

# 2025 Yılı İçin Web Güvenlik Analizöründe En Son ve En Etkili 10 Teknik/Trend

## 1. Giriş: Gelişen Tehdit Ortamı ve Web Güvenliğinin Önemi

Dijitalleşmenin hızla artmasıyla birlikte, web güvenliği, kuruluşların en kritik önceliklerinden biri haline gelmiştir. 2025 yılına girerken, siber tehdit ortamı daha önce hiç olmadığı kadar karmaşık ve dinamik bir yapı sergilemektedir. Saldırganlar, yapay zeka (YZ) gibi gelişmiş teknolojileri kullanarak savunma mekanizmalarını aşmakta, derin sahtekarlıklar (deepfakes), kimliğe bürünme dolandırıcılıkları ve YZ tarafından üretilen ortalama saldırıları ile yeni nesil tehditler oluşturmaktadır.<sup>1</sup> Bu durum, web sitelerini siber saldırılar için yüksek riskli giriş noktaları olarak konumlandırmaya devam etmektedir.<sup>1</sup>

Günümüzde, GDPR gibi sıkılaştıran düzenleyici baskılar ve finans ile sağlık sektörlerindeki zorunlu uygulamalar, bir güvenlik ihlalini sadece itibar kaybı değil, aynı zamanda ciddi bir yasal yükümlülük ve iş riski haline getirmektedir.<sup>1</sup> Kuruluşlar, kısıtlı bütçelere rağmen artan güvenlik beklentilerini karşılamak zorundadır. Bu bağlamda, YZ destekli araçlar, manuel çabayı azaltma ve operasyonel verimliliği artırma potansiyeli sunmaktadır.<sup>1</sup> Otomasyon, yama yönetimi, sürekli izleme ve günlük incelemesi gibi alanlarda yoğun bir şekilde kullanılmaktadır.<sup>1</sup> Genel olarak, siber güvenlik stratejileri reaktif "yangın söndürme" yaklaşımından proaktif önlemlere ve iş sürekliliği planlamasına doğru evrilmektedir.<sup>1</sup>

### Web Güvenlik Analizörlerinin Rolü

Web güvenlik analizörleri, ağlarda, sistemlerde, uygulamalarda ve cihazlarda güvenlik zafiyetlerini belirlemek için tasarlanmış otomatik yazılım çözümleridir.<sup>6</sup> Bu araçlar, bilinen zafiyetleri, hatalı yapılandırmaları ve saldırganların istismar edebileceği güncel

olmayan yazılımları tarar.<sup>6</sup> 2025'te bu analizörler, YZ/makine öğrenimi (ML) entegrasyonu, otomasyon ve kapsamlı görünürlük gibi gelişmiş yeteneklerle daha da kritik bir rol oynayacaktır.<sup>7</sup>

YZ'nin siber güvenlik alanındaki çift yönlü etkisi, bu alandaki stratejik adaptasyonun zorunluluğunu ortaya koymaktadır. YZ'nin hem saldırganlar tarafından sofistike saldırılar için kullanılması hem de savunmacılar tarafından tehdit tespiti ve otomasyon için benimsenmesi, bir "YZ silahlanma yarışı"nın varlığını göstermektedir. Kuruluşlar, sadece YZ destekli savunma araçlarını kullanmakla kalmayıp, aynı zamanda saldırganların YZ kullanımına karşı proaktif stratejiler geliştirmek zorundadır. YZ'nin kötüye kullanım potansiyeli, derin sahtekarlıklar aracılığıyla dijital içeriğe olan güvenin aşınmasına yol açarken, savunmacılar için YZ destekli karşı önlemler, örneğin YZ su damgalama teknolojileri, hayati önem taşımaktadır.<sup>9</sup> Bu durum, güvenlik liderlerinin YZ'nin hem risklerini hem de sunduğu fırsatları bütünsel bir yaklaşımla değerlendirmesini gerektirmektedir. YZ'nin yaygınlaşmasıyla birlikte, "Web Güvenlik Analizörü" tanımı genişleyerek, sadece bilinen zafiyetleri taramakla kalmayıp, aynı zamanda YZ'nin ürettiği veya YZ tarafından hedeflenen yeni nesil tehditleri de analiz edebilen, öğrenen ve adapte olabilen sistemleri içermelidir. Bu, geleneksel imza tabanlı tespit yöntemlerinden davranışsal analize ve tahmine dayalı modellere doğru köklü bir değişimi zorunlu kılmaktadır.

Bütçe kısıtlamaları ve artan güvenlik beklentileri, YZ ve otomasyonun güvenlik operasyonlarında bir verimlilik katalizörü olarak benimsenmesini hızlandıran temel bir faktördür. Kuruluşlar, daha az kaynakla daha fazla güvenlik sağlamak durumundadır. YZ, güvenlik ekiplerinin rutin, tekrarlayan görevlerden (yama, izleme, günlük incelemesi) kurtularak daha stratejik ve karmaşık tehditlere odaklanmasını sağlamaktadır.<sup>1</sup> Bu yaklaşım, siber güvenlik profesyoneli eksikliğinin getirdiği baskıyı hafifletmeye yardımcı olurken <sup>2</sup>, aynı zamanda daha hızlı ve tutarlı yanıt süreleri sunar. YZ ve otomasyon, sadece maliyetleri düşürmekle kalmaz, aynı zamanda güvenlik operasyonlarının hızını ve etkinliğini artırarak iş sürekliliğini doğrudan destekler. Bu, reaktif "yangın söndürme" modundan proaktif "tehdit avcılığı" ve "risk yönetimi"ne geçişi mümkün kılar. Web güvenlik analizörleri, bu bağlamda, otomasyon ve YZ entegrasyonu sayesinde sürekli izleme ve erken tespit yeteneklerini güçlendirerek, bir ihlal meydana gelmeden önce önleyici tedbirler alınmasını sağlar.

## **2. 2025 Yılı İçin Web Güvenlik Analizöründe En Son ve En Etkili 10 Teknik/Trend**

2025 yılında web güvenlik analizörleri, gelişen tehdit ortamına uyum sağlamak ve kuruluşları daha etkin bir şekilde korumak için bir dizi yenilikçi teknik ve trendi benimseyecektir. Aşağıda, bu yılın en etkili 10 tekniği/trendi detaylandırılmıştır:

**Tablo 1: 2025 Web Güvenlik Analizörü Trendlerine Genel Bakış**

Trend No.	Trend Başlığı	Odak Noktası
1	YZ Destekli Tehdit Tespiti ve Yanıt	Anomali Tespiti, Tahmine Dayalı Analitik, Otomatik Yanıt
2	Sıfır Güven Mimarisi (Zero Trust Architecture) Entegrasyonu	Sürekli Doğrulama, En Az Ayricalık, Mikro Segmentasyon
3	API Güvenliği ve İş Mantığı Saldırıları	Gerçek Zamanlı Trafik Analizi, Davranışsal Anomali Tespiti
4	Yazılım Tedarik Zinciri Güvenliği Analizi	Üçüncü Taraf Bağımlılıkları, Yazılım Bill of Materials (SBOM)
5	DevSecOps ve "Shift-Everywhere" Güvenlik Entegrasyonu	Geliştirme Yaşam Döngüsü Boyunca Güvenlik Otomasyonu
6	Çalışma Zamanı Uygulama Kendi Kendini Koruma (RASP)	Uygulama İçi Gerçek Zamanlı Tehdit Engelleme
7	Sunucusuz (Serverless) ve Kapsayıcı (Container) Güvenliği	Ephemeral İş Yükleri, Çalışma Zamanı Koruması
8	Kuantum Hazır Şifreleme (Quantum-Resistant Cryptography)	Geleceğe Yönelik Veri Koruma, Şifreleme Algoritması Geçişi
9	Kapsamlı Görünürlük (Observability) ve Varlık Yönetimi	Tam Yığın Görünürlüğü, Gerçek Zamanlı İzleme, Risk Korelasyonu
10	Düzenleyici Uyum ve Otomatik Güvenlik Doğrulaması	Otomatik Uyum Kontrolleri, Sürekli Denetim

---

## 1. YZ Destekli Tehdit Tespiti ve Yanıt

YZ destekli güvenlik platformları, 2025 yılında tehdit tespiti ve yanıtında devrim yaratmaya devam edecektir. Bu sistemler, büyük veri kümelerini eş benzeri görülmemiş bir hızda analiz ederek anormal davranışları ve potansiyel ihlalleri belirler.<sup>5</sup> Makine öğrenimi algoritmaları, olay yanıtlarını otomatikleştirerek bu yeteneği daha da geliştirir, böylece kuruluşların tehditleri daha hızlı tespit etmesini ve azaltmasını sağlar.<sup>7</sup>

- **Nasıl Çalışır:** YZ destekli analizörler, SentinelOne ve Datadog gibi araçlarda görüldüğü gibi, tahmine dayalı analitik kullanarak tehditleri erken aşamada yakalar.<sup>1</sup> Sistemler, normal davranış kalıplarını öğrenir ve bu kalıplardan sapmaları anomali olarak işaretler. Bu, özellikle gerçek zamanlı ses klonlama ve deepfake videolar gibi YZ destekli ortalama saldırılarının tespitini zorlaştırdığı bir ortamda kritik öneme sahiptir.<sup>1</sup> YZ, multimodal veri kaynaklarından (metin, ses, görüntüler) kapsamlı bilgiler sağlayarak, saldırganlar tarafından kullanılan daha karmaşık ve hedefli saldırıların önüne geçmek için tahmine dayalı analiz yeteneklerini entegre eder.<sup>7</sup>
- **Neden Önemli:** YZ'nin siber güvenlikte yaygınlaşması, hem saldırganların hem de savunmacıların yeteneklerini artırmaktadır.<sup>2</sup> YZ destekli araçlar, insan müdahalesine olan bağımlılığı azaltır ve operasyonel verimliliği artırarak güvenlik ekiplerinin daha stratejik görevlere odaklanmasını sağlar.<sup>7</sup> Bu, siber güvenlik profesyoneli eksikliğinin yaşandığı bir dönemde özellikle değerlidir.<sup>2</sup>
- **2025'teki Potansiyel Etkileri ve Uygulama Alanları:** 2025'te YZ destekli güvenlik platformları, gerçek zamanlı tehdit istihbaratı ve otonom yanıt mekanizmaları sunarak, güvenlik operasyonlarını daha proaktif ve uyarlanabilir hale getirecektir.<sup>3</sup> Bu, özellikle web uygulamaları, bulut ortamları ve API'ler gibi genişleyen saldırı yüzeylerinde tehditlerin daha hızlı ve doğru bir şekilde tespit edilmesini sağlayacaktır.<sup>4</sup> Uygulama alanları arasında gelişmiş tehdit avcılığı, otomatik olay yanıtı, bulut güvenlik duruş yönetimi (CSPM) ve API anomali tespiti yer almaktadır.<sup>4</sup>
- **Güvenilir Kaynak/Referans:** Optiv Insights: AI Trends in Cybersecurity <sup>7</sup>, TeamColab: Website Security in 2025.<sup>1</sup>

## 2. Sıfır Güven Mimarisi (Zero Trust Architecture) Entegrasyonu

Sıfır Güven Mimarisi (ZTA), 2025 yılında kuruluşlar için bir norm haline gelecektir. Bu model, varsayılan olarak hiçbir kullanıcıya veya cihaza güvenilmemesini ve her etkileşimin sürekli olarak doğrulanmasını gerektirir.<sup>2</sup> Web güvenlik analizörleri, bu prensipleri web uygulamaları ve API'ler genelinde uygulayarak, veri üzerinde daha iyi segmentasyon ve kontrol sağlar.

- **Nasıl Çalışır:** ZTA, geleneksel çevre tabanlı güvenlik modellerinin aksine, her erişim isteğini, kaynağına veya konumuna bakılmaksızın doğrular.<sup>2</sup> Web güvenlik analizörleri, API etkileşimlerinin sürekli doğrulanmasını gerektirerek ZTA çerçevelerinin temel bir bileşeni haline gelecektir.<sup>4</sup> Bu, katı erişim kontrolleri, sürekli kimlik doğrulama ve en az ayrıcalık ilkesinin uygulanmasını içerir.<sup>4</sup> Sunucusuz ortamlar gibi kısa ömürlü ve dinamik altyapılarda, her fonksiyonun potansiyel bir giriş noktası olması nedeniyle ZTA, kapsamlı koruma sağlamak için kritik öneme sahiptir.<sup>12</sup>
- **Neden Önemli:** Geleneksel güvenlik modelleri, güvenli iç ağlar varsayımına dayanır; ancak modern, API odaklı uygulamalar hibrit ve çoklu bulut ortamlarında çalıştığı için bu varsayım geçerliliğini yitirmiştir.<sup>4</sup> ZTA, bu dağıtık ortamda güvenin varsayılamayacağı durumlarda, iç tehditlere ve yanlamasına hareketlere karşı daha sağlam bir savunma sunar.
- **2025'teki Potansiyel Etkileri ve Uygulama Alanları:** 2025'te ZTA, modern işletmelerin güvenliğini sağlamak için temel bir beklenti haline gelecektir.<sup>2</sup> Web güvenlik analizörleri, API ağ geçitlerine entegre edilerek gerçek zamanlı tehdit analizi ve otomatik yanıtlar sağlayacak, böylece yetkisiz erişimi ve veri ihlallerini önleyecektir.<sup>11</sup> Uygulama alanları arasında hibrit ve çoklu bulut ortamlarındaki API etkileşimlerinin güvenliğini sağlama, hassas verilere erişimi sıkılaştırma ve mikro segmentasyon yoluyla saldırı yüzeyini azaltma yer almaktadır.<sup>4</sup>
- **Güvenilir Kaynak/Referans:** SecureWorld: Cybersecurity Predictions for 2025<sup>2</sup>, Rakuten Sixth Sense: The Future of API Security.<sup>4</sup>

### 3. API Güvenliği ve İş Mantığı Saldırıları

API'ler, modern web uygulamalarının omurgasını oluşturmakta ve 2025 yılında siber saldırganların artan hedefi haline gelmektedir. Saldırganlar, geleneksel zafiyetler yerine API iş mantığındaki boşlukları istismar etmeye odaklanacaklardır.<sup>4</sup> Web güvenlik analizörleri, bu tür sofistike saldırıları tespit etmek ve engellemek için davranışsal anomali tespiti yeteneklerini geliştirecektir.

- **Nasıl Çalışır:** YZ destekli API tehdit tespiti, API trafiğindeki anormallikleri

belirlemek, saldırı kalıplarını tanımlamak ve tehdit yanıtlarını otomatikleştirmek için makine öğrenimini kullanır.<sup>4</sup> Geleneksel güvenlik araçları, meşru davranışları taklit eden API kötüye kullanımını tespit etmekte zorlanırken, YZ odaklı çözümler API trafiğini gerçek zamanlı olarak analiz ederek dolandırıcılık, bot saldırıları ve veri sızması gibi ince göstergeleri tanımlayabilir.<sup>4</sup> API güvenlik gözlemlenebilirliği, kimin API'lere eriştiği, ne yaptıkları ve davranışlarının kötü niyetli olup olmadığı hakkında tam yığın görünürlüğü sağlar.<sup>4</sup>

- **Neden Önemli:** API'ler, hassas veriler ve iş süreçleri için kritik erişim noktalarıdır. Geleneksel güvenlik araçları genellikle SQL enjeksiyonu veya bozuk kimlik doğrulama gibi bilinen zafiyetlere odaklanırken, iş mantığı saldırıları meşru API fonksiyonlarını manipüle ederek işlemleri değiştirebilir veya güvenlik önlemlerini atlayabilir.<sup>4</sup> Bu, kuruluşların API'lerinin amaçlandığı gibi çalıştığından emin olmaları için yeni nesil analizörlere ihtiyaç duyduğu anlamına gelir.
- **2025'teki Potansiyel Etkileri ve Uygulama Alanları:** 2025'te YZ tabanlı API güvenlik çözümleri bir lüks olmaktan çıkıp bir zorunluluk haline gelecektir.<sup>4</sup> Otomatik API güvenlik testi, CI/CD boru hatlarına entegre edilerek "solak güvenlik" (shift-left security) yaklaşımını standart hale getirecektir.<sup>4</sup> Bu, API penetrasyon testi, fuzz testi ve güvenlik taramalarının her sürüm döngüsüne dahil edilmesini sağlayacaktır. Uygulama alanları arasında e-ticaret platformları, finansal hizmetler ve sağlık uygulamaları gibi API'lerin yoğun kullanıldığı sektörler yer almaktadır.<sup>11</sup>
- **Güvenilir Kaynak/Referans:** Rakuten Sixth Sense: The Future of API Security<sup>4</sup>, API7.AI: 2025 Top 8 API Management Trends.<sup>11</sup>

#### 4. Yazılım Tedarik Zinciri Güvenliği Analizi

Yazılım tedarik zinciri saldırıları, 2025 yılında artan bir endişe kaynağı olmaya devam edecektir. Saldırganlar, açık kaynaklı yazılım (OSS) depolarındaki kötü amaçlı paketler ve sızdırılmış geliştirici sırları gibi zafiyetleri hedeflemeye devam edecektir.<sup>14</sup> Web güvenlik analizörleri, bu genişleyen risk yüzeyini ele almak için daha kapsamlı tedarik zinciri analizi yetenekleri sunacaktır.

- **Nasıl Çalışır:** Tedarik zinciri güvenlik analizörleri, yalnızca bilinen zafiyetleri (CVE'ler) değil, aynı zamanda gizli anahtarların açığa çıkması, derleme ortamının kurcalanması ve dosya bozulması gibi daha geniş bir risk yelpazesini de değerlendirir.<sup>14</sup> Bu araçlar, yazılımın bileşenlerini (üçüncü taraf kütüphaneler, açık kaynak bağımlılıkları) ve bunların kökenini (provenance) doğrulamak için Yazılım Bill of Materials (SBOM) oluşturma ve analiz etme yeteneğini içerir.<sup>16</sup> Gelişmiş ikili

analiz ve tekrarlanabilir derlemeler gibi teknolojiler, yazılımın bütünlüğünü sağlamak için kritik öneme sahiptir.<sup>14</sup>

- **Neden Önemli:** Açık kaynaklı yazılımlardaki güvenlik politikalarının sıkılaştırılmasına rağmen (örneğin, 2FA zorunluluğu), saldırılar devam etmekte ve daha sofistike hale gelmektedir.<sup>14</sup> Geliştirici sırlarının sızdırılması ve ticari yazılımlardaki "kara kutu" zafiyetleri, kuruluşları önemli risklere maruz bırakmaktadır.<sup>14</sup> Ayrıca, Ulusal Zafiyet Veritabanı (NVD) gibi CVE raporlama sistemlerindeki aksaklıklar, geleneksel zafiyet yönetiminin yetersiz kaldığını göstermektedir.<sup>14</sup>
- **2025'teki Potansiyel Etkileri ve Uygulama Alanları:** 2025'te yazılım tedarik zinciri güvenliği, düzenleyici gerekliliklerin de etkisiyle daha fazla vurgulanacaktır.<sup>3</sup> Analizörler, yapay zeka tarafından oluşturulan kod ve görseller aracılığıyla yapılan saldırıları tespit etme yeteneğini entegre edecek, zira bu tür saldırılar CI/CD boru hatlarına kötü niyetli kod enjekte etmek için kullanılmaktadır.<sup>16</sup> Uygulama alanları, kritik altyapı sektörlerinden finans ve sağlık gibi veri hassasiyeti yüksek alanlara kadar genişleyecektir.<sup>2</sup>
- **Güvenilir Kaynak/Referans:** ISACA: The 2025 Software Supply Chain Security Report <sup>14</sup>, ReversingLabs: The 2025 Software Supply Chain Security Report.<sup>15</sup>

## 5. DevSecOps ve "Shift-Everywhere" Güvenlik Entegrasyonu

2025 yılında DevSecOps, güvenlik uygulamalarını yazılım geliştirme yaşam döngüsünün (SDLC) her aşamasına entegre ederek "shift-left" yaklaşımından "shift-everywhere" felsefesine doğru evrilecektir.<sup>13</sup> Web güvenlik analizörleri, bu sürekli entegrasyonu sağlamak için otomasyon ve YZ'den güç alacaktır.

- **Nasıl Çalışır:** DevSecOps araçları, güvenlik kontrollerini CI/CD boru hatlarına gömerek, geliştiricilerin güvenlik açıklarını erken aşamada tespit etmelerini ve gidermelerini sağlar.<sup>8</sup> Bu, statik uygulama güvenlik testi (SAST) için kaynak kodu analizi, dinamik uygulama güvenlik testi (DAST) için çalışan uygulamaların taranması ve yazılım bileşimi analizi (SCA) için üçüncü taraf bağımlılıklarının incelenmesi gibi süreçleri içerir.<sup>17</sup> YZ, bu otomasyonu hızlandıracak ve ölçeklenebilirliği artıracak, kod zafiyetlerinin incelenmesi ve düzeltilmesi gibi görevleri otomatikleştirecektir.<sup>13</sup> Bulut yerel uygulama koruma platformları (CNAPP), koddan buluta güvenliği sağlamak için çeşitli güvenlik araçlarını birleştirir.<sup>16</sup>
- **Neden Önemli:** Geleneksel güvenlik denetimleri, modern DevOps iş akışları için



çok yavaş ve tutarsızdır.<sup>4</sup> Güvenlik kontrollerini geliştirme sürecinin başlarına ve her aşamasına entegre etmek, zafiyetlerin üretim ortamına ulaşmadan önce yakalanmasını sağlar, bu da maliyet ve zaman tasarrufu sağlar.<sup>18</sup> YZ'nin daha hızlı yazılım üretimine yol açmasıyla, sağlam ve olgun DevSecOps ortamlarına olan ihtiyaç artmaktadır.<sup>13</sup>

- **2025'teki Potansiyel Etkileri ve Uygulama Alanları:** 2025'te DevSecOps, YZ ve otomasyonun birleşimiyle yazılım teslimatını daha hızlı, akıllı ve güvenli hale getirecektir.<sup>13</sup> Analizörler, geliştirici iş akışlarıyla (IDE'ler, bulut araçları, biletleme sistemleri) sorunsuz bir şekilde entegre olacak ve geliştiricilerin riskler ve çözümler hakkında eğitim almasını sağlayacaktır.<sup>17</sup> Uygulama alanları arasında web tabanlı mikro hizmet mimarileri, bulut yerel uygulamalar ve sürekli entegrasyon/sürekli teslimat (CI/CD) boru hatları yer almaktadır.<sup>16</sup>
- **Güvenilir Kaynak/Referans:** DevPro Journal: 3 DevSecOps Trends ISVs Should Watch in 2025 <sup>13</sup>, Checkmarx: Features the Best DevSecOps Tools Will Have in 2025.<sup>17</sup>

## 6. Çalışma Zamanı Uygulama Kendi Kendini Koruma (RASP)

Çalışma Zamanı Uygulama Kendi Kendini Koruma (RASP) yazılımı, 2025 yılında siber tehditlere karşı kritik bir savunma mekanizması olarak öne çıkmaktadır. RASP, uygulamaların içine entegre olarak, çalışırken gerçek zamanlı tehditlere ve zafiyetlere karşı koruma sağlar.<sup>22</sup>

- **Nasıl Çalışır:** RASP teknolojisi, uygulamanın girdilerini izler ve saldırılara yol açabilecek girdileri engellerken, çalışma zamanı ortamını istenmeyen değişikliklerden ve kurcalamalardan korur.<sup>23</sup> Geleneksel güvenlik duvarları veya ağ çevre kontrollerinin aksine, RASP, gerçek zamanlı veri ve olay akışlarına daha derinlemesine bir bakış açısı sunarak, geliştirme sırasında öngörülemeyen zafiyetleri veya yeni tehditleri engellemeyi hedefler.<sup>23</sup> Bu, uygulamanın kendisinin bir güvenlik sensörü ve savunma mekanizması gibi davranmasını sağlar.
- **Neden Önemli:** Kuruluşlar çevik metodolojileri ve DevOps uygulamalarını benimsemeye devam ettikçe, güvenliği uygulama yaşam döngüsüne entegre etmek zorunlu hale gelmiştir.<sup>22</sup> Kapsayıcılaştırma ve mikro hizmet mimarilerinin yükselişi, bu ortamlar için özel güvenlik önlemleri gerektirdiğinden RASP çözümlerine olan talebi artırmaktadır.<sup>22</sup> RASP, uygulama güvenlik testi (AST) ve ağ güvenlik kontrollerinin bıraktığı boşluğu doldurarak, saldırıların çalışma zamanında durdurulmasını sağlar.



- **2025'teki Potansiyel Etkileri ve Uygulama Alanları:** 2025'te RASP pazarının önemli ölçüde büyümesi beklenmektedir.<sup>23</sup> Bulut tabanlı uygulamalara artan bağımlılık ve veri koruma düzenlemelerinin uygulanması, RASP'ın benimsenmesini hızlandıracaktır.<sup>22</sup> RASP, özellikle hassas verileri işleyen veya karmaşık iş mantığına sahip web uygulamaları için kritik öneme sahip olacaktır. Finans, sağlık ve e-ticaret gibi sektörlerde, gerçek zamanlı saldırı engelleme yeteneği, veri ihlallerini ve iş kesintilerini önlemede hayati bir rol oynayacaktır.
- **Güvenilir Kaynak/Referans:** GitHub: Runtime Application Self-Protection Software Market Dynamics 2025 <sup>22</sup>, LLCBuddy: Runtime Application Self Protection Software Statistics 2025.<sup>23</sup>

## 7. Sunucusuz (Serverless) ve Kapsayıcı (Container) Güvenliği

Sunucusuz bilişim ve kapsayıcı teknolojileri, 2025 yılında bulut güvenliğini yeniden şekillendirmeye devam edecektir. Bu mimariler, maliyet verimliliği, ölçeklenebilirlik ve operasyonel yükün azaltılması gibi avantajlar sunarken, kendine özgü güvenlik zorluklarını da beraberinde getirmektedir.<sup>5</sup> Web güvenlik analizörleri, bu dinamik ortamlar için özel olarak tasarlanmış çözümler sunacaktır.

- **Nasıl Çalışır:** Sunucusuz ve kapsayıcı güvenlik çözümleri, Kubernetes ve mikro hizmetlerin benimsenmesiyle birlikte çalışma zamanı tehdit tespiti, otomatik yama yönetimi ve Sıfır Güven modelleri gibi özelliklerle savunmayı güçlendirecektir.<sup>5</sup> Geleneksel güvenlik araçları, sunucusuz mimariler için tasarlanmadığından görünürlük eksikliği yaratır; bu nedenle, 2025'te odak noktası, olay sonrası günlük analizinden gerçek zamanlı çalışma zamanı korumasına kayacaktır.<sup>12</sup> Kapsayıcı izleme trendleri, CI/CD boru hatlarına "shift-left" izlemeyi ve YZ destekli anomali tespitini entegre edecektir.<sup>8</sup>
- **Neden Önemli:** Her sunucusuz fonksiyon, potansiyel bir saldırı yüzeyi oluşturur ve kısa ömürlü olmaları, gerçek zamanlı tehdit tespiti ve yanıtını zorlaştırır.<sup>12</sup> Yanlış yapılandırmalar ve veri sızması riskleri, bu ortamların doğasında vardır. Kapsayıcı ortamlar da YZ tarafından oluşturulan kod ve görseller aracılığıyla artan saldırılarla yeni saldırı yüzeyleri açmıştır.<sup>16</sup>
- **2025'teki Potansiyel Etkileri ve Uygulama Alanları:** 2025'te sunucusuz ve kapsayıcı güvenlik çözümleri, kuruluşların bulut tabanlı tehditlere karşı dayanıklılığını artırırken maliyetleri optimize etmelerine olanak tanıyacaktır.<sup>5</sup> Uygulama alanları arasında bulut yerel uygulamalar, mikro hizmet mimarileri ve DevOps ortamları yer almaktadır. Kapsayıcı güvenlik analizörleri, görüntü zafiyet

taraması, çalışma zamanı koruması, politika ve yanlış yapılandırma tespiti ve Kubernetes Güvenlik Duruşu Yönetimi (KSPM) gibi temel yetenekleri sunacaktır.<sup>16</sup>

- **Güvenilir Kaynak/Referans:** Cymulate: The Future of Cloud Security: 7 Key Trends in 2025<sup>5</sup>, Webasha: Securing the Future: Runtime Protection for Serverless Applications in 2025.<sup>12</sup>

## 8. Kuantum Hazır Şifreleme (Quantum-Resistant Cryptography)

Kuantum bilişim henüz ana akım olmasa da, 2025'te eski şifreleme yöntemlerini giderek daha kırılgan hale getirecek kadar yakınlaşmaktadır.<sup>1</sup> Web güvenlik analizörleri, uzun vadeli veri koruma stratejisinin bir parçası olarak kuantum hazır şifrelemeyi benimsemeye başlayacaktır.

- **Nasıl Çalışır:** Kuantum hazır şifreleme, mevcut bilgisayarlar tarafından kırılmayan ve gelecekteki kuantum bilgisayarların da kıramayacağı şekilde tasarlanmış yeni şifreleme algoritmaları ve protokolleridir. Web güvenlik analizörleri, kuruluşların mevcut şifreleme altyapılarının kuantum tehditlerine karşı direncini değerlendirmelerine ve kuantum sonrası şifreleme (PQC) standartlarına geçiş planları oluşturmalarına yardımcı olacaktır. Bu, şifreleme anahtarlarının yönetimini, veri şifrelemesini ve iletişim protokollerini güncellemeyi içerecektir.
- **Neden Önemli:** Kuantum bilgisayarların ortaya çıkması, günümüzde kullanılan birçok şifreleme algoritmasını (örneğin RSA, ECC) kırma potansiyeline sahiptir. Bu, özellikle uzun ömürlü ve hassas veriler için büyük bir risk oluşturur. Kuantum sonrası döneme hazırlık, gelecekteki veri gizliliğini ve bütünlüğünü sağlamak için proaktif bir adımdır.<sup>1</sup>
- **2025'teki Potansiyel Etkileri ve Uygulama Alanları:** 2025'te, erken benimseyenler kuantum tehditlerine dayanıklı şifrelemeyi uygulamaya başlayacaktır.<sup>1</sup> Web güvenlik analizörleri, özellikle finans, hükümet ve sağlık gibi hassas verilerin uzun süre korunması gereken sektörlerde, kuantum hazır şifreleme geçiş planlarının bir parçası olarak kullanılacaktır. Bu, web uygulamaları arasındaki güvenli iletişim kanallarının ve depolanan hassas verilerin korunmasını kapsayacaktır.
- **Güvenilir Kaynak/Referans:** TeamColab: Website Security in 2025<sup>1</sup>, RSA Conference 2025 Trends.<sup>24</sup>

## 9. Kapsamlı Görünürlük (Observability) ve Varlık Yönetimi

2025'te kuruluşlar, temel izlemeden tam API güvenlik gözlemlenebilirliğine geçiş yapacak, web uygulamaları ve API trafiği üzerinde gerçek zamanlı, tam yığın görünürlük sağlamayı hedefleyecektir.<sup>4</sup> Bu, web güvenlik analizörlerinin sadece olayları kaydetmekle kalmayıp, aynı zamanda tehditleri, yanlış yapılandırmaları ve iş mantığı kötüye kullanımlarını proaktif olarak belirlemesini gerektirecektir.

- **Nasıl Çalışır:** Kapsamlı gözlemlenebilirlik, gerçek zamanlı telemetri, günlük kaydı ve davranışsal analitik kombinasyonunu kullanarak API'lere kimin eriştiği, ne yaptıkları ve davranışlarının kötü niyetli olup olmadığı hakkında derinlemesine bilgi sağlar.<sup>4</sup> Kapsayıcı izlemede, bu, CPU ve bellek gibi geleneksel metriklerin ötesine geçerek günlükleri, dağıtılmış izlemeleri ve gerçek zamanlı olay analizini içerir.<sup>8</sup> Web güvenlik analizörleri, bu verileri toplayıp korele ederek, güvenlik ekiplerine potansiyel zafiyetler ve saldırı yolları hakkında bağlamsal bilgiler sunar.<sup>17</sup>
- **Neden Önemli:** Modern web uygulamaları, mikro hizmetler ve dağıtılmış bulut ortamları üzerinde çalıştığı için, geleneksel izleme araçları yetersiz kalmaktadır. Temel izleme araçları yalnızca API etkinliğini kaydederken, tehditleri veya iş mantığı kötüye kullanımlarını tanımlayamaz.<sup>4</sup> Kapsamlı görünürlük, karmaşık sistemlerdeki sorunların kök nedenini daha hızlı tespit etmeye ve güvenlik duruşunu güçlendirmeye olanak tanır.
- **2025'teki Potansiyel Etkileri ve Uygulama Alanları:** 2025'te şirketler, tehditleri tırmanmadan önce tespit etmek ve durdurmak için gelişmiş API gözlemlenebilirlik platformları konuşlandıracaktır.<sup>4</sup> Bu, özellikle büyük ve karmaşık web altyapılarına sahip kuruluşlar için, binlerce kapsayıcıyı yönetirken veya çoklu bulut ortamlarında tutarlı güvenlik izlemesi sağlarken kritik öneme sahip olacaktır.<sup>8</sup> Uygulama alanları arasında sürekli izleme, tehdit avcılığı, olay yanıtı ve bulut güvenlik duruş yönetimi yer almaktadır.
- **Güvenilir Kaynak/Referans:** Rakuten Sixth Sense: The Future of API Security <sup>4</sup>, DEV Community: 8 Container monitoring trends in 2025.<sup>8</sup>

## 10. Düzenleyici Uyum ve Otomatik Güvenlik Doğrulaması

2025 yılında, artan düzenleyici baskı ve veri koruma yasalarının evrimi, web güvenlik analizörlerinin uyum süreçlerinde daha merkezi bir rol oynamasını gerektirecektir.<sup>1</sup> Kuruluşlar, uyumluluğu sağlamak ve manuel çabayı azaltmak için otomatik güvenlik

doğrulama araçlarına yönelecektir.

- **Nasıl Çalışır:** Otomatik güvenlik doğrulama araçları, YZ destekli platformları kullanarak gerçek dünya senaryolarını simüle eder, yanlış yapılandırmaları tespit eder, güvenlik kontrollerini doğrular ve düzenleyici standartlara uyumu gerçek zamanlı olarak sağlar.<sup>5</sup> Bu, otomatik veri sınıflandırması ve sürekli izleme dahil olmak üzere belirli düzenleyici gereksinimleri karşılamak için iş akışlarını otomatikleştiren uyarlanabilir uyum platformlarını içerebilir.<sup>5</sup> Web güvenlik analizörleri, güvenlik denetimlerini, şifreleme standartlarını ve uyum raporlamasını otomatikleştirerek, GDPR, CCPA ve NIS2 gibi düzenlemelere uyumu kolaylaştıracaktır.<sup>3</sup>
- **Neden Önemli:** Bir güvenlik ihlali, sadece kötü bir halkla ilişkiler sorunu değil, aynı zamanda önemli yasal ve finansal sonuçları olan bir iş riskidir.<sup>1</sup> Düzenleyici kurumlar, tüketici verilerinin korunmasını sağlamak için API güvenlik gereksinimleri gibi daha sıkı kurallar getirmektedir.<sup>4</sup> Manuel uyum süreçleri zaman alıcı, hataya açık ve güncel tehdit ortamına ayak uydurmakta yetersiz kalmaktadır.
- **2025'teki Potansiyel Etkileri ve Uygulama Alanları:** 2025'te, zorunlu API güvenlik denetimleri, şifreleme standartları ve uyum raporlaması beklenmekte olup, uyumsuzluk durumunda ciddi cezalar uygulanacaktır.<sup>4</sup> Otomatik doğrulama, kuruluşların güvenlik duruşlarını güçlendirmelerine, yanlış pozitifleri azaltmalarına ve güvenlik boşluklarını en aza indirmelerine olanak tanıyarak saldırılara karşı daha proaktif olmalarını sağlayacaktır.<sup>5</sup> Uygulama alanları arasında finansal hizmetler, sağlık, kamu sektörü ve AB pazarında faaliyet gösteren tüm kuruluşlar (NIS2 direktifi nedeniyle) yer almaktadır.<sup>3</sup>
- **Güvenilir Kaynak/Referans:** Cymulate: The Future of Cloud Security: 7 Key Trends in 2025<sup>5</sup>, Rakuten Sixth Sense: The Future of API Security.<sup>4</sup>

### 3. Sonuç

2025 yılına doğru ilerlerken, web güvenlik analizörleri, siber tehdit ortamının artan karmaşıklığına ve dinamizmine yanıt olarak önemli bir dönüşüm geçirmektedir. Yapay zekanın hem saldırganlar hem de savunmacılar tarafından çift yönlü kullanımı, güvenlik stratejilerinin sürekli adaptasyonunu zorunlu kılmaktadır. Bütçe kısıtlamaları ve artan beklentiler, YZ ve otomasyonun güvenlik operasyonlarında verimlilik ve proaktiflik için birincil itici güçler olmasını sağlamaktadır.

Bu rapor, 2025 yılında web güvenlik analizörlerini şekillendirecek en etkili 10

teknîği/trendi detaylandırmıştır. YZ destekli tehdit tespiti ve yanıt sistemlerinden Sıfır Güven Mimarisi entegrasyonuna, API güvenliğinden yazılım tedarik zinciri analizine kadar, her bir trend, kuruluşların dijital varlıklarını koruma yeteneklerini geliştirmede kritik bir rol oynamaktadır. DevSecOps'un "shift-everywhere" felsefesi, çalışma zamanı uygulama kendi kendini koruma (RASP), sunucusuz ve kapsayıcı güvenliği, kuantum hazır şifreleme, kapsamlı görünürlük ve otomatik düzenleyici uyum, geleceğin web güvenliği duruşunu tanımlayan diğer temel unsurlardır.

Kuruluşların bu gelişen tehdit ortamında başarılı olabilmeleri için, web güvenlik analizörlerini sadece zafiyet tarama araçları olarak değil, aynı zamanda YZ destekli, otomatik, entegre ve sürekli adapte olabilen güvenlik ekosistemlerinin temel bileşenleri olarak görmeleri gerekmektedir. Bu trendleri stratejik yol haritalarına dahil etmek, yalnızca savunmaları güçlendirmekle kalmayacak, aynı zamanda giderek karmaşılaşan dijital dünyada iş dönüşümünü de mümkün kılacaktır.

### **Alıntılanan çalışmalar**

1. Website Security in 2025: What IT Leaders Need to Know - COLAB, erişim tarihi Haziran 30, 2025, <https://www.teamcolab.com/insights/website-security-in-2025-what-it-leaders-need-to-know/>
2. 2025 Cybersecurity Predictions: Not Getting Easier, but there Is Hope - SecureWorld, erişim tarihi Haziran 30, 2025, <https://www.secureworld.io/industry-news/cybersecurity-predictions-for-2025>
3. The Future of Cybersecurity: Insights and Predictions for 2025 - Obrela, erişim tarihi Haziran 30, 2025, <https://www.obrela.com/blog/the-future-of-cybersecurity-insights-and-predictions-for-2025/>
4. Data Observability | Rakuten SixthSense, erişim tarihi Haziran 30, 2025, <https://sixthsense.rakuten.com/data-observability/blog/The-Future-of-API-Security-Trends-and-Predictions-for-2025>
5. The Future of Cloud Security: 7 Key Trends in 2025 - Cymulate, erişim tarihi Haziran 30, 2025, <https://cymulate.com/blog/cloud-security-trends/>
6. 10 Vulnerability Scanning Tools to Know in 2025 - Pynt, erişim tarihi Haziran 30, 2025, <https://www.pynt.io/learning-hub/application-security/10-vulnerability-scanning-tools-to-know-in-2025>
7. AI Considerations for 2025: Preparing for the Future of ... - Optiv, erişim tarihi Haziran 30, 2025, <https://www.optiv.com/insights/discover/blog/ai-trends-in-cybersecurity>
8. 8 Container monitoring trends in 2025 - DEV Community, erişim tarihi Haziran 30, 2025, [https://dev.to/swetha\\_suresh\\_18c9975c236/8-container-monitoring-trends-in-2025](https://dev.to/swetha_suresh_18c9975c236/8-container-monitoring-trends-in-2025)

[25-3mkj](#)

9. AI Security: 2025 Predictions & Recommendations - HiddenLayer, erişim tarihi Haziran 30, 2025, <https://hiddenlayer.com/innovation-hub/ai-security-2025-predictions-recommendations/>
10. Gartner Reports, The Trends Reshaping Security Strategies - The National CIO Review, erişim tarihi Haziran 30, 2025, <https://nationalcioreview.com/articles-insights/cybersecurity-in-2025-the-trends-reshaping-security-strategies/>
11. Top 8 API Management Trends in 2025 - API7.ai, erişim tarihi Haziran 30, 2025, <https://api7.ai/blog/2025-top-8-api-management-trends>
12. Securing the Future: Runtime Protection for Serverless Applications ..., erişim tarihi Haziran 30, 2025, <https://www.webasha.com/blog/securing-the-future-runtime-protection-for-serverless-applications-in-2025>
13. 3 DevSecOps Trends ISVs Should Watch in 2025 - DevPro Journal, erişim tarihi Haziran 30, 2025, <https://www.devprojournal.com/software-development-trends/devsecops/3-devsecops-trends-isvs-should-watch-in-2025/>
14. ISACA Now Blog 2025 The 2025 Software Supply Chain Security ..., erişim tarihi Haziran 30, 2025, <https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2025/the-2025-software-supply-chain-security-report>
15. The 2025 Software Supply Chain Security Report - National ..., erişim tarihi Haziran 30, 2025, <https://ntsc.org/wp-content/uploads/2025/03/The-2025-Software-Supply-Chain-Security-Report-RL-compressed.pdf>
16. The 2025 Container Security Platform Landscape: What You Need ..., erişim tarihi Haziran 30, 2025, <https://checkmarx.com/learn/the-2025-container-security-platform-landscape-what-you-need-to-know/>
17. Features the Best DevSecOps Tools Will Have in 2025 - Checkmarx, erişim tarihi Haziran 30, 2025, <https://checkmarx.com/learn/appsec/features-the-best-devsecops-tools-will-have-in-2025/>
18. DevSecOps Pipeline Best Practices For 2025 | Wiz, erişim tarihi Haziran 30, 2025, <https://www.wiz.io/academy/devsecops-pipeline-best-practices>
19. 5 DevSecOps Checklists to Embrace Advanced Techniques in 2025 - ChaosSearch, erişim tarihi Haziran 30, 2025, <https://www.chaossearch.io/blog/checklists-for-advanced-devsecops-techniques>
20. Top 10 DevSecOps Tools (June 2025) - Scalr, erişim tarihi Haziran 30, 2025, <https://scalr.com/learning-center/top-10-devsecops-tools/>
21. 15 DevSecOps Tools to Know in 2025 | Codefresh, erişim tarihi Haziran 30, 2025, <https://codefresh.io/learn/devsecops/15-devsecops-tools-to-know-in-2025/>

22. Runtime Application Self-Protection Software Market Dynamics ..., erişim tarihi Haziran 30, 2025, <https://github.com/Atikaislam51/9poyackkbh7pcjd-1/issues/38>
23. Runtime Application Self Protection Software Statistics 2025, erişim tarihi Haziran 30, 2025, <https://ilcbuddy.com/data/runtime-application-self-protection-software-statistics/>
24. RSA Conference 2025: Top Cybersecurity Trends, AI Security, & Future Threats - YouTube, erişim tarihi Haziran 30, 2025, <https://www.youtube.com/watch?v=2K8SrrofH-Y>