Your Security Strategy and Unified CCE

Security Evolves Constantly

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

This chapter discusses how the security architecture of the contact center enterprise products and the Cisco security process supports your security strategy. It also discusses the Collaboration Security Control Framework (SCF) which encapsulates our vision of a security strategy.

How We Support Your Security Strategy

We support your security strategy with synergies between security processes, technologies and tools, and security policies for compliance in your contact center enterprise solution. These directly derive from:

- Cisco’s Product Security Requirements
- Market-based Security and Compliance Requirements
- Mandatory Regulations, Security, and Compliance Requirements
- Collaboration Security Control Framework

Your security adherence should incorporate the goals of the Collaboration Security Control Framework (SCF). The Cisco Secure Development Lifecycle (CSDL) processes aligns our development efforts with the SCF.

Related Topics

Our Secure Development Processes, on page 16

Collaboration Security Control Framework

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

The SCF defines security actions that help enforce the security policies and improve visibility and control. The SCF revolves around two security ideals, each with three supporting pillars:

- Total Visibility
  - Identify
  - Monitor
  - Correlate
- Complete Control
  - Harden
  - Isolate
  - Enforce

The SCF requires a foundation of architectural resiliency in the contact center enterprise solutions.

Security Architecture Principles

Cisco's Secure Development Lifecycle aligns with and, in some areas, leads the industry in creating highly secure solution architectures. Our Secure Coding Standards design the CSDL principles into every Unified CCE release. These standards work 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 the following:

- Trust, but verify
- Securing weak entities and significant entities
- Mandatory 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 eco system (Ops, Release, and Security)
- Protection of PII data and any sensitive data, both at-rest and in-transmission
- Log all failures and all CRUD (Create, Read, Update, and Delete) actions and protect the logs

Unified CCE Solution Security Architecture

Our security architecture comprises multiple, layered security options and controls. You can deploy these security features to meet your individual security requirements. You can combine these features to achieve a robust security posture against attacks.

The contact center enterprise solutions include some servers that run on a Windows 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 Unified CCE servers leverage the Windows Firewall, Windows NT LAN Manager version 2 (NTLMv2), Windows Hardening Policies, and Active Directory. These servers include:

- The Router and Logger
- The Peripheral Gateway
- The Administration & Data Server
- Cisco Voice Portal
- Unified Contact Center Management Portal

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

- Cisco Finesse
- Cisco Unified Intelligence Center
- Virtual Voice Browser
- Unified Communications Manager
- Cisco Unity Connection
- Cisco Identity Service
- Live Data
- Customer Collaboration Platform

This figure shows the core elements of a Unified CCE instance:

Application endpoints, like desktops and phones, involve Computer Telephony Interface (CTI), JTAPI, and any TAPI applications. These endpoints are secured by leveraging TLS and SRTP. The solution also uses a Certificate Trust List (CTL) which you create that establishes signaling authentication between Client and Server.

Network Security Architecture

The contact center enterprise solution offers a flexible network security model. There are many areas on the network where, based on your unique needs and compliance requirements, you can apply security to the solution. These include Firewalls, Access Control Lists (ACLs), private network addressing, Network Address Translation (NAT), setting up a DMZ, SRTP, and Internet Protocol Security (IPsec).

You can secure in-flight data by deploying IPsec. IPsec is an Internet layer 3 framework of open standards that are designed to ensure private, secure communications over Internet Protocol (IP) networks. The use of cryptographic security services and policies provides security. 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 your contact center enterprise solution. LAN or WAN network endpoints support either transport mode or tunnel mode deployments. Contact Center nodes (such as Peripheral Gateways, Routers, and Loggers) support only transport mode IPsec.

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 do not terminate within the core contact center enterprise solution. Adjunct devices, such as Unified CM and voice gateways, supply the media termination within the solution.

Secure Real-Time Transport Protocol (SRTP) is the method that secures the voice and video traffic.

Unified CCE web servers use Microsoft Internet Information Services (IIS) for web server responses and Apache Tomcat for the client authentication. Communication between Web servers and web-based users is trusted and encrypted using HTTPS and Transport Layer Security (TLS) protocols.

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 sit behind a firewall or DMZ. The only exceptions are Microsoft Active Directory Domain Controllers, Customer Collaboration Platform servers, and the Email and Chat web servers which reside inside a DMZ.

This guide focuses primarily on the premises-based deployment of our solutions. Cisco also offers cloud-based contact center applications, such as the Customer Journey Platform. We are thorough in ensuring compliance with international standards requirements for cloud data handling. Cisco has completed Binding Corporate Rules with the EU, the EU-US Privacy Shield, and the APEC agreements for cloud data handling and cross-border transfers. The Cisco Trust Center website provides details of these protections: https://www.cisco.com/c/en/us/about/trust-center.html.

The Goal of Total Visibility

The SCF model defines a structure of security objectives and supporting security actions to organize security controls. The SCF model is based on proven industry practices and security architecture principles. The model

grows from the accumulated practical experience of Cisco engineers in designing, implementing, assessing, and managing service provider, enterprise, and small and medium-sized business (SMB) infrastructures.

Using the SCF model, you gain an insight into the system's activities through total visibility objectives. The SCF mandates that the system knows the following:

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

Key considerations for the goal of total visibility include the following:

- 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 Everything in the System

Contact center enterprise solutions leverage two common methods for user authentication and authorization. Unified CCE leverages NTLMv2 for Server-to-Server authentication. Administrative user accounts use Active Directory (AD) for authentication and authorization to perform tasks that are 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 SAMLv2 assertions for authentication. In an SSO deployment, the application's configuration database does not store user passwords. After authentication succeeds, Unified CCE supplies OAuth tokens through the Identity Service (IdS) for authorization to protected resources with its Identity Service (IdS).

Identify Your Users

Contact center enterprise solutions recognize these classes of users:

- Administrators
- Agents and supervisors
- API users

Contact center enterprise recognizes 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 only require local Administrative privileges in AD. Such tasks include 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 are also authenticated calls through HTTPS. You define authorized API users during the initial system deployment.

Identify Your 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 a lightweight audit through the change control history.

The Unified CCE Administration and Data Server contains a copy of the Unified CCE configuration schema in a 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 by using Unified CCE's Feature Control Set.

To support Single Sign-On (SSO) for agents and supervisors, the solution deploys Cisco Identity Service (IdS), a VOS-based appliance. The Cisco IdS has a trust relationship with 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 agent and supervisor authentication data reside in your IdP and not in the Unified CCE database.

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 the 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 that AD stores reside in the local Security Accounts Manager (SAM) database and are part of the Unicode Pwdattribute hash value. Windows generates this hash value as a product of the LAN Manager and Windows NT hash. Unified CCE accounts that you create for use with Web Setup and Web Administrator authenticate with an AD user account.

Identify Your 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 AD staging. You create a root OU (Organizational Unit) in the target AD domain where the Unified CCE servers reside. You can 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. Provide Domain Administrator rights or delegated (full control) rights to a sub-OU where our root OU is nested. Once the Domain Manager creates the root OU, you no longer require Domain Administrator rights for the rest of the installation.

After installing the core software, you run WebSetup to create the AD Service accounts required for the 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 DB services to pre-configured 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

The Cisco Unified Contact Center Security Wizard is a standalone server hardening deployment tool that simplifies your security configuration. You can do the following tasks in the Security Wizard:

- 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 IIS.

We qualify each software release to operate with specific versions of third-party anti-virus software. Ensure that your solution uses a qualified anti-virus software.

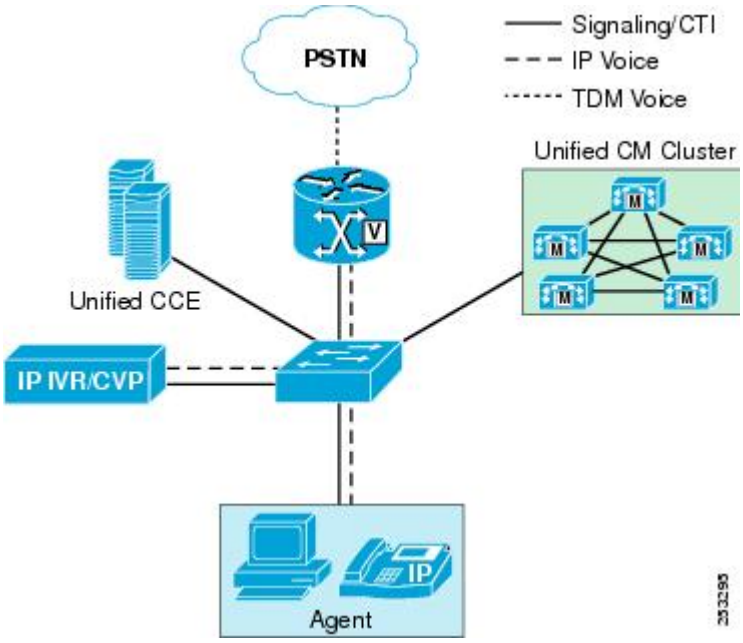
Monitor Everything in the System

Monitoring plays a vital role in effectively managing the operations which must cover all the critical components of the product architecture. Monitoring helps in detecting any security issues for analysis and mitigation as soon as possible based on their severity.

Security issues can come from network attacks, network breakages, application security attacks, and transaction failures which can result in a Denial of Services.

Monitor Your Network

You can monitor your contact center enterprise solution with the Unified Communications Manager Real-Time Monitoring Tool (RTMT). RTMT collects diagnostic information and also gathers platform and application configuration data. RTMT provides an administrative interface for collecting health and status information and requests for all devices in its network topology. By configuring RTMT, you can then use other security tools to analyze its data for security issues, like network-based attacks (Slow-TCP attacks, "Slowloris," or packet bombardment such as "ping of death"). This figure shows the solution components that RTMT monitors for their network interactions.



Contact center enterprise solutions capture specific network events. They report abnormalities in network requests. Each component checks for the heartbeat of the other components with which it interfaces. Our solutions can track these network events:

- Host not reachable
- TCP Timeouts
- Excessive Response Delays

Your contact center enterprise solution has built-in capabilities to aid reporting on network abnormalities and to integrate with third-party security intelligence tools:

- 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, device 360
- Event alert generation in the form of email messages, for user-configured thresholds
- Trace collection and viewing 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 its own security intelligence tools:

Cisco AMP

https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html

Cisco AMP (Advanced Malware Protection) provides global threat intelligence, advanced sandboxing, and real-time malware blocking to prevent breaches. But, you can’t rely on prevention alone. AMP also

continuously analyzes the file activity across your extended network, so you can quickly detect, contain, and remove advanced malware.

Cisco Stealthwatch

https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html

Cisco Stealthwatch 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 the telemetry from your network infrastructure. This capability helps protect your critical data with smarter network segmentation.

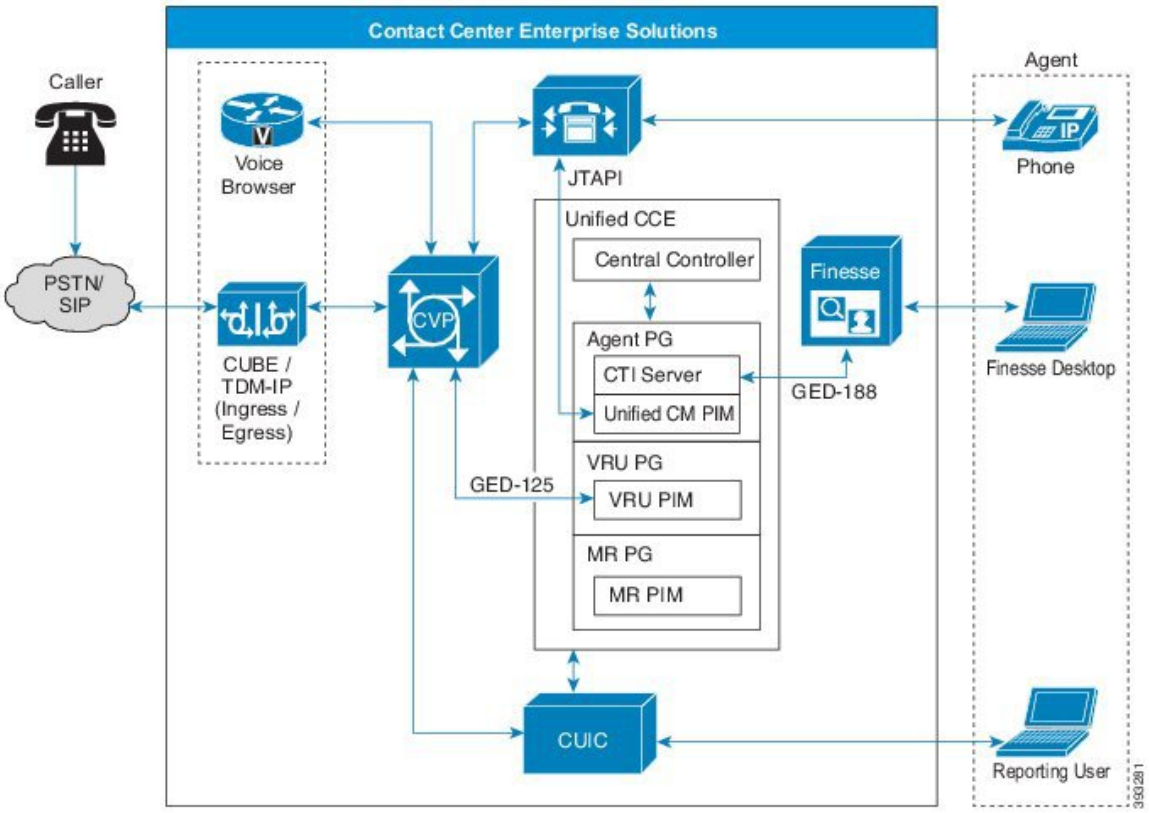
Cisco Prime Assurance

https://www.cisco.com/c/en/us/products/cloud-systems-management/prime-collaboration/index.html

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

Monitor Your Data

The components in contact center enterprise solutions communicate with other components as part of their business transaction orchestration. The components monitor major data transmission for the segments that this figure shows.



Incoming Calls

Unified CCE receives calls in two primary ways. Inbound calls can come through a PSTN or an IP-based SIP trunk that uses VoIP technology to stream media services to a telephony endpoint. In both cases, the physical media traverses between the ingress carrier, voice gateways, and Unified CM 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.

The contact center enterprise solution includes security features that are designed to actively detect and prevent inbound call attacks that are 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:

- Unified Communications Manager class of service (CoS)
- Voice gateway toll fraud prevention applications
- Voice gateway class of restriction (CoR)
- Cisco Unity Connection restriction rules

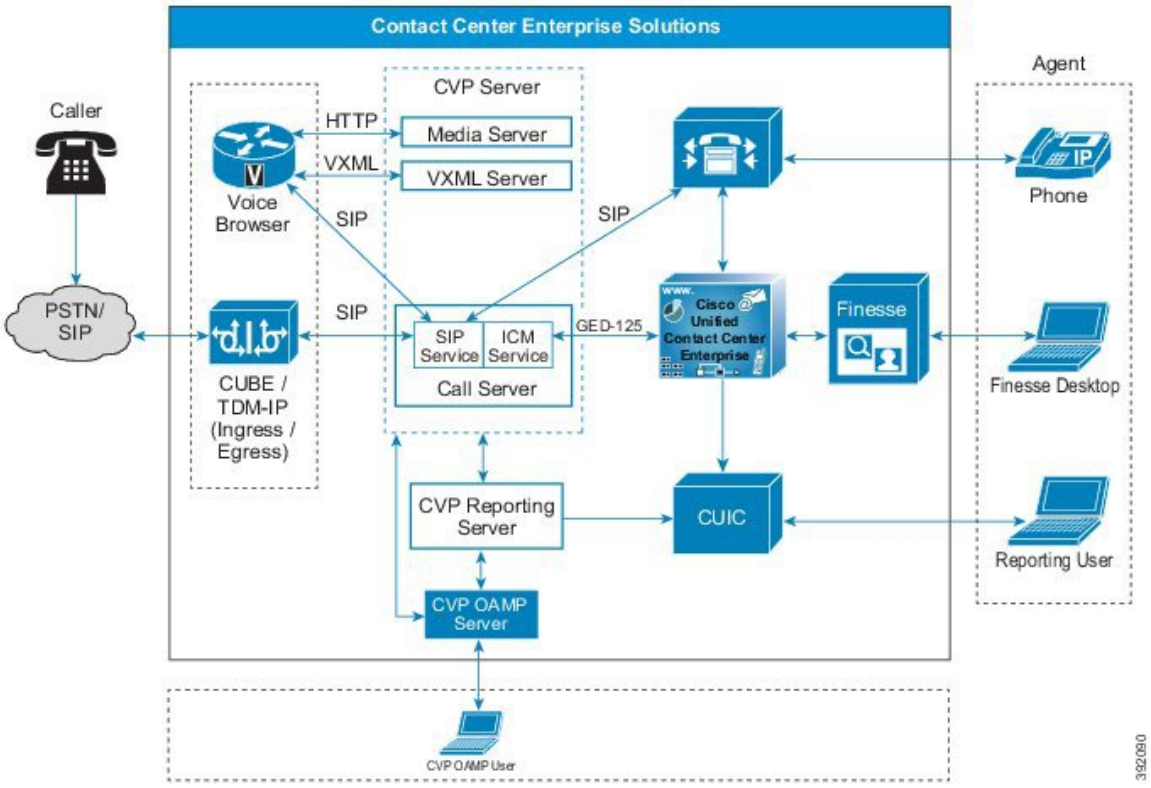
TDoS attacks generally follow the same model as a data network Denial of Service (DoS). Unauthorized users flood the system with too many access requests and prevent legitimate users from accessing the system. Unified CCE comes equipped with a congestion control capability. You can use Congestion Control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

Business Transactions

These are some of the business transactions for which our solution captures data and monitors for diagnostic data and any failure:

- **Routing control**—Messages that enable a Unified CM 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 Unified CM cluster to receive instructions from Unified CCE

Figure 1: Unified CCE Business Transactions (Call Flows between Components)



Record What You Monitor

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 SNMP and Syslog protocols.

Security auditing requires a more tightly integrated method that blends reactive logging with proactive tools and analysis to prevent possible system health-impacting issues from occurring. Our solutions have built-in auditing features capable of the following:

- 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 support that enables the tracking of administrative changes by leveraging the t_Event and the Recovery tables
- RTMT for automated alerting

Syslog and the central repository service log business transactions and other data transmissions. Unified Intelligence Center provides reporting and analysis capabilities for auditing.

RTMT sends alerts for any configured violations (incidents) as an email message. 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
- Real-time performance monitoring of contact center devices
- Events and Alarms along with a root cause analysis
- Contact Center device dashboards—Prebuilt and custom
- Threshold, Syslog, Correlation, and System Rules—Prebuilt and custom
- Multi-tenancy and logged-in agent licensing information

Correlate Everything in the System

Applying context and meaning to information security requires the correlation of recorded events, incidents, and failures from the application logging and auditing. Correlation adds critical information value by evaluating the relationships between various information silos. Unified CCE can correlate real-time and historical events within the solution to increase the value of your security information.

The correlation of events, incidents, and failures helps to identify, understand, and troubleshoot system failures and issues. The correlation is more effective than finding individual root causes in an isolated manner.

Make Use of Alerts and Notifications

Alerts, notifications, and alarms are a system capability that notifies system administrators of an event. The system can take corrective or preventive actions based on these alerts to ensure smooth business operations. The solution enables you to track significant events, such as, account sign-in attempts.

Some of the alert capabilities available in contact center enterprise solutions are:

- The SNMP Event Translator facility converts Windows events, in real time, into an SNMP trap.
- Microsoft SQL server includes events capturing and reporting through its new audit capabilities. See Microsoft documentation for details.

Note Cisco does not support C2 event capturing for audits in Microsoft SQL Server in contact center enterprise solutions due to degradation in transaction performance.

- The alerting mechanism of the event log monitoring system is a crucial part of AD design. This mechanism helps channel an administrator's attention toward any undesirable incidents to ensure AD security is not compromised.

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

- Contact center enterprise solutions allow remote administration of the Unified CCE server with Windows Remote Desktop. The solution logs all security events for such administration activities. The centralized logging features in Windows Remote Desktop enable you to log events with Windows Server Event Log or an SNMP event monitor.

  For more details on how Unified CCE solutions capture system events, refer to the auditing chapter in this guide.

Related Topics

Auditing

Correlate Events with Security Incidents

Any business event can become an incident. Your business must also classify some system events as an incident by default. Address corrective and preventive actions for those events in your Operations Run Book or Standard Operational Procedures. Contact center enterprise defines the following business events as incidents which require administrative notifications and corrective actions.

- Host not reachable
- TCP Timeouts
- Excessive Response Delays
- Unknown Link status
- Unknown device status
- Device & call control & monitoring message failures
- Routing control message failures

Our solutions provide alert and notification capabilities for these incidents. They send information of such critical failures to administrators for predefined corrective actions.

For more details, refer to the chapter on auditing in this guide.

Related Topics

Auditing

The Goal of Complete Control

The Collaboration Security Control Framework mandates system resiliency through its complete control objective. The SCF provides enough parameters to make the system secure and resilient by default, reducing known security vulnerabilities.

Harden What You Can

Hardening is the process of closing off avenues for potential attacks by changing default settings in hardware and software.

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 only enable what your business needs require. System hardening applies for operating systems, webservers, application servers, database servers, middleware, firewalls, routers, and the hardware that runs them – irrespective of vendors and manufacturers.

For more information, see the sections on hardening and compliance in this guide.

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

OS 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 the correct and relevant permissions and privileges on applications, the file system, and network settings. It also deletes unused files and applies the latest patches.

Database Hardening

Database hardening follows the principle of least privilege. It restricts user access by locking down functions that your users do not require and might misuse. Database hardening also includes segregation of privileges and access restrictions to different schemas and tables for the correct and relevant users only. Applying database hardening principles ensures greater security through "Role Separation Privileges" for the Systems Administrator and Database Administrators.

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 for a 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* at https://www.cisco.com/c/en/us/about/security-center/firewall-best-practices.html.

Server Hardening

Server or infrastructure hardening applies the 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 impact your product or site. Identify all aspects of your environment (such as components in the Web tier) that could be insecure. Before deploying the product or service, remove any known weaknesses through configuration changes.

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 little security, because it relies on a community string to protect data exchanged between two computers. This community string is in clear text, which effectively voids many security measures. 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:

- The section on fortifying SNMP in *Cisco Guide to Harden Cisco IOS Devices* at https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html#anc54
- *SNMP Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html

AD hardening requires a complete investigation of who has elevated privileges throughout a Microsoft Windows environment. You can then reconfigure these settings to ensure that all users have the appropriate access. This is a multistep, yet straightforward process which covers the following:

- Local users and groups
- AD Users
- AD groups User Rights
- AD Delegation
- Group Policy Delegation
- Password management
- Auditing and monitoring of AD
- Service Accounts

For more information, see the Microsoft TechNet article on securing AD at https://docs.microsoft.com/en-us/previous-versions/technet-magazine/cc160982(v=msdn.10).

Related Topics

SQL Server Hardening
Windows Security Hardening

Isolate What You Can

The focus of isolation is to add extra controls that limit the scope of attacks and vulnerabilities. Isolation minimizes their impact on users, services, and systems. By creating logical and physical security zones, you can prevent access between the functional blocks in the infrastructure. This method limits the scope of a security breech exploitation.

Systems and Architecture Isolation

Contact center enterprise solutions follow a defense-in-depth approach. This approach functionally segments all major components and segments the firewalls for a tiered, functional security management.

User Segmentation

Contact center enterprise classifies its users as administrators, supervisors, and agents. Each role has specific allocated tasks. Agents and administrators are separated through their sign-in capabilities, any applied location restrictions, 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

Contact center enterprise isolates applications based on their functional role. Firewall segmentation secures the applications and enables the applications so that only relevant components can connect to them.

The system administrators use NAT-enabled sign-in credentials to manage these individual components remotely with SSH terminals or secure remote screen sharing protocols on Windows. Such isolation minimizes the risk of an attack spawning further to other system functions.

Enforce What You Can

The SCF's main focus is on enhancing visibility and control. The success of your security policies ultimately depends on the degree that 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 the conformance with a 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 is 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 they do and don't permit. The policies define how management governs and provide direction to their security strategy and architecture.

Cisco enforces its internal security policies and procedures, such as CSDL, on the contact center enterprise products by default from its development to its deployment and operations.

Our Secure Development Processes

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

- Cisco Secure Development Lifecycle (CSDL)
- 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 continuous improvement cycles. They also define secure development requirements and tools to support CSDL.

CSDL ensures a consistent product security through proven techniques and technologies, reducing the number and severity of vulnerabilities in software. CSDL conforms to guidelines of ISO 27034, "Information Technology – Security Techniques – Application Security". Enforcement and mandatory implementation of

CSDL is part of Cisco's ISO compliance process. Since 2013, Cisco has used ISO/IEC 27034–1 as a baseline to evaluate CSDL. All current mandatory application-security-related policies, standards, and procedures along with their supporting people, processes, and tools meet or exceed the guidance in ISO/IEC 27034–1 as published in 2011.

For more information, see the section on CSDL at https://www.cisco.com/c/en/us/about/trust-center/technology-built-in-security.html.

Cisco's internal security policies ensure that we harden our release staging environments and FCS sandbox environments identically to production deployment security standards and procedures.

Cisco enforces auto-hardening scripts and hardened images of its software stack such as web servers, application servers, database servers, middleware software, and operating systems. This hardening helps speed up deployment and avoids chances of a human error in hardening systems.

Our internal deployments for release testing and FCS testing must clear all the security scanning tools that are deployed within the development cycle.

Our Deployment and Operations Security Processes

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

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.

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

Our Compliance, Data Security, and Privacy Processes

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

Our internal security and compliance processes are rigorous. Since our offerings contain third-party software components, our solution iterates through technical, legal, and supply-chain security verification processes to ensure security is not compromised. These processes are integral to our product development lifecycle and act as an entry criteria for release.

However, our built-in security covers only part of a comprehensive security strategy. 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 a release criterion. 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 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:
  - National Institute of Standards and Technology (NIST) SP 800 Series
  - Federal Information Security Management Act (FISMA)
- Other market-demand-based security and compliance requirements:
  - 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* at 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 is of the utmost priority in your contact center. 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.

Organizations generally choose to not store PII or credit card data on any local system unless necessary. The Unified CCE solution uses Extended Call Context (ECC) variables for PII data within the call script applications. Unified CCE does not write these variables to the historical database or otherwise stored.

If an 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 the credit card information is spoken. Others look to a more automated method using desktop analytics or an integration with third-party applications that provide an automatic pause and resume functionality. If the path to the data source traverses “open, public networks,” like the Internet, ensure that you encrypt the data while in transit.

Security for PII and Other Sensitive Data

Contact center enterprise products use Cisco’s internal definition of sensitive personal information. We base that definition on multiple security requirements.

Contact center enterprise products internally use secure channels to communicate sensitive information such as user-ids, passwords, session information, and PII. When connecting to any third-party application services, connecting over secure protocols for data communications is mandatory.

PII includes the following:

- Contact information (name, email, phone, postal)
- Forms of identification (SSN, Driver's License, Passport, Fingerprints)
- Demographic info (age, gender)
- Occupational Info (Job title, Company name, Industry, Employee email, phone, pager)
- Health care info (Plans, providers, history, insurance, genetic info)
- Financial info (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, Personal Identification Number)
- Telecommunications and traffic data (Call details records, internet traffic, invoicing, call histories)
- Customer's real-time location
- Credit card numbers and bank account information
- Government-issued identifiers such as Social Security Number and Driver's License
- Data that could be used to discriminate (such as, race, ethnic origin, religions 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)