

Cloud Solutions

Avaya Cloud Office Secure Cloud Communications and Collaboration



Table of Contents

- Security Team and Organizational Security1
- Avaya Cloud Office Security.....2
- Independent Verification.....8
- Conclusion.....10
- About Avaya10

Of the many questions companies have when considering a move to the cloud, security often sits at the top of the list. In particular, the sensitive nature of business communication—with employees and with customers—is a critical focus for security teams. After all, each day employees call, message, meet, fax, email, and use other forms of communication to share strategies and secrets that define their competitive advantage.

In today’s world, data security is a high priority for your business. As a UCaaS provider, we understand the security implications of the cloud model. We make security a priority to protect our own operations, and to secure your customer data, as well. Our cloud services are designed to deliver world-class security and as a Avaya Cloud Office customer, you benefit from the best practices built into our policies, architecture, and operational processes, which are designed to satisfy the requirements of our most security-sensitive customers. This white paper provides insight into the security and trust built into our products and services.

Security Team and Organizational Security

Security begins with our culture. Security and customer trust are core business values, and we build these into our services as well as invest in dedicated security.

As part of our organizational structure, we have a dedicated security department, with security engineering, security audit/compliance, application security, security data science, and service abuse functions that report to the company’s Chief Security Officer (CSO).

All employees receive in-depth training on data protection and confidentiality, as well as information security. This type of security training is mandatory and occurs at least annually.

In addition, we have employee background checks, deliver security awareness training to new hires and current employees, and require employees to acknowledge company policies each year, including our robust security policy.

All employees receive in-depth training on data protection and confidentiality, as well as information security. This type of security training is mandatory and occurs at least annually. All employees must acknowledge and sign a data protection and confidentiality agreement. All employees also receive a certificate of completion following training and assessment.

Avaya Cloud Office Security

Our commitment to security has been proven to be second to none. The commitment starts with a global team of cybersecurity experts that participate not just in the planning and development of the platform but also its daily operations.

We implement:

- Secure software development
- Strong access controls
- Resilient services
- Threat detection and mitigation
- Service operations controls
- Customer admin and user controls
- Built-in support for regulatory requirements
- Secure application programming interfaces (APIs)
- Pre-built integrations
- Transparency

The following cloud security model illustrates the approach we take to achieve these security goals:

Governance: Risk Management and Measurements	
User Service Administration	Customer Controlled
Application Security	Designed In and Tested
Border Security	Data Entering the Service Cloud
Data Security	Data Encrypted in Transit and At-Rest
Platform Security	Infrastructure and Operations
Toll Fraud Mitigation	Detect and Stop Service Abuse
Physical Security	Protected Environments
Independent Verification	Third-Party Audits and Security Testing



**Data
encryption
protects
sensitive
customer and
call data from
unauthorized
access.**

Physical Security

Our services are hosted globally in enterprise-class Tier 4 data centers and leading public clouds. Security and availability are top-of-mind considerations when selecting our service delivery locations. These environments include state-of-the-art physical security, environmental controls, and facility operations. Network operations centers (NOCs) are continuously monitored 24/7 and staffed by highly trained, on-site engineering specialists. Entry to each data center location requires biometric identification, as well as dual-person authentication and a built-in system of “man traps.” Security and safety systems are audited monthly for maximum insurance, and each data center is certified SSAE 18 compliant.

Access Management

Access to production environments is tightly controlled with Identity and Access Management (IAM) and multi-factor access controls. These robust access management measures enable only authorized personnel to access our production environments.

Data Encryption

Data encryption protects sensitive customer and call data from unauthorized access. All customer data is encrypted in transit and at rest, using applicable industry-leading encryption, standards, and protocols.

We have a thorough change management process in place. The change-control practices include regular meetings to review and manage changes to our production environment.

We use two enterprise-grade security protocols to provide additional security for IP phone calls—TLS authentication and SRTP encryption:

Transport Layer Security (TLS) is a cryptographic protocol that provides encryption on the Session Initiation Protocol (SIP) signaling data. This protocol secures the SIP signaling communication between supported endpoint devices and the our cloud servers.

Secure Real-Time Transport Protocol (SRTP) is a profile of the Real-Time Transport Protocol (RTP) that provides encryption, message authentication, and integrity, as well as replay protection to the RTP packet stream that is transported between supported endpoint devices and our cloud servers.

In addition, all internet facing portals use secure and encrypted (SSL Certificate / https) protocols; all non-voice customer data is TLS encrypted; and hard phones use digital certificates to establish secure connections to download their provisioning data.

Network Security

We have deployed best-of-breed network protections optimized for voice and data. These protections—together with our experts continuously monitoring systems for anomalies—help to prevent service disruption, data breaches, fraud, and service hijacking.

Vulnerability Management

We have implemented system hardening practices and automated the ongoing vulnerability scanning of production assets. We scans servers, network devices, and other applicable systems to identify unpatched vulnerabilities and issues of noncompliance to established security configurations. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity, and assigned an owner.

Patch Management

Avaya Cloud Office includes patch management as part of its vulnerability management efforts. Patches are prioritized and installed based on internal patching prioritization standards. All patches are tested on non-production systems prior to installation on any production systems.

Change Management

We have a thorough change management process in place. The change-control practices include regular meetings to review and manage changes to our production environment. Prior to deployment into production, change requests are documented and approved by multiple stakeholders. Upon deployment, verification procedures are followed to ensure success. In the event that verification steps fail, we have thorough rollback procedures and policies in place. We implement configuration monitoring, flow monitoring, EDR, and other monitoring measures.



We enforce security and incorporates best practices during our Software Development lifecycle process.

Application Security

We continuously implements best software development practices to ensure security throughout the development, build, deployment, and release phases of any software project, including:

- Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and Runtime Application Security Testing (RAST)
- Application scanning
- Analysis of third-party libraries
- Signed commits
- Software composition analysis
- Application programming interface (API) scanning
- Penetration testing

Secure Software Development

We enforce security and incorporates best practices during our Software Development lifecycle process which includes secure code training to all developers.

As part of the vulnerability management process, OWASP Top 10 vulnerabilities and CWE Top 25 software errors are checked on a regular basis.

Every external developer on the platform is required to have a developer account where they register and set permissions for their applications.

Developer Platform

Any developer of a public-facing application that runs on Avaya Cloud Office is required to use Open Authentication (OAuth), which prevents the transmission of customer credentials to the application and developer server. Upon requesting access to the third-party application, customers are directed to our portal, where they enter their username and password. During this process, customers are informed of the exact permissions the application is requesting, and they may cancel the request at any time.

If a customer accepts the application request for permissions, the application and developer server receives a bearer token that may be used to act on the customer's behalf. This token expires if not refreshed by the application and may be revoked by us or the customer at any time via the Admin Portal.

For private applications that are intended to be used only by the organization that created them, developers may use their username and password to request a bearer token. This process helps obfuscate the customer credentials and prevents multiple use and placement of customer credentials. However, because there is no way to prevent customer credentials from being accessed should the application or server be hacked, this method is not recommended.

Every external developer on the platform is required to have a developer account where they register and set permissions for their none this applications. Each application is assigned a client ID and a client secret credential. This allows each application to be monitored individually and, if need be, updated or terminated should the application's security be compromised or the intent of the application becomes malicious.

Beyond having a unique client ID and secret credentials, developers must set the specific permissions their application will use. If an application requests more permissions than is needed, it will not be able to be used in production until either those permissions are employed or removed from the application's scope. This prevents broad permission requests from being misused or abused. As an additional layer of application security, each application must pass through an extensive graduation process, which includes a manual review of the submitted application's name, description, requested permissions, and rate limits. It also includes automatic checks to ensure the application does not have failing API calls or high error rates, while also ensuring the application doesn't use any permissions not requested or have any permissions requested that are not being used. Developers are also unable to modify their application type or permissions requested once the application has been made public.

Threat Detections And Mitigations

Our service includes multiple measures to prevent and detect service interruptions, account takeover, service abuse, and telecom fraud, including service operations monitoring, access controls, detection controls, usage throttling, and customer controlled international dialing plans. We implements Unified Communications Threat Management (UCTM) capabilities to aid in the detection and mitigation of robo calls and other forms of nuisance calling. In addition, our security department performs active monitoring to detect and notify customers of suspicious login activity, unrecognized devices, and anomalous calling patterns on their account.



Within each major data center, we provide a high availability, redundant architecture.

Business Continuity and Disaster Recovery

We house our core technology infrastructure and global network in multiple geographically diverse, state-of-the-art, Tier 4 data centers, minimizing the risk of loss and regional service interruption due to natural disasters and other catastrophic situations.

Within each major data center, we provide a high availability, redundant architecture. Our service components are designed with high availability, fault tolerance, and fault impact segregation in mind. Customer data—including service configurations and messages—is fully replicated across our data centers in real time.

In the event of a failure, our automated systems, in conjunction with an always-on, world-class network operations center (NOC), ensure rapid transition to back-up systems as needed to maintain uninterrupted service availability. We also perform disaster recovery tests periodically to gauge the system's high availability for the best, most seamless customer experience possible.

Logical Segregation and Multi-tenancy Model

We provide a multi-tenant environment for our customers and maintain a high degree of security to ensure that one customer's data is never available to another customer. We use a multi-tenant architecture and dynamic database views to form application layer boundaries between customer instances.

Account Security as a Shared Responsibility

Customer Admin Controls

Avaya Cloud Office, like most cloud solutions providers, operates under a shared security responsibility model. This framework identifies the shared responsibilities between the customer and the cloud provider.



Avaya Cloud Office operates under a shared security responsibility model with our customers.

We are responsible for the service delivery, architecture, and security of the core service as well as the physical and environmental security of the infrastructure employed to deliver our service.

Our customers are responsible for managing their account policies, granting the correct roles and permissions to users, properly implementing Single Sign-on, tracking administrative changes made on their account, controlling international dialing plans, and working with us to identify suspicious activity. Administrative controls made available to administrators include:

Roles and permissions

Role-based access controls provide an extra layer of security to help you enforce company security policies by providing complete oversight into which permissions are in use. The same level of access is unilaterally given to every user assigned to that role to ensure a consistent approach can easily be enforced and maintained. Roles can be created for functions or positions in the company with all the appropriate permissions built in. We have defined seven standard, ready-to-use roles to make it simple to quickly grant the right level of system access to many users at the same time, virtually eliminating errors that can happen when permissions are set individually. Custom roles can be defined to support countless permission combinations, extending the range of granular control over how users can access features. For each role, you can select the precise permissions you want to grant and update your selections at any time.

Audit trail

Audit trails allow customers to track configuration changes made to an account for auditing and troubleshooting purposes. Login attempts, phone number changes, license purchases, and other changes to admin/employee settings and permissions can be identified.

Single Sign-On (SSO)

We offer SSO capabilities making logins seamless across the board. While SSO is convenient for users, it also presents new security challenges. If a user's primary password is compromised, attackers may be able to gain access to multiple resources. In addition, as sensitive information makes its way to cloud-based services, it is even more important to secure access by implementing two-factor authentication.

Admins can define policies that enforce unique controls for each individual SSO application, which would entail duo checking the user, device, and network against an application's policy before allowing access to the application. For example, admins could require that CRM users complete two-factor authentication at every login, but only once every seven days when accessing the core solution.

Independent Verification

In addition to the security measures deployed as part of the physical and cloud infrastructure, we undergo independent verification and audits of our security controls by major partners and third parties. These assessments ensure our customers' compliance needs are met. Special efforts are undertaken to comply with regulations posed by specific industries.

In addition to the security measures deployed as part of the physical and cloud infrastructure, we undergo independent verification and audits of our security controls by major partners and third parties.

In addition to the security measures throughout product development, production environments, and service operations, we also engage outside auditors to review our security controls. These assessments ensure our safeguards are verified and tested, with visibility available to our customers. Special efforts are undertaken to comply with specific industry regulations and data privacy laws. They include:

Certifications and Reports

SOC 2 Type II

The SOC 2 report validates the effectiveness of our operating controls as a service organization against the criteria set forth by the [American Institute of Certified Public Accountants \(AICPA\)](#) Trust Services Principles. We annually undergo a third-party audit to certify our services against this standard.

A copy of the most recent report is available upon request from your account manager or sales representative.

SOC 3

Unlike a SOC 2 report, a SOC 3 report can be freely distributed to the public for general use. We have undergone a third-party audit to certify our services against this standard.

To view our SOC 3 report, [click here](#).

HITRUST

Our video has earned Certified status for information security by HITRUST. HITRUST CSF Certified status indicates that we have met HITRUST's defined security requirements and are appropriately managing cyber security risk.

HIPAA

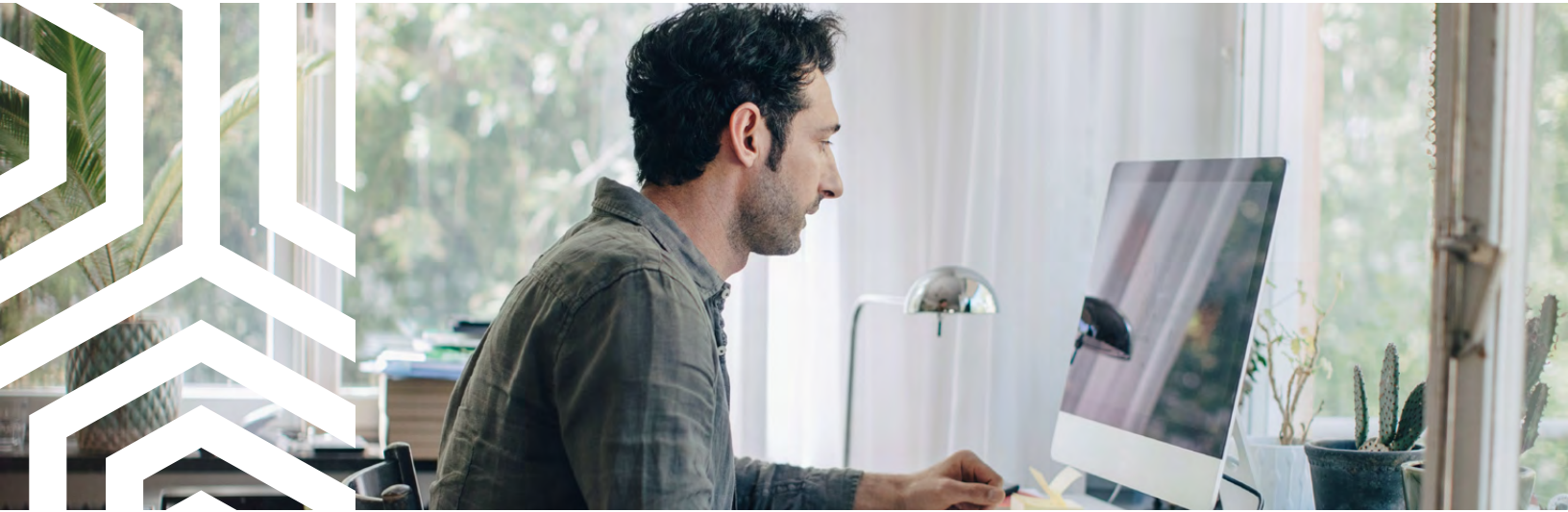
To better serve our customers in the highly regulated healthcare industry, we have implemented HIPAA security safeguards. We annually undergo a third-party SOC 2+ audit—which includes an assessment of controls mapped to the HIPAA Security Rule requirements—which demonstrates the implementation of the security safeguards and requirements outlined in the HIPAA Security Rule. We offer HIPAA Business Associate Agreements to covered entities. A copy of the most recent report is available upon request from your account manager or sales representative.

McAfee's CloudTrust Program

We have earned a McAfee CloudTrust rating of Enterprise-Ready, the highest rating possible. McAfee provides this status to cloud services that fully satisfy the most stringent requirements for data protection, identity verification, service security, business practices, and legal protection.

General Data Protection Regulation (GDPR)

We provide customers with a robust Data Processing Addendum (DPA) governing the relationship between the customer and Avaya Cloud Office. Our DPA contains strong privacy commitments that few software companies can match and has been updated to confirm our compliance with the GDPR.



About Avaya

Businesses are built on the experiences they provide and every day millions of those experiences are built by Avaya (NYSE:AVYA). For over one hundred years, we've enabled organizations around the globe to win—by creating intelligent communications experiences for customers and employees. Avaya builds open, converged and innovative solutions to enhance and simplify communications and collaboration—in the cloud, on premise, or a hybrid of both. To grow your business, we're committed to innovation, partnership, and a relentless focus on what's next. We're the technology company you trust to help you deliver Experiences that Matter. Visit us at www.avaya.com.

Conclusion

We recognize security as a critical component to every organization's internal and external communications. As such, we're committed to providing customers with the highest levels of integrity, confidentiality, compliance, and control.

Combined with a robust back-end infrastructure and global security team, our multilayered approach to security—revolving around multiple disciplines spanning everything from software development to access controls—ensures that customers' data and communications are defended at every stage. This not only protects your business from attacks, but also allows your IT department to focus on business functions rather than application security.

Today's organizations need technology vendors that continuously improve their security capabilities while delivering world-class services. We are proud to be one of those vendors and seek to provide our expertise in helping our customers advance their business needs while remaining committed to providing them with the highest levels of security, data confidentiality, compliance, availability, and control.

