CORDONIQ

7 Pitfalls of using WebRTC

At first glance, WebRTC appears to be a simple and straightforward way for developers to add video conferencing and collaboration to an existing product. But a closer look reveals that WebRTC often comes with more pitfalls than perks.

1

MYTH:
WebRTC is accessible (used) in a web browser

REALITY:
Browser compatibility issues are common and vary widely depending on the platform, operating system, or even device, especially when users are connecting with older phones or tablets. This results in an inconvenient and uneven user experience.

2

MYTH:
WebRTC functions simply with peer-to-peer communication OR WebRTC relies on simple connections

REALITY:
WebRTC runs into Firewalls, Network Address Translator (NAT), and router issues that add new layers of complexity that require additional infrastructure as well as resources to configure, maintain and update these systems.

3

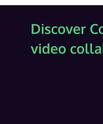
MYTH:
Adaptable and capable of wide functionality

REALITY:
Using WebRTC for any type of large-scale service needs a cloud backend, which means routing communications through a dedicated data center. Operating a cloud backend involves cloud computing resources, systems administration, and other resources to adequately scale a solution.

4

MYTH:
Setup involves adding simple components

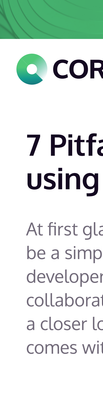
REALITY:
The process of adding WebRTC is more than simply introducing components to an interface. Controlling and managing the video experience requires significant integrations, creating APIs, and managing multiple integration points.



5

MYTH:
Video and audio quality are adaptable

REALITY:
WebRTC does not provide everything needed to handle scalable video encoding for synchronous communications. It cannot guarantee available bandwidth and processing power for users.
Video conferencing experiences in your product or application will be compromised and lower quality when users don't have sufficient bandwidth.



6

MYTH:
Uses secure encryption

REALITY:
There is no unified security model with WebRTC. Instead, security depends on the web browser's socket transport layer based on WebSockets, which means every platform and browser must be monitored. It's impossible to guarantee a secure environment for each meeting attendee because the security on each individual user device is unknown.

7

MYTH:
WebRTC is a free, open-source platform

REALITY:
Building and deploying a real time video service with WebRTC can quickly become an expensive proposition. The costs involved with properly configuring and integrating WebRTC components into an existing product are variable. Cloud computing, software engineering and other systems resources, modifications, and customizations are expensive and can escalate rapidly.

Avoid being dissatisfied with WebRTC.

Discover Cordoniq, the easy-to-implement, secure video collaboration experience that you control.

cordoniq.com