Vidyo®

An Enghouse Company

VidyoConnect™

Sichere Videokommunikationslösung
für Meetings und Team-Kollaboration

Inhalt

Vidyo
An Enghouse Company

Über VidyoConnect™

VidyoConnect ist eine videobasierte Meeting-Lösung für die Zusammenarbeit im Team. Sie beschleunigt die globale Abstimmung im gesamten Unternehmen und ermöglicht damit bessere Entscheidungen und schnellere Reaktionen. Mit einer einheitlichen Nutzerführung in der Meeting-Kommunikation via Desktop, in Konferenzräumen und über mobile Endgeräte bietet VidyoConnect zahlreiche Funktionen und eine komfortable Bedienung. Dadurch kann die Lösung in Ihrem Unternehmen schnell eingesetzt werden und wird von Nutzern umgehend in die täglichen Arbeitsprozesse eingebunden. VidyoConnect ermöglicht eine umfangreiche, unternehmensweite Video-Zusammenarbeit für jede Situation. Sie bietet Ihnen eine einfache Browser-basierte Video-Kommunikation auf dem Desktoprechner und auf mobilen Endgeräten, die Verwendung von Meeting-Raum-Systemen anderer HerstellerMeeting eine unkomplizierte Telefoneinwahl sowie die Aufzeichnung von Meetings und Gesprächen. Die unkomplizierte Bereitstellung in der Cloud bedeutet für Unternehmen einen schnelleren Return on Investment. Außerdem machen die verlässlichen Cloud-Services das bisherige, zentrale Management eines eigenen Video-Netzwerks obsolet und entlasten Ihre IT-Ressourcen. So kann sich die IT-Abteilung wieder mehr auf strategisch wichtige Projekte konzentrieren und damit nachhaltig zum Unternehmenserfolg beitragen.

Mehr als nur Verschlüsselung

- Authentifizierung von Benutzern
- Getrennte Verwaltung
- Passwortschutz
- Verschlüsselung des Signalprotokolls
- Medienverschlüsselung
- Sicheres Firewall-Management

Sichere Kommunikation

Vidyo macht die visuelle Kommunikation ganz selbstverständlich, überall einsetzbar und erschwinglich. Die Basis für VidyoConnect bildet seine revolutionäre Plattform. Der Service nutzt eine patentierte Routing-Kerntechnologie und verbindet sie mit dem Industriestandard in der skalierbaren Videocodierung (SVC). So können Endnutzer von nahezu jedem Ort aus via Internet-Verbindung an qualitativ hochwertigen Vidyo-Konferenzen teilnehmen.

Vidyo beachtet und gewährleistet außerdem den Schutz sensibler Informationen und schützt das System vor Angriffen von Hackern. Dieses Whitepaper bietet Ihnen einen Überblick über die Sicherheitsrichtlinien von Vidyo sowie die Sicherheitsfunktionen von VidyoConnect. Sie wurden entwickelt, um Ihre unternehmerischen und privaten Informationen in der Kommunikation zu schützen.

Vidyo
An Enghouse Company

Unser Sicherheits-Design

Sicherheit beginnt mit verlässlichen Prozessen. Vidyo setzt daher Richtlinien zur Steuerung der Informationssicherheit um, mit denen wir festlegen, wie die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Daten gehandhabt werden. So verhindern wir Datenmissbrauch oder feindliche Beschädigung, die Auswirkungen auf den Betrieb von Vidyo und letztendlich auf unsere Kunden und Partner haben würden.
Die Maßnahmen zum Datenschutz orientieren sich an den strengen Vorgaben des Bundesministeriums für Sicherheit in der Informationstechnik und sowie an der ISO 27001 Zertifizierung. Darin sind klare Richtlinien definiert, wie ein sicheres Datenmanagement umgesetzt und eingehalten werden muss.

Weitere Aspekte zu unseren umfassenden Richtlinien für ein sicheres Informationsmanagement:

Aufbau der Informationssicherheit

- Reduziert das Sicherheitsrisiko für unsere Organisation und unsere Kunden.
- Entwickelt durch Schulungen ein Sicherheitsbewusstseins bei Mitarbeitenden.
- Ständige Optimierung der Prozesse, um die Anforderungen an Informationssicherheit und Compliance-Vorgaben zu erfüllen.
- Umsetzung von technischen Schutzvorkehrungen, um Bedrohungen für unsere Organisation und unsere Kunden zu verhindern.
- Entwicklung von Maßnahmen, um mit potenziellen Sicherheitsproblemen umzugehen.
  So können wir im Fall der Fälle die Auswirkungen auf unsere Kunden und unsere Leistung minimieren und gleichzeitig die Vertraulichkeit und Verfügbarkeit aller kritischen Informationen und Geschäftsgeheimnisse gewährleisten.
- Sofortige Meldung von Vorfällen an die zuständigen Behörden.
- Konsequente und professionelle Reporting von Zwischenfällen.

Der VidyoConnect-Service wird in sicheren Rechenzentren gehostet. Sie basieren auf den neuesten NIST-Standards und bieten den Abruf von SOC 2-Auditberichten zur ständigen Überprüfung aller Prozesse.

Darüber hinaus beauftragt Vidyo akkreditierte Firmen, die die Sicherheit unserer Produkte und Dienstleistungen bewerten. Eine Bescheinigung von unseren externen Sicherheitsauditoren können wir gerne jederzeit zur Verfügung stellen.

Vidyo
An Enghouse Company

Maßnahmen gegen Cyberkriminalität

Vidyo hat einen eigenen Sicherheitsrat aus IT-Experten, der regelmäßig die Sicherheitsrichtlinien und -prozesse des VidyoCloud-Service überprüft sowie aktualisiert und zudem potenzielle Bedrohungen oder Probleme erfasst. Der Rat umfasst Vidyo-Vertreter aus der Betriebsführung, dem Hosting-Management, der Entwicklung, der Qualitätssicherung und anderen Abteilungen. Diese Mitarbeiter sind zugleich Sicherheits-Multiplikatoren innerhalb ihrer jeweiligen Abteilungen und sorgen dort dafür, dass alle Richtlinien und Prozesse umgesetzt werden. Sie stellen Erfahrungen aus ihrer täglichen Arbeit vor und bringen zugleich wichtiges Feedback und Wissen aus ihren Abteilungen ein.
Das Produktmanagement von Vidyo berücksichtigt die Auswirkungen auf den Datenschutz bei jeder Produktanpassung. Vidyo nutzt Ressourcen wie die NIST National Security Database, MITRE und OWASP, um Software von Drittanbietern zu überwachen und sowohl deren Schwachstellen als auch deren Updates vor der Integration in Vidyo zu prüfen. Das Software-Entwicklungsteam führt außerdem regelmäßige Codeüberprüfungen durch, um potenzielle Sicherheitsschwachstellen zu ermitteln. Für die Qualitätssicherung kommen branchenführende Tools wie Nessus von Tenable, Nexpose von Rapid 7 und eine Reihe von Open-Source-OWASP-Tools zum Einsatz. Das Qualys SSL Labs-Dienstprogramm stellt sicher, dass sich Sicherheit und Datenschutz unserer serverbasierten Lösungen auf dem höchstmöglichen Niveau befinden.

Benutzeranmeldung und Datenbanksicherheit

Sicherheitsmerkmale

- SRTP-Medienverschlüsselung
- FIPS 140-2-zertifizierte Bibliotheken
- Sichere HTTPS-Anmeldung mit Industriestandard PKI
- TLS verwendet starke Verschlüsselungs-Algorithmen
- Passwort-Hashing in der Datenbank
- Verschlüsselte Token-Technologie für Sitzungssicherheit
- Keine Speicherung der Login-Daten des Teilnehmers

Der Login-Prozess ist grundsätzlich vor Hackern geschützt und die sichere Anmeldung im VidyoConnect-Service damit gewährleistet. Vidyo schützt diesen Prozess durch die Einrichtung einer virtuellen IT-Verteidigungslinie mit TLS, wie man sie aus dem Online-Banking kennt. Unser VidyoConnect-Service unterstützt dabei die Verwendung des Industriestandards einer Public-Key-Infrastruktur, bei der jede Komponente ein digitales Zertifikat durch eine vertrauenswürdige Zertifizierungsbehörde erhält. So kann die Identität eines Teilnehmers überprüft werden und Angreifer daran gehindert werden, die Kommunikation in VidyoConnect abzuhören. Ist die TLS-Security aktiviert, stellt VidyoConnect mit jedem Endpunkt, der auf das System zugreifen möchte, einen eigenen verschlüsselten HTTPS-Kanal her. Bevor ein Teilnehmer seine Anmeldedaten übermittelt, validiert der Vidyo-Endpunkt oder Webbrowser das VidyoConnect-Zertifikat und überprüft, ob es von einer vertrauenswürdigen Drittpartei ausgestellt wurde. Ist das Zertifikat verifiziert, kann sich der Teilnehmer anmelden. Seine Passwortinformationen werden über den verschlüsselten HTTPS-Kanal sicher an VidyoConnect übertragen.

Bei HTTPS-Verbindungen hängen die verwendeten Algorithmen und Schlüsselaustauschverfahren davon ab, welche der Browser des Teilnehmers unterstützt. Die Vidyo-Infrastruktur zieht es vor, die stärksten, verfügbaren Algorithmen zu verwenden, und lehnt die Verwendung von Lösungen mit Schwachstellen ab. Um die Login-Daten der Benutzer zu schützen, werden sie von den Vidyo Softclients nicht gespeichert. Bei externen Datenbanken für die Verwaltung von Benutzerkonten, wird LDAP, SAML und Active Directory (AD) unterstützt. Nutzen sie LDAP/SAML/AD, werden keine Passwörter innerhalb von VidyoConnect gespeichert. Zusätzlich unterstützt Vidyo etwaige Passwortrichtlinien über die LDAP-Integration mit dem Unternehmensverzeichnis-System (wie AD, Oracle, Novell usw.).

Vidyo
An Enghouse Company

Bei SAML-Authentifizierung, agiert VidyoConnect als Service Provider und kann Benutzer über externe SAML 2.0 Identitätsprovider bestätigen. Die Nutzung von SAML bietet eine sichere Möglichkeit, Benutzer zu authentifizieren, ohne dass die Zugangsdaten auf VidyoConnect gespeichert oder offengelegt werden. Für Benutzer, die nicht LDAP/SAML/AD verwenden, verarbeitet die VidyoConnect Datenbank die Passwortinformationen immer mittels PBKDF2. Dadurch stellen wir sicher, dass Passwörter nicht offengelegt werden können, selbst wenn eine Sicherheitsverletzung auftritt.

Verschlüsselung des Signalprotokolls

Mit Hilfe von Signalen kommunizieren verschiedene Komponenten innerhalb der Vidyo-Architektur miteinander. Deshalb ist es wichtig, Informationen aus dieser Machine-to-Machine-Kommunikation im Netzwerk vor Hackern zu schützen. VidyoConnect nutzt die AES-Verschlüsselung über TLS für die Kommunikation zwischen den Vidyo-Endpunkten und den Servern. Vidyo unterstützt die elliptische Kurve Diffie-Hellman (ECDH), Diffie-Hellman (DH) oder RSA für den Schlüsselaustausch. Die Keys für diese Medienverschlüsselung werden ebenfalls über diese sichere Verbindung ausgestellt und dann zur Verschlüsselung des SRTP-Traffics verwendet.

Medien Encryption

Für Audio, Video und gemeinsam genutzte Inhalte nutzt VidyoCloud eine AES-Verschlüsselung über den Industriestandard SRTP. Dadurch werden Informationen in Vidyo-Konferenzen davor geschützt, ohne Ihr Wissen abgefangen und entschlüsselt zu werden.

Komponenten-Authentifizierung (Spoof-Prävention) und Session-Security

„Spoofing“ ist eine Methode von Hackern, mit der sie die Identität einer vertrauenswürdigen Komponente eines Netzwerks „stehlen“ und dadurch Zugang erhalten. Vidyo hilft, Spoofing durch ein strenges Authentifizierungsschema für Komponenten zu verhindern. Jeder Server im VidyoConnect-Netzwerk hat eine eindeutige Kennung, die über eine sichere Verbindung an die Portallösung übermittelt wird und ansonsten nicht zugänglich ist. Neue Komponenten im VidyoConnect-Netzwerk müssen im Portal erst konfiguriert werden. Gelingt solch eine Konfiguration mit einer spezifischen ID eines Rechners nicht, wird der Rechner für den Zugang zum Netzwerk gesperrt. Der VidyoConnect Administrator muss dann die neue ID akzeptieren und die Komponenten manuell konfigurieren.

Auf der Client-Seite wird anstelle des Passworts ein eindeutiges Token verwendet, um den Endpunkt gegenüber der Portalanwendung zu authentifizieren. Außerdem kann der Administrator Ablaufregeln definieren, die eine erneute Authentifizierung der Benutzer erfordern.

Zugang zum virtuellen Konferenzraum

Alle Vidyo-Endpunkte werden über die Cloud verbunden und sind von einem anderen Endpunkt aus nicht direkt zugänglich. Daher sind Vidyo-Endpunkte auch in öffentlichen Netzwerken vor einem unbefugten direkten Zugriff über eine IP-Adresse geschützt. Die Architektur bietet dem Endpunkt Sicherheit vor Hackerangriffen und Datenspionage mittels einer integrieten Technologie zur Spoof-Prävention, wie z.B:

Verschlüsselte Token-Technologie für Sitzungssicherheit

HTTPS mit Zertifikatsunterstützung bei der Anmeldung

TLS mit Zertifizierung für Signale

Ganz gleich, welchen Vidyo-Endpunkt Sie verwenden: Ihr Vidyo Meetingraum ist das Herzstück Ihres virtuellen Büros. Genau wie in einem physischen Büro möchten Sie vielleicht eine Offene-Tür-Politik für Ihren Vidyo-Besprechungsraum haben, sodass jeder mit einem Konto in ihrem VidyoConnect-Netzwerk jederzeit vorbeikommen könnte. Oder Sie möchten „die Tür“ zu Ihrem Vidyo-Treffen vielleicht doch lieber schließen. Vidyo bietet Ihnen die Flexibilität, beides zu tun. Wenn Sie einen offenen Zugang bevorzugen, brauchen Sie nichts zu tun. Wenn Sie den Zugang lieber kontrollieren möchten, können Sie eine PIN für Ihren Meetingroomfestlegen und sie nur mit jenen Personen teilen, die teilnehmen sollen. Zusätzlich können Sie die Vorteile der Click-to-Connect-Links für die Einladung von Teilnehmern (einschließlich nicht registrierter Benutzer) nutzen, um sie in Ihren virtuellen Konferenzraum einzuladen.

Wenn nicht authentifizierte Benutzer einer Besprechung beitreten, werden sie als Gäste in der Teilnehmerliste gekennzeichnet, damit alle anderen Teilnehmer wissen, dass sie keine sensiblen Themen diskutieren sollten. Jeder Benutzer kann außerdem den Hyperlink zu seinem persönlichen Meetingroom so oft ändern wie er möchte. Administrativ kann der PIN-Code auf drei bis zwölf Stellen konfiguriert werden.

Zusätzlich zum persönlichen virtuellen Besprechungsraum unterstützt Vidyo auch einen „Raum“ zur einmaligen Nutzung für anstehende Besprechungen. Wenn eine Besprechung geplant wird, erstellt Vidyo einen neuen Meetingroom mit einem eindeutigen Gästelink, einem PIN-Code und einer Meeting-ID. Solch ein einmalig angelegter Sitzungsraum beugt vor, dass es eventuell Absprachenkonflikte gibt, weil ein Raum für zwei verschiedene Sitzungen belegt wurde. Dies ist eine weitere Sicherheitsmaßnahme, um sensible Informationen besser zu kontrollieren und Besprechungen komfortabler zu gestalten. Als Initiator des Besprechungsraums sind Sie zugleich auch der Moderator. Damit stehen Ihnen bei einer Konferenz entsprechende Funktionen zur Verfügung. Dazu gehört die Möglichkeit, den Sitzungsraum zu sperren, um keine weiteren Teilnehmer zuzulassen. Sie können auch das Stummschalten steuern, ob ein Teilnehmer Audio- und Videodaten senden kann, oder eine Verbindung per Mausklick trennen. Auf Wunsch können Besprechungsräume auch mit einer Wartezimmer-Option konfiguriert werden. So können Sie verhindern, dass Teilnehmer einander sehen oder hören können, bis Sie als Moderator dazustoßen.

Vidyo
An Enghouse Company

VidyoConnect Hosting

Der VidyoConnect-Service nutzt erstklassiges Hosting, um ein hohes Maß an Sicherheit mit minimalen Ausfallzeiten zu kombinieren. Unser Hostingi st SOC-2-konform und besitzt einen 24/7-Schutz, um den gesetzlichen Bestimmungen zu entsprechen. Firewalls werden regelmäßig bewertet, konfiguriert und aktualisiert, um gegen Angriffe wirksam zu bleiben. Eine fortgeschrittene Filterung und fortschrittliche Routing-Techniken helfen zusätzlich beim Schutz vor Distributed Denial of Service (DDoS)-Angriffen. Zudem bieten Systeme zur Erkennung und zum Schutz vor Angreifern eine proaktive Netzwerküberwachung und -kontrolle. So bleibt die kritische Anwendungsumgebung sicher.

Vidyo weiß: Sicherheit zählt. Deshalb bewerten wir unsere Sicherheitsmaßnahmen regelmäßig, um mit der Dynamik beim Thema Datensicherheit Schritt zu halten. Vidyo hat verschiedene Sicherheitsstufen implementiert, um die Nutzer zu schützen. Zum Beispiel wird der Zugriff zur VidyoConnect-Cloud überwacht und kontrolliert, und die Audit-Protokolle werden von Vidyo über sechs Monate lang archiviert. Auch das Cloud-Management wird nur auf Subnetze und Sicherheitsgruppen von Vidyo beschränkt. Darüber hat nur das Team für den Vidyo-Betrieb auf einer Super-Admin-Ebene Zugriff. Autorisierte und qualifizierte Teammitglieder erhalten außerdem ein eigenes Konto für die Nachverfolgung und Auditunterstützung.

Die Modelle zur Sicherheitskontrolle von VidyoConnect decken die folgenden Bereiche ab:

Service

Der gesamte VidyoCloud-Traffic wird vom Server zum Client sowie von Server zum Server verschlüsselt

Applikation

Ständige Sicherheitsüberprüfung, Sicherheitsrichtlinie für den Software-Lebenszyklus, Release-Kontrollen usw.

Verwaltung

Kontrolle der Konfirguarationen und Rechtemanagements, Änderungsprüfung, Netzwerktrennung, Multi-Faktor-Authentifizierung usw.

Netzwerk

Firewalls, Sicherheitsgruppen, Anti-DDoS, Sicherheit Patches, Scans usw.

Trusted Computing

AgileCLOUD und AWS sowie physische Hardware beim Hosting-Setup

HR Sicherheit

Hintergrundüberprüfung, Arbeitsverträge (NDAs), Zugang auf Basis eines „need to have“-Servers

Physisch

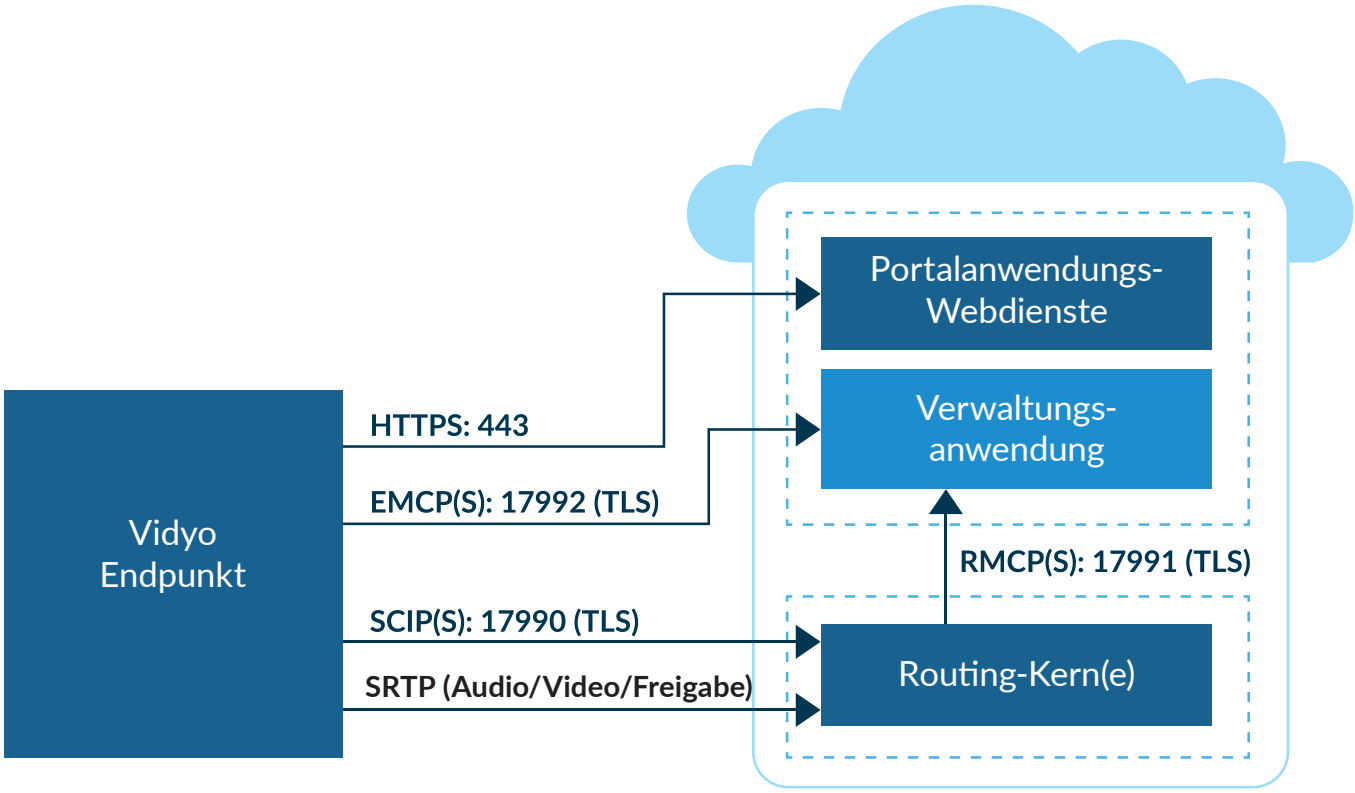
Sicherheit im Rechenzentrum (24/7-Überwachung), physische Zugangskontrolle, CCTV und Sicherheitsdienste

Vidyo
An Enghouse Company

Ablauf eines Anrufs bei VidyoConnect

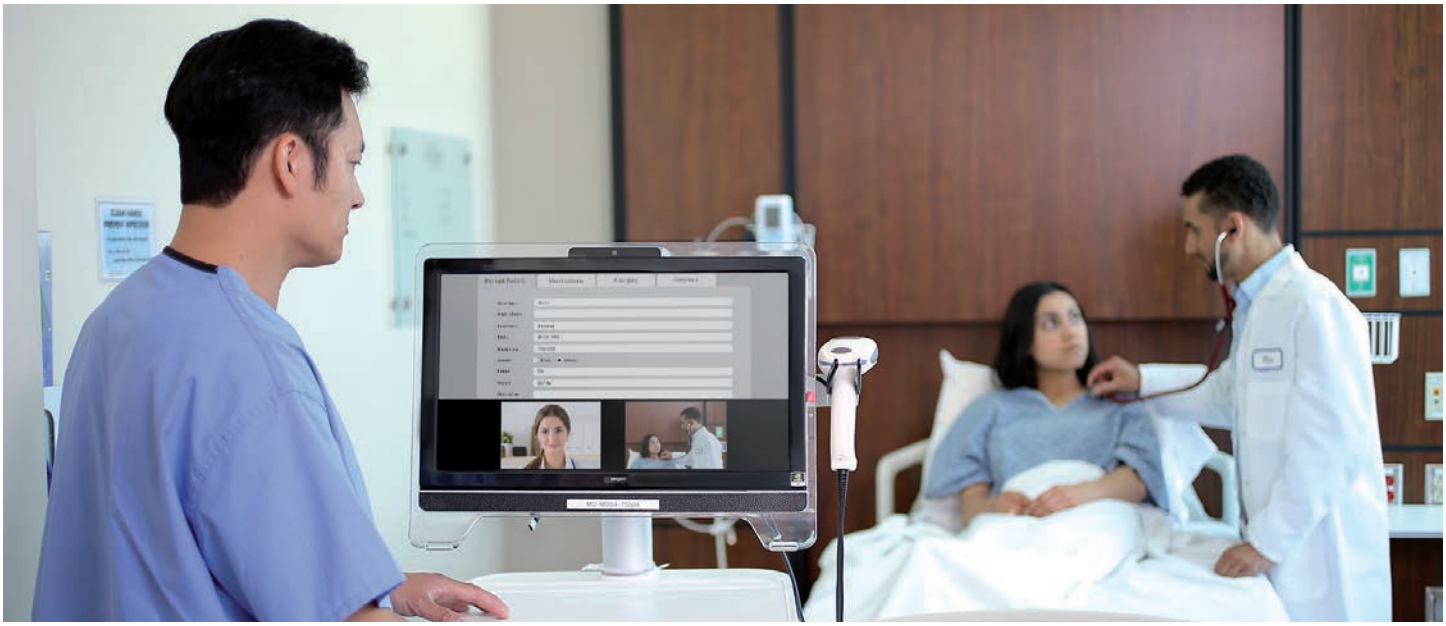
Ein verschlüsselter Vidyo-Anruf läuft in den folgenden Schritten ab:

1. HTTPS-Authentifizierung erfolgt vom Vidyo-Endpunkt bis zur Portalanwendung über TLS mit x509-Zertifikat.
2. Über die HTTPS-Verbindung wird eine EMCPS-Adresse einer Vidyo-Verwaltungsanwendung zur Verfügung gestellt.
3. Eine EMCPS TLS-Verbindung zur Vidyo-Verwaltungsanwendung wird auf Port 17992 mit einem x509 Zertifikat hergestellt.
4. Die SCIPS-Adresse wird über einen EMCPS-verschlüsselten Kanal an den Vidyo-Endpunkt gesendet.
5. SRTP-Schlüssel werden über die sichere SCIP-Verbindung ausgetauscht.
6. Der SRTP-Transport wird unter Verwendung von AES-128 eingerichtet, und für jede Verbindung werden eindeutige Schlüssel generiert.



Anmerkungen:

- HTTPS 443 - Sichere Verbindung mit Server-Zertifikat-Validierung, einschließlich SNI
- EMCP(S) mit TLS - Sichere Verbindung mit Server-Zertifikatsvalidierung, einschließlich SNI
- SCIP(S) mit TLS - Sichere Verbindung mit Server-Zertifikatsvalidierung, einschließlich SNI
- RMCP(S) mit TLS - Sichere Verbindung mit Server-Zertifikatsvalidierung, einschließlich SNI
- SRTP unter Verwendung von AES-128 mit Schlüsselaustausch über SCIP(S) über TLS-Verbindung (oben)
  - Jede SRTP-Verbindung erstellt eindeutige, periodisch gemäß dem SRTP-Standard aktualisierte Schlüssel.
  - Die Schlüssel verlassen den laufenden Prozess nicht.
  - Alle Medienpakete werden zwischen Clients und Servern verschlüsselt.



HIPAA und Vidyos Cloud-Dienste für Kunden aus dem Gesundheitswesen

Der Health Insurance Portability and Accountability Act (HIPAA) bietet Standards zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit geschützter Gesundheitsinformationen (Protected Health Information, PHI) einschließlich elektronischer geschützter Gesundheitsinformationen (Protected Health Information, ePHI). HIPAA bietet eine Orientierung für ein sinnvolles Schutzniveau für ePHI und ermöglicht zugleich den Leistungserbringern im Gesundheitswesen Zugang zu Informationen, die sie zur Erfüllung ihrer täglichen Aufgaben benötigen.

Es gibt viele Überlegungen, die ein Gesundheitsdienstleister oder ein vergleichbares Unternehmen (wie im HIPAA definiert) erfüllen muss, um den HIPAA-Richtlinien zu entsprechen. Die Vidyo Healthcare-Cloud-Angebote – und damit auch VidyoConnect und vidyo.io für das Gesundheitswesen – haben wir deshalb so konzipiert, dass Gesundheitsdienstleister und andere vergleichbare Organisationen bei ihrer Videokommunikation den HIPAA-Anforderungen entsprechen. Vidyo speichert keine PHI von Nutzern unserer Healthcare-Cloud-Dienste und greift auch nicht darauf zu. Doch entsprechend den Compliance-Bedarfen von Organsiationen wird Vidyo HIPAA-konforme Verträge für jene Kunden unterzeichnen, die eine Healthcare-Cloud anbieten.

Fazit

Die Kundenkommunikation und private Informationen zu sichern, ohne die Funktionen zur Kollaboration zu beschränken, hat für Vidyo höchste Priorität. Denn Vidyo bietet eine Plattform für eine videobasierte Zusammenarbeit, die Industriestandards entspricht und bewährte Technologien einsetzt, um den Datenschutz der Benutzer zu sichern. Das gelingt uns mit umfangreichen Security-Maßnahmen, die für jede Phase unseres VidyoConnect-Service entwickelt wurden, sowie kontinuierlicher Überwachung, Qualifizierung und gezielten Maßnahmen zur Bekämpfung neuer Sicherheitsbedrohungen.

Vidyo
An Enghouse Company

Häufig gestellte Fragen

1 Führt Vidyo Sicherheitsaudits für seine Vidyo-Lösungen durch?

Ja. Vidyo scannt seine Software vor der Veröffentlichung bis ins Detail und verwendet dabei zahlreiche Scanning-Tools von Drittanbietern, um Schwachstellen aufzudecken, die Software zu prüfen, zu bewerten und ihre Konformität zu gewährleisten. Zudem prüft ein externes SSL Labs Dienstprogramm die Software. Vidyo evaluiert kontinuierlich neue Tools, um sicherzustellen, dass die Systeme mit äußerster Sorgfalt getestet werden.

2 Was unternimmt Vidyo, um sicherzustellen, dass die Komponenten der VidyoConnect-Infrastruktur vor Hacker- und Virenangriffen geschützt sind?

Die VidyoConnect-Infrastrukturkomponenten sind Linux-basiert. Um den Hackerzugriff auf die Server zu verhindern, nutzt Vidyo die Security-Funktionen von Linux. Zugleich schließen wir auf dem Server alle nicht verwendeten Ports und Dienste und deaktivieren den Zugriff auf das System ohne gültige Administratorenrechte. Bei den Komponenten der Vidyo-Infrastruktur handelt es sich um gesperrte Anwendungen.
So wird nur Software eingesetzt, die für Vidyo validiert wurde, um zu verhindern, dass gefährliche Inhalte in das Netzwerk gelangen.

3 Wie überprüft Vidyo, ob die VidyoConnect-Komponenten von Drittanbietern auf dem neuesten Update-Stand sind?

Vidyo hat einen multidisziplinären Sicherheitsrat, der regelmäßig die neuesten Aktivitäten und eventuell damit verbundene Schwachstellen von Drittanbietern überwacht. Dieser Rat entscheidet auch, ob ein bestimmtes Sicherheitsupdate notwendig ist. Zu den überwachten Ressourcen gehören Apache, Ubuntu-Sicherheitshinweise, die NIST National Security Datenbank, MITRE und OWASP. Sicherheitspatches werden rechtzeitig herausgegeben und alle Patches werden im folgenden System-Release ausgeführt.

4 Welche Strategie verfolgt Vidyo bei Sicherheitsverletzungen im Code oder in Drittanbieter-Bibliotheken, die von Vidyo verwendet werden?

Wenn eine potentielle Sicherheitslücke identifiziert wird (sei es in Vidyo's Software oder in der Bibliothek eines Drittanbieters), bewertet unser Sicherheitsrat sofort die Relevanz, die Auswirkungen und den Schweregrad der Schwachstelle. Hält der Rat es für notwendig, werden eine oder beide der folgenden Maßnahmen ergriffen:

- Veröffentlichung einer Sicherheitsanweisung mit Schritten zur Eindämmung der Schwachstelle.
- Umsetzung eines Sicherheitsupdates, das die Schwachstelle dauerhaft behebt.

Vidyo
An Enghouse Company

5 Wie stellt Vidyo sicher, dass im Netzwerk keine Gesprächsdaten über einen „man-in-the-middle“ abgefangen werden können?

Der Endpunkt stellt über TLS mittels x509-Zertifikatsvalidierung eine vertrauenswürdige Verbindung zur Plattform her. Ausgehend davon werden alle nachfolgenden Verbindungen orchestriert. Jeder der nachfolgenden Kanäle (EMCPS und SCIPS) erstellt ebenfalls vertrauenswürdige Verbindungen mit x509-Zertifikat.

6 Welche Standards werden für die Medienverschlüsselung verwendet?

Vidyo verwendet die in SRTP RFC-3711 festgelegten Standards. Für jeden SRTP-Stream wird mit Hilfe des Vidyo Krypto-Kernels (FIPS 140-2 zertifiziert) ein eindeutiger Hauptschlüssel generiert. Dieser wird über eine sichere SCIPS (TLS)-Verbindung ausgetauscht. Gemäß dem SRTP-RFC wird ein Sitzungsschlüssel periodisch von beiden Seiten aktualisiert, sodass Angreifer keine Daten aus einzelnen Schlüsseln sammeln können.

7 Wie wird die Sicherheit für den H.323- und SIP-Verkehr gehandhabt?

VidyoConnect ermöglicht verschlüsselte Verbindungen von H.323- und SIP-basierten Endpunkten. Für H.323-Endpunkte können Anrufe mit H.235-Verschlüsselung getätigt werden. SIP-Endpunkte können TLS/SRTP verwenden, um die Signalisierung und die Medien zu verschlüsseln. VidyoCloud unterstützt beide Standards. Die Kunden-Endpunkte müssen für verschlüsselte Anrufe konfiguriert werden.

8 Wird die verschlüsselte Speicherung aufgezeichneter Videos unterstützt?

Ja, VidyoConnect verwendet einen verschlüsselten Speicher zur Archivierung der Aufzeichnungen (LUKS über LVM mit Chiffre: aes-cbc-essiv:sha256). Derzeit ist dies bei Bedarf nur auf Anfrage für ausgewählte Kunden verfügbar. Für Kunden aus dem Gesundheitswesen steht diese Möglichkeit leider nicht zur Verfügung. Allerdings können sich Kunden aus dem Gesundheitswesen (und andere) dafür entscheiden, VidyoReplayTM vor Ort zu implementieren und sich mit dem VidyoConnect-Dienst zu verbinden.

9 Welche physischen Sicherheitsmaßnahmen, Prozesse und Überwachungsmöglichkeiten im Hinblick auf unbefugten Zugang bietet Vidyo?

- 24/7 Sicherheitspersonal vor Ort und sichere Laderampen
- Biometrische Sperrmechanismen per Fingerabdruck
- Systeme mit Gewichtssensoren, um festzustellen, ob Ausrüstung aus der Einrichtung ausgeführt wird.
- 90-tägige Videoüberwachung mit Sicherheitskameras (nach Bedarf für einzelne Umgebungen verfügbar)
- Aufgezeichnete Protokolle, die festhalten, welche Personen die Umgebung betreten oder verlassen
- Passwortgeschützter Zugang sowohl zu physischen Standorten als auch zu Web-Portalen

10 Welche Dienstanbieter unterstützen das Cloud-Computing-Angebot und wo befinden sich Ihre Rechenzentren?

Die Dienste werden in Google Cloud, Internap oder AWS gehostet und von Vidyo betrieben. Wir verfügen derzeit über eine Vidyo-Infrastruktur in Kalifornien, Texas, New Jersey, London, Amsterdam, Frankfurt, Hongkong und Singapur.

Vidyo
An Enghouse Company

11 Wie sehen Policy und Verfahren rund um das Patch-Management aus?

Wir haben monatliche Wartungsfenster. Wenn jedoch ein schwerwiegendes Problem gefunden wird, kann ein zweckmäßigerer Patch angewendet werden.

12 Verfügt Vidyo über einen Plan zur Reaktion auf Sicherheitsvorfälle?

Selbst mit den in diesem Dokument beschriebenen Sicherheitsvorkehrungen ist kein Dienst vor Sicherheitsvorfällen 100%ig geschützt. Deshalb verfügt Vidyo über einen Plan, wie Teams auf Zwischenfälle zu reagieren haben. Alle Kunden werden über Vorfälle informiert, die ihre Dienste betreffen.

13 Wie sieht die Strategie hinsichtlich Backup und Disaster Recovery aus?

Jedes Portal verfügt über lokale Live-HA-Replikation & -Synchronisation. Stündlich erfolgt ein DR-Snapshot und die Wiederherstellung auf einer DR-Portalseite. Die Snapshots werden in stündlicher Taktung für die ersten 24 Stunden zentral gespeichert. Der letzte Snapshot eines Tages wird drei Wochen lang archiviert.

14 Wie und wie häufig wird die Infrastruktur für ein Backup und die Wiederherstellung getestet?

Wir loggen uns mindestens einmal pro Monat in das DR-Portal ein und führen ausführliche Tests durch, um die Gültigkeit und Funktionsfähigkeit der aktuell wiederhergestellten DB zu überprüfen. Zweimal pro Jahr wird außerdem ein vollständiger Failover-Test durchgeführt.

15 Unterhält Vidyo ein von der Industrie akzeptiertes Sicherheits-Framework?

Zusätzlich zum Hosting in sicheren Datenzentren, die SOC 2-Auditberichte zur Überprüfung zur Verfügung stellen, beauftragt Vidyo externe Beratungs- und Wirtschaftsprüfungsunternehmen mit der Bewertung nach den Richtlinien von SOC 2. Anschließend steht der Audit-Status unserer Dienstleistungen zur Verfügung – ähnlich wie die Berichte aus dem Data-Center SOC 2. Darüber hinaus nutzt Vidyo akkreditierte Drittfirmen für Stresstests, um unsere Produkte und Dienstleistungen zu beurteilen. Eine entsprechende Bescheinigung solcher Tests können unsere Assessment-Anbieter auf Anfrage zur Verfügung stellen.

16 Ist ein SOC 2-Bericht verfügbar?

Der SOC 2-Bericht ist auf Anfrage für Kunden erhältlich.

17 Ist VidyoCloud GDPR-konform?

Vidyo ist seit langer Zeit in der EU aktiv und erfüllt auch die entsprechenden Anforderungen der DSVGO.

Vidyo
An Enghouse Company

Ressourcen

Für weitere Informationen über Vidyo-Produkte und den VidyoConnect-Service, wenden Sie sich bitte an unser Sales Team.

Enghouse AG
Neumarkt 29-33
04109 Leipzig
+49 341 33975530
info.cee@enghouse.com

Vidyo
An Enghouse Company