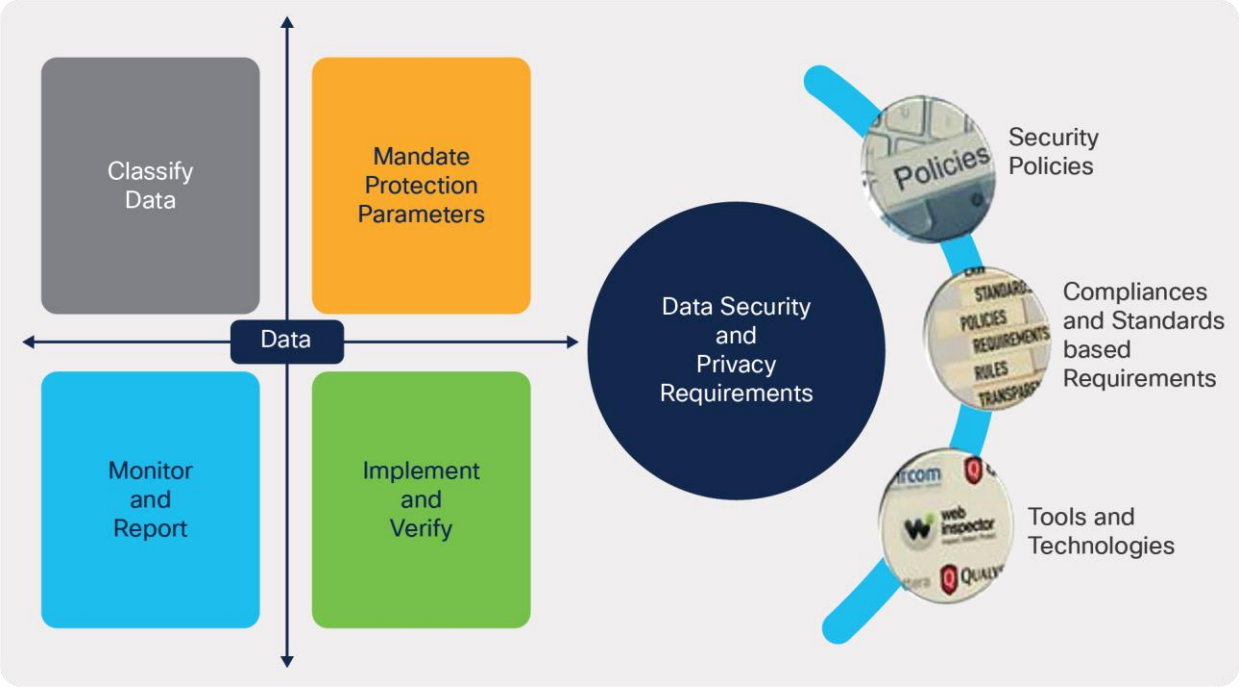

Figure 18.
Data security and privacy

Definition of sensitive data

Cisco Contact Center Enterprise products use Cisco's internal definition of sensitive personal information. That definition is based on research into multiple security requirements and compliances.

Securing PII data

Contact Center Enterprise products internally use secure channels to communicate sensitive information such as user IDs, passwords, session information, and PII. They also support masking of such data in logs. When connecting to any third-party application services, connecting over secure protocols for data communications is mandatory.

PII includes:

- Contact information (name, email, phone, address)
- Forms of identification, including government-issued documents (social security number, driver's license, passport, fingerprints)
- Demographic information (age, gender)
- Occupational information (job title, company name, industry, employee email / phone, pager)
- Healthcare information (plans, providers, history, insurance, genetic information)
- Financial information (bank, credit, and debit card account numbers, purchase history, credit records)
- Online activity (IP address, cookies, flash cookies, sign-in credentials)
- Data that permits access to a customer's account (password, PIN)
- Telecommunications and traffic data (call detail records, internet traffic, invoicing, call logs)
- Customer's real-time location
- Data that could be used to discriminate (such as, race, ethnic origin, religion or philosophical beliefs, political opinions, trade union memberships, sexual lifestyle, physical or mental health)
- Data that could be used to facilitate identity theft (such as mother's maiden name)

For further information on this, please refer the Contact Center Enterprise Solution privacy data sheet: https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-privacy-data-sheet-contact-center-enterprise.pdf

For privacy and security related information on third parties, please refer their respective documentation.

Here is some relevant security, privacy and compliance documentation from Google:
https://cloud.google.com/terms

https://cloud.google.com/terms/cloud-privacy-notice

https://cloud.google.com/security/compliance/

https://cloud.google.com/security/compliance/pci-dss

Transport security

Cisco Contact Center Enterprise solutions use the following methods to protect data during transport.

HTTPS with TLS v1.2

Cisco Contact Center Enterprise solutions use TLS v1.2 protocol at the application layer for all internal and external communications. This includes SNMP to transport sensitive PII data. The solutions deploy FIPS-140-2 and NIST approved cryptographic algorithms.

Mandatory TLS parameters

Cisco Contact Center Enterprise solutions mandate a cipher order parameter by the server, SSLHonorCipherOrder On.

The highest priority is given to ciphers that support “forward secrecy” (that is, ephemeral Diffie-Hellman key exchange).

Cisco Contact Center Enterprise solutions favor Galois/Counter Mode (GCM)-Block Cipher Mode rather than Cipher Block Chaining (CBC)-Block Cipher Mode or other cipher modes. If GCM is not available, a minimum fallback to Counter (CTR) modes is allowed, regardless of the cipher size. In other words, Cisco Contact Center Enterprise solutions use Authenticated Encryption with Associated Data (AEAD), such as Advanced Encryption Standard (AES)-GCM and AES-CCM.

Strong cipher suites

Cisco Contact Center Enterprise solutions use TLS 1.2 and strong cipher suites by default, which are configurable for each service and interface. By default, these solutions disable weak ciphers as part of secure deployment practices and server-hardening practices. For further details, refer to the product documentation.

IPsec

Wherever required, Cisco Contact Center Enterprise solutions use IPsec at Layer 3 for performance reasons, as explained in the Security Guide for Cisco Unified ICM/Contact Center Enterprise: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_12_6_1/configuration/guide/ucce_b_security-guide_12_6_1.html.

Secure Real-Time Transport Protocol (SRTP)

Cisco Contact Center Enterprise use SRTP to secure VoIP packets and provide encryption, message authentication, and replay protection regardless of whether the network circuits are encrypted.

Persistence security

Your contact center might receive sensitive user data from voice and Voice Response Unit (VRU) calls or from Customer Relationship Management (CRM) portals for outbound campaigns. The contact center temporarily stores that data in ECC variables or persistent call variables. Your contact center also fetches sensitive data through call flow scripts that call relevant user data from the customer’s database temporarily. (In upcoming releases, these will be encrypted and stored with proper cryptographic key management based on the NIST.SP.800-130 standard using Cisco OpenSSL and Cisco Crypto-Common Modules.)

Mandatory data encryption parameters and settings

Your contact center solution deploys NIST-recommended cryptographic algorithms to encrypt sensitive data. It deploys AES 256-bit encryption to encrypt PII data.

Encrypted disk drives

To protect data at rest, use hardware-encrypted disk drives.

Feedback

To provide comments about this document, send an email message to the following address: contactcenterproducts_docfeedback@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**.

Printed in USA C11-740413-01 08/21