Ağ Trafiği Analizi 2025: Gelişmiş Güvenlik ve Performans için Temel Eğilimler ve Teknolojiler

1. Yönetici Özeti

Bu rapor, 2025 yılına kadar ağ trafiği analizini şekillendirecek dönüştürücü eğilimleri ve teknolojileri derinlemesine incelemektedir. Gelişmiş Yapay Zeka (AI) ve Makine Öğrenimi (ML) tekniklerinin entegrasyonu, Sıfır Güven Mimarisi (ZTA) gibi temel güvenlik yaklaşımları, Birleşik Güvenli Erişim Hizmeti Kenarı (SASE) gibi mimari evrimler, Genişletilmiş Tespit ve Yanıt (XDR) ile kapsamlı tehdit görünürlüğü, gelişmiş Ağ Gözlemlenebilirliği ile proaktif içgörüler ve Kuantum Güvenli Ağ Oluşturma gibi uzun vadeli zorunluluklar ele alınmaktadır. Bu birbirine bağlı gelişmelerin, kuruluşların reaktif izlemeden öngörücü güvenlik duruşlarına ve optimize edilmiş ağ performansına nasıl geçiş yapmalarını sağlayacağı vurgulanmaktadır. Nihayetinde, bu rapor, iyi huylu ve kötü niyetli ağ davranışlarını etkili bir şekilde ayırt etmek için gerekli stratejileri ve araçları sunmaktadır.

2. Giriş: Ağ Trafiği Analizinin Gelişen Manzarası

Günümüzün dijital ortamında, ağ trafiği analizi, ağ güvenliği ve performansının temel taşı olmaya devam etmektedir. Kullanıcının mevcut projesi, Scapy gibi kütüphanelerle gerçek zamanlı ağ trafiğini dinleyerek HTTP, TCP ve UDP gibi protokolleri tanımlamaya ve anormal davranışları tespit etmeye odaklanmaktadır. Bu temel çalışma kritik olmakla birlikte, modern ağların artan karmaşıklığı ve siber tehditlerin gelişmiş doğası karşısında sürekli olarak evrim geçirmesi gerekmektedir.

Ağlar, artan veri hacimleri, bulut, hibrit, uç ve Nesnelerin İnterneti (IoT) gibi dağıtık ortamların yaygınlaşması ve gelişmiş kalıcı tehditlerin yükselişi ile karakterize edilen, hızla genişleyen ve giderek daha karmaşık hale gelen bir tehdit ortamında faaliyet

göstermektedir. Bu bağlamda, ağ izlemede geleneksel, çevre odaklı ve reaktif yaklaşımlardan daha akıllı, proaktif ve öngörücü bir analitik yaklaşıma doğru bir paradigma kayması gözlemlenmektedir. Bu evrim, yalnızca güvenlik olaylarını tespit etmekle kalmayıp, aynı zamanda performans düşüşlerini ve güvenlik ihlallerini öngörme ve önleme zorunluluğundan kaynaklanmaktadır. Bu rapor, 2025 ve sonrasında etkili ve yaygın olması beklenen kritik eğilimlere ve teknolojilere odaklanarak, tüm bilgilerin güncel, doğrulanabilir ve kanıta dayalı olmasını sağlamaktadır.

3. 2025 Ağ Trafiği Analizi için Temel Eğilimler ve Teknolojiler

3.1. Yapay Zeka Destekli Anomali Tespiti ve Öngörücü Gözlemlenebilirlik

Yapay zeka destekli anomali tespiti ve öngörücü gözlemlenebilirlik, ağ trafiği analizinde önemli bir dönüşümü temsil etmektedir. Bu eğilim, ağ telemetri verilerinin (günlükler, metrikler, izlemeler) devasa akışlarını analiz etmek için gelişmiş yapay zeka (AI) ve makine öğrenimi (ML) algoritmalarını kullanır. Bu algoritmalar, normal davranıştan sapmaları belirleyebilir ve potansiyel sorunları tırmanmadan önce tahmin edebilir.[1] Geleneksel kural tabanlı sistemlerin aksine, AI/ML modelleri, insan analistlerinin veya imza veritabanlarının gözden kaçırabileceği ince, alışılmadık kalıpları tanıyarak yeni veya "sıfır gün" saldırılarını tespit etme yeteneğine sahiptir.[1]

Özellikle, denetimsiz öğrenme teknikleri, örneğin otomatik kodlayıcılar, Destek Vektör Makineleri (SVM) ve Kendi Kendini Organize Eden Haritalar (SOM) gibi, kötü niyetli etkinliğin önceden etiketlenmiş veri kümelerini gerektirmediği için kritik öneme sahiptir. Bu, daha önce görülmemiş tehditlerin tespit edilmesini mümkün kılar.[1] Ayrıca, Büyük Dil Modelleri (LLM'ler) anomali modellemesine yardımcı olmak için ortaya çıkmaktadır. Bu modeller, çeşitli hata modlarını sistematik olarak üreterek, ilgili metrikleri belirleyerek ve anormal davranışları tanımlayarak bu bilgiyi gerçek dünya bulut altyapısı metrikleriyle eşleştirir.[3] Bu, AIOps'u sadece izlemeden öteye, otomatik teşhis, çözüm ve önleyici eylemlere taşımaktadır.[4]

Ağ trafiğinin muazzam hacmi ve hızı, özellikle 5G ağlarının ve hızla büyüyen ML eğitim kümelerinin ortaya çıkmasıyla, manuel veya imza tabanlı anomali tespitini uygulanamaz

hale getirmektedir.[1] AI destekli çözümler, bu ölçekteki verileri işlemek, hesaplama yükünü azaltmak ve gelişmiş, bilinmeyen tehditlerin gerçek zamanlı tespitini sağlamak için vazgeçilmezdir.[1] Bu, reaktif problem teşhisinden öngörücü analitiğe ve otomatik iyileştirmeye geçiş, sistem güvenilirliğini önemli ölçüde artırır, kesinti süresini azaltır ve kaynak tahsisini optimize eder.[2]

2025 yılına gelindiğinde, yapay zeka destekli anomali tespiti, ağ güvenliği ve operasyonlarının ayrılmaz bir parçası olacaktır. Bu teknoloji, sistem arızalarını tahmin ederek ve kök neden analizini otomatikleştirerek gelişmiş güvenilirlik ve azaltılmış manuel müdahale sağlayacaktır.[2] Uygulama alanları arasında akıllı uyarı önceliklendirme, dağıtık ML eğitimi gibi benzersiz iş yükleri için ağ yapılandırmalarını optimize etme [5] ve kaynak tahsisinin sürekli optimizasyonu yer almaktadır. Bu yetenek, bulut altyapıları, 5G ağları ve özel ML kümeleri gibi modern, yüksek dinamik ortamların karmaşıklığını yönetmek ve kararlılıklarını sağlamak için hayati öneme sahiptir.[1]

Veri hacmi ve saldırıların karmaşıklığı, anomali tespitinde sürekli bir "silahlanma yarışı"nı tetiklemektedir. Geleneksel paket tabanlı analiz ve imza tabanlı tespit, 5G ağlarının getirdiği yüksek paket sayıları ve sıfır gün saldırılarını tespit edememe gibi nedenlerle yetersiz kalmaktadır.[1] Ayrıca, makine öğrenimi eğitim kümelerinin büyümesi [5], benzersiz, patlamalı trafik modelleri sunarak basit kural tabanlı izlemenin ötesine geçmeyi gerektirmektedir. Bu durum, kuruluşların yalnızca statik kurallara veya insan gözetimine güvenemeyeceğini göstermektedir. Ağ trafiğinin artan hacmi ve karmaşıklığı, AI destekli ve akış tabanlı analize doğru sürekli bir evrimi zorunlu kılmaktadır. Bu, savunma yeteneklerinin yeni saldırı vektörlerine ve ağ özelliklerine sürekli uyum sağlamasını gerektiren bir rekabet ortamı yaratmaktadır.

Yapay zeka, sadece otomasyon sağlamakla kalmayıp, aynı zamanda insan-makine işbirliğini de güçlendirmektedir. AIOps'un insan iş yükünü azalttığı ve kendi kendini iyileştiren BT ortamlarını mümkün kıldığı belirtilmektedir.[4] LLM destekli anomali modellemesi, LLM'lerin hata modları ve metrikler hakkında bilgi ürettiği bir süreci içerir ve bu bilgiler insan mühendisleri veya diğer AI modelleri tarafından kullanılır.[3] Bu durum, yapay zekanın insan yeteneklerini artırdığını, tam otomasyondan ziyade bir destekleyici rol oynadığını göstermektedir. Yapay zeka rutin görevleri otomatikleştirirken ve daha hızlı yanıtlar sağlarken, daha derin etkisi, öngörücü içgörüler, bağlamsal anlayış ve anomali modellerinin oluşturulmasının otomatikleştirilmesi yoluyla insan yeteneklerini artırmaktır. Bu, gelecekte insan güvenlik analistlerinin, uyarı yorgunluğundan bunalmak yerine, stratejik karar alma ve karmaşık araştırmalara odaklanan "yapay zeka orkestratörleri" veya "yapay zeka destekli tehdit avcıları" haline geleceğini düşündürmektedir. AIOps için etik uygulama standartlarının belirtilmesi [4], uygun insan gözetimi ve yapay zeka sistemleriyle işbirliğinin önemini

daha da vurgulamaktadır.

Özelleşmiş iş yükleri için özel ağ analizine olan ihtiyaç artmaktadır. Makine öğrenimi eğitim trafiğinin benzersiz özellikleri (yüksek bant genişliği, düşük gecikme süresi, düşük entropi desenleri, patlamalı davranış) ve özel trafik mühendisliği optimizasyonlarına duyulan ihtiyaç açıkça belirtilmiştir.[5] Sanal Gerçeklik (VR) teknolojisi de gerçek zamanlı, düşük ek yük UDP iletişimi gereksinimleriyle öne çıkmaktadır.[6] Bu durum, yapay zeka/makine öğrenimi eğitimi ve VR gibi özel, yüksek talep gören uygulamalar yaygınlaştıkça, genel ağ analiz araçlarının yetersiz kalacağını göstermektedir. Kullanıcının şu anda genel HTTP/TCP/UDP'ye odaklanan projesi, bu yeni protokol davranışlarının ve trafik modellerinin nüanslarını anlamak için kapsamını genişletmek zorunda kalacaktır. Bu, ağ trafiği analizinin daha alan odaklı hale geldiği, uygulama katmanı davranışlarının ve bunların temel ağ altyapısı üzerindeki kesin etkilerinin daha derinlemesine anlaşılmasını gerektirdiği bir geleceğe işaret etmektedir. Bu, "iyi" ve "kötü" trafiği doğru bir şekilde tanımlamak için kritik öneme sahiptir.

Aşağıdaki tablo, 2025 yılında ağ anomali tespiti için temel AI/ML tekniklerini özetlemektedir:

Tablo 1: 2025 Ağ Anomali Tespiti için Temel AI/ML Teknikleri

Teknik	Nasıl Çalışır?	Ağ Analizi için Temel Fayda	İlgili Kaynak
Denetimsiz Öğrenme (örn. Otomatik Kodlayıcılar, SVM, SOM)	Etiketli veri olmadan normal kalıpları öğrenir ve sapmaları anomali olarak işaretler.	Bilinmeyen tehditleri ve sıfır gün saldırılarını tespit eder.	1
Büyük Dil Modelleri (LLM'ler)	Hata modları, metrikler ve anormal davranışlar hakkında bilgi üreterek bunları gerçek dünya verileriyle eşleştirir.	Anomali modeli oluşturmayı ve bağlamsallaştırmayı otomatikleştirir.	3
Öngörücü Analitik	Geçmiş verilere dayanarak gelecekteki sistem durumlarını ve potansiyel sorunları tahmin eder.	Proaktif sorun önleme ve optimize edilmiş kaynak tahsisi sağlar.	2

3.2. Sıfır Güven Mimarisi (ZTA) Temel Bir Güvenlik Paradigması Olarak

Sıfır Güven Mimarisi (ZTA), siber güvenlik felsefesinde temel bir kaymayı temsil etmektedir. Geleneksel çevre tabanlı güvenlik modelinden uzaklaşarak "asla güvenme, her zaman doğrula" yaklaşımına geçiş yapar.[7] Bu, ağ içinde veya dışında konumundan bağımsız olarak hiçbir kullanıcı, cihaz veya uygulamanın doğal olarak güvenilir olmadığı anlamına gelir. Temel ilkeler arasında güçlü kimlik doğrulama (genellikle çok faktörlü kimlik doğrulama - MFA), en az ayrıcalık ilkesinin uygulanması (yalnızca işlevler için gerekli izinlerin verilmesi), tüm ağ etkinliğinin sürekli izlenmesi ve analizi ile ayrıntılı erişim kontrol politikaları yer alır.[7] Mikro segmentasyon, şifreleme, uç nokta güvenliği ve bulut güvenliği gibi teknolojiler kritik kolaylaştırıcı unsurlardır.[7] Erişim kontrolü, yapılandırılmış izinler için Rol Tabanlı Erişim Kontrolü (RBAC) veya daha dinamik, bağlam duyarlı kararlar için Nitelik Tabanlı Erişim Kontrolü (ABAC) aracılığıyla uygulanabilir.[7]

Giderek karmaşıklaşan ve dinamikleşen dijital ortamda, geleneksel güvenlik modelleri gelişmiş siber tehditlere ve ağ içindeki yanal hareketlere karşı yetersiz kalmaktadır.[7] ZTA, hassas bilgileri korumak, güvenli operasyonları sürdürmek ve kapsamlı ve esnek güvenlik duruşları sağlamak için hayati öneme sahiptir.[7] Aşırı ayrıcalıkları en aza indirerek ve her erişim isteğini sürekli doğrulayarak saldırı yüzeyini önemli ölçüde azaltır, böylece ele geçirilmiş kimlik bilgilerinden veya içeriden gelen tehditlerden kaynaklanan riskleri azaltır.[7]

2025 yılına gelindiğinde, ZTA kurumsal güvenlik stratejilerinin temel taşı olacaktır. Uygulama alanları arasında hibrit ve çoklu bulut ortamlarının güvenliği, kritik altyapının korunması ve dağıtık işgücü genelinde veri bütünlüğünün sağlanması yer almaktadır.[8] Yetkisiz erişimi ve yanal hareketi önleyerek ihlal risklerinde ve finansal kayıplarda önemli düşüşlere yol açacaktır.[8] ZTA ilkelerinin SASE [9] ve XDR [12] gibi diğer teknolojilerle entegrasyonu, daha sağlam ve uyarlanabilir bir güvenlik ekosistemi oluşturacaktır. Uygulama, stratejik altyapı değerlendirmesi, gelişmiş kimlik doğrulama, akıllı güvenlik entegrasyonu ve departmanlar arası kültürel benimsemenin teşvik edilmesine odaklanacaktır.[10]

ZTA, sadece bir teknoloji dağıtımı olmaktan öte, kültürel ve operasyonel bir dönüşümü ifade etmektedir. Araştırmalar, "işgücü benimseme direnci", "kültürel benimsemenin teşvik edilmesi", "personel eğitimi" ve "değişikliklerin neden gerekli olduğunun

iletilmesi" gibi konuları önemli zorluklar olarak vurgulamaktadır.[8] Bu, sadece teknik entegrasyon zorluklarının ötesine geçmektedir. Ayrıca, güvenlik farkındalığı kültürünün teşvik edilmesi de ZTA'nın başarısı için kritik bir faktördür.[7] Başarılı ZTA uygulamasının, organizasyonel değişim yönetimi, açık iletişim ve sürekli eğitimle, doğru teknolojilerin dağıtılması kadar yakından ilişkili olduğu anlaşılmaktadır. İnsan faktörünün ihmal edilmesi, önemli sürtünmelere, verimlilikte düşüşe ve nihayetinde başarısız bir güvenlik dönüşümüne yol açabilir. Bu durum, ZTA ortamındaki ağ trafiği analizinin, tehdit tespiti için kullanıcı davranış analitiğini (UEBA) kullanmanın yanı sıra, benimseme kalıplarını anlamak ve kullanıcı deneyimi optimizasyonu alanlarını belirlemek için de kullanılması gerektiğini göstermektedir.

ZTA, daha geniş BT modernizasyonu ve entegrasyonu için bir katalizör görevi görmektedir. ZTA'nın eski sistemler, çeşitli bulut ortamları ile entegrasyonu ve ara katman çözümlerine duyulan ihtiyaç vurgulanmaktadır.[8] Ayrıca, ZTA'nın "tutarlı bir güvenlik çerçevesi oluşturmak için bileşenler" içerdiği belirtilmiştir.[7] ZTA'yı uygulamak, genellikle kuruluşları veri akışlarının ve erişim noktalarının kapsamlı bir haritalamasını yapmaya [8], teknoloji yığınlarını düzene sokmaya ve güncel olmayan sistemleri güncellemeye zorlar. Bu, ZTA'yı sadece bir güvenlik girişimi değil, daha geniş BT modernizasyonu için önemli bir itici güç haline getirir ve birleşik politikalar ile entegre güvenlik çözümlerini teşvik eder. ZTA'ya geçiş, tüm varlıklar üzerinde daha iyi görünürlük ve kontrol gerektirir; bu da kullanıcının "iyi" ve "kötü" trafiği belirleme projesine doğrudan fayda sağlar, doğrulanmış kimliklere ve yetkili erişime dayalı daha tanımlı bir "iyi" taban çizgisi sağlar.

Dinamik ortamlar için ayrıntılı erişim ve sürekli izleme arasındaki etkileşim kritik öneme sahiptir. ZTA, "ayrıntılı erişim kontrol politikaları" (RBAC/ABAC) ve "sürekli izleme ve analitik" arasındaki sinerjiyi vurgular.[7] Ayrıca, "kesintisiz izleme" ve "meşru ve şüpheli erişim kalıplarını belirleme"nin önemi de belirtilmiştir.[8] XDR çözümleri de kimlik güvenliğini ve erişim olaylarının takibini vurgulamaktadır.[12] Dinamik ortamlarda (örn. bulut, uzaktan çalışma), erişim ihtiyaçları sürekli değişir. ZTA'nın gücü, statik (RBAC) ve dinamik (ABAC) erişim kontrollerini gerçek zamanlı, sürekli izlemeyle birleştirmesinde yatmaktadır. Bu sürekli geri bildirim döngüsü, anormal davranış tespit edildiğinde ayrıcalıkların anında iptal edilmesini sağlayarak ağı doğal olarak daha esnek hale getirir. Ağ trafiği analizi için bu, sadece hangi protokollerin kullanıldığını belirlemekten öteye, kimin, nereden ve neden kullandığını anlamaya doğru bir kayma anlamına gelir ve daha hassas anomali tespiti için kritik bağlamsal bilgiler ekler.

Aşağıdaki tablo, Sıfır Güven Mimarisinin temel ilkelerini ve bunların güvenlik faydalarını detaylandırmaktadır:

Tablo 2: Sıfır Güven Mimarisinin Temel İlkeleri ve Güvenlik Faydaları

İlke	Açıklama	Doğrudan Güvenlik Faydası	İlgili Kaynak
Güçlü Kullanıcı Doğrulaması	Erişime izin vermeden önce her kullanıcıyı/cihazı Çok Faktörlü Kimlik Doğrulama (MFA) ile doğrular.	Yetkisiz erişimi ve kimlik bilgisi ihlalini önler.	[7]
En Az Ayrıcalık Erişimi	Bir kullanıcının veya cihazın işlevini yerine getirmesi için yalnızca minimum gerekli izinleri verir.	Potansiyel saldırı yüzeyini ve ihlallerin etkisini azaltır.	[7]
Sürekli İzleme ve Analitik	Tüm ağ etkinliğinin ve erişim girişimlerinin gerçek zamanlı olarak toplanması ve analizi.	Proaktif tehdit tespitini ve hızlı yanıtı mümkün kılar.	[7]
Ayrıntılı Erişim Kontrolü	Kullanıcı, cihaz ve çevresel özelliklere dayalı ince taneli erişim politikaları uygular.	Aşırı ayrıcalıklardan kaynaklanan riskleri en aza indirir ve bağlam duyarlı erişim sağlar.	[7]
Mikro Segmentasyon	Ağları küçük, izole güvenlik segmentlerine ayırarak yanal hareketi sınırlar.	İhlalleri sınırlar ve ağ içinde yayılmasını engeller.	[7]

3.3. Birleşik Güvenli Erişim Hizmeti Kenarı (SASE) ile Birleşik Ağ Güvenliği

Güvenli Erişim Hizmeti Kenarı (SASE), geniş alan ağı (WAN) ve ağ güvenliği işlevlerini tek, birleşik, bulut tabanlı bir hizmette birleştiren bulut tabanlı bir mimari modeldir.[9] Temel entegre güvenlik işlevleri arasında Hizmet Olarak Güvenlik Duvarı (FWaaS), Sıfır Güven Ağ Erişimi (ZTNA), Güvenli Web Ağ Geçidi (SWG), Bulut Erişim Güvenlik Aracısı (CASB) ve Veri Kaybı Önleme (DLP) bulunmaktadır.[9] SASE, küresel bir Erişim Noktaları

(PoP) ağı kullanarak güvenliği kullanıcıya ve ağın kenarına, konumlarından bağımsız olarak getirir.[11] Bu model, birden fazla, ayrı güvenlik çözümüne ve karmaşık donanıma olan ihtiyacı azaltarak yönetimi basitleştirir.[9]

Uzaktan ve hibrit çalışma modellerine geçiş, bulut hizmetlerinin ve SaaS uygulamalarının yaygınlaşmasıyla birleştiğinde, geleneksel çevre tabanlı güvenliği etkisiz hale getirmiştir.[9] SASE, dağıtık ekipler için tutarlı güvenlik politikaları ve optimize edilmiş performans sağlayarak, herhangi bir konumdan güvenli bağlantı sağlayarak bu zorlukları ele almaktadır.[11] Karmaşıklığı azaltır, yerleşik sıfır güven ilkeleri aracılığıyla güvenliği artırır ve modern, dinamik iş operasyonları için kritik olan ağ kaynak dağıtımını (hız, gecikme) optimize eder.[9]

2025 yılına gelindiğinde, SASE, özellikle uzaktan ve hibrit işgücüne sahip kuruluşlar için kurumsal ağ stratejilerinin ayrılmaz bir bileşeni olması beklenmektedir.[11] Bulut tabanlı yapısı, gelişen iş ihtiyaçlarını karşılamak için kolay ölçeklenebilirlik sağlar ve genişleyen dijital ortamları yönetmek için uygun maliyetli bir yol sunar.[9] SASE, sıfır güven ilkelerini uygulayarak, tüm iletişim kanalları için uçtan uca şifreleme sağlayarak ve IoT/uç cihazlarını güvence altına alarak güvenliği artıracaktır.[11] Ayrıca, merkezi güvenlik politikaları ve veri koruma önlemleri aracılığıyla düzenleyici uyumluluğun (örn. NIS2, DORA) sağlanmasında da kritik bir rol oynayacaktır.[11] Dahası, SASE çerçevelerine AI/ML ve Kullanıcı ve Varlık Davranış Analitiği (UEBA) entegrasyonu, otomatik tehdit tespitini ve proaktif tehdit yönetimini önemli ölçüde iyileştirecektir.[11]

SASE, dağıtık ortamlar için Sıfır Güven'in mimari bir tezahürü olarak işlev görmektedir. SASE'nin "sıfır güven ilkelerini içerdiği" ve "yalnızca kimliği doğrulanmış ve yetkilendirilmiş kullanıcıların ağa erişmesini sağladığı" açıkça belirtilmiştir.[9] Ayrıca, SASE içinde "Sıfır Güven Ağ Erişimi (ZTNA) Yükselişi" de vurgulanmaktadır.[11] Bu durum, SASE'nin sadece bir güvenlik ve ağ araçları koleksiyonu olmadığını, modern, dağıtık işgücü için ZTA'yı ölçeklenebilir ve etkili kılan pratik, bulut tabanlı bir uygulama modeli olduğunu göstermektedir. Kullanıcının projesi için bu, SASE ortamındaki ağ trafiği analizinin, yalnızca IP adresleri veya geniş ağ segmentleri yerine, giderek kimlik tabanlı bağlama (kimin neye, nereden eriştiği) dayanacağı anlamına gelir. Bu, ayrıntılı ZTNA politikalarına dayalı olarak daha hassas "iyi" ve "kötü" trafik sınıflandırmasına olanak tanır ve basit protokol tanımlamasının ötesine geçer.

SASE'nin benimsenmesi için ekonomik ve operasyonel bir zorunluluk bulunmaktadır. SASE'nin "karmaşıklığı azalttığı", "operasyonları düzene soktuğu", "uygun maliyetli" olduğu ve "TCO optimizasyonu" sağladığı belirtilmiştir.[9] Ayrıca, sınırlı kaynaklara sahip KOBİ'lerin (Küçük ve Orta Ölçekli İşletmeler) de SASE'yi benimsediği vurgulanmaktadır.[11] Güvenlik faydalarının ötesinde, SASE, birden fazla nokta çözümünü

tek, birleşik bir platformda birleştirerek önemli operasyonel verimlilikler ve maliyet tasarrufları sunmaktadır. Bu, SASE'yi sadece büyük işletmeler için değil, aynı zamanda KOBİ'ler için de cazip hale getirerek daha geniş bir benimsemeyi teşvik etmektedir. Bu durum, ağ trafiği analiz araçları pazarının, SASE platformlarıyla sorunsuz bir şekilde entegre olabilen veya bunların bir parçası olabilen çözümleri giderek daha fazla tercih edeceğini göstermektedir. Bu, bağımsız izlemeden, daha geniş iş hedefleriyle uyumlu entegre güvenlik ve performans yönetimine doğru bir kaymayı işaret etmektedir.

SASE/Sıfır Güven dünyasında ağ segmentasyonunun rolü de evrim geçirmektedir. "Ağ segmentasyonu tehditleri içerir" ve "ağları segmentlere ayırmak ihlal yayılımını sınırlar" ifadeleri yer almaktadır.[9] Ancak, ZTNA'nın "erişim kontrollerini ağ tabanlıdan kimlik tabanlıya kaydırdığı" da vurgulanmıştır.[11] Geleneksel ağ segmentasyonu (örn. VLAN'lar, güvenlik duvarları) tehditleri içermede önemli olmaya devam etse de, SASE/ZTNA modeli

mikro segmentasyona ve *kimlik tabanlı segmentasyona* doğru ilerlemektedir. Bu, geniş ağ segmentleri yerine, erişimin çok daha ince bir düzeyde, bireysel uygulamalara veya hatta bir uygulama içindeki belirli işlevlere kadar, kullanıcı kimliği ve bağlamına göre kontrol edildiği anlamına gelir. Ağ trafiği analizi için bu, izlemenin daha ayrıntılı ve bağlam duyarlı hale gelmesi gerektiği anlamına gelir; sadece "segmentler arası trafik" değil, "belirli kullanıcılar/cihazlar ile belirli kaynaklar arasındaki trafik" anlaşılmalıdır. Bu, Sıfır Güven çerçevesinde yanal hareketi ve ayrıcalık yükseltme girişimlerini belirlemek için kritik öneme sahiptir.

Aşağıdaki tablo, SASE ile geleneksel ağ güvenliği yaklaşımları arasındaki karşılaştırmalı bir genel bakışı sunmaktadır:

Tablo 3: SASE ve Geleneksel Ağ Güvenliği: 2025 için Karşılaştırmalı Bir Genel Bakış

Özellik/Yön	Geleneksel Model	SASE Modeli	SASE'nin Avantajı	İlgili Kaynak
Mimari	Çevre tabanlı, cihaz merkezli	Bulut tabanlı, kimlik merkezli	Uzaktan ve hibrit işgücü için gelişmiş güvenlik	[9]
Güvenlik Modeli	Güvenlik yığınına merkezi trafik geri taşıma	Güvenlik kenarda sağlanır	Optimize edilmiş performansla iyileştirilmiş kullanıcı	[9]

			deneyimi	
Yönetim Karmaşıklığı	Ayrı güvenlik araçları, karmaşık yönetim	Birleşik güvenlik platformu, basitleştirilmiş yönetim	Azaltılmış operasyonel yük ve Toplam Sahip Olma Maliyeti (TCO)	[9]
Ölçeklenebilirlik	Sınırlı ölçeklenebilirlik	Yüksek düzeyde ölçeklenebilir	İş büyümesine ve gelişen tehditlere uyum sağlama çevikliği	[9]
Temel Entegre Bileşenler	Ayrı güvenlik duvarları, VPN'ler, SWG'ler	Entegre FWaaS, ZTNA, SWG, CASB, DLP	Herhangi bir konumdan tutarlı güvenlik politikaları	[9]

3.4. Bütünsel Tehdit Görünürlüğü için Genişletilmiş Tespit ve Yanıt (XDR)

Genişletilmiş Tespit ve Yanıt (XDR), bir kuruluş içindeki birden fazla güvenlik katmanı ve alanı genelinde tehdit verilerini toplayan ve otomatik olarak ilişkilendiren birleşik bir güvenlik çözümüdür. Bu alanlar tipik olarak uç noktaları, ağları, bulut ortamlarını, kimlik ve erişim yönetimi (IAM) sistemlerini ve e-postayı içerir.[12] XDR araçları, bu farklı kaynaklardan telemetri alarak verileri tehdit istihbaratıyla zenginleştirir, ilgili güvenlik olaylarını belirler ve bunları tutarlı olay anlatılarına veya "çok adımlı olay zaman çizelgelerine" birleştirir.[13] Bu bütünsel görünüm, Güvenlik Operasyon Merkezi (SOC) ekipleri için daha hızlı önceliklendirme, uyarı gürültüsünün azaltılması ve ana bilgisayar izolasyonu veya kullanıcı hesabı devre dışı bırakma gibi önceden tanımlanmış veya uyarlanabilir yanıt eylemlerini kolaylaştırır.[13] XDR, EDR veya güvenlik duvarları gibi mevcut araçların yerini almaz, ancak bağlam sağlayarak ve yanıtları koordine ederek yeteneklerini artırır.[13]

Modern siber saldırılar karmaşıktır ve genellikle birden fazla saldırı yüzeyini kapsar, bu da birbirinden ayrı güvenlik araçlarının etkili bir şekilde tespit etmesini ve yanıt vermesini zorlaştırır.[12] XDR, görünüşte ilgisiz şüpheli faaliyetler (örn. şüpheli oturum açma girişimleri, yanal hareket, dosya yürütme, veri sızdırma) arasındaki "noktaları birleştirerek" bir saldırının tüm kapsamına ilişkin kapsamlı bir anlayış sağlayarak bu

durumu ele alır.[13] Bu entegre yaklaşım, tehdit avcılığı yeteneklerini önemli ölçüde artırır, tespit ve yanıt sürelerini azaltır ve tehdit sınıflandırmasının genel doğruluğunu iyileştirir.[12]

2025 yılına gelindiğinde, XDR, Gelişmiş Kalıcı Tehditler (APT'ler), fidye yazılımları, kötü amaçlı yazılımlar ve sıfır gün açıklıkları gibi karmaşık tehditleri belirlemek için gelişmiş tehdit tespiti ve yanıt stratejilerinin temel taşı olacaktır.[12] Yetenekleri arasında gerçek zamanlı ağ saldırı yüzeyi kontrolü, çeşitli kaynaklardaki şüpheli unsurların otomatik keşfi ve otomatik iyileştirme yer alacaktır.[12] XDR çözümleri, bulut ve IoT ağları dahil olmak üzere karmaşık BT ortamlarında gelişmiş görünürlük sunacak ve ayrıcalıklı kullanıcılar için erişim olaylarını izleyerek ve analiz ederek kimlik güvenliğini iyileştirecektir.[12] Güçlü olmasına rağmen, XDR'nin bulut tabanlı ortamlardaki etkinliği, özellikle dinamik, geçici iş yüklerinde iyi huylu ve kötü niyetli faaliyetleri ayırt etmede ve ayrıntılı API/kontrol düzlemi faaliyetlerini izlemede gelişmeye devam edecektir.[13]

XDR, parçalanmış bir ortamda güvenlik verilerinin "orkestratörü" olarak konumlanmaktadır. XDR'nin "güvenlik araçlarından gelen farklı veri kaynaklarını birleştirdiği" ve "birden fazla ve farklı güvenlik katmanından tehdit sinyallerini ilişkilendirdiği" belirtilmiştir.[13] Ayrıca, XDR çözümlerinin uç noktalar, ağlar, bulut ve kimlik gibi çeşitli alanları kapsayan özelliklere sahip olduğu görülmektedir.[12] Bu durum, kuruluşların genellikle çok sayıda güvenlik aracıyla çalıştığını ve bunun da veri silolarına yol açtığını göstermektedir. XDR'nin temel değeri, mevcut araçları değiştirmek yerine, merkezi bir istihbarat merkezi olarak işlev görerek onları daha etkili hale getirmesidir. Karmaşık BT ortamlarında yaygın olan "uyarı yorgunluğu" ve "silolanmış veri" sorunlarını doğrudan ele almaktadır. Ağ trafiği analizi için bu, (Scapy tarafından toplanan gibi) ham trafik verilerinin, uç nokta, kimlik ve bulut günlüklerinden bağlam kazanarak, çok daha zengin ve doğru bir "iyi" ve "kötü" ayrımı yapılmasına olanak tanıyan birçok önemli girdiden biri haline geldiği anlamına gelir. Bu aynı zamanda güvenlik ekiplerinin odağını bireysel araç uyarılarını yönetmekten, birleşik olay anlatılarını anlamaya doğru kaydırmaktadır.

Bulut tabanlı görünürlük için XDR'nin gelişen bir zorluk olduğu gözlemlenmektedir. XDR'nin bulut tabanlı ayrıntı düzeyindeki sınırlamaları açıkça belirtilmiştir; Kubernetes, sunucusuz işlevler ve geçici kapsayıcı iş yüklerindeki yanlış yapılandırmaları gözden kaçırabileceği belirtilmiştir.[13] Ayrıca, temel API ve kontrol düzlemi izlemesinin genellikle yetersiz olduğuna dikkat çekilmiştir. XDR, geleneksel ve hibrit ortamlar için güçlü olsa da, bulut tabanlı mimarilerin hızlı evrimi, görünürlük boşlukları için yeni bir sınır sunmaktadır. Bu durum, gelecekteki XDR geliştirme ve dolayısıyla bulut ortamlarındaki ağ trafiği analizinin, gerçekten kapsamlı tespit sağlamak için buluta özgü telemetri (örneğin, Kod Olarak Altyapı (IaC), iş yükü kimliği, kaynak yapılandırması) ile daha

derinlemesine entegre olması gerekeceğini düşündürmektedir. Bu, modern, dinamik bulut dağıtımlarındaki trafiği analiz etme ve anormallikleri tespit etme yeteneğini doğrudan etkileyen kritik bir araştırma ve geliştirme alanıdır.

XDR'nin, uyarı yönetiminden olay anlatılarına geçişteki rolü önemlidir. XDR'nin, sadece uyarıları bir araya getirmek yerine "çok adımlı olay zaman çizelgeleri oluşturma" yeteneği ve "tutarlı olay anlatıları" sağlayarak "önceliklendirmeyi basitleştirme" yeteneği vurgulanmıştır.[13] Bu, reaktif uyarı yönetiminden proaktif olay yönetimine doğru önemli bir kavramsal sıçramayı temsil etmektedir. Güvenlik ekiplerinin bireysel, bağlantısız uyarılardan bunalmak yerine, XDR saldırının tutarlı bir "hikayesini" sunarak daha hızlı anlama ve daha etkili yanıt verme olanağı sağlar. Ağ trafiği analizi için bu, izole edilmiş anormal paketleri veya akışları tanımlamanın ötesine geçerek, bunların daha büyük bir saldırı zincirine nasıl uyduğunu anlamaya doğru bir kayma anlamına gelir, bu da daha stratejik ve daha az parçalı iyileştirme çabalarına olanak tanır. Bu yetenek, karmaşık, çok aşamalı saldırıları belirlemek için kritik öneme sahiptir.

Aşağıdaki tablo, 2025 yılındaki Genişletilmiş Tespit ve Yanıt (XDR) sistemlerinin temel yeteneklerini özetlemektedir:

Tablo 4: 2025 Yılında Genişletilmiş Tespit ve Yanıt (XDR) Sistemlerinin Temel Yetenekleri

Yetenek	Açıklama	Ağ Güvenliği için Fayda	İlgili Kaynak
Alanlar Arası Korelasyon	Uç noktalar, ağlar, bulut, kimlik ve e-postadan gelen verileri birleştirir ve bağlamsallaştırır.	Saldırı kampanyalarının bütünsel bir şekilde anlaşılmasını sağlar.	13
Otomatik Olay Yanıtı	Tehdit istihbaratına dayalı olarak önceden tanımlanmış veya uyarlanabilir yanıt eylemleri gerçekleştirir.	Daha hızlı ve daha kararlı iyileştirme sağlar.	13
Gelişmiş Tehdit Avcılığı	Tüm saldırı yüzeyinde proaktif olarak tehdit arar.	Ortaya çıkan tehditlere karşı proaktif savunmayı iyileştirir.	12

Azaltılmış Yanlış Pozitifler	Gerçek tehditleri iyi huylu faaliyetlerden doğru bir şekilde ayırt etmek için AI/ML kullanır.	Uyarı yorgunluğunu azaltır ve SOC verimliliğini artırır.	[12]
Saldırı Yüzeyi Kontrolü	Bağlı cihazların ve güvenlik açıklarının gerçek zamanlı olarak belirlenmesi ve yönetilmesi.	Saldırı yüzeyini en aza indirir ve Sıfır Güven ilkelerini uygular.	[12]
Kimlik Güvenliği	Kimlik kötüye kullanımını ve ayrıcalık yükseltmeyi engellemek için erişim olaylarını izler ve analiz eder.	Kimlik bilgisi kötüye kullanımına ve içeriden gelen tehditlere karşı koruma sağlar.	[12]

3.5. Gelişmiş Ağ Gözlemlenebilirliği ve OpenTelemetry

Ağ gözlemlenebilirliği, geleneksel izlemenin ötesine geçerek karmaşık sistemlerin iç durumuna ilişkin derin, gerçek zamanlı içgörüler sağlar ve bir şeyin *neden* olduğunu anlamayı mümkün kılar, sadece *olduğunu* değil.[2] Bunu, üç ana telemetri veri türünü toplayarak ve analiz ederek başarır: günlükler (ayrık olaylar), metrikler (zaman içindeki sayısal ölçümler) ve izlemeler (dağıtık sistemler genelinde uçtan uca istekler).[2] 2025 için önemli bir eğilim, kuruluşların bu telemetri verilerini verimli bir şekilde toplamasına, yönlendirmesine, işlemesine ve zenginleştirmesine olanak tanıyan

Gözlemlenebilirlik Boru Hatlarının yükselişidir. Bu, alım hacimlerini ve maliyetleri azaltırken, eski verileri standart tabanlı formatlara dönüştürür.[14] Ayrıca, sektör, birbirinden ayrı, tescilli araçlardan uzaklaşarak, satıcı kilitlenmesini azaltan ve birlikte çalışabilirliği teşvik eden, Cloud Native Computing Foundation (CNCF) tarafından kuluçkalanan bir proje olan

OpenTelemetry (OTEL) gibi açık standartlara yönelmektedir.[2] Tahmine dayalı analitik ve anomali tespitini içeren yapay zeka destekli gözlemlenebilirlik, potansiyel sistem arızalarını tahmin ederek ve kök neden analizini otomatikleştirerek bu alanı dönüştürmektedir.[2]

BT altyapılarının, özellikle çoklu bulut ortamları, mikro hizmetler ve Kubernetes ile artan karmaşıklığı, ezici miktarda çeşitli veri üretmektedir.[2] Geleneksel izleme araçları, bu farklı kaynaklardan gelen verileri ilişkilendirmede zorluk çekerek, gecikmeli sorun çözümü, parçalanmış görünürlük ve önemli operasyonel maliyetlere yol açmaktadır.[2] Gelişmiş gözlemlenebilirlik, özellikle yapay zeka ve standardizasyonla birlikte, kapsamlı, tam yığın görünürlük (ön uçtan bulut tabanlıya), sorunları proaktif olarak belirleme, BT bütçelerini optimize etme (FinOps) ve güvenlik entegrasyonunu (SecOps Gözlemlenebilirlik) geliştirme için kritik öneme sahiptir.[2]

2025 yılına gelindiğinde, gelişmiş ağ gözlemlenebilirliği, sistem kullanılabilirliğini, esnekliğini ve performansını sürdürmek için vazgeçilmez olacaktır. Tahmine dayalı bakımı, otomatik kök neden analizini ve daha hızlı iyileştirme stratejilerini mümkün kılarak kesinti süresini ve manuel müdahaleyi önemli ölçüde azaltacaktır.[2] SecOps Gözlemlenebilirliği, gerçek zamanlı tehdit tespiti, uyumluluk izleme ve denetim için güvenlik günlüklerini ve olay verilerini sorunsuz bir şekilde entegre edecektir.[2] Tam yığın gözlemlenebilirlik, sistem davranışının eksiksiz bir resmini sağlamak için ön uç uygulamalarını, uç cihazları ve bulut tabanlı ortamları kapsayacak şekilde genişleyecektir.[2] OpenTelemetry'nin benimsenmesi, standardizasyonu teşvik edecek, satıcı kilitlenmesini azaltacak ve çeşitli teknoloji yığınları genelinde veri yönetimini basitleştirecektir.[2] Bu, kuruluşların özellikle karmaşık hibrit bulut kurulumlarında BT harcamalarını optimize etmelerini sağlayacaktır.[14]

Gözlemlenebilirlik, yapay zeka destekli güvenlik ve operasyonlar için bir veri temeli görevi görmektedir. "Yapay Zeka Destekli Gözlemlenebilirlik" ile "tahmine dayalı analitik ve anomali tespiti" arasındaki bağlantı açıkça belirtilmiştir.[2] Ayrıca, yapay zekanın siber güvenlik için büyük veri hacimlerini analiz ettiği de belirtilmiştir.[14] Bu durum, gözlemlenebilir verinin kalitesi ve kapsamının, ağ analizinde yapay zeka/makine öğreniminin etkinliğini doğrudan etkilediğini vurgulamaktadır. Kapsamlı, yüksek kaliteli telemetri (günlükler, metrikler, izlemeler) verimli bir şekilde toplanıp işlenmeden (gözlemlenebilirlik boru hatları ve OpenTelemetry aracılığıyla), yapay zeka modelleri doğru içgörüler sağlamak için gerekli girdiden yoksun kalacaktır. Bu, gözlemlenebilirliğe yatırım yapmanın sadece operasyonel bir iyileştirme değil, aynı zamanda yapay zeka ve gelişmiş güvenlik çözümlerinin değerini en üst düzeye çıkarmak için bir ön koşul olduğu anlamına gelir. Bu durum, kullanıcının sofistike "iyi" ve "kötü" trafik modelleri oluşturma yeteneğini doğrudan etkilemektedir.

Gözlemlenebilirlik aracı konsolidasyonu ve açık standartların stratejik bir zorunluluk olduğu anlaşılmaktadır. Kuruluşların şu anda ortalama on gözlemlenebilirlik aracı kullandığı, bunun da parçalanmaya, artan maliyetlere ve veri yüküne yol açtığı belirtilmiştir.[14] Önerilen çözüm, "gözlemlenebilirlik aracı konsolidasyonu" ve satıcı

kilitlenmesini önlemek için OpenTelemetry'nin benimsenmesidir. Gözlemlenebilirlik araçlarının mevcut parçalanmış durumu, artan karmaşıklık ve operasyonel maliyetler nedeniyle sürdürülemezdir. Konsolidasyona ve OpenTelemetry gibi açık standartlara doğru hareket, sadece teknik bir tercih değil, operasyonel verimlilik, maliyet optimizasyonu (FinOps) ve iyileştirilmiş veri yönetişimi elde etmek için stratejik bir zorunluluktur. Kullanıcının projesi için bu, gelecekteki ağ trafiği analiz çözümlerinin, birlikte çalışabilirliği sağlamak ve tescilli veri formatlarına kilitlenmemek için OpenTelemetry ile entegre olması veya ondan yararlanması gerektiği anlamına gelir. Bu, analizi daha uyarlanabilir ve çeşitli BT ortamlarında ölçeklenebilir hale getirecektir.

Bulut tabanlı karmaşıklığı yönetmede gözlemlenebilirliğin kritikliği giderek artmaktadır. "Kubernetes Ortamlarının Artan Zorluğu" izleme ve sorun giderme açısından vurgulanmıştır.[14] Ayrıca, "tam yığın gözlemlenebilirlik evrimi"nin bulut tabanlı ortamları kapsayacak şekilde genişleyeceği belirtilmiştir.[2] Bulut tabanlı mimariler (örn. Kubernetes, sunucusuz işlevler, mikro hizmetler) geleneksel araçlarla izlenmesi zor olan dinamik, geçici bileşenler sunmaktadır. Gözlemlenebilirlik, bu karmaşık, hızla değişen ortamları yönetmek için gerekli derinlik ve genişlikte içgörü sağlayarak hem performansı hem de güvenliği garanti eder. Bu durum, 2025'teki ağ trafiği analizinin, trafiği doğru bir şekilde sınıflandırmak için kapsayıcı düzeyinde ve hizmet ağı etkileşimlerini anlamak üzere, basit paket denetiminin ötesine geçerek bulut tabanlı trafik akışlarının ve temel altyapılarının benzersiz özelliklerini giderek daha fazla hesaba katması gerektiğini ima etmektedir.

Aşağıdaki tablo, ağ izlemeden yapay zeka destekli gözlemlenebilirliğe geçişi detaylandırmaktadır:

Tablo 5: Ağ İzlemeden Yapay Zeka Destekli Gözlemlenebilirliğe Evrim (2025)

Yön	Geleneksel İzleme	Gelişmiş Gözlemlenebilirlik (2025)	Fayda	İlgili Kaynak
Birincil Odak	"Açık mı?"	"Neden böyle davranıyor?"	Daha hızlı Ortalama Çözüm Süresi (MTTR)	[2]
Veri Kaynakları	Cihaz merkezli (örn. CPU, bellek, bant genişliği)	Tam yığın (günlükler, metrikler, izlemeler, uygulamalardan,	Proaktif sorun önleme	[2]

		altyapıdan, buluttan gelen olaylar)		
Analiz Yöntemi	Eşik tabanlı uyarılar	AI/ML destekli analitik (tahmine dayalı, anomali tespiti, kök neden analizi)	Verimli veri yönetimi yoluyla maliyet optimizasyonu	[2]
Temel Hedef	Reaktif problem teşhisi	Tahmine dayalı ve Proaktif sorun çözümü	Dağıtık sistemler genelinde bütünsel görünürlük	[2]
Temel Teknolojiler	SNMP, Syslog, Ping	OpenTelemetry, Gözlemlenebilirlik Boru Hatları, AIOps platformları	Entegre SecOps aracılığıyla gelişmiş güvenlik duruşu	[2]

3.6. Geleceğe Yönelik Güvenlik için Kuantum Güvenli Ağ Oluşturma

Kuantum güvenli ağ oluşturma, gelecekteki, yeterince güçlü kuantum bilgisayarlarından gelecek saldırılara direnmek için tasarlanmış kriptografik yöntemlerin uygulanmasını ifade eder. İki ana yaklaşım bulunmaktadır:

- **Kuantum Sonrası Kriptografi (PQC):** Bunlar, klasik bilgisayarlarda çalışan ancak kuantum bilgisayarların bile verimli bir şekilde çözmesinin hesaplama açısından imkansız olduğu varsayılan matematiksel problemlere (örn. kafes tabanlı, kod tabanlı, karma tabanlı) dayanan yeni kriptografik algoritmalar. PQC zaten standartlaştırılmıştır ve satıcılar tarafından uygulanmaktadır.[15]
- **Kuantum Anahtar Dağıtımı (QKD):** Bu yaklaşım, kriptografik anahtarları güvenli bir şekilde oluşturmak ve değiş tokuş etmek için kuantum fiziği ilkelerini kullanır. BB84 (hazırla ve ölç) ve BBM92/MDI (dolaşıklık tabanlı) gibi QKD protokolleri, herhangi bir dinleme girişiminin kuantum durumunu temelden değiştirmesini sağlayarak tespitin kaçınılmaz olmasını sağlar.[15] QKD, IPsec gibi mevcut protokollerle standart anahtar dağıtım arayüzleri aracılığıyla entegre edilebilir.[15]

Genellikle, geleneksel kriptografiyi PQC ve/veya QKD ile birleştiren **hibrit kuantum**

direnci yaklaşımı önerilir. Bu, bir algoritma tehlikeye girse bile güvenlik sağlamak için derinlemesine savunma sağlar.[15]

Büyük ölçekli, hataya dayanıklı kuantum bilgisayarların mevcut açık anahtarlı kriptografiyi (örn. RSA, Diffie-Hellman) kırabilecek kadar yaygın olmamasına rağmen, "Şimdi Hasat Et, Sonra Şifresini Çöz" (HNDL) saldırıları nedeniyle tehdit önemlidir.[15] Bu, rakiplerin bugün şifrelenmiş hassas verileri toplayabileceği ve kuantum bilgisayarlar yeterince güçlü hale geldiğinde gelecekte şifresini çözebileceği anlamına gelir. Bu nedenle, kuruluşların uzun vadeli gizli bilgileri korumak için kuantum güvenli güvenliğe hemen geçiş yapmaları gerekmektedir.[15]

2025 yılına gelindiğinde, kuantum sonrası kriptografinin benimsenmesi, özellikle uzun vadeli veri koruması gerektiren uygulamalar için iyi bir şekilde ilerlemiş olacaktır. Pratik uygulamalar arasında kritik altyapı (örn. enerji şebekeleri, telekomünikasyon), finansal işlemler, tıbbi kayıtlar, yüksek değerli fikri mülkiyet ve devlet verileri için güvenli iletişim yer alacaktır.[15] Güvenli ağ iletişimi için temel olan IPsec tünelleri, PQC yöntemleriyle yapılandırılabilir veya gelişmiş güvenlik için QKD ile entegre edilebilir.[15] Dolaşıklık tabanlı QKD, yalnızca anahtar dağıtımının ötesinde gelecekteki kuantum ağ uygulamaları için daha yüksek güvenlik, ölçeklenebilirlik ve esneklik sunar.[15] Bu eğilim, siber güvenliğe proaktif bir yaklaşımı, gelecekteki tehditleri bugün ele almayı vurgulamaktadır.

"Şimdi Hasat Et, Sonra Şifresini Çöz" (HNDL) tehdidi, acil eylem için bir itici güçtür. HNDL saldırılarından açıkça bahsedilmiş ve kuruluşların "bu geçişi hemen önceliklendirmesi" gerektiği belirtilmiştir.[15] Ayrıca, "Kuantum sonrası kriptografinin benimsenmekte olduğu" da belirtilmiştir.[16] Bu durum, kuantum tehdidinin sadece uzak bir geleceğe yönelik teorik bir endişe olmadığını, uzun vadeli değere sahip veriler için bugün iletilen ve depolanan veriler için mevcut bir endişe olduğunu vurgulamaktadır. Reaktif olan diğer birçok güvenlik tehdidinin aksine, kuantum tehdidi proaktif, ileriye dönük bir strateji gerektirmektedir. Kuruluşlar, uzun vadeli gizliliğe ihtiyaç duyan verileri tanımlamalı ve tam kapasiteli kuantum bilgisayarlar yaygın olarak mevcut olmasa bile, kuantum güvenli çözümlere şimdi geçiş yapmaya başlamalıdır. Ağ trafiği analizi için bu, şifrelenmiş trafiğin içeriği opak olsa da, şifreleme için kullanılan protokollerin kuantum güvenliği durumu açısından izlenmesi gerektiği anlamına gelir. Bu, "iyi" trafiğin gelecekteki rakiplere karşı gerçekten güvenli bir şekilde iletilmesini sağlar.

Hibrit yaklaşımlar, pragmatik bir geçiş stratejisi sunmaktadır. "Geleneksel mekanizmalar (DH, ECDH, RSA vb.), PQC ve QKD gibi birden fazla güvenlik mekanizmasını birbiriyle birlikte kullanmak mümkündür (ve yaygındır). Buna hibrit kuantum direnci denir ve çeşitli avantajlar sağlar: Derinlemesine savunma sağlar...".[15]

Kuantum güvenli ağlara geçiş, ani, yıkıcı bir geçiş değil, kademeli, hibrit bir yaklaşım olacaktır. Bu, kuruluşların mevcut sistemlerle uyumluluğu sürdürmesine, mevcut düzenleyici gereksinimleri (hala kuantum saldırılarına açık algoritmaları zorunlu kılan) karşılamasına ve kuantum hesaplama zaman çizelgesindeki veya yeni PQC algoritmalarının uzun vadeli güvenliğindeki belirsizliklere karşı korunmasına olanak tanır. Ağ trafiği analizi için bu, karmaşık hibrit kriptografik el sıkışmalarını anlama ve izleme ihtiyacını ve tüm şifreleme katmanlarının hem klasik hem de kuantum tehditlerine karşı sağlam olmasını sağlama ihtiyacını ima etmektedir.

Kuantum güvenli ağ oluşturma, yüksek değerli veri koruması için bir farklılaştırıcı olarak ortaya çıkmaktadır. QKD'nin ek güvenlik katmanından faydalanan belirli uygulamalar arasında "kritik altyapı, tıbbi uygulamalar, finansal uygulamalar, yüksek değerli fikri mülkiyet korumaları, devlet verileri, savunma güvenliği ve uzun vadeli koruma gerektiren her şey" bulunmaktadır.[15] PQC'nin genel internet güvenliği için bir temel haline gelmesi muhtemel olsa da, QKD, özellikle dolaşıklık tabanlı QKD, en hassas ve uzun ömürlü veriler için premium bir güvenlik katmanı olarak hizmet edecektir. Bu, ağ güvenliğine katmanlı bir yaklaşım olduğunu düşündürmektedir; uygulanan kuantum direnci seviyesi, iletilen verinin değeri ve ömrüne bağlıdır. Kullanıcının projesi için bu, "iyi" trafiği sınıflandırmanın, belirli veri türleri için daha yüksek bir güvenlik standardını gösteren kuantum güvenliği seviyesini de değerlendirmeyi içerebileceği ve potansiyel olarak veri işleme hakkındaki politika kararlarını etkileyebileceği anlamına gelmektedir.

Aşağıdaki tablo, 2025 yılı için kuantum güvenli ağ oluşturma yaklaşımlarını özetlemektedir:

Tablo 6: 2025 için Kuantum Güvenli Ağ Oluşturma Yaklaşımları

Yaklaşım	Mekanizma	Temel Fayda/Rol	Uygulama Alanları	İlgili Kaynak
Kuantum Sonrası Kriptografi (PQC)	Kuantum bilgisayarlar için çözülmesi zor matematiksel problemlere dayalı klasik algoritmalar.	Temel kuantum direnci için yazılım tabanlı bir çözüm sağlar.	Genel güvenli iletişim, internet protokolleri için yaygın benimseme.	[15]
Kuantum Anahtar Dağıtımı (QKD)	Anahtar değişimini güvence altına almak için	Anahtar değişimi için bilgi-teorik güvenlik sunar,	Kritik altyapı, uzun vadeli gizli devlet ve finansal veriler.	[15]

	kuantum fiziği ilkelerini kullanır.	dinlemeyi tespit eder.		
Hibrit Kuantum Direnci	Katmanlı güvenlik için geleneksel kriptografiyi PQC ve/veya QKD ile birleştirir.	Derinlemesine savunma sağlar ve kademeli bir geçişi kolaylaştırır.	Kuantum güvenliğine geçiş yapan kuruluşlar için geniş uygulanabilirlik.	[15]

4. Sonuç: 2025 Ağ Trafiği Analizi için Stratejik Zorunluluklar

2025 yılına doğru ilerlerken, ağ trafiği analizi alanı, her biri ağ güvenliği ve performansında önemli ilerlemeler vaat eden bir dizi birbirine bağlı eğilim ve teknoloji tarafından yeniden şekillendirilmektedir. Yapay zeka destekli anomali tespiti ve öngörücü gözlemlenebilirlik, XDR'nin sağladığı bütünsel tehdit görünürlüğü için veri temelini oluşturmaktadır. Bu çözümler, Sıfır Güven Mimarisinin temel ilkeleriyle uyumlu bir şekilde SASE çerçevesi içinde çalışmaktadır. Uzun vadeli veri gizliliğini sağlamak için kuantum güvenli ağ oluşturma bu yaklaşımları tamamlamaktadır. Bu eğilimlerin birleşik olarak benimsenmesi, bireysel uygulamaların sağlayabileceğinden çok daha büyük bir sinerjik etki yaratmaktadır.

Kuruluşlar için kritik zorunluluk, ağ trafiği analizine bütünsel, proaktif ve akıllı bir yaklaşım benimsemektir. Geleneksel reaktif izleme modeli, modern siber tehditlerin karmaşıklığına ve ölçeğine ve çağdaş ağ mimarilerinin karmaşıklığına karşı artık yeterli değildir. Yapay zeka ve makine öğreniminin gelişmiş yetenekleri, büyük veri hacimlerini işleme, bilinmeyen tehditleri tespit etme ve potansiyel sorunları tırmanmadan önce tahmin etme yeteneği ile bu dönüşümün merkezinde yer almaktadır. Sıfır Güven ilkeleri, her erişim isteğinin sürekli doğrulandığı ve ayrıcalıkların en aza indirildiği bir güvenlik duruşu sağlayarak bu gelişmiş analitik için bir çerçeve sunar. SASE, bu ilkeleri bulut tabanlı, birleşik bir hizmet aracılığıyla dağıtık ortamlar için pratik bir şekilde hayata geçirirken, XDR, farklı güvenlik katmanlarından gelen verileri ilişkilendirerek saldırıların tam kapsamına ilişkin kapsamlı bir görünüm sunar. Gelişmiş gözlemlenebilirlik ve OpenTelemetry gibi açık standartlar, bu sistemlerin çalışması için gerekli yüksek kaliteli telemetri verilerini sağlayarak bu ekosistemi güçlendirir. Son olarak, kuantum güvenli ağ oluşturma, uzun vadeli veri gizliliğini gelecekteki kuantum tehditlerine karşı

koruyarak güvenlik stratejilerini geleceğe hazırlar.

Bu kapsamlı strateji, kuruluşların dinamik dijital ortamda "iyi" ve "kötü" ağ davranışlarını benzeri görülmemiş bir doğruluk ve hızla etkili bir şekilde tanımlamasını ve ayırt etmesini sağlamaktadır. Bu, yalnızca sağlam güvenlik duruşları sağlamakla kalmaz, aynı zamanda ağ performansını optimize eder ve 2025 ve sonrasının karmaşık dijital ortamında esneklik oluşturur. Eski sistemlerin entegrasyonu ve insan faktörünün yönetimi gibi devam eden zorluklar, sürekli adaptasyon ve becerilere yatırımın bu evrimsel yolculukta kritik olacağını göstermektedir.

Alıntılanan çalışmalar

1. A systematic literature review of unsupervised learning algorithms ..., erişim tarihi Haziran 17, 2025, https://arxiv.org/pdf/2503.08293
2. Top 6 Observability Trends Look out for 2025 - Motadata, erişim tarihi Haziran 17, 2025, https://www.motadata.com/blog/observability-trends/
3. LLM Assisted Anomaly Detection Service for Site Reliability ..., erişim tarihi Haziran 17, 2025, https://arxiv.org/pdf/2501.16744?
4. A Practical Approach to Defining a Framework for Developing an Agentic AIOps System, erişim tarihi Haziran 17, 2025, https://www.mdpi.com/2079-9292/14/9/1775
5. arXiv:2504.20854v1 [cs.NI] 29 Apr 2025, erişim tarihi Haziran 17, 2025, https://arxiv.org/pdf/2504.20854
6. [2502.00785] Forecasting Global Network Traffic Trends: The Role of Virtual Reality - arXiv, erişim tarihi Haziran 17, 2025, https://arxiv.org/abs/2502.00785
7. Zero trust architecture: A paradigm shift in network security - ResearchGate, erişim tarihi Haziran 17, 2025, https://www.researchgate.net/publication/390558157_Zero_trust_architecture_A_paradigm_shift_in_network_security
8. Zero Trust Implementation Challenges & How to Solve Them - InstaSafe, erişim tarihi Haziran 17, 2025, https://instasafe.com/blog/challenges-in-zero-trust-implementation/
9. 5 Tips to Improve Network Security and Speed in 2025 - Beacon Inside, erişim tarihi Haziran 17, 2025, https://www.beaconinside.com/blog/5-ways-to-enhance-network-security-and-performance-in-2025
10. Conquering the Top Zero Trust Challenges in 2025 - F12.net, erişim tarihi Haziran 17, 2025, https://f12.net/blog/conquering-the-top-zero-trust-challenges-in-2025/
11. Top 6 Trends for SASE in 2025 - Open Systems, erişim tarihi Haziran 17, 2025, https://www.open-systems.com/blog/top-6-trends-for-sase-in-2025/
12. Top 10 XDR Solutions for 2025 - SentinelOne, erişim tarihi Haziran 17, 2025, https://www.sentinelone.com/cybersecurity-101/endpoint-security/xdr-solutions/
13. XDR Tools in 2025: Why Runtime Security is Essential for Cloud ..., erişim tarihi Haziran 17, 2025, https://www.upwind.io/glossary/xdr-tools-in-2025

14. Key Data Observability Trends in 2025 | Secoda, erişim tarihi Haziran 17, 2025, https://www.secoda.co/blog/key-data-observability-trends
15. Real-world implementation of Quantum-safe IPsec, erişim tarihi Haziran 17, 2025, https://www.aliroquantum.com/blog/real-world-implementation-of-quantum-safe-ipsec
16. 5 Real-World Applications of Quantum Computing in 2025 - Datafloq, erişim tarihi Haziran 17, 2025, https://datafloq.com/read/5-real-world-applications-of-quantum-computing-in-2025/