Zoom Video Konferans Uygulaması Üzerine
Bilgi Notu

Zoom Kimdir?

Zoom Video Communications, halen şirketin Genel Müdürlüğünü yapan Eric Yuan tarafından 2011 yılında kuruldu. Şirketin merkezi San Jose, Kaliforniya, ABD'de olup 2019 yılı sonu itibarı ile 1.958 çalışanı vardır.

Zoom Nedir?

Zoom, küresel olarak insanların etkileşim biçimlerini temelden değiştiren, video öncelikli bir iletişim platformudur.

Farklı cihazlardan ve konumlardan bireylere ve şirketlere kolay bir video, ses, sohbet ve içerik paylaşımı ile tek bir toplantıda yüz yüze video görüşmesine (Video Konferans) olanak sağlayan bulut tabanlı bir platformdur. Kullanımı, yönetimi ve dağıtımı kolay ve ölçeklenebilir bir uygulamadır. Bulut tabanlı platform, olanak tanır ve binlerce kullanıcıyı farklı cihazlarda ve konumlarda tek bir toplantıda birbirine bağlar ve yüz yüze video görüşme olanağı sağlamaktadır.

Zoom özellikle toplantı ve eğitim gibi faaliyetlerin lokasyondan bağımsız olarak, farklı tür cihazlarla (*Windows, Mac, Android, iOS vb.*) internet üzerinden yapılmasına olanak kılmaktadır.

Zoom Kullanımı?

Günlük toplantı katılımcıları için Aralık ayında günlük 10 milyon olan Zoom uygulaması, koronavirüs salgınının bütün dünyada milyonlarca insanı evde kalmaya zorlaması ile birlikte birkaç ay içinde birden seçim uzaktan eğitim ve toplantılar için hazır bir seçenek sundu. Platformunda günlük (*ücretli-ücretsiz*) katılımcı sayısı birden 200 milyona yükseldi.

Türkiye'de Milli Eğitim Bakanlığı ve özel okullar, dünyanın diğer bölgelerinde olduğu gibi uzaktan eğitim için Zoom altyapısını kullanmaya başladı. Benzer biçimde, çoğu üniversiteler için de uzaktan eğitimde hazır altyapı olarak Zoom hızlı ve ekonomik bir seçenek oldu. Ayrıca, şirketler ve STK'lar ile bireyler için de kolay ve çok düşük maliyetli (*40 dakikalık sınırlama ile maliyetsiz*) uygulama olarak Zoom'u kullanmaya başladı.

Bu yaygın kullanım Zoom'un uygulama **açıklarını ve gizlilik risklerini** de ortaya çıkartmıştır.

Zoom Hizmet Koşulları?

Zoom uygulaması için sitesinde yer alan Hizmet Koşulları;

15. ***GARANTİ YOK.*** *SİZ, HİZMETLERİN "OLDUĞU GİBİ" SUNULDUĞUNU VE ZOOM, İŞTİRAKLERİ, TEDARİKÇİLERİ VE SATICILARININ, İFADE VEYA İMA EDİLMİŞ, HERHANGİ BİR GARANTİYİ KABUL ETMEDİKLERİNİ ANLAYIP KABUL EDİYORSUNUZ. ZOOM, İŞTİRAKLERİ VE TEDARİKÇİLERİ HİZMETLERİN KULLANILMASINDAN, HİZMETLERİN KULLANIM SONUÇLARININ, HİZMETLERİN VEYA BUNLARA UYGUN OLAN HERHANGİ BİR BİLGİNİN DOĞRULUĞU VEYA GÜVENİLİRLİĞİ, KESİNTİSİZ, ZAMANINDA, GÜVENLİ VEYA HATASIZ OLACAĞI İLE İLGİLİ HİÇBİR GARANTİ VERMEZ. HİZMETLERİN KULLANIMININ SORUMLULUĞU VE RİSKİ SİZE AİTTİR. HİZMETLERİN KULLANIMI SIRASINDA ALINAN HERHANGİ BİR MALZEME VE/VEYA İNDİRİLEN VERİ VEYA DİĞER HİZMETLERİN KULLANIMINDAN KAYNAKLANAN HERHANGİ BİR HASAR İÇİN SADECE SORUMLU OLACAKSINIZ. HİZMETLERİN KULLANIMINDAN VEYA PERFORMANSINDAN KAYNAKLANAN TÜM RİSK SİZE AİTTİR. ZOOM, KULLANICI BİLGİLERİNİN VEYA KULLANICILARIN İLETİŞİMİNİN MUHAFAZA EDİLMESİ İÇİN HERHANGİ BİR SORUMLULUK ÜSTLENMEZ. ZOOM, HİZMETLERİN KULLANIMINA YÖNELİK ÖZEL BİR SONUÇ İÇİN HERHANGİ BİR SÖZ VERMEZ VE GARANTİ VEREMEZ. KULLANIM KENDİ RİSKİNİZDEDİR.*

Zoom Hizmet Koşulları'na göre **uygulamanın kullanılmasından kaynaklanacak her türlü risk kullanıcı sorumluluğundadı**r.

Zoom Mahremiyet Politikası'nda;

> *Zoom, hizmetlerimizi sağlamanın bir parçası olarak herhangi bir nedenle müşteri içeriğini izlemez veya kullanmaz. Zoom müşteri içeriğini kimseye satmaz veya herhangi bir reklam amacıyla kullanmaz.*

açıklamaları yer almaktadır. Ayrıca;

> ***Avrupa Birliği (AB), İngiltere, Lichtenstein, Norveç, İzlanda veya İsviçre sakinleri***
>
> *Avrupa Birliği (AB), İngiltere, Lichtenstein, Norveç, İzlanda veya İsviçre'de yaşıyorsanız, AB'nin Genel Veri Koruma Yönetmeliği (GDPR) altında belirtilenler de dâhil olmak üzere kişisel verilerinizle ilgili yasal haklarınız olabilir.*
>
> *GDPR, verilerinizi işlemek için bir "temel" oluşturmamızı gerektirir. Kişisel verilerinizi (i) (varsa) rızanızla, (ii) bir müşteriyle sözleşme yapmak ve (iii) diğer meşru menfaatler ve ticari amaçlar için işliyoruz.*
>
> ***AB-ABD Gizlilik Kalkanı ve İsviçre-ABD Gizlilik Kalkanı***
>
> *Zoom Video Communication, Inc., AB-ABD Gizlilik Kalkanı Çerçevesi ve İsviçre-ABD Gizlilik Kalkanı'na katılmakta ve onun uyumluluğunu belgelemektedir. Zoom, AB üyesi ülkeler, İsviçre ve Birleşik Krallık'tan alınan tüm kişisel verileri, Gizlilik Kalkanı Çerçevelerine dayanarak Çerçevenin geçerli İlkelerine tabi tutmayı taahhüt eder. Gizlilik Kalkanı Çerçeveleri hakkında daha fazla bilgi edinmek ve sertifikamızı görüntülemek için ABD Ticaret Bakanlığı'nın Gizlilik Kalkanı Listesi'ni ziyaret edin.*
>
> *Zoom, Gizlilik Kalkanı Çerçevesi kapsamında aldığı kişisel verilerin işlenmesinden sorumludur ve daha sonra kendi adına bir temsilci olarak hareket eden üçüncü bir tarafa aktarır. Zoom, AB, İsviçre ve Birleşik Krallık'tan kişisel transfer yükümlülükleri de dâhil olmak üzere tüm kişisel veri aktarımları için Gizlilik Kalkanı İlkeleri'ne uygundur.*
>
> *Gizlilik Kalkanı Çerçeveleri uyarınca alınan veya aktarılan kişisel verilerle ilgili olarak Zoom, ABD Federal Ticaret Komisyonu'nun düzenleyici güçlerine tabidir. Bazı durumlarda Zoom'un kamu yetkililerinin geçerli ve yasal taleplerine yanıt olarak veya kolluk kuvvetlerinden gelen talepler doğrultusunda kişisel verileri ifşa etmesi gerekebilir.*

Zoom GDPR tarafından öngörülen temel ilkelere uyduğunu ifade etmektedir. Ancak, KVKK açısından her hangi bir sorumluluk veya yükümlülük ifadeleri yer almamaktadır.

KVK Kurumunun Görüşleri?

KVK Kurulu 07.04.2020 tarihinde "*Uzaktan Eğitim Platformları Hakkında Kamuoyu Duyurusu*" başlıklı aşağıdaki duyuruyu yapmıştır.

> *Uzaktan eğitim platformlarında, öğrencilerin ad ve soyadları gibi kişisel verileri ile ses ve görüntü gibi biyometrik veri kapsamında değerlendirilebilecek bazı özel nitelikli kişisel verilerinin işlendiği görülmektedir. …*
>
> *Bununla birlikte uzaktan eğitim amacıyla kullanılan yazılımların birçoğunun bulut hizmet sağlayıcılar aracılığıyla hizmet verdiği ve bu yazılımlara ait veri merkezlerinin çoğunlukla **yurt dışında olduğu** gözlemlenmektedir. Veri merkezleri yurtdışında olan platformların kullanılması durumunda **yurtdışına veri aktarımı söz konusu olacağından**, Kişisel Verilerin Korunması Kanununun **9 uncu maddesinde belirtilen şartlara uygun olmayan aktarımların Kanunun ihlali anlamına gelebileceği** unutulmamalıdır.*
>
> *Bu bağlamda, uzaktan eğitim hizmeti amacıyla kullanılan bu platformların gerekli veri güvenlik tedbirlerini alıp almadıkları ile ilgili Kişisel Verileri Koruma Kurulu tarafından hazırlanan "Kişisel Veri Güvenliği Rehberi (İdari ve Teknik Tedbirler) ile Kişisel Verileri Koruma Kurulunun 31/01/2018 tarihli ve 2018/10 sayılı "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" Kararı göz önünde bulundurulmalıdır.*

Zoom Kullanmanın Riskleri?

Koronavirüs salgını ile başlayan izolasyon / karantina / sokağa çıkma yasakları bu süreçte Zoom uygulamasının kullanımında bir patlamaya yol açmış, bu yaygın kullanım ise Zoom'un uygulama **açıklarını ve gizlilik risklerini** ortaya çıkartmıştır.

Bu güvenlik açıklarının yol açtığı riske "**Zoombombing**" adı takılmıştır. Zoombombing; "*davetsiz katılımcıların nefret dolu veya pornografik içeriklerle toplantılara/eğitimlere girmesi ve bu toplantı/eğitim oturumlarını bozması*" eylemidir.

Zoom'a özel bir diğer siber saldırı da "**Zoomraids**" olarak adlandırılmıştır. Davetsiz misafirlerin özel toplantı katılımcılarını taciz ettiği ve kötüye kullandığı koordine "*toplu Zoombombing*" eylemi için "**Zoomraids**" terimi kullanılmaya başlanmıştır.

Son 2 ayda açıklanan güvenlik açık ve riskleri ilgili gelişmeler aşağıda sıralanmıştır;

26 Mart Zoom'un iOS uygulamasının, Facebook hesabı olmayan Zoom kullanıcıları için bile Facebook'un Grafik API'sı ile etkileşimi yoluyla Facebook'a kullanıcı analizi verileri gönderdiği ortaya çıktı.

30 Mart Zoom çağrı verilerinin belirtildiği gibi uçtan uca şifreleme olmadan şirkete geri gönderildiği fark edildi.

Kullanıcıları parola hırsızlığına uğratan Windows ile ilgili bir Zoom hatası bulundu.

Kötü niyetli kişilerin Zoom kullanıcı mikrofonu veya web kamerasının kontrolünü ele geçirmesine izin verebilecek iki hata daha keşfedildi.

Zoom'un en iyi riskli erişim düzeyi olan MacOS masaüstlerinde root erişimi sağlamasına izin verdi.

Zoom'un Kaliforniya'dan yeni veri koruma yasasını, Zoom verilerinin Facebook'a aktarılması konusunda kullanıcılardan uygun bir onay alamamak suretiyle ihlal ettiği iddiasıyla ilk grup davası açıldı.

Bilgisayar korsanları bir sınıf toplantısına girdi ve öğrencilerin ekranlarında gamalı haç görüntüledi.

FBI "**Zoombombing**" vakaları üzerine Zoom'un güvenlik açıkları hakkında genel bir uyarıda bulundu.

1 Nisan Zoom uygulamasının bir şirketin dizini olarak çalışmak için gevşek bir şekilde tasarlanmış bir özellik aracılığıyla kullanıcıların e-posta adreslerini ve fotoğraflarını yabancılara sızdırdığı bulundu.

Zoom CEO'su Yuan özür diledi;

Yuan herkese açık bir özür yayınladı ve güvenliği artırmaya söz verdi. Tüm çağrılar için bekleme odaları ve şifre korumasını getirildi. Ayrıca şirketin 90 gün içinde güvenlik sorunlarını gidermek için özellik güncellemelerini donduracağını söyledi.

2 Nisan Güvenlik araştırmacıları, otomatik bir aracın bir saat içinde yaklaşık 100 Zoom toplantı kimliği bulabildiğini ve tek bir tarama gününde yaklaşık 2.400 Zoom toplantısı için bilgi topladığını açıkladı.

Zoom'un veri madenciliği özelliği ile bazı katılımcıların gizlice erişmesine ve diğer kullanıcılar hakkında profil verilerini toplayabilmesine izin verdiğini keşfedildi.

3 Nisan Zoom görüntülü aramalara ait binlerce kaydın korumasız bırakıldığı ve açık webde görüntülenebildiği ortaya çıkartıldı. Korumasız çağrıların büyük bir kısmı, özel terapi seansları, telesağlık eğitim çağrıları, özel şirket finansal tablolarını tartışan küçük işletme toplantılarının ve öğrenci bilgilerinin açığa çıktığı ilkokul sınıfları gibi kişisel olarak tanımlanabilir bilgilerin tartışılmasını içeriyordu.

Zoom, özel şifrelemesinin (*AES-256 şifrelemesi yerine daha az güvenli bir AES-128 anahtarı*) standart dışı olduğunu kabul etti.

Tycko ve Zavareei LLP, kullanıcıların kişisel bilgilerini Facebook ile paylaştığı için Zoom'a karşı ikinci grup davasını açtılar.

ABD'li bir senatör Zoom'dan şirketin gizlilik uygulamalarıyla ilgili endişelerini ve sorularını dile getiren bir mektup göndererek 10 Nisan'a kadar bir yanıt istedi.

5 Nisan Bazı toplantılara yanlışlıkla beyaz listeye eklenen Çin'deki sunuculara bağlanma izni verildiği söylendi.

6 Nisan Siber güvenlik firması Sixgill, popüler bir karanlık web forumunda bir korsanın ele geçirdiği 352 Zoom hesabına bir bağlantı gönderdiğini açıkladı.

Bu bağlantıların e-posta adreslerini, şifrelerini, toplantı kimliklerini, ana bilgisayar anahtarlarını ve adlarını ve Zoom hesabı türünü içerdiği belirtildi.

ABD Elektronik Gizlilik Bilgi Merkezi Federal Ticaret Komisyonu'nu Zoom'u araştırmaya ve video konferans platformları için gizlilik yönergelerini yayınlamaya çağırdı.

8 Nisan Zoom hissedarı Michael Drieu şirketi "*yetersiz veri gizliliği ve güvenlik önlemleri*" ile suçlayarak şirkete karşı dava açtı.

Sanal bekleme odalarını etkinleştirmek ve sınıfta içerik paylaşabilen sadece öğretmenlerin olmasını sağlamak için K-12 programına kaydolan eğitim kullanıcılarının varsayılan ayarları değiştirildi.

Zoom, güvenliği artırmaya yönelik güncelleme ile toplantı kimliğini başlık çubuğundan kaldıracağını açıkladı.

13 Nisan Siber güvenlik istihbarat şirketi Cyble, karanlık web ve korsan (*hacker*) forumlarında 500.000'den fazla Zoom hesabının satıldığını keşfetti.

14 Nisan Kaliforniya'da Facebook ve LinkedIn aleyhine açılan yeni bir davada, iki şirketin Zoom kullanıcılarının kişisel verilerini "*dinlendiğini*" iddia edildi.

Zoom, 18 Nisan başlayarak tüm ödeme yapan abonelerin olacak kullandıkları istediği bölgesel sunucuyu seçmesinin mümkün olacağını belirtti. Bu hareket, Citizen Lab tarafından Zoom arama trafiğinin Çin sunucuları üzerinden yönlendirildiğini ve Çin hükümetinin şifreleme anahtarları alma yeteneğine dayanarak gizlilik kaygılarına yol açtığını tespit eden bir soruşturmanın ardından geldi.

15 Nisan Bilgisayar korsanları birinin Windows ve diğeri MacOS için olmak üzere iki kritik istismar keşfetti. Windows'a özgü güvenlik açığı, endüstriyel casusluk için uygun olduğu bildirilen istismar türüdür ve yeraltı pazarında 500.000 $'a satılmaktadır.

16 Nisan Bir güvenlik araştırmacısı tarafından daha önce güvenli olmayan bir bağlantı yoluyla buluta kaydedilmiş bir şirketin videolarına erişmenin ve indirmenin bir yolunu buldu.

Araştırmacı ayrıca önceden kaydedilmiş kullanıcı videolarının, kullanıcı tarafından silindikten sonra bile saatlerce bulutta kalabileceğini keşfetti.

Uzun vadeli güvenlik iyileştirmesinin bir parçası olarak Zoom, Perşembe günü Luta Security'yi işe aldığını ve hata ödül programını yenileyerek beyaz korsanların güvenlik kusurlarını aramasına yardımcı olacağını açıkladı.

Ülkeler ve Şirketler Tarafından Alınan Tedbirler?

Zoom'un kullanımı aşamasında gündeme gelen önemli güvenlik açıkları ve bu açıkların yol açtığı risklerden dolayı çeşitli ülke ve şirketler Zoom kullanımına bazı kısıtlar getirirken, bazıları da tamamen yasaklama yoluna gittiler;

1 Nisan **SpaceX** roket şirketi, "*önemli gizlilik ve güvenlik endişeleri*"ni belirterek çalışanların Zoom'u kullanmalarını **yasakladı.**

6 Nisan **New York Eğitim Bakanlığı**, okullarda Zoom kullanımını **yasakladı.**

ABD Elektronik Gizlilik Bilgi Merkezi, Federal Ticaret Komisyonu'nu (FTC) Zoom'u araştırmaya ve video konferans platformları için gizlilik yönergelerini yayınlamaya çağırdı.

*T.C. Milli Eğitim Bakanı, **EBA dışındaki programlara** öğretmenleri zorlayan eğitim yöneticilerinin takibe alınacağını söyledi.*

7 Nisan **Tayvan**, hükümetin Zoom'u kullanmasını **yasakladı.**

8 Nisan **Google**, çalışanların şirkete ait cihazlarında Zoom kullanımını **yasakladı.**

9 Nisan ABD Senatosu senatörlerin alternatif bir platform kullanmalarını istendi.

Singapur Eğitim Bakanlığı, uzaktan eğitimde Zoom kullanımını **yasakladı.**

Alman hükümeti Zoom kullanımını **yasakladı.**

Zoom Kullanırken Alınması Önerilen Tedbirler?

Zoom eğitim/toplantı oturumu başlamadan önce, olası davetsiz misafirler için bazı tedbirler alınabilir:[1]

1) Tüm toplantılarda Kişisel Toplantı Kimliğini kullanılmamalıdır. Bunun yerine, tek bir toplantıya özel kimlik kullanın. Zoom'un destek sayfasında, ek güvenlik için rasgele bir toplantı kimliği oluşturmak ile ilgili bir video bulunmaktadır.
2) Erişime izin verilmeden önce kimlerin toplantıya katılmaya çalıştığını görmek için "**Bekleme Odası**" özelliği etkinleştirilmelidir.

   Bekleme Odası özelliğini etkinleştirmek için; **Hesap Yönetimi** > **Hesap Ayarları**'na gidilip, **Toplantı** seçilmeli ve ardından **Bekleme Odası** ayarı etkinleştirilmelidir.
3) Başkalarının **Ana Bilgisayardan Önce Katılma** yeteneği dâhil diğer seçenekler devre dışı bırakılmalıdır.

   Ardından, katılımcıların ekran paylaşımı ve ayrıca uzaktan kumanda işlevi devre dışı bırakılmalıdır.

   Son olarak, tüm dosya aktarımları, ek açıklamalar ve sohbetler için **otomatik kaydetme** özelliği devre dışı bırakılmalıdır.
4) Toplantı başladıktan ve ilgililer katıldıktan sonra, toplantı dışarıdaki kişilerin katılımının engellenmesi için kilitlenmelidir.

Bütün dikkat ve özene rağmen, bir bilgisayar korsanının Zoom eğitim/toplantı oturumuna yönelik olası "Zoombombing" girişiminde ise aşağıdakiler yapılmalıdır.

1) Gezinme çubuğunda **Katılımcılar Listesi** gidilerek **Daha** seçeneği tıklatılmalı ve başka katılımcıların eğitim veya toplantı oturumuna katılmalarını ve bazı katılımcıları kaldırabilmek için **Toplantıyı Kilitle** seçilmelidir.
2) **Katılımcılar Listesi**'nden -istenirse- toplantıya yardımcılık yapacak bir katılımcı belirlenerek, **Herkesi Sustur** seçeneği tıklanır. Bu, istenmeyen katılımcının mikrofonu kullanarak toplantıyı bozacak girişimlerde bulunmasını engeller.

Zoom'a Alternatif Video Konferans Uygulamaları?

Uzaktan eğitim ve toplantılara yönelik tek çözüm Zoom değildir. Zoom uygulamasına alternatif özel veya açık kaynak kodlu, ücretli veya ücretsiz oldukça fazla video konferans uygulaması mevcuttur;

Cisco Webex (www.webex.com)

Freemium sürümünün özellikleri 50 ila 100 katılımcı için genişletildi, toplantılardaki 40 dakikalık sınır kaldırıldı ve çağrı yapma yetenekleri eklendi.

Microsoft Teams (teamsdemo.office.com)

Microsoft Teams, Microsoft uygulama ekosisteminin bir parçası olarak, çeşitli Office belgelerinde işbirliği yapmak ve video konferans özellikleri sunmak iyi bir seçenektir.

Yalnızca Gmail veya diğer ücretsiz kullanan kişiler Skype'a yönlendirilmektedir.

Skype (www.skype.com/en/free-conference-call)

Skype video konferans platformu, süre sınırı olmaksızın 50 katılımcıya kadar ücretsiz olarak desteklemektedir.

Jitsi Meet (meet.jit.si)

Jitsi Meet açık kaynak bir uygulama olarak tamamen ücretsizdir. Jitsi Meet'ın ek özellikleri arasında hem iOS hem de Android için uygulamaları, toplantıları YouTube Live üzerinden akış olanağı ve odayı bir parola ile kilitleme seçeneği de mevcuttur.

[1] https://www.cnet.com/how-to/no-more-zoombombing-4-steps-to-a-more-secure-zoom-video-chat/

Google Hangouts Meeting (hangout.google.com)

Hangouts Meeting, G-Suite aboneleri için video toplantılarına izin verir, ancak harici katılımcıların da kullanması mümkündür.

G-Suite Basic'teki katılımcı sayısı 100 ile sınırlıdır, ancak Business için 150 ve Enterprise için 250'ye kadar çıkmaktadır. 100.000'e kadar kitleye canlı yayın yapmak ve toplantıları Drive'a kaydetmek için kullanıcıların G Suite Enterprise'a ihtiyacı vardır.

GoToMeeting (www.gotomeeting.com)

GoToMeeting'in web konferansı hizmetinde ses ve video oturumları, ekran paylaşımı ve Android ile iOS için mobil uygulamaları mevcuttur. En fazla 150 katılımcıya izin veren standart sürüm, aylık 12-14 $ dır.

BlueJeans (www.bluejeans.com)

Bulut tabanlı bir video konferans hizmeti olan BlueJeans'in, ücretsiz bir sürümü yoktur. 50 katılımcıya kadar sınırsız süreli toplantılar için ücret ayda 9,99 $ dan başlamaktadır.

Zoho Meetings (www.zoho.com)

Zoho Meetings, web seminerleri, eğitim ve çevrimiçi toplantılar için geliştirilmiş bir platformdur. Ses, video ve ekran paylaşımının yanı sıra telefon, ses kayıt ve takvim davetlerine de izin vermektedir.

Daha Fazla Seçenek

- 8x8 www.8x8.com
- RemoteHQ www.remotehq.com
- Slack www.slack.com
- Starleaf www.starleaf.com
- Talky Talky.io
- Houseparty www.houseparty.com
- Whereby whereby.com/testroom

YERLİ Video Konferans Uygulamaları?

Uzaktan eğitim ve toplantılara yönelik Zoom ve yabacı uygulamalara karşı, **YERLİ** çözümler de mevcuttur;[2]

- **11sight** https://11sight.com/tr
- **Augmency** http://www.augmency.com/home/
- **Bilig OpEx** www.bilig.co.uk
- **EasyCoideo** https://www.ccr.group/easyconnect-video/
- **FAREDU** http://far-education.com
- **İVME Video Platformu** www.ivmetech.com/
- **Jetlink** jetlink.io
- **K2M** https://k2m.gowebmeeting.com:9090/login
- **mercek.io** https://plusclouds.com
- **Odak** olcsancad.com
- **securKEY** www.securkey.net
- **SmartEvent** https://www.arneca.com
- **KAREL Video Konferans** https://www.karel.com.tr/video-konferans/bulutta-video-konferans
- **VİO** http://www.netas.com.tr/inovasyon-ve-urunler/vio-video-iletisim-ortami/
- **WORA Konferans** https://liberta.com.tr/wora-konferans-sistemi
- **WORKIT** www.icterra.com

[2] Melek Bar Elmas, TOBB Türkiye Yazılım Meclisi Başkanı, 17.04.2020