Kollective

Kollective Browser-Based Peering Solution

Scaling Live Video for Microsoft Teams and Stream

TECHNICAL BRIEF

This document is for IT administrators and other technical professionals who are evaluating Kollective as an enterprise content delivery network for video distribution. It describes technical aspects of the Kollective solution and addresses many of the questions raised regarding how it operates within an enterprise network environment. The document first outlines the benefits of the Kollective solution, then describes the installation requirements and footprint on the desktop, introduces its components and their interactions, and details its built-in security features.

Business Problem

The problems that arise from running live video events impacts many areas of the organization:

The Corporate Communication Challenge

- Challenging deadlines for live events
- Difficulty in achieving global reach – every office and employee
- Challenge meeting employee quality expectations
- Availability of real-time and historical analytics showing event success
- Visibility around content resonance

The Technical Challenge

- Challenging deadlines for live events
- Network impact of high bandwidth, high definition Live Events with many concurrent users
- The ability to measure the specific network impact of live events
- The constraints of security and compliance in achieving goals

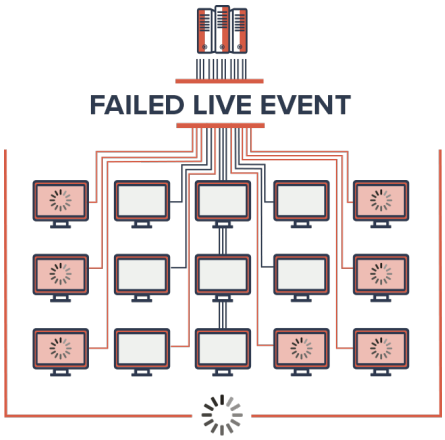
Kollective Solution Overview

Microsoft's collaboration suite enables simple communication within organizations that can scale to 1000s of users for live or on-demand content. Live video events in Microsoft Teams and Stream offer a seamless, easy to engage solution with no hurdles for your IT teams or employees. Kollective's browser-based peering solution scales these communications across your network, allowing you to achieve 100% delivery at a fraction of the bandwidth. With the Kollective platform you achieve the following benefits:

- No requirement to add hardware or increase bandwidth.
- Self-service integration of the Kollective platform with Microsoft Teams and Stream through a flexible Cloud architecture and browser-based delivery model for easy testing and deployment of live video across your enterprise.
- Utilize innovative peering technology to reduce the bandwidth required to deliver a high-quality Microsoft Teams/Stream

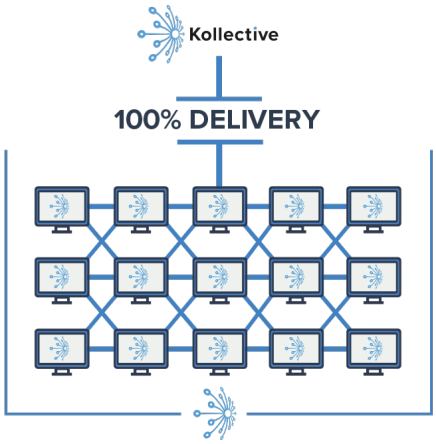
viewing experience to every user.

- All network topologies are supported, including wireless, VPN, and MPLS and there is no significant incremental load on machine resources beyond what is required to render video.
- Real-time analytics provide feedback about content consumption and user-experience with visibility into associated network usage, from which informed decisions can be made.



WITHOUT KOLLECTIVE

Many user's connecting simultaneously to live events saturate enterprise networks resulting in poor user experience.



WITH KOLLECTIVE

Kollective's Browser-Based Peering solution reduces bandwidth requirements by distributing the content within the network.

On-boarding

Kollective provides a self-service portal at **https://portal.kollective.app** that includes all the required configuration and instructions to enable the solution within the customer Teams and Stream environment. By applying the configuration into the Office 365 administration console this enables the Kollective platform within the customer environment. Once enabled, no further action is required.

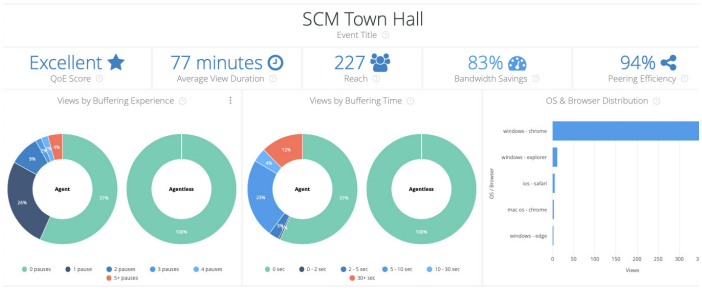
User-Experience

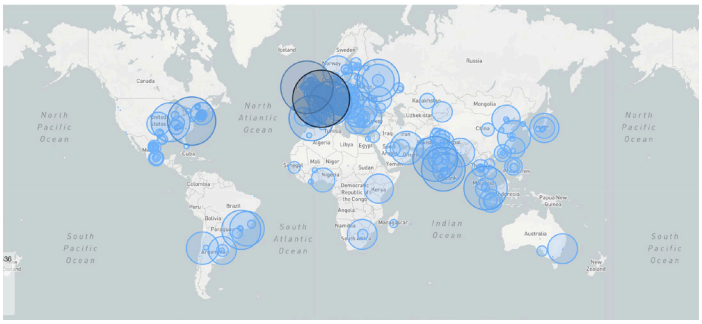
Kollective's Browser-Based Peering solution is designed to be transparent to users and simple to install by technical stakeholders. The browser-based delivery solution is built on standard web technologies already approved in the enterprise with the Microsoft Teams client and WebRTC enabled browsers. If users are running legacy browsers or unable to peer, content will be sourced directly from the Azure CDN.

Intelligence & Insights

Kollective IQ provides real-time business intelligence and insights for live events using pre-configured and customizable dashboards. These provide the key stakeholder metrics for live events including reach, quality of experience, user experience and network distribution to provide a rounded view of your communications events. Kollective IQ provides trend and drill-down functionality allowing you to perform trend analysis and additionally get into the details of individual events for deep analysis down to user level.

Kollective

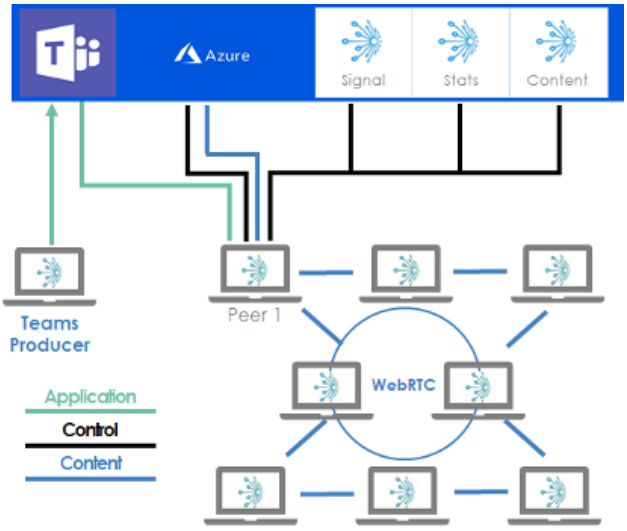




Technology Architecture

Kollective operates a cloud-native architect built on the following standards:

- Global, low-latency architecture
- High availability and fault tolerant built in Microsoft Azure
- CloudFlare global network security and reliability
- Automatic and elastic scaling
- Regional failover
- External monitoring of all core services
- Advanced telemetry of all systems and proactive alerting



Operation

Functionality is implemented at the edge to support peer-to-peer delivery utilizing a javascript SDK plugin which is the integration point for Teams, Stream or other integrated platforms. As an example, the plugin is activated on the initial Teams Live Event connection and automatically enables Kollective delivery within the Teams client or browser; no pre-installed software is required. The plugin incorporates the following stages:

Publishing

- The administrative integration enables event publishing within the Kollective cloud to enable peer-to-peer distribution of content. Within Microsoft Teams this is a server-side publish, cloud-to-cloud whereas Microsoft Stream utilizes the SDK via the first user.

Peering

- Registration: The process by which every node communicates with the cloud to determine which peering cluster the node belongs to, and at which tier the node sits within a peer cluster. As peers join the cluster, they automatically order themselves into an optimum configuration for content delivery.
- Peering Protocol: Each peering node communicates with other nodes to determine and request the required data from the available peers. WebRTC is used as the communication channel.

- WebRTC: WebRTC is supported natively by the Teams client or compatible browser. Kollective leverages this capability to enable a communication channel between peers using the WebRTC data channel as the transport mechanism.
- Ingest: The first user in the mesh will source content directly from the Azure CDN.
- Adaptability: Peers can join or leave the mesh without impact to other users. If a peer leaves the mesh, others will simply adapt and reposition themselves within the mesh, all without impact to the user experience of other viewers.

Telemetry

- The plugin reports in near realtime on viewership with user and network performance metrics.

Cloud Services

When a user connects to a live event, background connectivity to the Kollective cloud enables the efficiencies of Kollective Browser-Based Peering:

- signal.kollective.app, (HTTPS): provides the registration process including information about available peers.
- cdn.kollective.app, (HTTPS): hosts the browser plugin.
- stats.kollective.app, (HTTPS): used by the player to send telemetry to Kollective IQ analytics.
- content.kollective.app, (HTTPS): provides content metadata and authentication controls to ensure the user is authorized to receive the requested content.
- Peer communication, (WebRTC): used as the transport network between user machines.

Security

Secure by Design

The Kollective solution is Secure by Design, architected using standard web-based protocols with all data transfers encrypted and signed:

- TLS 1.2 with authenticated tokens is used for communication to cloud services.
- Communication between peers uses WebRTC (DTLS/SCTP).
- All communications between peers and cloud services are encrypted and signed.
- Kollective traffic is firewall and web-proxy compatible without additional configuration required.
- Integration with Microsoft Teams and Stream is implemented securely using a standard JSON Web Token mechanism to ensure that only authorized users have access to the requested data.
- The Kollective platform is multi-tenant environment with logical isolation of customer data. Access to other tenant is not possible.
- All application code is scanned for vulnerabilities through several industry standard best practices and third-party auditing tools.
- All application code is independently verified prior to deployment in a production environment.
- Penetration scans are run weekly with additional ongoing vulnerability detection using automated tools.

Data Compliance

Kollective are hosted within Microsoft Azure and automatically inherit certifications of the Azure cloud such as ISO27001, refer to **https://azure.microsoft.com** for details.

Kollective have the following certifications with regards to security and data compliance:

- SOC 2 Type II Service Organization Control for Data Security
- US/EU and US/Swiss Privacy Shield
- TrustArc TRUSTe Privacy Shield Verified - **https://privacy.truste.com/privacy-seal/validation?rid=55d03d19-f9a1-4f4a-b082-0e6a2f5753cd**
- GDPR Compliant - **https://kollective.com/wp-content/uploads/2018/08/Controller-Processor-Addendum_8-6.pdf**

Additional details can be found in the Kollective privacy policy at **https://kollective.com/privacy-policy**.

Frequently Asked Questions

Application FAQ

What is the difference between Browser-Based Peering and Kollective Agent Based Peering?

Both solutions provide efficient delivery of content however Kollective Browser-Based Peering supports live events only. An agent-based approach can support additional use cases including software-deployment, video-on-demand and full end-to-end large scale network readiness testing.

Which browsers are supported?

- Microsoft Teams Client – Windows, Mac
- Windows – Microsoft Edge (Chromium), Chrome (79+), Firefox (72+)
- Mac – Safari (12+), Chrome (79+), Firefox (72+)
- Tablet – Safari (13.2+), Chrome Android (79+), Firefox Android (68+)
- Mobile – Chrome Android (79+), Firefox Android (68+)

What is the expected time to first frame (start time) for users viewing for a live event?

Typically 2-5 seconds, comparable to a native connection that does not use an ECDN.

What are the common ports and protocols?

The solution uses HTTPS for all transfers of data and control information.

Does the platform support IPv6?

Yes.

What happens if a user can't communicate with other peers?

The machine will fall back to the CDN to retrieve content.

How does the Browser-Based Peering interoperate with Microsoft Adaptive Bitrate control?

Kollective natively supports the Microsoft ABR model.

How can the event delivery be validated and understood?

The customer portal provides near realtime analytics to display key metrics including bandwidth savings, peering efficiencies etc.

Kollective

Deployment FAQ

What are the configuration pre-requisites to enable the Kollective platform?

Kollective provides a self-service portal at **https://portal.kollective.app** that provisions the required configuration with detailed instructions for integration within Microsoft Teams and Stream.

What firewall or proxy changes are required in my environment?

No specific firewall or proxy changes are required. All communication with Kollective uses HTTPS which is typically enabled by default.

Does Kollective support the use of WebRTC mDNS anonymisation?

Yes, however we recommend disabling anonymization of local IP address for the purposes of reporting and location-based tuning although this is not a specific requirement.

Do I need to install an agent or any other software?

No.

How can I test the platform?

A demonstration and self-service integration for Microsoft Teams and Stream is available at **https://portal.kollective.app**.

I have an existing Microsoft ExpressRoute connection, can this be utilised to optimize traffic flow?

The Microsoft Teams and Stream content is sourced directly from the Microsoft Azure CDN and therefore whichever path you have configured for this source will be utilised by Kollective without any additional configuration.

Security FAQ

What is being sent to the cloud?

The only data sent to the Kollective platform is private IP address, public IP address, session ID, external ID, transfers, peering, buffering, time, connects, bytes. Data is sent using standard HTTPS and is encrypted at rest.

What is being downloaded to the browser?

The javascript plugin in which peering is implemented is downloaded from **cdn.kollective.app** using secure protocols. It is approximately 600kb in size and once downloaded is stored in the browser cache for future use until the cache is refreshed or the peer mesh client is upgraded.

How does this interact with my endpoint security or other agents including anti-virus?

The peer solution operates within the Microsoft Teams client or compliant browser and therefore does not typically interact with endpoint security.

How is content secured from unauthorized access?

The authorization mechanism is implemented within the Microsoft Teams or Stream application and shared with the ECDN using JSON web tokens.

Does Kollective have access to my content?

No, the encrypted content is sourced directly by the CDN. Kollective do not have access, nor are we able to decrypt.

How is the peering secured?

The protocol itself is built on top of trusted and well-defined network protocols including DTLS/SCTP for secure connections between nodes, and TLS with authenticated tokens for connections to cloud services.

How does the solution operate in the presence of a zero trust (desktop isolation) network?

An exception will be required to allow peer-to-peer communication if restrictions are in place that prohibit node-to-node connectivity.

Operational FAQ

Who has access to my data?

Kollective operational personnel manage the Kollective platform inline with the procedures defined within the SOC2 certification process and privacy policy. Kollective do not have access to the customer content.