VidyoConnect™

Secure enterprise meeting solution for team collaboration

Vidyo®

Table of Contents

About the VidyoConnect™ Service

VidyoConnect is a meeting solution for team collaboration that speeds global alignment across your enterprise, allowing for better-informed decisions, faster responses, and deeper trust. With a unified user experience across mobile, desktop, and conference room endpoints, VidyoConnect delivers the consistency, rich features, and ease of use that drive adoption.

As a leader in value, VidyoConnect provides all-inclusive, enterprise-grade video collaboration in any context, from simple browser-based video to desktop and mobile apps, unlimited legacy endpoint connectivity, phone dial-in, and recording. Rapid cloud deployment means faster ROI, and robust cloud services eliminate the tactical burden of managing a video network, freeing IT resources to focus on strategic projects that impact bottom-line results.

More Than Just Encryption

- User authentication/login
- Segregated management
- Password protection
- Signaling encryption
- Media encryption
- Secure firewall traversal

Secured Communication

Vidyo has made visual communications both ubiquitous and affordable with its revolutionary platform that forms the basis of the VidyoConnect service. The VidyoConnect service leverages patented routing core technology along with industry-standard scalable video coding (SVC). This enables end users to participate in high-quality Vidyo conferences from just about anywhere using standard broadband internet connections.

While this approach affords great flexibility in access and endpoints, Vidyo also recognizes the importance of protecting sensitive information transmitted over this medium from would-be hackers with malicious intent. This document provides an overview of Vidyo's security policy and the VidyoConnect security features designed to keep your communication and private information safe.

Security by Design

Security starts with sound processes. Vidyo maintains an information security governance policy that controls the way the confidentiality, integrity, and availability of information is handled, thereby preventing misuse and malicious damage that could impact Vidyo operations and ultimately our customers and partners.

The information security governance policy follows the domains of the ISO 27001 information security framework. These provide the guidelines necessary to enable compliance with various regulations regarding the oversight and management of information security and investigation services.

See below for more details about our comprehensive information security governance policy:

Information Security Governance Policy

- Reduces risk to our organization by building a culture of security awarenes" through employee education.
- Optimizes and enhances business-appropriate policies and procedures in support of Information Security and Compliance requirements.
- Ensures appropriate technical protections are put in place to detect, and as much as reasonably possible, prevent threats to our organization and clients.
- Ensures measure are put in place to address potential for a security breach, so that if one occurs, we can minimize the impact to our business and our customers while ensuring the confidentiality, integrity, and availability of our critical information and trade secrets.
- Ensures incidents are promptly reported to the appropriate authorities and are consistently and expertly responded to, and that significant incidents are properly monitored and mitigated.

The VidyoConnect service is hosted in secure data centers that have SOC 2 audit reports available for review and are based upon the latest NIST standards.

Furthermore, Vidyo uses accredited third-party security assessment companies to assess our products and services. A letter of attestation from our assessment vendors can be provided upon request.

Threat and Vulnerability Management

Vidyo has a security council that meets regularly to review and update the security policies and processes associated with the VidyoCloudTM service, as well as to review potential threats and issues. This council includes representatives from Vidyo's operations, cloud architecture, engineering, QA, and other departments. These individuals also act as security liaisons within their respective organizations to ensure implementation of the policies and processes set by the security council, and bring back relevant feedback and knowledge from their organizations.

Vidyo's product management team considers security implications for every proposed product and service modification. Vidyo uses resources such as the NIST National Security Database, MITRE, and OWASP, to monitor third-party software provider vulnerabilities and updates prior to their inclusion in Vidyo offerings. The software development team also performs regular code reviews to identify potential security vulnerabilities. Vidyo's quality assurance team uses industry-leading security scanning tools such as Tenable's Nessus, Rapid 7's Nexpose, and a host of open-source OWASP tools. Vidyo also uses the third-party Qualys SSL Labs utility to help qualify that its server-based solutions meet the high level of security targeted.

User Login and Database Security

Key Security Features

- SRTP media encryption
- FIPS 140-2 certified libraries
- Secure HTTPS login utilizing industry-standard PKI
- TLS using strong encryption ciphers for signaling
- Password hashing in database
- Encrypted token technology for session security
- No login information retained on the client

Protecting the login process from eavesdroppers and hackers is fundamental to securing the VidyoConnect service. Vidyo protects this process by establishing a critical front line of defense in a manner similar to the way online banking access is secured using TLS. The VidyoConnect service supports using industry-standard public key infrastructure, whereby each component is issued a digital certificate by a trusted third-party certifying authority. This allows endpoints to verify the identity of VidyoConnect and also helps prevent malicious users from eavesdropping on communication. With TLS security enabled, the VidyoConnect service always establishes an encrypted HTTPS channel with each Vidyo endpoint that attempts to access the system. Before transmitting any login information, the Vidyo endpoint or web browser validates the VidyoConnect certificate and verifies it was issued by a trusted third-party certifying authority. Once the certificate is verfied, login and password information is transmitted securely to VidyoConnect over the same encrypted HTTPS channel.

For HTTPS connections, the ciphers and key exchange method used are dependent on what the end user's browser can support. However, Vidyo infrastructure components prefer to use the strongest available ciphers and will reject the use of known weak ciphers.

To safeguard user login credentials, no login information is retained by the Vidyo soft clients. For organizations that use an external database for user account management, LDAP, SAML, and Active Directory (AD) are supported. When LDAP/SAML/AD are used, no passwords are stored within VidyoConnect. Additionally, password policies are supported via LDAP integration with the corporate directory system (such as AD, Oracle, Novell, etc.).

For users authenticated using SAML, VidyoConnect acts as a service provider and can authenticate users via external SAML 2.0 identity providers. Leveraging SAML provides a secure way to authenticate users without storing or exposing credential data on VidyoConnect.

For users who are not using LDAP/SAML/AD, password information is always hashed and salted using PBKDF2 in the VidyoConnect database. This ensures passwords cannot be revealed even if a security breach occurs.

Signaling Encryption

Signaling is the way different components within the Vidyo architecture communicate with one another. Protecting the information passed in this machine-to-machine communication from would-be hackers is important for securing the network. The VidyoConnect service leverages AES encryption over TLS for Vidyo endpoint and server communications with certificate support. Vidyo supports elliptic curve Diffie-Hellman (ECDH), Diffie-Hellman (DH), or RSA for key exchanges. The media encryption keys are also negotiated over this secure connection and are then used to encrypt the SRTP media traffic.

Media Encryption

VidyoCloud employs AES encryption over industry-standard SRTP for audio, video, and shared content. This helps protect the content of your Vidyo conferences from being intercepted and decoded without your knowledge.

Component Authentication (Spoof Prevention) and Session Security

“Spoofing” refers to a tactic used by hackers to “steal” the identity of a trusted component of a network in order to gain access. Vidyo helps prevent spoofing through a rigorous component authentication scheme. Each server in the VidyoConnect network has a unique identifier that is communicated to the portal application over a secure link and is otherwise not accessible. New components added to the VidyoConnect network go to the portal application for configuration. If the portal application does not have a configuration defined for that machine’s specific ID, the machine is blocked from joining the network until the VidyoConnect administrator accepts the new ID and manually configures the component.

On the client side, a unique token is used to authenticate the endpoint to the portal application in lieu of the password, and the administrator of the portal application can define expiration rules requiring users to reauthenticate.

Virtual Meeting Room Access

All Vidyo endpoints connect through the cloud and are not directly accessible from another endpoint. Therefore, even on public networks, Vidyo endpoints are protected from unauthorized direct access through an IP address. The architecture provides the endpoint with a layer of security from third-party hacking and voyeurism with built-in technology for spoof prevention, such as:

Encrypted token technology for session security

HTTPS with certificate support on login

TLS with certification for signaling

No matter which Vidyo endpoint you use, your Vidyo meeting room is the core of your virtual office. Just like with a physical office, you may want to have an open-door policy for your Vidyo meeting room where anyone with an account on your VidyoConnect subscription can drop in any time, or you may wish to "close the door" to your Vidyo meeting room. Vidyo affords you the flexibility to do both. If you prefer an open door, you don't need to do anything. If you wish to control access, you have the ability to define a PIN for your room and share it only with the people you want to have access. Additionally, you can take advantage of the click-to-connect links for inviting participants (including unregistered users) to join your virtual meeting room. When unauthenticated users join a meeting, they are identified as guests in the participant list so all participants know not to discuss sensitive topics. Every user has the ability to change the hyperlink to their personal meeting space as frequently as desired. Administratively, the PIN code can be configured to enforce a 3- to 12-digit PIN.

In addition to the personal virtual meeting room, Vidyo also supports a one-time-use meeting room for scheduled meetings. When a meeting is scheduled, a new meeting room is created with a unique guest link, PIN code, and meeting ID. The one-time meeting room eliminates conflicts between two different meetings taking place in the same meeting room. This is yet another level of security to provide control of sensitive information and make meetings more convenient.

As the meeting room owner, you are also the moderator and, as such, you have moderation capabilities over your virtual meeting room when conferences are in session. This includes the ability to lock the meeting room to prevent new participants from joining. You can also control each participant's ability to send audio and video by using the mute buttons, or you can disconnect anyone from the call with a simple click of a button. If desired, meeting rooms can be configured with a waiting room capability that prevents participants from seeing or hearing each other until the moderator joins the call.

VidyoConnect Hosting Facilities

The VidyoConnect service uses world-class hosting facilities to ensure high levels of security while also ensuring minimal down time. Our hosting facilities are SOC 2 compliant, with 24/7 protection to meet regulatory and best-practice requirements. Firewalls are regularly assessed, configured, and updated to remain effective against intrusion. Leading-edge filtering and advanced routing techniques help protect against distributed denial of service (DDoS) attacks. Intrusion prevention and detection systems provide proactive network surveillance and monitoring designed to protect the critical application environment.

Vidyo believes security is critical, and we regularly assess our security measures to keep pace with the dynamics of security threats. Vidyo has implemented different levels of security to protect our users. For example, physical and logical access are monitored and controlled, Vidyo audit logs are kept for over six months, and cloud management is restricted only to Vidyo subnets and controlled with security groups. In addition, super admin level access is only provided to the Vidyo operations team, and authorized and qualified team members receive their own account for tracking and auditing support.

VidyoConnect security control models cover the following areas:

Service

All VidyoCloud traffic encrypted server-to-client as well as server-to-server

Application

Constant security scanning, a software lifecycle security policy, release controls, etc. server.

Management

Configuration and operational change controls, change auditing, network segregation, multifactor authentication, etc.server.

Network

Firewalls, security groups, anti-DDoS, security patches, scans, etc.

Trusted Computing

AgileCLOUD and AWS as well as physical hardware at hosting facilities

HR security

Background verification, employment agreements (NDAs), and access provided based on “need to have”server.

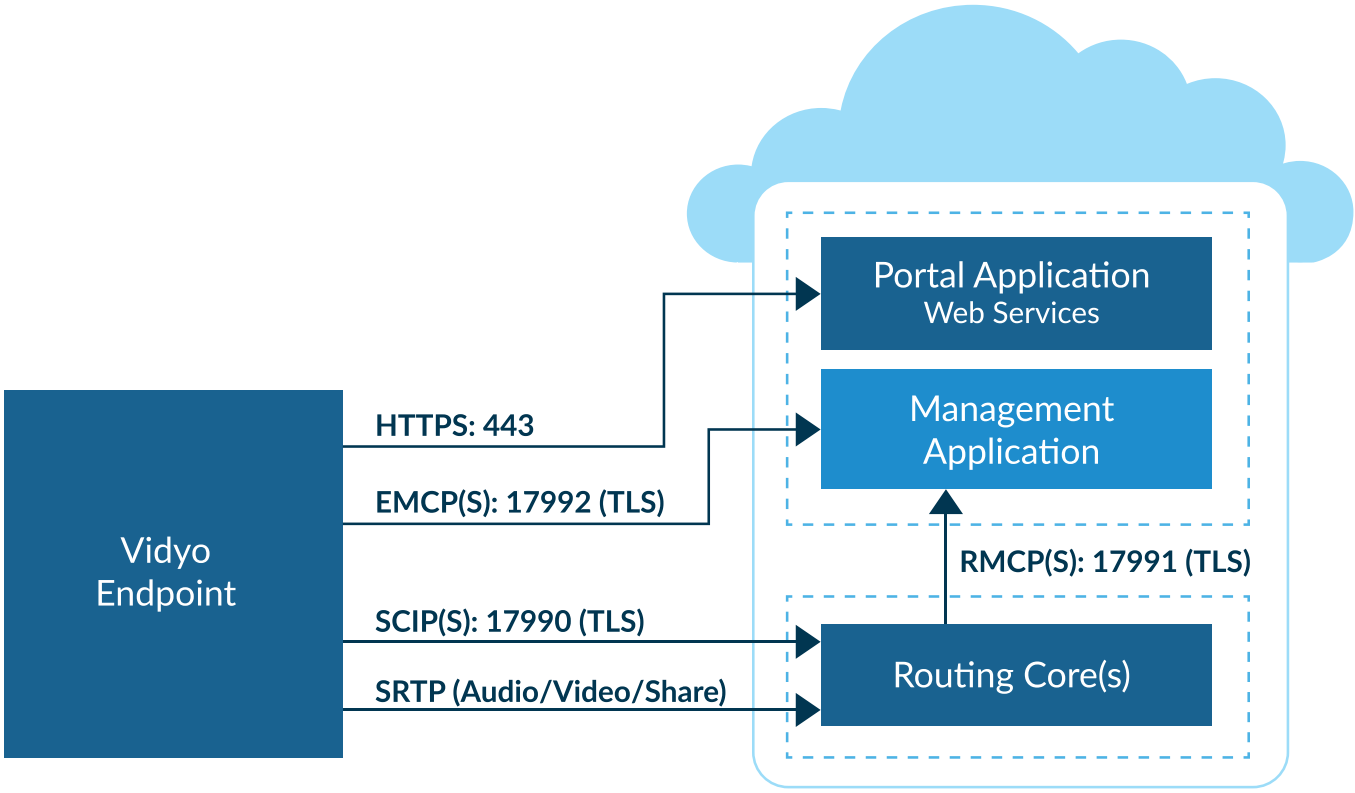
Physical

Data center security (24/7 surveillance), physical access control, CCTV, and guards

VidyoConnect Call Flow

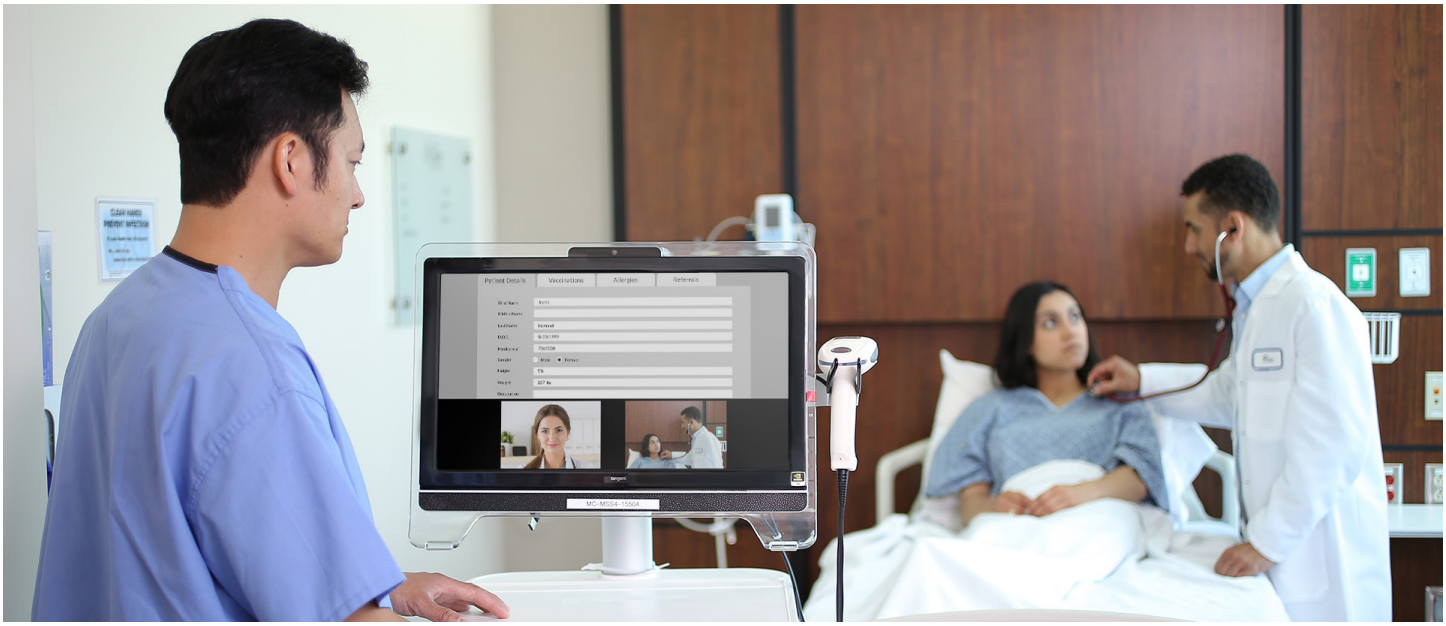
The following steps list the call flow for a Vidyo call into a conference. As described previously, all connections within a Vidyo call are encrypted.

1. HTTPS authentication is used from the Vidyo endpoint to the portal application via TLS with x509 certificate authentication.
2. Via the HTTPS connection, a Vidyo management application EMCPS address is negotiated.
3. An EMCPS TLS connection to the Vidyo management application is established on port 17992 with x509 certificate authentication.
4. The SCIPS address is sent to the Vidyo endpoint via EMCPS encrypted channel.
5. SRTP keys are exchanged via the secure SCIP connection.
6. SRTP transport is established using AES-128 and unique keys are generated for each connection.



Notes:

- HTTPS 443 — Secure connection with server certificate validation, including SNI
- EMCP(S) using TLS — Secure connection with server certificate validation, including SNI
- SCIP(S) using TLS — Secure connection with server certificate validation, including SNI
- RMCP(S) using TLS — Secure connection with server certificate validation, including SNI
- SRTP using AES-128 with key exchange via SCIP(S) over TLS connection (above)
  - Each SRTP connection negotiates unique keys, which are updated periodically as per the SRTP standard.
  - Keys do not leave the running process.
  - All media packets are encrypted between clients and servers.



HIPAA and Vidyo's Cloud Services for Healthcare Customers

The Health Insurance Portability and Accountability Act (HIPAA) provides standards to protect the confidentiality, integrity, and availability of protected health information (PHI), including electronic protected health information (ePHI). HIPAA provides guidance for an acceptable level of protection for ePHI while giving healthcare providers access to information necessary to perform their daily business functions.

There are many considerations a healthcare provider or other covered entity (as defined in HIPAA) must meet in order to satisfy HIPAA guidelines. The Vidyo healthcare cloud offerings, including VidyoConnect and vidyo.io for healthcare, have been designed such that healthcare providers and other covered entities can use our services for video communication in a manner consistent with their HIPAA obligations.

Vidyo does not store or access PHI of users of our healthcare cloud services. However, recognizing the compliance needs of covered entities, Vidyo will sign HIPAA-compliant business associate agreements for our healthcare cloud offering customers.

For more information about HIPAA compliance with Vidyo, go to https://www.vidyo.com/hipaa.

Conclusion

Securing customer communications and private information without inhibiting the value and capability of the collaboration solution is a priority for Vidyo. With security designed into each stage of our VidyoConnect service, and a process in place for continuous monitoring, qualification, and action to address new and emerging security threats, Vidyo delivers a visual collaboration service that leverages industry-standard and proven technologies with the goal of securing its users' communications and private information.

Frequently Asked Questions

1 Does Vidyo perform security audits on its Vidyo solutions?

Yes. Vidyo runs internal security scanners against its software prior to release. We use a variety of third-party vulnerability scanning tools to audit and evaluate software and ensure compliance. In addition, an external SSL Labs utility is run against Vidyo components. Vidyo continuously evaluates new tools to ensure systems are tested with the utmost rigor.

2 What are the steps Vidyo takes to make sure the VidyoConnect infrastructure components are protected from hackers and virus attacks?

The VidyoConnect infrastructure components are all Linux-based. To prevent hackers from accessing the servers themselves, Vidyo leverages the security features of Linux while hardening the server by closing all ports and services that are not used and disabling access to the underlying system without valid administrator credentials.

Vidyo infrastructure components are locked-down applications with the goal of enabling only Vidyo-validated software to be applied onto the system, preventing malicious content from being introduced into the network.

3 How does Vidyo check that VidyoConnect components are up to date with third-party software security fixes?

Vidyo has a multidiscipline security council that regularly monitors the latest vulnerabilities for the third-party software elements used in Vidyo solutions and determines whether a particular security update is needed. Some resources that are monitored include Apache, Ubuntu Security Notices, NIST National Security Database, MITRE, and OWASP. Security patches are issued in a timely manner and all patches are rolled into the following system release.

4 What is Vidyo's strategy when a security breach is identified in the code or in a third-party library used by Vidyo?

When a potential security vulnerability is identified (whether it is within Vidyo's software or a third-party library), our security council immediately assesses the exploitability, impact, and severity of the vulnerability. Based on these criteria, if/when it determines that it is appropriate, Vidyo will do one or both of the following:

- Issue a security bulletin with steps to mitigate the vulnerability.
- Issue a security update that permanently patches the vulnerability.

5 How does Vidyo ensure no call data can be intercepted via "man-in-the-middle" on the network?

The endpoint establishes a trusted connection to the portal application using TLS with x509 certificate validation. All subsequent connections are orchestrated from this trusted connection. Each of the subsequent signaling channels (EMCPS and SCIPS) also establishes trusted connections using x509 certificate validation.

6 What are the standards used for media encryption?

For media, Vidyo uses the standards set by SRTP RFC-3711. For each SRTP stream, a unique master key is generated using the Vidyo crypto kernel (which is FIPS 140-2 certified). This master key is exchanged via a secure SCIPS (TLS) connection. As per the SRTP RFC, periodically a session key is updated by both sides so that an attacker cannot collect large amounts of ciphertext from a single key.

7 How is security handled for H.323 and SIP traffic?

VidyoConnect allows H.323- and SIP-based endpoints to connect through encrypted connections. For H.323 endpoints, calls can be made using H.235 encryption. SIP endpoints can use TLS/SRTP to encrypt the signaling and media. These are the standards that SIP and H.323 endpoints use for encrypted calls, and VidyoCloud supports both. The customer endpoints must be configured for encrypted calls in order to take advantage of this.

8 Does the VidyoConnect service support encrypted storage for recorded videos?

Yes, VidyoConnect uses an encrypted volume to store the recordings. The encryption used is LUKS over LVM with cipher: aes-cbc-essiv:sha256. Currently, this is only available on request for select customers who have encrypted storage requirements and it is not available to healthcare customers. However, healthcare customers (and others) can choose to implement VidyoReplayTM on-premises and connect to the VidyoConnect service.

9 What physical security measures, processes, and monitoring capabilities does Vidyo have in place to prevent unauthorized access to its data centers and infrastructure?

- 24/7 on-site security personnel and secure loading docks
- Fingerprint-activated biometric locking mechanisms
- Mantraps with weight sensors to determine if equipment is being carried out of the facility
- 90-day video monitoring with security cameras available for individual cage environments as needed
- Recorded "in and out" logs
- Password-protected access to both physical locations and web portals

10 Who are the service providers that will assist with the cloud-computing offering and where are your data centers located?

Services are hosted in Google Cloud, Internap, or AWS and are operated by Vidyo. We currently have Vidyo infrastructure in California, Texas, New Jersey, London, Amsterdam, Hong Kong, and Singapore.

11 What is Vidyo's patch management policy and procedure?

We have monthly maintenance windows. However, if a high-severity issue is found, a more expedient patch can be applied.

12 Does Vidyo have an incident response plan?

Even with the security precautions described in this document, no service is immune to security incidents. With this in mind, Vidyo has an incident response plan in place. All clients are notified of incidents affecting their services. The plan is available upon request on a per-client basis.

13 What is Vidyo's backup and disaster recovery strategy?

Each portal has local live HA replication and sync. A DR snapshot and restore to a DR portal site is performed hourly. The snapshots are also stored in a central management server, one every hour for 24 hours, and the last one per day is retained for three weeks.

14 How and how often are backup and recovery infrastructure tested?

The DR portal is logged into and tested at least once a month to validate that its currently restored DB is valid and functional, with full failover testing twice a year.

15 Does Vidyo maintain an industry-accepted security framework?

In addition to hosting in secure data centers that have SOC 2 audit reports available for review, Vidyo has engaged third-party advisory and audit firms in preparation for assessment under SOC 2 guidelines. Upon completion of the processes, the audit status of our services will be available for review similar to the data center SOC 2 reports. Furthermore, Vidyo uses accredited third-party penetration testing companies to assess our products and services, and a letter of attestation to such testing can be made available from our assessment vendors upon request.

16 Is an SOC 2 review available?

The SOC 2 report is available upon request on a per-client basis.

17 Are privileged actions monitored and controlled?

As part of Vidyo's process, we log in to our infrastructure through an auditing and tracking tool, which provides audit trails and records the sessions.

18 Is VidyoCloud GDPR compliant?

Vidyo has been active in the EU for a long time. As such, Vidyo is actively working to meet the new GDPR requirement by May 2018.

Resources

For more information about the VidyoConnect service and the Vidyo products described in this document, contact your Vidyo sales representative or go to the following sites:

- Vidyo website:
  http://www.vidyo.com
- VidyoConnect site:
  https://www.vidyo.com/cloud-video-conferencing-service
- Vidyo Support Center:
  https://support.vidyocloud.com/
- Vidyo Resources (white papers, case studies, data sheets, etc.):
  http://www.vidyo.com/resources/

Start Building With

VidyoConnect™