Gerçek Zamanlı Akış ve Görüntülü Konferans Platformları için 2025 Yılında Gelişmiş Ağ Trafiği Analizi, Güvenlik ve Veri Akışı Kontrolü

Yönetici Özeti

Bu rapor, 2025 yılı itibarıyla Twitch, YouTube Stream, Microsoft Teams, Google Meet ve Zoom gibi çevrimiçi akış ve görüntülü görüşme platformlarının ağ trafiği analizi, güvenliği ve veri akışı kontrolüne yönelik en son ve en etkili teknikleri ve eğilimleri derinlemesine incelemektedir. Bu platformlar, küresel iletişim, işbirliği ve eğlencenin vazgeçilmez bir parçası haline gelmiş olup, kullanım yaygınlıkları ağ trafiği hacminde, çeşitliliğinde ve karmaşıklığında üstel bir artışa yol açmıştır. Bu durum, hassas verilerin korunması, iletişim gizliliğinin sağlanması ve hizmet sürekliliğinin sürdürülmesi açısından ileri düzey ağ görünürlüğü, sıkı güvenlik önlemleri ve etkili veri akışı kontrolünün kritik önemini ortaya koymaktadır.

2025 yılına gelindiğinde, yapay zeka (YZ) destekli tehditlerin artan sofistikasyonu ve şifreli trafiğin yaygınlaşması, geleneksel güvenlik yaklaşımlarının yetersiz kalmasına neden olmuştur.[1] Bu durum, reaktif, çevre tabanlı savunmalardan proaktif, akıllı ve bağlama duyarlı güvenlik duruşlarına doğru bir paradigma değişimi zorunluluğunu beraberinde getirmektedir. Rapor, bu dönüşümü destekleyen on adet çığır açan teknik ve eğilimi detaylandırmaktadır. Bu teknikler arasında YZ destekli tehdit tespiti, Sıfır Güven Ağ Erişimi (ZTNA), gelişmiş uçtan uca şifreleme ve kuantum sonrası kriptografi hazırlığı gibi konular yer almaktadır. Bu eğilimler, kuruluşların sürekli gelişen siber tehdit ortamında gerçek zamanlı iletişimlerini güvence altına alabilmeleri için kapsamlı ve adaptif stratejiler benimsemelerinin gerekliliğini vurgulamaktadır.

Giriş: Gerçek Zamanlı İletişimin Gelişen Ortamı

Çevrimiçi Akış ve Görüntülü Konferans Platformlarına Genel Bakış

Twitch, YouTube Stream gibi çevrimiçi akış platformları ve Microsoft Teams, Google Meet, Zoom gibi görüntülü konferans çözümleri, niş araçlardan küresel iletişim, işbirliği ve eğlence için vazgeçilmez bir altyapıya dönüşmüştür. Bu platformların yaygın olarak benimsenmesi, ağ trafiği hacminde, çeşitliliğinde ve karmaşıklığında katlanarak artan bir büyümeye yol açmıştır. Bu hizmetler, kritik iş operasyonlarını, uzaktan eğitimi ve büyük ölçekli halka açık etkinlikleri kolaylaştırmakta, bu da temel ağ performanslarının, güvenliklerinin ve veri bütünlüklerinin son derece önemli olmasını sağlamaktadır.

Ağ Görünürlüğü, Güvenlik ve Veri Akışı Kontrolünün Artan Önemi

Bu platformlar hassas konuşmaları, tescilli kurumsal verileri ve kişisel etkileşimleri barındırdığından, sağlam ağ görünürlüğü, sıkı güvenlik önlemleri ve etkili veri akışı kontrolü artık isteğe bağlı değil, stratejik bir zorunluluktur. Gerçek zamanlı trafiğin dinamik ve genellikle şifreli yapısı, geleneksel ağ izleme ve güvenlik araçları için benzersiz zorluklar ortaya koymakta, tespit, analiz ve kontrol için gelişmiş metodolojiler gerektirmektedir. Görüntülü konferansın günlük iş iletişiminin ayrılmaz bir parçası haline gelmesiyle birlikte, 2025 yılı boyunca hassas konuşmaları ve verileri korumak için daha sağlam güvenlik önlemleri getirileceği beklenmektedir.[5]

Bu platformların yaygınlaşması, ağ güvenliğinin artık sadece çevreyi korumakla ilgili olmadığını, uygulama katmanı anlayışına ve kullanıcı davranışına derinlemesine nüfuz ettiğini göstermektedir. Özellikle hibrit çalışma modellerine ve dağıtılmış ortamlara doğru hızlı geçiş göz önüne alındığında, bu durum daha da belirginleşmektedir. Kuruluşlar, günlük operasyonları için bu platformlara giderek daha fazla güvendikçe [5], ve BT ortamları hibrit çalışma nedeniyle daha dağıtılmış ve bulut merkezli hale geldikçe [6], geleneksel güvenlik çevresi (örneğin, kurumsal ağ sınırı) daha az alakalı hale gelmektedir. Güvenlik, verilerin ve etkileşimlerin nerede gerçekleştiğine bakılmaksızın korunacak şekilde uyarlanmalıdır. Bu, güvenlik odağının ağ altyapısından uygulama katmanına ve bireysel kullanıcı davranışına kaydırılmasını zorunlu kılmaktadır. Teams/Zoom gibi belirli platformların trafik modellerini anlamak, erişimi ayrıntılı uygulama düzeyinde kontrol etmek (ZTNA'nın yaptığı gibi) ve kullanıcı etkinliklerini izlemek kritik hale gelmektedir. Bu nedenle, "veri akışı kontrolü" terimi, sadece ağa giriş/çıkışı değil, aynı zamanda kullanıcının konumundan bağımsız olarak uygulamanın içindeki veriler üzerindeki kontrolü de kapsayan daha geniş bir anlam kazanmaktadır.

Ağ Ayak İzlerini Belirleme: IP'ler, Sunucular ve Portlar

Dinamik, Bulut Tabanlı Hizmetlerin Ağ Parametrelerini Keşfetme Teknikleri

Twitch, YouTube, Microsoft Teams, Google Meet ve Zoom gibi platformlar tarafından kullanılan tam IP adreslerini, sunucuları ve port numaralarını belirlemek önemli zorluklar sunmaktadır. Bu hizmetler İçerik Dağıtım Ağlarından (CDN) yoğun bir şekilde yararlanmakta, dinamik IP atamaları kullanmakta ve geniş, dağıtılmış bulut altyapıları üzerinde çalışmaktadır. Geleneksel statik kural tabanlı tanımlama ve engelleme, bu tür dinamik ortamlarda büyük ölçüde etkisizdir. Bunun yerine, teknikler gerçek zamanlı çözünürlüğe ve uygulamaya duyarlı trafik sınıflandırmasına odaklanmalıdır.[8] WebRTC güvenliğini detaylandıran bir kaynak, TURN sunucuları için tüm medya trafiği için 443 numaralı portun kullanılmasının önemini belirtmektedir. Ayrıca, çoğu WebRTC uygulamasının medya için 10.000'den yüksek portları kullanacağı UDP efemeral port aralığına da dikkat çekilmektedir.[9] Bu, belirli portlar kullanılsa da, dinamik tahsislerinin

statik güvenlik duvarı kurallarını zorlaştırdığını göstermektedir.

Şifreleme ve İçerik Dağıtım Ağlarının (CDN'ler) Yarattığı Zorluklar

TLS/SSL ve QUIC gibi yeni protokoller de dahil olmak üzere şifrelemenin yaygın kullanımı, geleneksel paket denetleme yöntemlerini gizlemektedir. Bu durum, gelişmiş şifre çözme yetenekleri olmadan uygulama katmanı protokollerini ve ilişkili ağ parametrelerini belirlemeyi önemli ölçüde zorlaştırmaktadır. CDN'ler içeriği küresel olarak dağıttığından, bir kullanıcının bağlantısı coğrafi olarak farklılaşmış çeşitli uç konumlarda sonlanabilir; bu da güvenlik politikası uygulaması için tek bir "sunucu" veya statik bir IP kümesi belirlemeyi zorlaştırmaktadır.[8]

QUIC protokolü, ilk pakette bile her şeyi şifreleyerek güvenliği ve gizliliği birinci sınıf bir vatandaş haline getirmektedir.[10] Bu kapsamlı şifreleme, geleneksel pasif ağ analizini önemli ölçüde karmaşıklaştırmaktadır. Pasif analiz cihazlarının, özellikle TLSv1.3 nedeniyle ilk bağlantıları izlemede ve sonrasında hiçbir şey görmemede daha zor bir işi olacağı belirtilmektedir.[10] Ancak, Cisco Secure Firewall'un 7.6 sürümü ve sonrası, QUIC trafiği şifre çözme için deneysel destek sunmakta, bu protokolü TCP tabanlı HTTPS ile "eşit seviyeye" getirmeyi amaçlamaktadır.[11] Bu, şifre çözme zorluğuna rağmen, QUIC trafiğinin içeriğine daha derinlemesine bakış açısı kazanmak için şifre çözmenin gerekli bir yetenek haline geldiğini göstermektedir.

IP'lerin dinamik olması ve trafiğin yoğun bir şekilde şifrelenmesi durumunda, statik IP/port kurallarına dayanan geleneksel ağ güvenlik araçları giderek kör ve etkisiz hale gelmektedir. Görünürlük kazanma yeteneği, hangi portun veya IP'nin kullanıldığını basitçe belirlemekten, hangi uygulamanın trafiği oluşturduğunu, şifreli tünel içindeki içeriğin ne olduğunu ve kimin iletişim kurduğunu anlamaya doğru kaymaktadır. Bu durum, daha sofistike teknolojilere geçişi zorunlu kılmaktadır. Derin Paket Denetimi (DPI) [12] dinamik ortamlarda bile paket yüklerini analiz etmek için kritik hale gelmektedir. YZ destekli analiz [12], büyük miktardaki trafikteki anormallikleri ve kalıpları belirlemek için gereklidir. Ayrıca, QUIC gibi protokoller için şifre çözme yeteneklerinin geliştirilmesi [11], kapsamlı güvenlik ve trafik akışı analizi için şifrelemenin aşılmasının giderek artan bir zorunluluk olduğunu göstermektedir. Trafik akışının nasıl gerçekleştiği sorusu, bu gelişmiş teknikler olmadan yeterince yanıtlanamaz.

Bu durum, ağ ayak izlerinin statik yapısından dinamik, bulut tabanlı ve yoğun bir şekilde şifrelenmiş trafiğe geçişin, ağ güvenliği ve trafik analizine yaklaşım biçimini temelden değiştirdiğini göstermektedir. Bu, basit port/IP engellemeden, genellikle şifre çözme ve gelişmiş trafik sınıflandırması gerektiren, uygulamaya duyarlı, bağlam açısından zengin denetime doğru bir kayış anlamına gelmektedir. Bu, geleneksel çevre tabanlı yöntemlere güvenmek yerine, ağ ayak izi belirleme metodolojisinin temelden

değiştiğini ve artık dinamik bulut ortamları ve şifreli protokollerle başa çıkmak için derin uygulama katmanı denetimi, genellikle şifre çözme içeren gelişmiş araçlar ve adaptif analiz gerektirdiğini vurgulamaktadır.

Gerçek Zamanlı Medya için Trafik Akışı Analizine Derinlemesine Bakış

Derin Paket Denetiminin (DPI) Evrimi ve 2025'teki Rolü

Derin Paket Denetimi (DPI) teknolojisi, temel başlıklardan öte paket yüklerini analiz eden bir teknoloji olup, 2025'ten 2034'e kadar %25,20'lik bir YBBO ile 2034 yılına kadar 254,37 milyar ABD dolarına ulaşması beklenen küresel pazar büyüklüğü ile hızlı bir büyüme kaydetmektedir.[12] Bu büyüme, temel olarak ağ güvenliği endişelerinin artması ve performans optimizasyonu ihtiyacından kaynaklanmaktadır.[12] DPI, ağ kullanım modellerine ilişkin ayrıntılı bilgiler sağlayarak, ağ operatörlerinin bant genişliğini daha verimli bir şekilde önceliklendirmesine ve yönetmesine olanak tanır; bu da gerçek zamanlı medya için Hizmet Kalitesi (QoS) ve Deneyim Kalitesi (QoE) sürdürmek için kritik öneme sahiptir.[12] DPI'ın "ağ güvenliği ve trafik yönetimi, ağ performansını iyileştirme"deki uygulamaları ve "veri paketlerinin içeriğinde görünmeyen tehditleri ve siber saldırıları tespit etmek için devlet kuruluşları" için faydası açıkça belirtilmiştir.[12]

Yapay Zeka'nın (YZ) DPI pazarı üzerindeki dönüştürücü etkisi de önemlidir. YZ entegrasyonu, ağ verilerinin büyük miktarlarını analiz ederek tehdit tespit doğruluğunu artırır, böylece ağ güvenliğini güçlendirir. Ayrıca, ağ filtreleme ve trafik tespit yeteneklerini önemli ölçüde geliştirir. Trafik yönetimi için YZ destekli DPI, trafik modellerini analiz ederek ve gecikmeyi azaltarak ağ performansını optimize edebilir.[12]

Gerçek Zamanlı Uygulama Performansı ve Güvenliği için Ağ Gözlemlenebilirliği Araçlarından Yararlanma

Ağ gözlemlenebilirliği, geleneksel izlemenin ötesine geçerek tüm ağ altyapısına kapsamlı görünürlük sağlar. Bu, gerçek zamanlı uygulama performansını etkileyen darboğazların, anormalliklerin ve verimsizliklerin belirlenmesine olanak tanır.[14] 2025 yılında, gözlemlenebilirlik, YZ destekli tahmine dayalı operasyonların, tam yığın gözlemlenebilirliğin ve gelişmiş güvenlik entegrasyonunun entegrasyonu yoluyla dönüşmektedir.[15] YZ destekli analitik araçlar, gerçek zamanlı büyük verileri işleyerek anormallikleri belirler, potansiyel sistem arızalarını tahmin eder ve otomatik iyileştirme faaliyetleri gerçekleştirir; bu da gerçek zamanlı medya ortamlarında yüksek QoE'yi sürdürmek için kritik öneme sahiptir.[15] YZ destekli tahmine dayalı operasyonlar, "hizmet kesintilerini, kapasite sorunlarını ve performans düşüşünü gerçekleşmeden önce tahmin eder".[15] Bu proaktif yaklaşım, proaktif risk yönetimi sağlayarak ve son

kullanıcılar üzerindeki etkiyi en aza indirerek sistem arızalarını önler. Ayrıca, YZ destekli tam yığın gözlemlenebilirliğin, daha derinlemesine bilgi ve daha hızlı sorun çözümü için birden fazla veri kaynağından günlükleri, izlemeleri ve metrikleri ilişkilendirdiği vurgulanmaktadır.[15] Paessler PRTG, AKIPS Network Monitoring ve Obkio gibi önde gelen ağ gözlemlenebilirliği araçları, özelleştirilebilir uyarılar, panolar, ağ keşfi, cihaz parmak izi ve son kullanıcı deneyimi izlemeye odaklanma gibi özellikleriyle öne çıkmaktadır.[14]

Trafik Akışında QUIC ve WebRTC gibi Modern Protokollerin Analizi

QUIC (Quick UDP Internet Connections): HTTP/3 için taşıma protokolü olarak resmileştirilen QUIC, UDP'yi kullanır ve daha hızlı bağlantı kurulumu, iyileştirilmiş performans ve gelişmiş gizlilik ve güvenlik sunar.[11] Temel bir özelliği, "ilk pakette bile her şeyin" şifrelendiği yaygın şifrelemesidir, bu da "güvenlik ve gizliliği birinci sınıf bir vatandaş" haline getirir.[10] Bu kapsamlı şifreleme, geleneksel pasif ağ analizini önemli ölçüde karmaşıklaştırmaktadır. Pasif analiz cihazlarının, özellikle TLSv1.3 nedeniyle ilk bağlantıları izlemede daha zor bir işi olacağı belirtilmektedir.[10]

Bu şifreleme zorluğuna bir çözüm olarak, Cisco Secure Firewall sürüm 7.6 ve sonrası, QUIC trafiği şifre çözme için deneysel destek sunmakta, bu protokolü güvenlik denetimi için TCP tabanlı HTTPS ile "eşit seviyeye" getirmeyi amaçlamaktadır.[11] Bu, şifrelenmiş QUIC trafiğine izinsiz giriş ve kötü amaçlı yazılım korumalarının uygulanmasını sağlar. Ancak, QUIC şifre çözmenin deneysel doğası, protokol evrimi ile güvenlik aracı olgunluğu arasında önemli bir boşluk olduğunu göstermektedir.[11] Bu durum, saldırganların şifreli kanallardan yararlanabileceği bir fırsat penceresi yaratmaktadır [2], bu da proaktif tehdit istihbaratını ve davranışsal anomali tespitini [16] bazı senaryolarda tam şifre çözmeden daha kritik hale getirmektedir. QUIC'in UDP tabanlı olması nedeniyle gelecekteki kötüye kullanım potansiyeli konusunda da uyarılar bulunmaktadır, örneğin Hizmet Reddi fırsatları ve "port vuruşu" teknikleri.[10]

WebRTC (Web Gerçek Zamanlı İletişim): Bu protokol, tarayıcı tabanlı gerçek zamanlı iletişim platformları (örn. Google Meet, Zoom) için temeldir. WebRTC medya akışları için otomatik olarak şifreleme sağlarken, eşlerin bağlantı ayrıntılarını değiştirdiği sinyalizasyon aşaması, HTTPS ve WSS gibi güvenli protokoller kullanılarak ek koruma gerektirir.[9] 2025 için temel güvenlik uygulamaları arasında güvenli sinyalizasyon (TLS sertifikaları, token tabanlı kimlik doğrulama), Uçtan Uca Şifreleme (DTLS-SRTP ile güvenli anahtar değişimi, şifrelenmemiş bağlantıların engellenmesi), sıkı erişim kontrollerinin uygulanması (Rol Tabanlı Erişim Kontrolü) ve güvenlik duvarlarının doğru yapılandırılması (WebRTC trafiğine 80/443 portları ve efemeral UDP portları (>10.000) üzerinden izin verilmesi) yer almaktadır.[9] Devam eden izleme, haftalık kural incelemeleri

ve olağandışı etkinlikler için trafik analizi de önemlidir.[9]

QUIC ve WebRTC gibi yüksek düzeyde şifrelenmiş protokollerin artan benimsenmesi, geleneksel ağ analiz araçlarının eskimeye başladığı anlamına gelmektedir. Trafik analizinin geleceği, YZ destekli zeka ile DPI'ı birleştiren, anomali tespiti için özel şifre çözme yetenekleri ve uç ortamlar da dahil olmak üzere tüm ağ yığını boyunca kapsamlı gözlemlenebilirlik sağlayan çok yönlü bir yaklaşımda yatmaktadır. Bu, güvenlik araçları QUIC gibi yaygın olarak benimsenen bir protokolün şifre çözme konusunda hala deneysel aşamadayken, saldırganların zaten şifrelemeyi faaliyetlerini gizlemek için aktif olarak kullandığı bir "siber silahlanma yarışı" dinamiği yaratmaktadır.[2] Bu durum, savunmacıların tek başına şifre çözmeye güvenemeyeceğini, bunun yerine şifreli trafik meta verileri içinde veya trafik akışı özellikleri aracılığıyla kötü niyetli faaliyetleri tanımlayabilen davranışsal analiz ve gelişmiş makine öğrenimi/derin öğrenme tabanlı anomali tespitine yoğun yatırım yapmaları gerektiğini göstermektedir.[16] Bu proaktif, davranışsal yaklaşım, şifre çözme yetenekleri hala olgunlaşırken kritik bir telafi mekanizması haline gelmektedir.

2025 Yılında Güvenlik ve Veri Akışı Kontrolü için En İyi 10 Çığır Açan Teknik ve Eğilim

Bu bölümde, belirlenen en iyi 10 teknik ve eğilimin her biri, mekanizmaları, faydaları ve gerçek zamanlı akış ve görüntülü konferans platformlarının güvenliğine olan ilgileri derinlemesine incelenecektir.

1. YZ Destekli Tehdit Tespiti ve Otomatik Yanıt

Mekanizma ve Faydaları: YZ destekli siber güvenlik sistemleri, makine öğrenimi algoritmalarını ve veri analizini kullanarak siber tehditleri gösteren kalıpları ve anormallikleri geleneksel sistemlerden daha doğru ve hızlı bir şekilde tespit ederek tehdit tespit ve yanıtını devrim niteliğinde değiştirmektedir.[3] Temel yetenekler arasında, geçmiş verilere ve ortaya çıkan kalıplara dayanarak potansiyel tehditleri tahmin eden tahmine dayalı tehdit tespiti; tespit edilen tehditlere önceden tanımlanmış yanıtları otomatik olarak başlatan ve tepki sürelerini önemli ölçüde azaltan otomatik olay yanıtı; ve olağandışı davranışları hızlı bir şekilde tespit etmek için ağ etkinliklerinin sürekli, gerçek zamanlı izlenmesini sağlayan gerçek zamanlı ağ analizi yer almaktadır.[3] YZ ayrıca güvenlik analistlerine olay özetlemesinde yardımcı olabilir, daha hızlı soruşturma ve karar verme için önceki bilgilerden yararlanabilir.[3]

Gerçek Zamanlı Medyaya İlişkin Önemi: Bu teknoloji, canlı akışları ve görüntülü konferansları hedef alan sofistike, YZ destekli saldırıları proaktif olarak belirlemek ve azaltmak için kritik öneme sahiptir. Örnekler arasında YZ destekli DDoS saldırıları [1],

deepfake kimlik avı [1] ve daha gizli şifreli komuta ve kontrol (C2) faaliyetleri [2] yer almaktadır. YZ, meşru ve kötü amaçlı bot trafiğini etkili bir şekilde ayırt edebilir ve hızla değişen saldırı imzalarına gerçek zamanlı olarak uyum sağlayabilir.[1] Görüntülü konferans için YZ ve makine öğreniminin "güvenlik tehditlerini gerçek zamanlı olarak belirlemeye, yetkisiz kullanıcıların toplantılara erişmesini tespit etmeye ve engellemeye yardımcı olacağı" belirtilmektedir.[5] Ayrıca, YZ destekli tehdit tespiti ve otomatik yanıtın, uç bilişim güvenliğinde 2025'in en önemli eğilimlerinden biri olduğu belirtilmektedir. YZ'nin "ağ etkinliğindeki olağandışı kalıpları tespit etme, riskleri gerçek zamanlı olarak analiz etme ve hasar oluşmadan önce proaktif olarak yanıt verme" yeteneği vurgulanmaktadır.[18]

Siber güvenlikte "silahlanma yarışı" hızlanmaktadır. YZ, savunma yeteneklerini önemli ölçüde artırırken, aynı zamanda saldırganları daha sofistike, adaptif ve gizli tehditler oluşturma konusunda güçlendirmektedir.[1] Saldırganlar, YZ'yi saldırıları otomatikleştirmek, ölçeklendirmek, kişiselleştirmek ve daha kaçamak ve etkili hale getirmek için kullanmaktadır. Bu durum, savunma YZ'sinin sunduğu faydaları doğrudan ortadan kaldırmaktadır. Bu nedenle, gerçek zamanlı iletişimi güvence altına almak için savunma YZ'sinin etkinliğini sürdürebilmesi için, saldırgan YZ kadar dinamik ve sofistike olması gerekmektedir. Bu, statik kuralların veya basit anomali tespitinin ötesine geçerek, tehditleri tahmin edebilen, karmaşık davranışsal kalıpları analiz edebilen (sadece hacim tabanlı anormallikler yerine) ve yeni saldırı imzalarına gerçek zamanlı olarak uyum sağlayabilen sürekli öğrenen modellere geçiş anlamına gelmektedir. "Gizli şifreli C2 etkinliği" [2] özellikle "hacim tabanlı anormallikleri tespit eden YZ destekli savunma sistemlerinden" kaçınmayı hedeflemektedir. Bu da daha gelişmiş, nüanslı YZ/ML yeteneklerine olan ihtiyacı pekiştirmektedir. Bu nedenle, siber güvenlikte YZ'yi, savunma YZ'sinin YZ destekli saldırıların artan sofistikasyonuna etkili bir şekilde karşı koymak için stratejilerini (örn. tahmine dayalı, davranışsal ve adaptif analitik) sürekli olarak yenilemesi ve uyarlaması gereken devam eden, hızla gelişen bir "silahlanma yarışı" olarak çerçevelendirmek gerekmektedir.

2. Sıfır Güven Ağ Erişimi (ZTNA)

Mekanizma ve Faydaları: ZTNA, geleneksel çevre tabanlı güvenlikten temel bir kaymayı temsil eder ve "varsayılan olarak asla güvenme, her zaman doğrula" ilkesiyle çalışır.[6] Bağlantı kurulduktan sonra geniş ağ erişimi sağlayan VPN'lerin aksine (VPN'ler genellikle bunu yapar), ZTNA, yalnızca güçlü kimlik doğrulama ve sürekli bağlam kontrolünden sonra belirli uygulamalara veya kaynaklara ayrıntılı, bağlama duyarlı erişim sağlar.[6] Bu yaklaşım, saldırı yüzeyini önemli ölçüde azaltır, ele geçirilmiş hesapların etkisini belirli uygulamalarla sınırlar (tüm ağı değil) ve en az ayrıcalık ilkesini doğal olarak uygular.[6] ZTNA ayrıca, bir cihaz uyumluluğunu kaybederse otomatik

bağlantı kesme gibi sürekli kontrolleri de içerir.[6]

Gerçek Zamanlı Medyaya İlişkin Önemi: ZTNA, modern hibrit ve çoklu bulut ortamlarında bulut tabanlı akış ve görüntülü konferans platformlarına erişimi güvence altına almak için idealdir.[6] Genellikle basit bir web tarayıcısı veya ince bir aracı aracılığıyla modern bir kullanıcı deneyimi sunar, ayrı VPN istemcilerine olan ihtiyacı ortadan kaldırır ve merkezi VPN'lerle ilişkili yavaşlamaları önler, böylece video gibi yoğun kullanımlar için performansı optimize eder.[6]

Eğilim: Gartner, 2025 yılına kadar yeni uzaktan erişim dağıtımlarının en az %70'inin geleneksel VPN'ler yerine ZTNA çözümlerine dayanacağını tahmin etmektedir.[6] Uç bilişim güvenliğinde 2025'in en önemli eğilimlerinden biri olarak "Sıfır Güven Mimarisi ile Saldırı Yüzeyini Küçültme" belirtilmektedir. Bu yaklaşım, yetkisiz kullanıcıların güvenlik açıklarından yararlanmasını önlemek için "her kullanıcı, cihaz ve uygulama için sürekli doğrulama" gerektirmektedir.[18]

ZTNA'nın yaygın olarak benimsenmesi, ağ merkezli güvenlikten kimlik ve uygulama merkezli güvenliğe temel bir kaymayı ifade etmektedir. Gerçek zamanlı medya için bu, sadece ağ bağlantısını değil, *oturumun* ve *uygulama erişiminin* kendisini güvence altına almak anlamına gelmektedir. Hassas verilerin dinamik, genellikle dışsallaştırılmış ortamlarda değiş tokuş edildiği durumlarda bu kritik öneme sahiptir ve ayrıntılı veri akışı kontrolünü doğrudan desteklemektedir. Geleneksel VPN'ler, geniş ağ erişimi sağlayarak, ele geçirilmiş bir hesabın tüm dahili ağda yanal harekete yol açabileceği bir "güçlendirilmiş kale" sendromu yaratmaktadır. Bu model, bulut tabanlı uygulamalar ve hibrit işgücü için uygun değildir. ZTNA, bu durumu, tüm ağ yerine *belirli uygulamalara* erişimi güvence altına almaya odaklanarak ve kimliği ve bağlamı sürekli doğrulayarak doğrudan ele almaktadır. Bu paradigma değişimi, güvenlik çevresini statik bir ağ sınırından dinamik, kimlik ve uygulama farkındalığına sahip bir sınıra dönüştürmektedir. Akış ve görüntülü konferans için bu, yalnızca yetkili kullanıcıların belirli bir toplantıya veya akışa bağlanabilmesini ve erişimlerinin rolleri, cihazları ve bağlamları temelinde sürekli olarak doğrulanmasını sağlamak anlamına gelmektedir. Bu ayrıntılı kontrol, *kimin hangi* veri akışına ve hangi koşullar altında, fiziksel konumları veya ağ bağlantıları ne olursa olsun erişebileceğini belirlediği için "veri akışı kontrolü" için hayati öneme sahiptir. Bu, güvenliği verilere ve kullanıcıya daha yakın hale getirmektedir.

3. Gelişmiş Uçtan Uca Şifreleme (E2EE) ve Kuantum Sonrası Kriptografi Hazırlığı

Mekanizma ve Faydaları: Uçtan Uca Şifreleme (E2EE), iletişimin göndericinin cihazında şifrelenmesini ve yalnızca alıcının cihazında şifresinin çözülmesini sağlar, yani mesajları yalnızca iletişim kuran taraflar okuyabilir.[9] Bu, hassas verileri yetkisiz

erişimden, dinlemeden ve aracıların kurcalamasından korur. Örneğin WebRTC, güvenli anahtar değişimi ve medya akışı koruması için DTLS-SRTP kullanır ve her oturum için yeni bir şifreleme anahtarı üreten ileri gizlilik ilkesini içerir.[9]

Kuantum Sonrası Kriptografi (PQC) Hazırlığı: Kritik bir yükselen endişe, gelecekteki kuantum bilgisayarların oluşturduğu tehdittir. Tehdit aktörleri, kuantum sonrası kriptografi uygulanabilir hale geldiğinde mevcut şifreli iletişimleri şifresini çözmek amacıyla arşivleyerek buna hazırlanmaktadır.[2] Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), ilk kuantum sonrası şifreli standartları Ağustos 2024'te tamamlamıştır.[2] Kriptoanalitik olarak ilgili kuantum bilgisayarların 2030'lara kadar beklenmemesine rağmen, kuruluşlar verilerini bu gelecekteki şifre çözme tehditlerine karşı korumak için PQC standartlarını benimsemeye öncelik vermelidir.[2] Çeşitli şifreleme türleri (Tek Anahtarlı, İki Anahtarlı, Kuantum) ve özellikleri açıklanmakta, kuantum şifrelemenin ultra güvenli veri iletimi için kuantum fiziği ilkelerini kullanması nedeniyle "en yüksek" güvenlik seviyesine sahip olduğu belirtilmektedir.[19]

Gerçek Zamanlı Medyaya İlişkin Önemi: E2EE, görüntülü konferanslarda değiş tokuş edilen hassas konuşmaların, paylaşılan belgelerin ve verilerin gizliliğini ve bütünlüğünü korumak için esastır.[5] Görüntülü konferans platformlarının 2025 yılına kadar E2EE'yi standart bir özellik olarak uygulaması beklenmektedir.[5] Yayıncılar için E2EE, gerçek zamanlı içerik engelleme ve ele geçirmeye karşı temel bir karşı önlemdir.[1] PQC hazırlığı, uzun süreli arşivlenmiş hassas iletişimlerin bile gelecekteki kuantum saldırılarına karşı güvende kalmasını sağlar. Uç bilişim güvenliğinde 2025'in bir eğilimi olarak "Kuantum Dirençli Şifrelemeye Hazırlanma" da listelenmektedir. Bu bağlamda, OTAVA'nın S.E.C.U.R.E.™ çerçevesinin, "şifreli verilerin kuantum sonrası bir dünyada bile korunmasını" sağlayarak geleceğe yönelik şifreleme stratejilerine öncelik verdiği belirtilmektedir.[18]

Kuantum Sonrası Kriptografi (PQC) hazırlığına geçiş, kriptoanalitik olarak ilgili kuantum bilgisayarlar yaygın olarak kullanılmadan önce bile (2030'lar bekleniyor [2]), günümüzdeki şifrelenmiş verilerin gelecekte tehlikeye girebileceği anlayışından kaynaklanan proaktif, uzun vadeli bir güvenlik stratejisini göstermektedir. Bu, hassas gerçek zamanlı iletişimler için kriptografik çeviklik ve öngörüye önemli bir yatırım anlamına gelmekte, reaktif güvenlikten önleyici güvenliğe doğru bir kaymayı ifade etmektedir. Eğer hassas veriler (örneğin, gizli görüntülü konferans kayıtları, tescilli akış içeriği) bugün mevcut standartlar kullanılarak şifrelenirse ve bu standartlar gelecekte kuantum bilgisayarlar tarafından kırılırsa, o veriler savunmasız hale gelecektir. Bu durum, yüksek derecede hassas veya uzun ömürlü gerçek zamanlı iletişimleri yöneten kuruluşların "geleceğe yönelik" bir şifreleme stratejisi düşünmeleri gerektiği anlamına gelmektedir. Bu, sadece mevcut E2EE en iyi uygulamalarını uygulamakla kalmayıp [5],

aynı zamanda PQC'yi aktif olarak araştırmayı, planlamayı ve benimsemeye başlamayı da içermektedir. Bu, güvenlik stratejisinde sadece mevcut güvenlik açıklarını ele almaktan, gelecekteki on yıllar boyunca kriptografik dayanıklılık oluşturmaya doğru önemli bir değişimi temsil etmekte ve önemli Ar-Ge ve altyapı yükseltmeleri gerektirmektedir.

4. Anomali Tespiti için Gelişmiş Makine Öğrenimi ve Derin Öğrenme

Mekanizma ve Faydaları: Makine Öğrenimi (ML) ve Derin Öğrenme (DL) tabanlı anomali tespiti, yerleşik normal davranıştan önemli ölçüde sapan veri noktalarını veya kalıplarını belirleyerek potansiyel dolandırıcılık, siber tehditler veya sistem arızalarını işaret eder.[17] Statik kural tabanlı yöntemlerin aksine, ML/DL modelleri zamanla öğrenir ve gelişir, bu da onları büyük veri kümelerini ele almada ve yeni, gelişen riskleri, hatta etiketlenmemiş verilerde bile tespit etmede son derece etkili kılar.[17]

Uygulamalar: Siber güvenlikte, ML/DL, bir saldırı gerçekleşmeden önce tuhaf ağ etkinliğini tespit etmek, yetkisiz girişleri saptamak ve şüpheli veri erişimini belirlemek için kullanılır.[17] Süreç tipik olarak veri toplama ve hazırlama (örn. ağ günlükleri), "normal" davranışın ne olduğunu öğrenme, bu temel çizgiden sapmaları tespit etme ve ardından eyleme geçme (örn. uyarı gönderme, şüpheli eylemleri engelleme) adımlarını içerir.[17]

Algoritmalar: Ağ anomali tespiti için yaygın algoritmalar arasında Isolation Forest (dolandırıcılık gibi nadir olaylar için etkili), K-Means Clustering (web sitesi saldırıları gibi grup davranışlarını tespit etmek için kullanışlı) ve Autoencoders (karmaşık kalıpları öğrenmede ve yüksek frekanslı ortamlarda olağandışı verileri işaretlemede yetenekli Derin Öğrenme modelleri) yer almaktadır.[17] Derin Sinir Ağları (DNN), şifreli trafikte Gelişmiş Kalıcı Tehditleri (APT'ler), özellikle komuta ve kontrol (C2) trafiğini tespit etmede yüksek doğruluk (%98) göstermiştir.[16] TMA Konferansı 2025'in Çağrı Bildirileri, "şifreli kanallar ve tescilli protokoller dahil olmak üzere ağ trafiğinin sınıflandırılması" ve "ağ ölçümü ve analizinde yapay zeka ve makine öğrenimi kullanımı"nı temel ilgi alanları olarak içermektedir.[20] Ayrıca, 2025 için "Sinir Ağı Anomali Tespiti ve Adversarial Saldırıları Engellemek için Uzman Panel Modelleri" için bir patent başvurusu (WO/2025/109469) açıklanmaktadır. Bu, anomali türlerini tespit etmek, bunları filtrelemek ve mevcut ML modellerini yeniden eğitmek için birden fazla model ve test kullanmayı içermektedir.[21]

İmza tabanlı tespitten ML/DL tabanlı anomali tespitine geçiş, polimorfik, sıfır gün ve YZ tarafından oluşturulan saldırıların artan sofistikasyonu nedeniyle sadece bir yükseltme değil, temel bir zorunluluktur.[16] Gerçek zamanlı medya için, trafik modellerinin oldukça dinamik ve genellikle şifreli olabileceği durumlarda, bu, "bilinmeyen bilinmeyenleri"

tanımlayabilen davranışsal analitiklere doğru kritik bir geçiş anlamına gelmektedir. Bu, bazı şifre çözme yöntemlerinin deneysel doğası göz önüne alındığında özellikle hayati öneme sahiptir. Gerçek zamanlı medya trafiği yüksek hacimli, dinamik kalıplara sahip ve giderek artan şifrelemeyle karakterize edilmektedir. Saldırganlar, YZ'yi son derece sofistike ve kaçamak tehditler oluşturmak için kullanmaktadır.[1] İmza tabanlı sistemler doğası gereği reaktif olup, yeni saldırıları tespit edemezler. ML/DL, özellikle denetimsiz öğrenme [17], "normal" davranışı sürekli öğrenerek ve istatistiksel olarak önemli sapmaları işaretleyerek daha önce görülmemiş tehditleri tespit edebilir. Bu, akış ve görüntülü konferans platformlarını koruyan güvenlik sistemlerinin sürekli öğrenme ve adaptasyon yeteneğine sahip olması gerektiği anlamına gelmektedir. Trafik akışı analizi için bu, içerik şifreli olsa bile veri sızdırma, gizli kanal iletişimi veya C2 etkinliğini işaret edebilecek davranışsal özelliklerin (örn. akış süresi, paket boyutu dağılımları, protokol türleri [16]) çıkarılmasına ve analiz edilmesine odaklanmayı gerektirmektedir. "Uzman panel modelleri" [21], yüksek riskli güvenlik ortamlarında güveni artırmak ve yanlış pozitifleri azaltmak için birden fazla ML modelini birleştiren bir topluluk yaklaşımını önermektedir.

5. Güvenli WebRTC Uygulamaları ve En İyi Uygulamalar

Mekanizma ve Faydaları: WebRTC (Web Gerçek Zamanlı İletişim), birçok tarayıcı tabanlı görüntülü konferans ve akış platformunun (örn. Google Meet, Zoom) temel bir teknolojisidir. WebRTC, medya akışları için doğal olarak şifreleme sağlarken, genel güvenlik duruşu büyük ölçüde en iyi uygulamaların doğru şekilde uygulanmasına bağlıdır. 2025 için bu uygulamalar şunları vurgulamaktadır:

- **Güvenli Sinyalizasyon Protokolleri:** Eşlerin bağlantı ayrıntılarını değiştirdiği ilk el sıkışma sürecini HTTPS ve WSS (WebSocket Secure) ile TLS şifrelemesi kullanarak korumak. Bu, yetkisiz erişimi ve ortadaki adam (MITM) saldırılarını önler.[9] Temel adımlar arasında TLS sertifikalarını kurmak, token tabanlı kimlik doğrulama uygulamak ve sertifika son kullanma tarihlerini düzenli olarak kontrol etmek yer almaktadır.[9]
- **Uçtan Uca Şifreleme (E2EE):** WebRTC, güvenli bağlantı kurulumu için DTLS ve medya akışı koruması için SRTP kullanmasına rağmen, grup aramalarında gerçek E2EE genellikle medya sunucusunun ötesinde uygulama düzeyinde uygulama gerektirir.[9] İleri gizlilik, mevcut anahtarlar ele geçirilse bile geçmiş iletişimlerin şifresinin çözülememesini sağlayarak kritik öneme sahiptir. Şifreleme protokollerinin düzenli denetimleri hayati önem taşımaktadır.[9]
- **Erişimi Kontrollerle Kısıtlama:** Farklı kullanıcı rollerine (yöneticiler, moderatörler, katılımcılar) belirli izinler atamak için Rol Tabanlı Erişim Kontrolü (RBAC) uygulamak, yetkisiz eylemleri en aza indirmek. Bu, izinleri açıkça tanımlamayı,

oturum zaman aşımlarını zorunlu kılmayı ve oturum etkinliklerini günlüğe kaydetmeyi içerir.[9]

- **Doğru Güvenlik Duvarı Yapılandırması:** WebRTC trafiğine izin verirken yetkisiz erişimi engellemek için kritik öneme sahiptir. Bu, TURN sunucuları için öncelikli olarak 443 numaralı portun kullanılması ve UDP trafiğine efemeral port aralıkları (medya için genellikle 10.000'den yüksek) üzerinden izin verilmesi anlamına gelir. Belirli TURN/medya sunucularının beyaz listeye alınması ve kurumsal kurulumlar için Uygulama Katmanı Ağ Geçitleri (ALG'ler) ile entegrasyon önerilir.[9] Devam eden izleme, haftalık kural incelemeleri ve olağandışı etkinlikler için trafik analizi de esastır.[9]

Gerçek Zamanlı Medyaya İlişkin Önemi: Doğrudan Google Meet ve Zoom gibi WebRTC'ye dayanan platformlar için geçerlidir. Bu uygulamaların güvenliğini sağlamak, yetkisiz erişimi, dinlemeyi, içerik manipülasyonunu ve sohbet yoluyla sıfır tıklamalı kötü amaçlı yazılımları önlemek için hayati önem taşımaktadır.[1] Güvenli Akış Protokolleri (SRT, WebRTC), gerçek zamanlı içerik ele geçirmeye karşı bir karşı önlem olarak listelenmekte ve bunların kurcalamaya dayanıklı tasarımları vurgulanmaktadır.[1]

WebRTC için "doğru güvenlik duvarı yapılandırması" ve "IDS/SIEM ile entegrasyon" vurgusu [9], protokolün yerleşik şifrelemesine rağmen, *uygulama bağlamının* ve *ağ ortamının* kritik güvenlik açıkları olduğunu göstermektedir. Bu, geliştiricilerin ve BT yöneticilerinin güvenli bir uçtan uca WebRTC iletişim kanalı sağlamak için yakın işbirliği yapması gerektiği anlamına gelmektedir. Güvenlik, sadece protokolün kendisine değil, aynı zamanda onun dağıtıldığı ve yönetildiği ortama da bağlıdır. Örneğin, güvenlik duvarı kurallarının haftalık olarak gözden geçirilmesi ve ayarlanması [9], gereksiz izinlerin ortadan kaldırılması ve ağdaki potansiyel ihlalleri işaret edebilecek olağandışı WebRTC trafiğinin sürekli izlenmesi, protokolün içsel güvenlik özelliklerini tamamlayan kritik operasyonel uygulamalardır. Bu, güvenlik sorumluluğunun sadece yazılım geliştiricilerde değil, aynı zamanda ağ altyapısını yöneten ve yapılandıran BT ekiplerinde de olduğu anlamına gelmektedir. Bu işbirliği, gerçek zamanlı iletişim platformlarının dinamik doğası ve sürekli gelişen tehdit ortamı göz önüne alındığında, 2025 yılında WebRTC güvenliği için vazgeçilmezdir.

6. Bulut Tabanlı Çözümler ve SaaS Güvenliği

Mekanizma ve Faydaları: Video gözetiminde bulut tabanlı çözümler, 2025 yılında önem kazanmaya devam edecektir.[8] Dahua gibi sağlayıcılar, bulut entegrasyonları aracılığıyla video gözetim sistemlerinin esnek ve ölçeklenebilir yönetimini sağlamaktadır.[8] Bulut çözümleriyle video gözetim verilerini yönetmek, video meta verilerine erişimi kolaylaştırırken, konum sayısından bağımsız olarak gözetim

sistemlerinin daha verimli yönetimini sağlamaktadır.[8] SaaS (Hizmet Olarak Yazılım) benimsenmesinin artmasıyla birlikte, siber güvenlik tehditleri de artmaktadır.[22] 2025 SASI Raporu gibi kaynaklar, SaaS kullanıcı davranışlarını, ortaya çıkan riskleri ve güvenlik eğilimlerini inceleyerek iş ve verileri etkili bir şekilde korumak için eyleme geçirilebilir bilgiler sağlamaktadır.[22] Bu, token ele geçirme ve yetkisiz erişim gibi tehditlere karşı korunmayı, kullanıcı davranışı, oturum açma etkinliği ve coğrafi konum verileri hakkında görünürlük elde etmeyi ve konuk kullanıcı hesapları ile riskli dosya paylaşım davranışlarının güvenlik kör noktaları oluşturduğunu anlamayı içermektedir.[22]

Gerçek Zamanlı Medyaya İlişkin Önemi: Microsoft Teams, Google Meet ve Zoom gibi platformlar genellikle SaaS modelleri aracılığıyla sunulduğundan, bulut tabanlı çözümlerin ve SaaS güvenliğinin benimsenmesi doğrudan bu platformların güvenliğini etkilemektedir. 2025'te SaaS güvenliğine yönelik yeni özellikler arasında, SaaS Güvenliği Inline için basitleştirilmiş Güvenlik Politikası Önerileri ve Kullanıcı Oturumu Takibi yer almaktadır.[23] Kullanıcı oturumu takibi, SaaS Güvenliği Inline'ın belirli uygulamalar için kiracı düzeyinde politika önerileri sunmasına ve hatta bireysel kullanıcı hesapları için daha fazla ayrıntı sağlamasına olanak tanır.[23] Bu, belirli bir kiracı için bazı uygulama trafiğine izin verilirken, aynı kiracıdaki belirli kullanıcı hesaplarından gelen trafiğin engellenmesi gibi senaryolara olanak tanır.[23] Bu gelişmiş görünürlük ve kontrol, hassas verilerin bulutta barındırılan ve erişilen gerçek zamanlı iletişim platformları aracılığıyla korunması için kritik öneme sahiptir.

Bulut hizmetlerinin artan kötüye kullanımı, şifreli saldırıların büyümesini tetikleyecektir.[2] Kuruluşlar güvenilir bulut platformlarına giderek daha fazla güvendikçe, siber suçlular da şifreli tehditleri iletmek için bu bulut platformlarına yöneleceklerdir.[2] Varsayılan TLS/SSL şifrelemesinden ve yaygın olarak kullanılan bulut sağlayıcılarına ve sertifikalarına verilen güvenden yararlanarak, saldırganlar kötü amaçlı içeriği şifreli trafiğe gömebilir, bu da tespiti çok daha zor hale getirir.[2] 2024'te ThreatLabz araştırması, gelişmiş kalıcı tehdit (APT) grupları tarafından bulut hizmetlerinin kötüye kullanımında bir artış olduğunu ortaya koymuştur.[2] Bu durum, bulut ortamlarında şifreli trafiğin gelişmiş denetimine olan acil ihtiyacı vurgulamaktadır.[2] Bu nedenle, SaaS uygulamaları için gelişmiş güvenlik, özellikle de YZ destekli tehdit tespiti ve kullanıcı davranışı analizi ile entegre edilmiş olanlar, bulut tabanlı gerçek zamanlı iletişim platformlarının güvenliğini sağlamak için hayati önem taşımaktadır.

7. Uç Bilişim Güvenliği ve 5G Entegrasyonu

Mekanizma ve Faydaları: Veri işleme, merkezi veri merkezlerinden "uç"a doğru kaymaktadır. Gartner, 2025 yılına kadar kurumsal verilerin %75'inin uçta işleneceğini tahmin etmektedir.[18] YZ, IoT ve 5G'nin benimsenmesi bu değişimi körüklemiştir.[18] Bu

faktörler verimliliği artırmış ancak aynı zamanda yeni riskler de getirmiştir. Genişleyen saldırı yüzeyleri ve gerçek zamanlı tehdit tespiti zorlukları, güçlü güvenlik önlemleri gerektirmektedir.[18] OTAVA'nın S.E.C.U.R.E.™ çerçevesi, gelişen siber tehditlere karşı uç ortamları korumak için yapılandırılmış bir yaklaşım sunmaktadır.[18]

5G ağlarının yaygınlaşması, gecikmeyi azaltarak ve bağlantıyı iyileştirerek uç bilişim güvenliğinin benimsenmesini hızlandırmıştır.[18] GSMA, 5G bağlantılarının yıl sonuna kadar iki milyara ulaşacağını tahmin etmektedir.[18] Ancak, bu faydalar aynı zamanda yeni riskler de getirmektedir, çünkü çoklu erişimli uç bilişim (MEC) ortamları siber saldırılar için daha fazla giriş noktası oluşturmakta ve sniffing saldırıları ve uç nokta zayıflıkları gibi güvenlik açıkları hassas verileri açığa çıkarabilmektedir.[18] OTAVA'nın S.E.C.U.R.E.™ 'C – Saldırı vektörlerini kontrol altına al' stratejisi, ağları bölümlere ayırarak, uç noktaları güvence altına alarak ve trafiği sürekli izleyerek işletmelere yardımcı olmaktadır.[18]

Gerçek Zamanlı Medyaya İlişkin Önemi: Gerçek zamanlı akış ve görüntülü konferans platformları, düşük gecikme ve yüksek bant genişliği gerektirdiğinden, 5G ve uç bilişim entegrasyonundan büyük ölçüde faydalanmaktadır. Örneğin, otonom araçlar ve akıllı şehirler gibi uygulamalar, 5G'nin hızlı veri iletişimi ve uç bilişimin yerel işlem yetenekleri sayesinde anında karar verme yeteneğinden yararlanmaktadır.[24] Ancak, bu dağıtılmış ortamlar, saldırı yüzeyini genişlettiği için yeni güvenlik zorlukları da sunmaktadır. Bu nedenle, uç bilişim güvenliği stratejileri, YZ destekli tehdit tespiti, Sıfır Güven modelleri ve kuantum şifrelemesi gibi unsurları içermelidir.[18] Mikro YZ yenilikleri, IoT sensörleri ve giyilebilir cihazlar gibi sınırlı kaynaklara sahip cihazlarda yerel veri işlemeyi mümkün kılarak uç bilişimi dönüştürmektedir. Bu, veri gizliliğini korurken ve hızlı işlemeye izin verirken bulut bağlantısına sürekli ihtiyaç duymadan sağlık metriklerini izleyen akıllı saatler gibi uygulamaları desteklemektedir.[24]

8. Blockchain Tabanlı İçerik Doğrulama ve Kimlik Doğrulama

Mekanizma ve Faydaları: Blockchain tabanlı içerik doğrulama, canlı video akışlarının hash'lerini bir blok zincirine kaydederek manipülasyon iddiaları durumunda doğrulanabilirlik güvencesi sağlar.[1] Bu, içeriğin bütünlüğünü ve orijinalliğini garanti eder. Kimlik doğrulama için, çok faktörlü kimlik doğrulama (MFA) ve biyometrik doğrulama (parmak izleri, yüz tanıma, ses tanıma gibi) gibi araçlar, yetkisiz erişimi önlemek için standart hale gelmektedir.[5] Bu yöntemler, geleneksel tek faktörlü kimlik doğrulamadan daha güçlü bir güvenlik katmanı sağlar.

Gerçek Zamanlı Medyaya İlişkin Önemi: Yayıncılar için blockchain tabanlı içerik doğrulama, gerçek zamanlı içerik ele geçirmeye karşı kritik bir karşı önlemdir.[1] Bu, saldırganların platform politikalarını ihlal eden, yanlış bilgi yayan veya sahte sponsorluk

mesajları gösteren rahatsız edici içerik enjekte etmesini önlemeye yardımcı olur.[1] YZ destekli deepfake saldırılarının artmasıyla birlikte, kimlik doğrulama için görsel veya işitsel ipuçlarına dayalı güvenilirlik azalmaktadır. Bu durum, çok katmanlı kimlik doğrulama için acil bir ihtiyaç yaratmaktadır.[4] Sentetik izleyici sahtekarlığına karşı, blockchain tabanlı izleyici doğrulaması, izleyici etkileşimlerini değişmez bir defterde saklayarak sponsorları yanıltan veya yayıncıların yasaklanmasına neden olan yapay olarak şişirilmiş sayıları önlemeye yardımcı olur.[1] Çok katmanlı CAPTCHA ve sohbet katılımı için kimlik doğrulama da insan doğrulaması gerektirerek bu sorunu ele alır.[1]

9. Gelişmiş Şifreli Trafik Denetimi

Mekanizma ve Faydaları: Şifreli trafiğin artan hacmi ve karmaşıklığı, geleneksel güvenlik araçları için zorluklar yaratmaktadır. YZ ve otomasyonun birleşimi, şifreli kanallarda gizlenen tehditlerde bir artışa yol açmaktadır.[2] Saldırganlar, kötü amaçlı betikler ve yükler oluşturmaktan, yerelleştirilmiş ve kişiselleştirilmiş kimlik avı e-postaları hazırlamaya kadar kötü amaçlı operasyonları otomatikleştirmek ve ölçeklendirmek için üretken YZ'den yararlanmaktadır.[2] Bu tehditleri TLS/SSL trafiğine gömerek, siber suçlular tespiti daha da zorlaştırmaktadır.[2]

Bu zorluklara karşı koymak için, şifreli saldırıları durdurmak, performanstan ödün vermeden şifreli trafiği denetleyebilen gelişmiş güvenlik çözümleri gerektirir.[2] Zscaler Zero Trust Exchange™ gibi çözümler, bir saldırının her aşamasında şifreli tehditlerle mücadele etmek için kapsamlı bir yaklaşım sunmaktadır.[2] Özellikle, Zscaler Internet Access™ (ZIA), her bağlantıyı doğrulamak ve gizli tehditleri performanstan ödün vermeden durdurmak için tam TLS/SSL denetimi gerçekleştirir.[2] YZ destekli analiz ve satır içi tespit kullanarak, şifreli trafikteki sofistike tehditleri belirler ve engeller.[2] Bu bulut tabanlı yaklaşım, kuruluşların performans darboğazları olmadan şifreli trafik denetim yeteneklerini ölçeklendirmelerine olanak tanır.[2]

Gerçek Zamanlı Medyaya İlişkin Önemi: Görüntülü konferans ve akış platformları, doğal olarak yüksek hacimli şifreli trafik üretir. Gelişmiş şifreli trafik denetimi, bu trafiğin içindeki gizli tehditleri (örn. şifreli C2 faaliyetleri, kötü amaçlı yazılım yükleri) tespit etmek ve engellemek için hayati öneme sahiptir.[2] Özellikle, gelişmiş kalıcı tehdit (APT) grupları, faaliyetlerini gizlemek için şifreli kanalları temel bir taktik olarak kullanmaktadır.[2] Bu gruplar, şifreli protokollerdeki zayıflıkları kötüye kullanma kaynaklarına ve uzmanlığına sahiptir.[2] Meşru trafiğe karışarak, kampanyalarının ömrünü uzatmakta ve komuta ve kontrol altyapılarını izlemeyi zorlaştırmaktadırlar.[2] Bu, bulut ortamlarında şifreli trafiğin gelişmiş denetimine olan acil ihtiyacı vurgulamaktadır.

10. Gelişmiş Ağ Gözlemlenebilirliği ve Tam Yığın Görünürlüğü

Mekanizma ve Faydaları: Gözlemlenebilirlik, 2025 yılında YZ, otomasyon ve gelişmiş güvenlik önlemlerinin entegrasyonuyla dönüşmektedir.[15] Bu evrim, genellikle veri silolarına ve sınırlı görünürlüğe yol açan geleneksel izlemenin ötesine geçerek, bulut tabanlı ortamlardaki dağıtılmış sistemlerin ve mikro hizmetlerin karmaşıklığını yönetmek için gerekli kapsamlı çerçevelere ulaşmaktadır.[15] Temel eğilimler arasında YZ destekli tahmine dayalı operasyonlar yer almaktadır. Bu sistemler, yalnızca sorunları ortaya çıktıktan sonra tespit eden geleneksel izlemenin aksine, kaynak darboğazları veya bellek sızıntıları gibi potansiyel arızaları tahmin etmek için performans verilerini analiz eder.[15] Bu proaktif yaklaşım, kesinti sürelerini önlemeye, kaynakları optimize etmeye ve daha dirençli sistemler oluşturmaya yardımcı olur.[15] YZ destekli zekanın entegrasyonu, YZ'nin sadece sorunları tespit etmekle kalmayıp, sorunlar büyümeden önce düzeltici çözümler de sunarak gözlemlenebilirliği dönüştürmesidir.[15] YZ destekli analitik araçlar, gerçek zamanlı büyük verileri işleyerek anormallikleri belirler, potansiyel sistem arızalarını tahmin eder ve otomatik iyileştirme gerçekleştirir.[15]

Gerçek Zamanlı Medyaya İlişkin Önemi: Gerçek zamanlı akış ve görüntülü konferans platformları, yüksek performans ve sürekli kullanılabilirlik gerektirir. Tam yığın gözlemlenebilirliği, günlükleri, izlemeleri ve metrikleri birden fazla veri kaynağı arasında ilişkilendirerek anormallikleri tespit etmek için YZ'yi kullanır.[15] Verileri ayrı ayrı analiz etmek yerine, YZ her şeyi bir arada ele alır, daha derinlemesine bilgi sağlar ve gerçek zamanlı ve geçmiş verileri analiz ederek sorunları hızlı bir şekilde belirler.[15] Bu, ekiplerin sorunlar büyümeden önce harekete geçmesine olanak tanır, kesinti sürelerini azaltır ve sorun çözme süresini hızlandırır.[15] Bu, gerçek zamanlı medya akışlarının kalitesini ve güvenliğini korumak için kritik öneme sahiptir. Ayrıca, kuruluşlar maliyetleri düşürmek için daha akıllı veri toplama yöntemleri benimsemektedir.[15] Temel izlemeleri örnekleme, yalnızca önemli günlükleri depolama ve daha az kritik verileri daha düşük maliyetli depolamaya taşıma gibi stratejiler, maliyetleri %60-80 oranında azaltabilir.[15] Bu, değerli bilgileri korurken harcamaları azaltmaya ve sorgu verimliliğini artırmaya yardımcı olur.

Sonuçlar ve Öneriler

2025 yılına girerken, çevrimiçi akış ve görüntülü konferans platformlarının güvenliği ve veri akışı kontrolü, YZ destekli tehditlerin artan sofistikasyonu, şifreli trafiğin yaygınlaşması ve dağıtılmış bulut ortamlarına geçiş nedeniyle önemli bir dönüşüm geçirmektedir. Geleneksel çevre tabanlı güvenlik modelleri, bu dinamik ve karmaşık ortamda yetersiz kalmaktadır. Bu durum, kuruluşların proaktif, akıllı ve bağlama duyarlı güvenlik duruşlarını benimsemelerini zorunlu kılmaktadır.

Bu raporun ortaya koyduğu on adet çığır açan teknik ve eğilim, bu paradigma değişiminin temelini oluşturmaktadır. YZ destekli tehdit tespiti ve otomatik yanıt, Sıfır

Güven Ağ Erişimi (ZTNA), gelişmiş uçtan uca şifreleme ve kuantum sonrası kriptografi hazırlığı, gelişmiş makine öğrenimi ve derin öğrenme ile anomali tespiti, güvenli WebRTC uygulamaları, bulut tabanlı çözümler ve SaaS güvenliği, uç bilişim güvenliği ve 5G entegrasyonu, blockchain tabanlı içerik doğrulama ve kimlik doğrulama, gelişmiş şifreli trafik denetimi ve gelişmiş ağ gözlemlenebilirliği ile tam yığın görünürlüğü, bu yeni güvenlik paradigmasının temel bileşenleridir.

Öneriler:

1. **YZ Tabanlı Savunma Sistemlerine Yatırım:** Kuruluşlar, YZ destekli saldırılara karşı koymak için davranışsal analitik, tahmine dayalı tehdit tespiti ve otomatik yanıt yetenekleri sunan YZ destekli güvenlik çözümlerine öncelik vermelidir. Güvenlik sistemleri, sürekli öğrenme ve adaptasyon yeteneğine sahip olmalıdır.
2. **Sıfır Güven Mimarisi Benimsenmesi:** Geleneksel VPN'lerden ZTNA çözümlerine geçiş, saldırı yüzeyini önemli ölçüde azaltacak ve en az ayrıcalık ilkesini uygulayarak hassas gerçek zamanlı iletişimlere ayrıntılı, bağlama duyarlı erişim sağlayacaktır.
3. **Kapsamlı Şifreleme Stratejileri:** Uçtan uca şifreleme, görüntülü konferans platformları için standart bir özellik haline getirilmelidir. Ayrıca, kuruluşlar, gelecekteki kuantum bilgisayarların mevcut şifrelemeyi kırma tehdidine karşı verileri korumak için kuantum sonrası kriptografi standartlarının benimsenmesine proaktif olarak hazırlanmalıdır.
4. **Anomali Tespiti için ML/DL Uygulaması:** İmza tabanlı tespitin sınırlamaları göz önüne alındığında, kuruluşlar, ağ trafiğindeki olağandışı davranışları tespit etmek için makine öğrenimi ve derin öğrenme modellerini kullanmalıdır. Bu, özellikle şifreli trafik içinde gizlenen bilinmeyen veya gelişen tehditleri tanımlamak için kritik öneme sahiptir.
5. **WebRTC Güvenlik En İyi Uygulamalarına Uygunluk:** WebRTC tabanlı platformları kullanan kuruluşlar, güvenli sinyalizasyon, doğru güvenlik duvarı yapılandırması ve sıkı erişim kontrolleri gibi en iyi uygulamaların titizlikle uygulanmasını sağlamalıdır. Geliştiriciler ve BT yöneticileri arasında yakın işbirliği, uçtan uca güvenliği sağlamak için hayati öneme sahiptir.
6. **Bulut ve SaaS Güvenliğine Öncelik Verilmesi:** Bulut tabanlı gerçek zamanlı iletişim platformlarının artan kullanımıyla birlikte, SaaS uygulamaları için gelişmiş güvenlik önlemleri, özellikle de YZ destekli tehdit tespiti ve kullanıcı davranışı analizi ile entegre olanlar, zorunludur.
7. **Uç Bilişim ve 5G Güvenliğinin Entegrasyonu:** Düşük gecikme ve yüksek bant genişliği gerektiren gerçek zamanlı uygulamalar için uç bilişim ve 5G'nin benimsenmesi, genişleyen saldırı yüzeylerini ele almak için sağlam güvenlik stratejileri gerektirmektedir.

8. **Blockchain Tabanlı Çözümlerin Keşfi:** İçerik orijinalliğini ve bütünlüğünü doğrulamak için blockchain tabanlı içerik doğrulama mekanizmalarının araştırılması, deepfake ve içerik ele geçirme tehditlerine karşı önemli bir karşı önlem sağlayabilir.
9. **Gelişmiş Şifreli Trafik Denetimi Yeteneklerinin Geliştirilmesi:** Kuruluşlar, şifreli trafiğin içindeki gizli tehditleri tespit etmek ve engellemek için tam TLS/SSL denetimi ve YZ destekli analiz gibi gelişmiş yeteneklere yatırım yapmalıdır.
10. **Kapsamlı Ağ Gözlemlenebilirliği Uygulaması:** YZ destekli tahmine dayalı operasyonlar ve tam yığın görünürlük de dahil olmak üzere gelişmiş gözlemlenebilirlik araçları, gerçek zamanlı medya akışlarının performansını ve güvenliğini sağlamak için kritik öneme sahiptir. Bu, sorunları proaktif olarak belirlemeye ve çözmeye yardımcı olacaktır.

Bu tekniklerin ve eğilimlerin benimsenmesi, kuruluşların 2025 yılında ve sonrasında sürekli gelişen siber tehdit ortamında gerçek zamanlı iletişimlerini güvence altına alabilmeleri için temel bir yol haritası sunmaktadır.

Alıntılanan çalışmalar

1. Web Security Trends Streamers Can't Afford to Ignore in 2025, erişim tarihi Haziran 5, 2025, https://onestream.live/blog/web-security-trends-for-streamers/
2. 5 Encrypted Attack Predictions for 2025 | Zscaler, erişim tarihi Haziran 5, 2025, https://www.zscaler.com/de/blogs/security-research/5-encrypted-attack-predictions-2025
3. AI-Driven Cybersecurity Threats in 2025 | Netrix Global - Netrix, LLC, erişim tarihi Haziran 5, 2025, https://netrixglobal.com/blog/cybersecurity/ai-driven-cyber-threats-what-to-expect-in-2025/
4. AI Security Report 2025: Understanding threats and building smarter defenses, erişim tarihi Haziran 5, 2025, https://blog.checkpoint.com/research/ai-security-report-2025-understanding-threats-and-building-smarter-defenses/
5. Top Video Conferencing Trends to Watch in 2025 - Neat, erişim tarihi Haziran 5, 2025, https://neat.no/resources/top-video-conferencing-trends-to-watch-in-2025/
6. VPN vs Zero Trust (ZTNA): The Key Transition for Secure Remote ..., erişim tarihi Haziran 5, 2025, https://blog.reemo.io/vpn-zero-trust-ztna-transition-2025
7. 5 Predictions for Zero Trust and SASE in 2025: What's Next? - Zscaler, erişim tarihi Haziran 5, 2025, https://www.zscaler.com/blogs/product-insights/5-predictions-zero-trust-and-sase-2025-what-s-next
8. Video surveillance in 2025: what trends stand out? - Controlex, erişim tarihi Haziran 5, 2025,

https://www.controlex.eu/en/blog-post/video-surveillance-trends-2025
9. 6 Essential WebRTC Security Best Practices for 2025 - DEV ..., erişim tarihi Haziran 5, 2025, https://dev.to/tsahil/6-essential-webrtc-security-best-practices-for-2025-1f9n
10. Scanning and abusing the QUIC protocol - SANS Internet Storm Center, erişim tarihi Haziran 5, 2025, https://isc.sans.edu/diary/30720
11. QUIC Decryption - Cisco Secure Essentials, erişim tarihi Haziran 5, 2025, https://secure.cisco.com/secure-firewall/docs/quic-decryption
12. Deep Packet Inspection Market Size to Hit USD 254.37 Billion by 2034, erişim tarihi Haziran 5, 2025, https://www.precedenceresearch.com/deep-packet-inspection-market
13. Deep Packet Inspection (DPI) Market Size and Growth Forecast - openPR.com, erişim tarihi Haziran 5, 2025, https://www.openpr.com/news/4045758/deep-packet-inspection-dpi-market-size-and-growth-forecast
14. Top 9 Network Observability Tools in 2025 - Research AIMultiple, erişim tarihi Haziran 5, 2025, https://research.aimultiple.com/network-observability-tools/
15. Observability Trends in 2025 – What's Driving Change? | CNCF, erişim tarihi Haziran 5, 2025, https://www.cncf.io/blog/2025/03/05/observability-trends-in-2025-whats-driving-change/
16. philarchive.org, erişim tarihi Haziran 5, 2025, https://philarchive.org/archive/JAYANT
17. Anomaly Detection Machine Learning: How It Works in 2025 | Label ..., erişim tarihi Haziran 5, 2025, https://labelyourdata.com/articles/anomaly-detection-machine-learning
18. 2025 Trends in Edge Computing | OTAVA, erişim tarihi Haziran 5, 2025, https://www.otava.com/2025-trends-in-edge-computing-security/
19. Data Transmission Security: 2025 Guide - Yomu AI, erişim tarihi Haziran 5, 2025, https://www.yomu.ai/blog/data-transmission-security-2025-guide
20. Call for Papers – TMA Conference 2025 - TMA Conferences, erişim tarihi Haziran 5, 2025, https://tma.ifip.org/2025/call-for-papers/
21. WO/2025/109469 EXPERT PANEL MODELS FOR NEURAL NETWORK ANOMALY DETECTION AND THWARTING ADVERSARIAL ATTACKS - WIPO Patentscope, erişim tarihi Haziran 5, 2025, https://patentscope.wipo.int/search/en/WO2025109469
22. SaaS Application Security Insights 2025, erişim tarihi Haziran 5, 2025, https://saasalerts.com/saas-application-security-insights-2025/
23. New Features Introduced in February 2025 - Palo Alto Networks, erişim tarihi Haziran 5, 2025, https://docs.paloaltonetworks.com/saas-security/release-notes/features-introduced-in-2025/february-2025
24. Edge Computing in 2025: Decentralizing Data for Enhanced Performance and Security, erişim tarihi Haziran 5, 2025, https://www.minovateck.com/edge-computing-in-2025-decentralizing-data-for-

enhanced-performance-and-security