Part of F5

ÇÖZÜME GENEL BAKIŞ

Shape Enterprise Defense

Web ve mobil uygulamalarda sofistike dolandırıcılık ve siber saldırıları önleyin

Saldırganlar, Web Sitelerinde ve Mobil Uygulamalarda Dolandırıcılık Yapmak için İnsan Davranışlarını Taklit Ediyor

Saldırganlar, uygulamaların güvenlik açıklarından yararlanmak yerine uygulamaların işlevselliğini kötüye kullanıyorlar. Taklit saldırıları, son derece gelişmiş otomatik araçlar kullanarak insan davranışını taklit eder ve böylece büyük ölçekte dolandırıcılık veya yetkisiz faaliyet gerçekleştirir. Aşağıdaki yöntemler, en yaygın saldırı çeşitleri arasında yer almaktadır:

Kimlik Bilgisi Doldurma
Saldırganlar, uygulamaya giriş sırasında, hali hazırda çalmış oldukları giriş bilgilerini test ederler. Son kullanıcılar genellikle farklı çevrimiçi hesaplarda aynı şifreleri yeniden kullandıkları için, herhangi bir çalıntı kimlik bilgisinin büyük bir web sitesinde veya mobil uygulamada oturum açma başarı oranı genellikle %0,5-2'dir ve bu da hesabın çalınmasına ve çevrimiçi dolandırıcılığa yol açar.

Yetkisiz Veri Toplama
Saldırganlar, kurumsal bir web sitesinden veya mobil uygulamadan değerli bilgilerinizi alır ve rakiplere satar veya izinsiz olarak kullanır. Bu süreç, altyapı açısından bir yük teşkil eder ve çok sayıda güvenlik sorununa yol açar.

Sahte Hesap Oluşturma
Saldırganlar, çeşitli dolandırıcılık aktivitelerini gerçekleştirmek için yüksek hacimlerde kullanıcı hesapları oluşturur. Shape, çevrimiçi ödül promosyonlarından yararlanmak, kara para aklamak ve kimlik bilgi doldurma saldırılarını gizlemek için sahte hesapların kullanıldığına şahit olmuştur.

Bu tür saldırılar, Yeni Nesil Güvenlik Duvarları ve Web Uygulaması Güvenlik Duvarları (WAF'lar) gibi geleneksel güvenlik kontrollerini ve IP tabanlı kara liste, hız sınırlama ve CAPTCHA gibi yaygın savunma tekniklerini alt edebilir.

Shape Enterprise Defense, Otomatik Saldırıların Yönünü Değiştirerek Dolandırıcılığı Önler

Shape Kurumsal Savunma, web ve mobil uygulamaları ve API uç noktalarını karmaşık saldırılardan koruyarak büyük ölçekli dolandırıcılığın önüne geçer. Shape Kurumsal Savunma, bir uygulama isteğinin sahte bir kaynaktan gelip gelmediğini gerçek zamanlı olarak belirler ve bu isteği engelleme, yeniden yönlendirme veya işaretleme gibi kuruluş tarafından belirlenen eylemleri gerçekleştirir.

ÇALINTI KIMLIK BILGILERININ BÜYÜK BIR WEB SITESINDE VEYA MOBIL UYGULAMADA OTURUM AÇMA BAŞARI ORANI GENELLIKLE %0,5-2,0'DIR

Shape Kurumsal Savunma, geleneksel bot azaltmanın ötesine geçer. Shape, birkaç yıldır dünyanın en büyük şirketlerini savunarak, yalnızca talebin bot kaynaklı mı yoksa insan kaynaklı mı olduğunu belirleme konusunda değil, aynı zamanda talebin kötü niyetle mi yoksa iyi niyetle mi yapıldığını belirleme konusunda da uzmanlık geliştirmiştir. Bu, işletmelere, kullanıcının işlem akışına dair tam bir süreç sunar ve dolandırıcılığın gerçek zamanlı olarak önlenmesini sağlar.

Nasıl Çalışır?

Shape Kurumsal Savunma, şirket içinde ters proxy (1) olarak yerinde kullanılarak Shape'in veri merkezlerinde barındırılabilir veya Shape tarafından yönetilen kurumsal bulut ortamında veya Shape API (2) aracılığıyla kullanılabilir.

Ziyaretçi Sinyalleri

Shape, savunma motorunun saldırıları algılama yeteneğini geliştirmek amacıyla gelişmiş telemetrileri toplar. Bu sinyaller web uygulamalarında JavaScript, yerel mobil uygulamalarında ise bir SDK aracılığıyla toplanır.

Shape Savunma Platformu

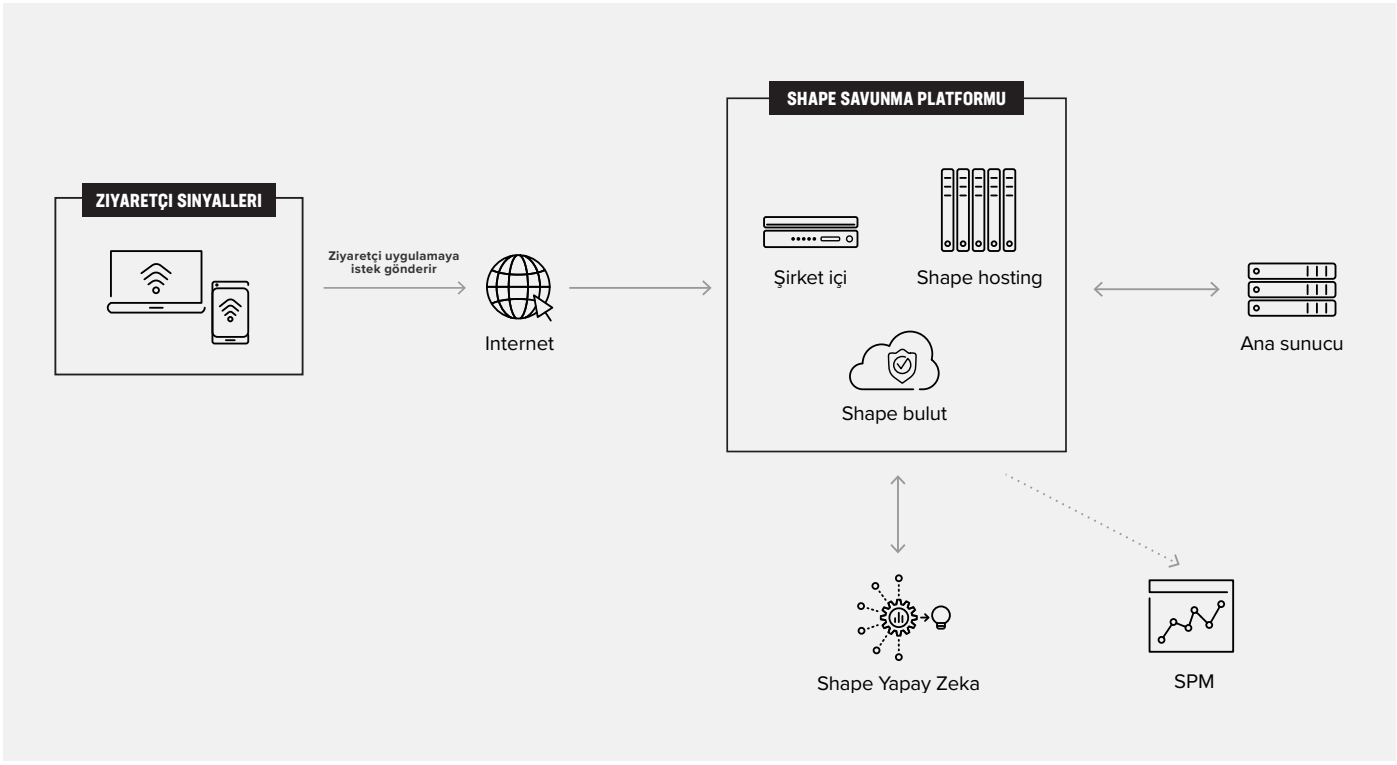
Shape Savunma Platformu, kurumun korunan uygulamalarına yönelik otomatik işlemleri algılayan ve azaltan, Shape Kurumsal Savunma'nın karar bileşenidir. Ağ, tarayıcı ve kullanıcı seviyelerinde otomasyonu tespit ederek hileli taleplerin yönünü değiştirmek için yüzlerce sinyali kullanarak çalışır. Ters proxy, şirket içinde konumlandırılabilir ve Shape'in veri merkezlerinde veya Shape tarafından yönetilen kurumsal bulut ortamında barındırılabilir.

Shape AI Cloud

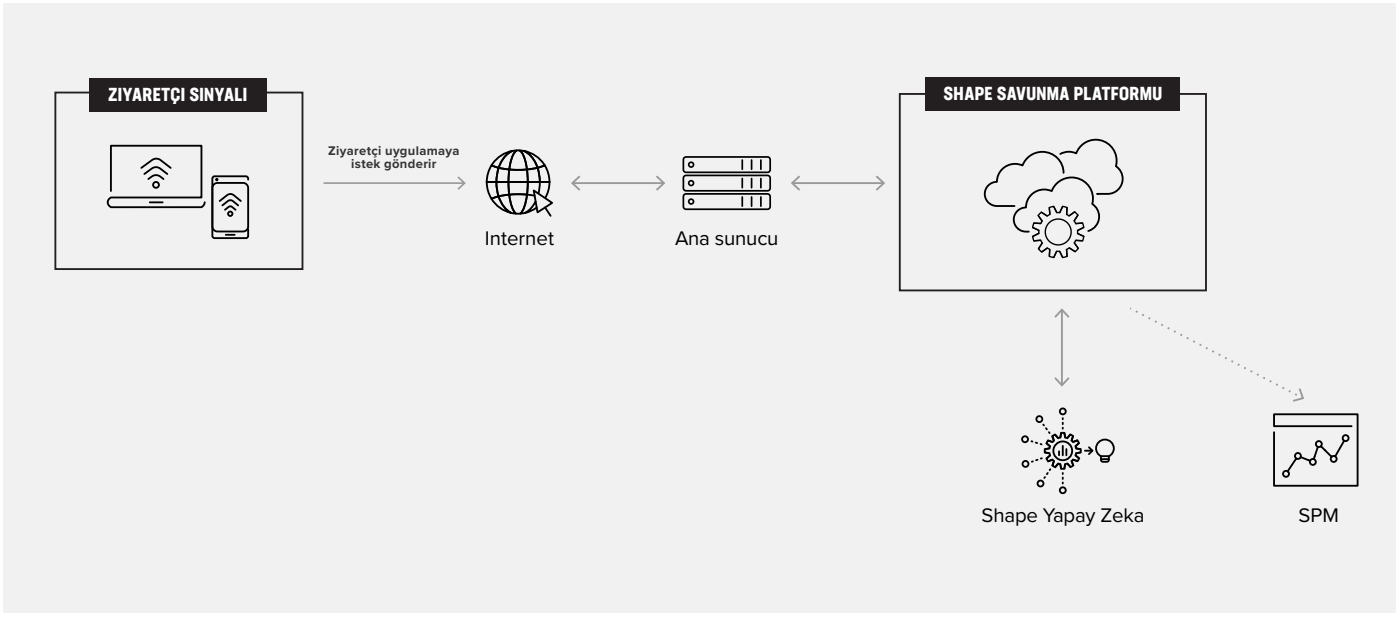
Shape AI Cloud, sürekli stratejilerini yenileyen saldırıları proaktif olarak tanımak, azaltmak ve yeni karşı önlemleri otonom bir şekilde devreye almak için tüm işlemleri analiz eder.

API Tabanlı

Ziyaretçi sinyalleri gönderildikten sonra, Shape API, işlemin otomatikleştirilmiş bir kaynak tarafından mı yoksa bir insan tarafından mı oluşturulduğunu tespit etmek için yanıt verir ve bu bilgiyi kaynak sunucuya iletir. Kuruluş, trafiğe izin aşamasına karar vermek için bu API yanıtını kullanır.



Şekil 1: Ters proxy



Şekil 2: API tabanlı

Shape Kurumsal Savunma'nın Temel Faydaları

Yöntemlerini Sürekli Yenileyen Gelişmiş Saldırganları Tespit Etme

Saldırganların %5-%10'u, yeni karşı savunma önlemleri uygulandığında, genellikle araçlarını yenilemeye çalışır. Shape Kurumsal Savunma, saldırganlar geliştikçe bile tam etkinliğini sürdürmek üzere tasarlanmıştır. Shape, saldırganların tekniklerini tespit etmek ve ardından uygun karşı savunmayı otonom olarak uygulamak için denetimli ve denetimsiz gelişmiş öğrenme yöntemleri kullanır. Shape AI, yıllar içinde Fortune 500 şirketlerinden elde edilen saldırı verileri ile geliştirildiği için, benzersiz bir şekilde uzun vadeli ve kalıcı etki gösterebilmektedir.

Çok Kanallı Koruma: Web, Mobil ve API'ler

Bir kuruluş tarafından bir uygulama için, güçlü bir savunma sunulduğunda, saldırganlar hızla farklı bir uygulamayı hedeflemeye başlarlar ve genellikle web'in ötesindeki başka kanallara geçerler. Shape, web siteleri, yerel mobil uygulamalar ve API uç noktalarına yönelik tam kurumsal korumayı garanti eden çözümler sunar.

Sıfır Effor

Shape Kurumsal Savunma, çalışanlar neredeyse hiç çaba sarf etmeden saldırıların yönünün değiştirilmesi için tam yönetimli bir hizmet olarak sunulmaktadır. Profesyonel hizmetler ekibi, müşteriler adına kurulumları yapılandırır, uygulamaları izler ve teknolojiyi korur. Güvenlik Operasyon Merkezi, kurulduktan sonra trafiği 7 gün 24 saat izler ve olaylara müdahale eder. Ek olarak, tehdit uzmanları Shape'in müşteri ağında toplanan saldırılar ve sektör istihbaratı hakkında düzenli bilgilendirmeler sunarak, kuruluşun güvenlik ve dolandırıcılık ekiplerinin bir uzantısı gibi işlev görür.

Kolektif Müşteri Savunması

Bir müşteride yeni bir saldırı tekniği gözlemlendiğinde, diğer tüm Shape müşterileri bu teknikten anında korunur. Amerika'nın en büyük 5 bankası, dünyanın en büyük 10 havayolu şirketinden 5'i ve dünyanın en büyük 5 otelinden üçü dahil olmak üzere dünyanın en büyük şirketleri Shape müşterileri arasında yer almaktadır. En gelişmiş saldırganlar önce en büyük B2C şirketlerini hedefleme eğiliminde olduğundan, tüm müşteriler kolektif saldırı veri kümesinden büyük ölçüde yararlanır.

Esnek Kurulum Seçenekleri

Shape Kurumsal Savunma, tüm kanallarda birleşik bir güvenlik duruşu sağlamak için tasarlanmış, mimariden bağımsız bir hizmettir. Bu hizmet, şirket içinde ters proxy olarak yerinde, Shape'in veri merkezlerinde veya Shape tarafından yönetilen kurumsal bulut ortamında barındırılabilir veya Shape API aracılığıyla kullanılabilir.

Kullanıcı Deneyimini Iyileştirme

Shape, son kullanıcıların güvenlik yükünü olabildiğince hafifletmeye olanak tanır. Birincisi, Shape'in benzersiz teknolojisi, kullanıcıları etkilemeden saldırganları tereyağından kıl çeker gibi ayırarak tanımlar. İkincisi, otomatik trafiğin kaynak sunucuya ulaşmasını engelleyerek, sunucu gecikmesini azaltır ve performansı arttırır. Son olarak, Shape'in etkinliği sayesinde birçok şirket, CAPTCHA ve çok faktörlü kimlik doğrulama dahil olmak üzere yüksek friksiyonlu mekanizmaları azaltabilmekte ve/veya ortadan kaldırabilmekte ve böylece genel kullanıcı deneyimini iyileştirebilmektedir.

Daha fazla bilgi edinmek için Shape Security ya da F5 temsilcinizle iletişime geçin veya shapesecurity.com ya da f5.com adresini ziyaret edin.