vidyo.io™

Secure Embedded Video Communications

Vidyo®

Table of Contents

About the vidyo.io™ Service

The vidyo.io service is a communication platform-as-a-service (CPaaS) offering that lets application developers and enterprises quickly and easily embed high-quality, reliable, scalable video collaboration into any WebRTC, mobile, or native application. Vidyo.io makes embedded video accessible for developers who are looking to rapidly integrate real-time visual communications into their own applications.

With no costly on-premise hosting or deep technical knowledge of video coding required, the vidyo.io service provides SDKs for web browsers (WebRTC and plug-in), iOS, Android™, macOS®, and Windows®, with a consistent API that speeds time to market and lowers development cost. The vidyo.io APIs allow for any number of video participants, from simple two-person video chats to large multiparty conferences.

The vidyo.io service is ideal for all types of network environments. It uses its own industry-leading scalable video technology (a key differentiator) to deliver the best possible video quality with the lowest latency. Vidyo's cloud-based infrastructure shapes and routes video streams in real time, with automatically discovered access points around the globe. The platform and SDK seamlessly provide all the necessary components (such as firewall traversal and resource management) to minimize connectivity issues and maximize uptime and quality connections — especially for challenging platforms such as mobile.

Hundreds of enterprise customers and thousands of developers have already video-enabled their applications using Vidyo APIs. With the vidyo.io APIs, you can get the same unparalleled scalability, error resiliency, and simplicity, and you can leverage the same patented scalable video coding (SVC) routing technology that has been used by Vidyo's enterprise customers and service providers for years to deliver industry-leading RTC reliability and quality over virtually any network and device.

Secured Communication

Vidyo has made visual communications both ubiquitous and affordable with its revolutionary platform, which is the basis of the vidyo.io service. The vidyo.io service leverages patented routing core technology along with industry-standard SVC. Together, these enable end users to participate in high-quality video collaboration from just about anywhere using standard broadband internet connections.

While this approach affords great flexibility, Vidyo also recognizes that it's just as important to protect the sensitive information transmitted over this medium from would-be hackers with malicious intent. The remainder of this document provides an overview of Vidyo's security policy as well as the vidyo.io security features designed to keep your communication and private information safe.

Comprehensive Security

- Segregated Management
- Signaling encryption
- Media encryption
- Secure firewall traversal

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 affect Vidyo, Inc., and ultimately our clients and partners.

Our comprehensive information security governance policy:

Optimizes and enhances business-appropriate policies and procedures

In support of information security and compliance requirements.

Ensures appropriate technical protections are in place

To detect, and as possible, prevent threats to our organization and our clients.

Ensures measures are in place to address any potential for a security breach

If such a breach does occur, Vidyo can minimize the impact to our clients and promptly restore operations.

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.

In addition, Vidyo adheres to the security and privacy trust service principles of SOC 2. Although SOC 2 is considered a technical audit, it actually goes beyond that: SOC 2 requires companies to establish and follow strict information security policies and procedures, encompassing the security and confidentiality of customer data. SOC 2 ensures that a company's information security measures are in line with the unique parameters of today's cloud requirements. Vidyo hosts in secure data centers that are SOC 2 compliant 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 vidyo.io service, as well as to review potential threats and issues. This council includes representatives from Vidyo's operations, cloud architecture, engineering, QA, and other organizations. These individuals also act as security-related 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-related implications for every proposed product and service modification. Vidyo uses resources such as the NIST National Security Database, MITRE, OWASP, etc., 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 vulnerability scanning tools as well as open-source OWASP tools to help ensure that its server-based solutions meet the high level of security targeted.

Key Security Features

- SRTP media encryption
- FIPS 140-2 certified libraries
- Secure HTTPS signaling encryption using industry standard PKI
- TLS using strong encryption ciphers for signaling
- Encrypted token technology for session security

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 vidyo.io service leverages AES encryption over TLS for Vidyo endpoint and server communications. Vidyo supports industry-standard PKI certificate validation to ensure that the connection to the Vidyo servers is trusted and secure.

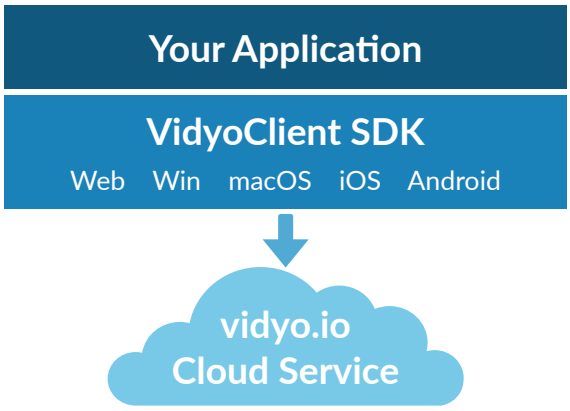
Vidyo supports elliptic curve Diffie-Hellman (ECDH), Diffie-Hellman (DH), or RSA for key exchanges. The media encryption keys are also negotiated over this secure connection and are then used to encrypt the SRTP media traffic. At no time does any signaling traffic touch the network via an unencrypted connection. This prevents an attacker from getting access to the media encryption keys by sniffing network traffic.

Media Encryption

The vidyo.io service employs AES 256-bit encryption over industry-standard SRTP for audio, video, and shared content. This helps to protect the content of your video sessions from being intercepted and decoded without your knowledge.

Connecting to vidyo.io

When a third-party application is ready to establish a video call, it launches the SDK via APIs to connect to the vidyo.io service. Connecting to the vidyo.io cloud requires the VidyoClient-based application to authenticate with the vidyo.io service. This is done by passing a token from the application through the VidyoClient SDK to the vidyo.io cloud. The token identifies both your application and the user. This architecture provides the framework that allows development of robust and secure Vidyo communications.



DeveloperKey and ApplicationID

A DeveloperKey is a shared secret between the vidyo.io service and the developer's back-end application. For each application, a DeveloperKey and ApplicationID must be created in the API Key section of the vidyo.io site and then securely stored on the application back end.

- The DeveloperKey is used to generate access tokens on the developer back end (see the following section for more information), and should never be sent to the endpoint itself. Access to the DeveloperKey must be restricted since every token that is signed using the key will be used for access and billing.

- The ApplicationID identifies the application when connecting to the vidyo.io platform. The application can automatically provision any user (for example, user1@ApplicationID) when generating a token. The ApplicationID is used to ensure that users and resources are restricted to users with a valid token (that is, a token that is signed and not expired).

Within vidyo.io, the DeveloperKeys are encrypted in the database using AES 256-bit encryption and are decrypted when necessary by the token validation process.

Tokens

A token is a short-lived authentication credential that grants access to the vidyo.io service to a specific user on behalf of the developer. When an endpoint requests access to the service, the developer's application back end must generate a token and pass it on to the client application. The token contains the following:

- **Username:** The username is an open-ended alphanumeric string of the developer's choosing that is provisioned on the fly. Vidyo.io refers to users in the participant- and chat-related APIs as user@applicationid.
- **ApplicationID:** Refer to the previous section for information about the ApplicationID.
- **Expiration Time:** Each token has a lifetime. Its lifetime is determined when the token is generated by specifying the number of seconds until it expires. The expiration time should be as short as possible. Expiration ensures that access to the system is secure and isn't open to abuse.

The developer combines these three items and creates a signed token using the DeveloperKey. Details about how to generate and sign a token are available on the vidyo.io Developer Center. By managing the token generation, the developer can ensure that only the intended user is able to join conferences.

Virtual Meeting Room Access (ResourceID)

As previously noted, connecting to the vidyo.io cloud is achieved by passing a token from the developer's application through the VidyoClient SDK to the vidyo.io cloud. The token identifies both the application and the user. The ResourceID is used to tell the participants where to meet. The secure generation of the token along with the ResourceID ensures that only authorized users can enter the conference.

The ResourceID is the name given to a resource. Resources are strings of text denoting meeting points in the application. They are ad hoc and simply direct a user to a resource. If the resource does not exist, it is created; if the resource already exists, the user joins the other participants who are already "connected" to the resource.

Resources can be thought of as the name of a meeting room. The application developer decides the manner in which names are chosen. However, in all cases, resources are unique to each ApplicationID. In other words, if a resource named "BlueRoom" is created by two different developers, each will be unique within vidyo.io.

Vidyo.io Hosting

The vidyo.io service utilizes world-class hosting facilities to ensure the highest level of security while also ensuring minimal down time. Our hosting facilities are SOC 2-, GDPR-, and HIPAA-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-detection systems provide proactive network surveillance and monitoring designed to protect your 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 its users. For example, physical and logical access are monitored and controlled, Vidyo audit logs are kept for 180 days, and cloud management is restricted to only Vidyo subnets and controlled with security groups. In addition, administrative-level access is only provided to the Vidyo operations team, and each authorized and qualified team member's activity is logged for tracking and auditing.

Vidyo.io security control models cover the following areas:

Service

All vidyo.io traffic is encrypted, server-to-client as well as server-to-server.

Application

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

Management

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

Network

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

HR security

Background verification, employment agreements (NDAs), and access provided on a “need-to-have” basis.

Physical

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

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 vidyo.io service, and a process in place for continuous monitoring, qualification, and action to address new and emerging security threats, Vidyo delivers a video 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 continually evaluates new tools to ensure systems are tested with the utmost rigor.

2 What steps does Vidyo take to make sure their Vidyo infrastructure components are protected from hackers and virus attacks?

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

3 How does Vidyo check that Vidyo solutions 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 next 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 do you ensure no call data can be intercepted via "man-in-the-middle" on the network?

The endpoint establishes a trusted connection to the vidyo.io XMPP application using TLS with x509 certificate validation. All subsequent connections are orchestrated from this trusted connection.

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 our Vidyo CryptoKernel (which is FIPS 140-2 certified). This master key is exchanged via a secure XMPP (TLS) connection. As per the SRTP RFC, a session key is periodically updated by both sides so that an attacker cannot collect large amounts of ciphertext from a single key.

7 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

8 What internal controls does Vidyo have in place to prevent unauthorized viewing, copying, or emailing of customer information?

As part of our process, we log all access to the VidyoServers to a centralized Splunk server, which generates security alerts as well as a daily report that provides audit trails and records of all activity. The daily report is compared to our change control system. Any access that does not have a corresponding record is investigated. This implementation restricts what can be done and records all access to the infrastructure. In addition, access is limited to operation and support subnets and team members.

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

Services are hosted in Internap, Google, or Amazon and are operated by Vidyo. We currently have Vidyo infrastructure in California, Texas, New Jersey, London, Amsterdam, Hong Kong, and Singapore. All data is stored within the US data centers.

10 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.

11 Does Vidyo have an incident response plan?

Vidyo has an incident response plan in place. All clients are notified of incidents affecting services. The plan is available upon request on a per-client basis.

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

Each vidyo.io portal has local 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.

13 Are privileged actions monitored and controlled?

As part of our process, all privileged actions are recorded using a Splunk server and are sent daily to be reviewed by the security and operations teams.

14 Is vidyo.io 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.

Start Building With

vidyo.io™

Vidyo