Forcepoint

Çözüm Özeti

Forcepoint Next Generation Firewall ve Amazon Web Hizmetleri

En güvenli ve etkili kurumsal güvenlik duvarı - merkezi olarak yönetilen, her zaman açık ve amansız

Sorun

- Şirketlerin ve kurumların, bulut ve karma ortamlarda, geleneksel şirket içi altyapılarla aynı güvenlik seviyesini sürdürmeleri gerekir.
- Güvenli bir bulut altyapısı veya karma altyapı oluşturmak ve sürdürmek masraflı olabilir ve teknik zorluklar arz edebilir
- Düzenlemelere uyum zor ve zaman alıcı olabilir

Çözüm

- Forcepoint Next Generation Firewall (NGFW) yazılım tabanlı çözümleri, minimum maliyet ve karmaşıklıkla maksimum güvenlik sağlayacak şekilde tasarlanmıştır
- Forcepoint NGFW Security Management Center (SMC), süreçleri kolaylaştıran, görünürlük ve kontrol sağlayan birleşik bir platformdur
- Forcepoint NGFW SMC, denetim raporlarına kolay erişim de dahil olmak üzere BT yöneticilerinin sanal ve fiziksel ağlardaki uyum çalışmalarını kolaylaştırmasını sağlar

Sonuç

- Minimum karmaşayla maksimum bulut ve karma ağ güvenliği
- Daha hızlı olay yanıtı
- Basitleştirilmiş mevzuat uyumu, uygulama ve yönetimi
- Ağ altyapısı ve güvenlik maliyetlerinde düşüş

Forcepoint Next Generation Firewall (NGFW), insanları ve tüm kurumsal bulut altyapısında veya karma altyapılarda kullandıkları verileri birbirine bağlar ve tüm bunları yüksek verimlilik, kullanılabilirlik ve güvenlikle yapar. Dünya çapında binlerce müşterinin güvendiği ve AWS pazarı üzerinden ulaşılabilen Forcepoint ağ güvenliği çözümleri, şirketlerin ve kurumların kritik sorunları etkin ve ekonomik bir şekilde ele almasını sağlar.

Halka Açık Bulut Ortamları için Forcepoint Güvenliği

Bulut tabanlı hizmetler ve sanal uygulamalar, her tür ve boyuttaki işletmeleri dönüştürüyor. Kurumlar, rekabetçi kalmak için bakım ve genel masrafların getirdiği yükle uğraşmadan daha yüksek verim, çeviklik ve maliyet kontrolüne ihtiyaç duyduklarından, geleneksel şirket içi donanımlar hızla ortadan kaybolmakta. Bulut mimarilerinin geniş çaplı olarak benimsenmesi, güvenlik uzmanlarına ve BT liderlerine bu yeni ortamların fiziksel öncüleri kadar güvenli olmasını sağlamak gibi bir ek sorumluluk getiriyor.

Forcepoint Next Generation Firewall (NGFW) yazılım tabanlı çözümleri, minimum maliyet ve karmaşıklıkla maksimum güvenlik sağlayacak şekilde tasarlanmıştır. Forcepoint NGFW Security Management Center (SMC) hem fiziksel altyapılarda hem de sanal ortamlarda ve bulut ortamlarında mevzuata uymanızı sağlayan benzersiz bir görünürlük, kontrol ve tutarlı politika uygulamaları sağlayan birleşik bir platformdur.

AWS Cloud Security

Forcepoint, bulut ortamlarında güvenliği sağlamak için ölçeklenebilirliği, operasyon verimi ve güvenliği kanıtlanmış, önde gelen yeni nesil güvenlik duvarı teknolojisini AWS'ye taşıyor. Güvenli bir Sanal Özel Ağ (VPN) ağ geçidiyle veri merkezlerinden ve ağ uç noktalarından şubelere ve uzak tesislere kadar tüm kurumsal ağınızı kolayca ve güvenli bir şekilde AWS bulut ortamınıza taşıyın. Merkezi yönetimimiz, tüm sistemleriniz için politikaları hızla ve tutarlı bir şekilde oluşturup uygulayabilmenizi sağlamaktadır. Hem AWS ortamınızda hem de fiziksel ağınızda olup bitenleri hızla görebilirsiniz.

Forcepoint NGFW'ye geçen müşteriler, siber saldırılarda %86, BT üzerindeki iş yükünde %53 ve planlı bakım çalışmalarında %70 düşüş olduğunu bildiriyor.

Maksimum Güvenlik, Minimum Karmaşıklık

Forcepoint'in gelişmiş tehdit koruması, derin paket denetleme ve uygulama seviyesinde kontrol gibi çözümlere yönelik yazılım tabanlı mimarisi, karmaşıklık ve ek maliyetler olmadan maksimum güvenlik sağlamak üzere kolayca kurulup uygulanacak şekilde tasarlanmıştır. Yazılım tabanlı Forcepoint güvenlik platformu; güvenlik duvarı, VPN, IPS ve URL filtreleme koruması da dahil olmak üzere her bir kişi, yer veya varlığın özel ihtiyaçlarına göre uyarlanabilecek kapsamlı ve entegre bir derinlemesine koruma sağlamaktadır. Bu yazılım platformu- herhangi bir donanıma ihtiyaç duyulmadan, durum denetimi, parçalı politikalar ve erişim kontrolü ve yedek ISP bağlantıları da dahil olmak üzere donanım tabanlı araçlardaki tüm özellikleri sunmaktadır.

Gerçek Zamanlı Görünürlük ve Kontrol

Forcepoint NGFW, hem sanal ortamlarda hem de bulut ortamındaki trafik akışı üzerinde geleneksel yönetim konsollarının sağlayamadığı eksiksiz görünürlük ve kontrol sağlar. SMC, sanal sistemler arasındaki trafik miktarını hızla rapor eder ve sistemin çökmek üzere olması durumunda yöneticileri uyarır. İstediğiniz sayı ve kombinasyondaki fiziksel veya sanal Forcepoint cihaz veya kümelerinin yanı sıra standart x86 donanım üzerinde çalışan yazılım tabanlı sürümleri de yönetin. SMC ayrıca tüm güvenlik uygulamaları üzerinde tam görünürlük ve detaylı kontrol sağlayan bütünsel bir takip panosuyla sanal sistem güvenliğini de artırır.

Düzenlemelere Uyumu Basitleştirin

Fiziksel dünyada PCI DSS, HIPAA, Sarbanes-Oxley ve FISMA gibi en son yasal düzenlemelere uyum sağlamak zor olsa da sanal dünyada uyumu sürdürmek daha da zordur. Her bir uygulama için kullanılan geleneksel kontroller, sanal ortamda mevcut değildir. Bu da hangi bilgilere kimlerin, ne zaman eriştiğini belirlemeyi neredeyse imkansız hale getirir ve denetmenler için bir ikaz işareti oluşturabilir. SMC, sanal ve fiziksel ağlarda düzenlemelere uyum sağlayabilmeniz için ihtiyaç duyduğunuz takip, analiz ve raporlama seviyesini sunar. Tüm ağ olayları hakkında kapsamlı veriler toplar ve bu verileri açık ve kolayca okunan denetim kayıtları şeklinde sunar. SMC, ayrıca tek bir düğmeye bastığınızda güvenlik ayarlarını listeler, sistem değişikliklerini bildirir ve ihtiyaç duyduğunuz doğru denetim raporlarını sunar.

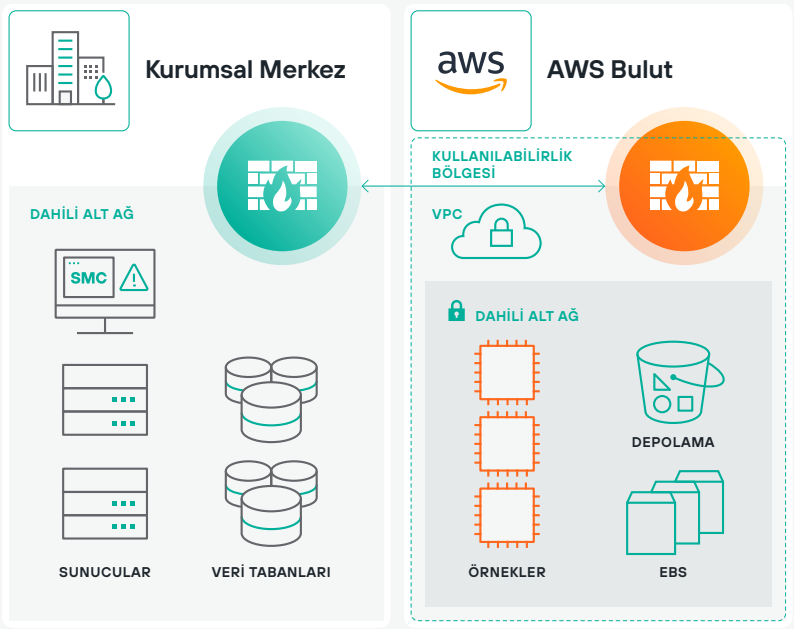
Hızlı ve Esnek Dağıtım

Forcepoint'in yazılım tabanlı mimari güvenliğini AWS ortamınızda hızla kurmak için, AWS pazarında mevcut olan seçeneklerden birini seçmeniz yeterlidir

→ Pazar Yerini Ziyaret Edin

Forcepoint NGFW ve AWS Çözümleri

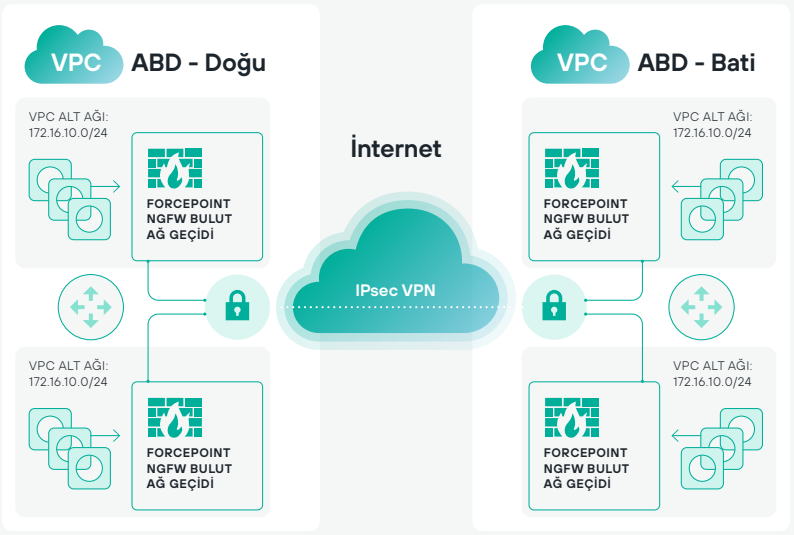
Forcepoint NGFW ile kurumsal ağlarınızı güvenle genişletin ve AWS'nin gücünden faydalanın



Kurumsal Ağlarınızı AWS Ortamlarına Taşıyıp Genişletin

Forcepoint NGFW, kurumların AWS ortam(lar)ındaki verileri sızdırmaya çalışan güvenlik açıklarına ilişkin suistimalleri, kötü amaçlı yazılımları ve sıfır gün güvenlik açıklarını durdurmak için uygulamaya özel tehdit önleme politikaları uygular. AWS Security Hub, politika uygulama uyarılarını tetikleyen eylem ve koşulları merkezi bir şekilde görmenizi sağlar.

- → Kurumunuzun ağını AWS'ye taşıyıp genişletin
- → Karma BT'yi verimli bir şekilde uygulayın ve AWS'den içeri ve dışarı veri aktarımını basitleştirin
- → Çok sayıda VPN bağlantısının her iki ucunu da tek bir yerden kolayca yönetin



Bölgeler arası VPC'den VPC'ye Yönlendirme

Çok sayıda AWS bölgesi arasında güvenli VPC bağlantıları sağlayın. Forcepoint'in sektöre liderlik eden ağ güvenliği teknolojisini kullanarak güvenlik politikalarını yönetebilir, kontrol edebilir ve uygulayabilirsiniz.

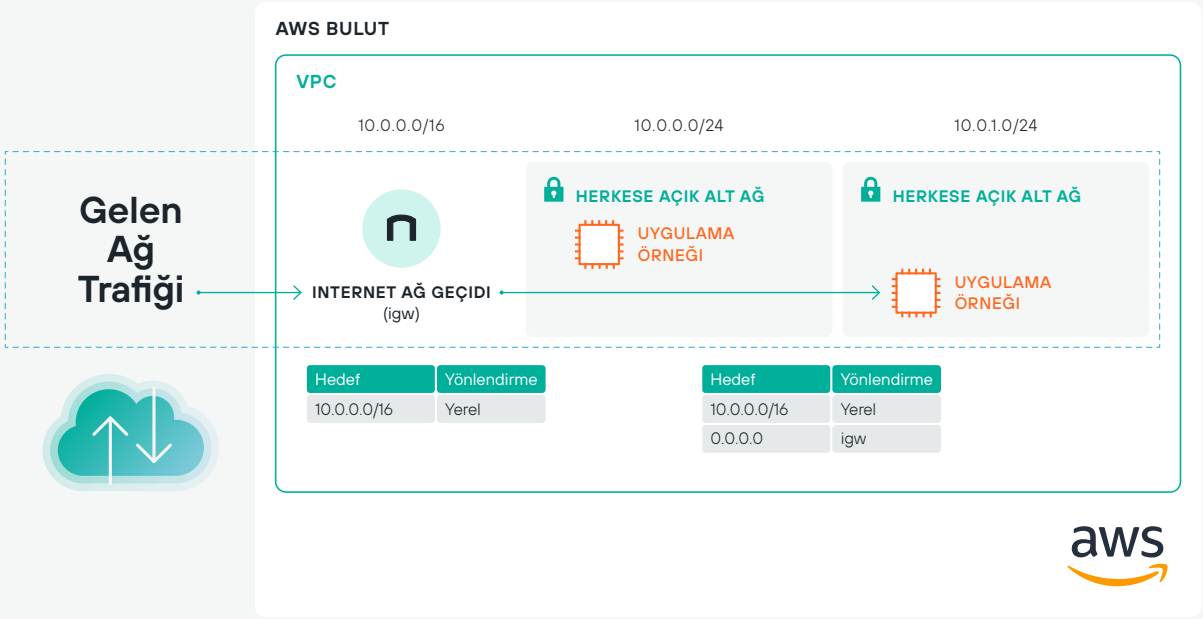
- → Bölgeler arasında akan verileri koruyun
- → Tüm bölgelerde tutarlı güvenlik politikaları uygulayın

Bir enerji şirketi, sıfır müdahale gerektiren bir kurulumla Forcepoint NGFW ve SD-WAN çözümlerini uygulayarak ve buluta geçiş yaparak WAN maliyetlerinde %90 tasarruf sağladı.

Amazon VPC Ingress Routing

Amazon VPC Ingress Routing, ağ güvenliğinin Amazon Virtual Private Cloud (VPC) altyapınızla entegrasyonunu basitleştirerek, tüm kurumsal ağınızda (hem bulut hem de şirket içi) aynı güvenlik politikalarını uygulamanızı kolaylaştırır ve AWS iş yükünüzü etkin bir şekilde korumanızı sağlar.

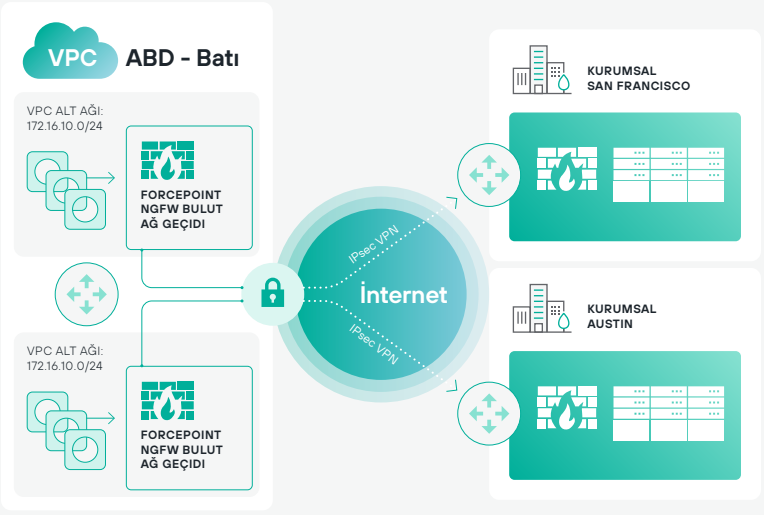
- → Amazon VPC'ye gelen tüm trafiği, kurumsal ağa erişmek için kullanılan aynı denetleme seviyesiyle koruyacak esnekliğe erişin
- → Ek gecikmeler yaşamadan tüm kurumsal ağda aynı ağ güvenliği politikalarını uygulayın
- → Minimum maliyet ve karmaşayla maksimum güvenlik sağlayın



AWS VPN CloudHub

Çok sayıda AWS bölgesi arasında güvenli VPC bağlantıları sağlayın. Forcepoint'in sektöre liderlik eden ağ güvenliği teknolojisini kullanarak güvenlik politikalarını yönetebilir, kontrol edebilir ve uygulayabilirsiniz.

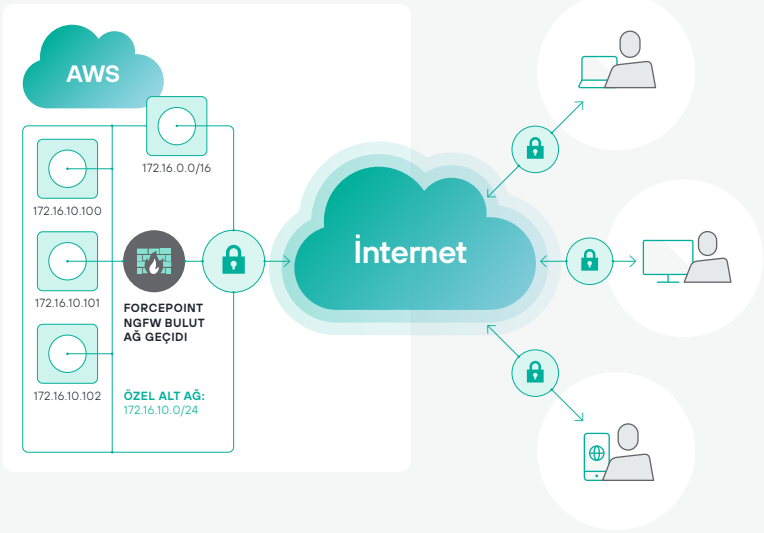
- → Bölgeler arasında akan verileri koruyun
- → Tüm bölgelerde tutarlı güvenlik politikaları uygulayın



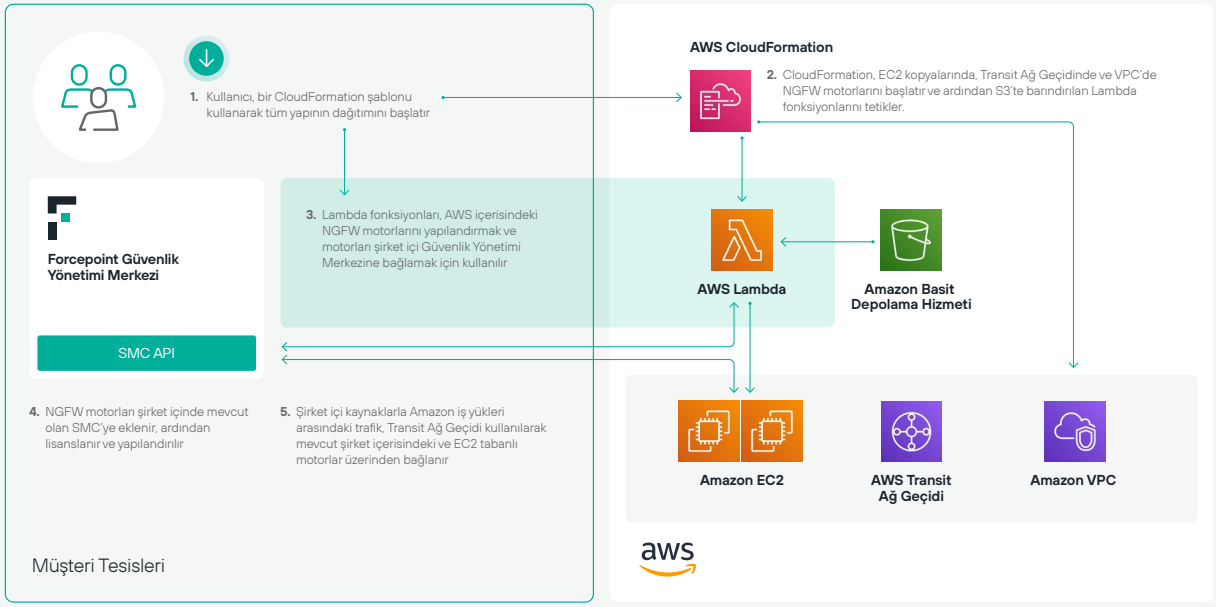
Uzaktan Erişim Bağlantıları

Forcepoint NGFW, uzaktan çalışan kullanıcıları Amazon Virtual Private Cloud'a (VPC) bağlamak için bir bulut uç nokta ağ geçidi olarak kullanılabilir. Forcepoint NGFW bulut ağ geçidi, bir Amazon Elastic Compute Cloud (EC2) ortamında kullanılarak, aşağıdakiler dahil olmak üzere EC2 kurulumlarınızı tüm gelen ve giden erişim bağlantılarında koruyan gelişmiş güvenlik duvarı özellikleri sunar:

- → Uygulama farkındalığı
- → Kullanıcı kimliği özellikleri



Forcepoint NGFW ve AWS Hizmetlerinin Entegrasyonu

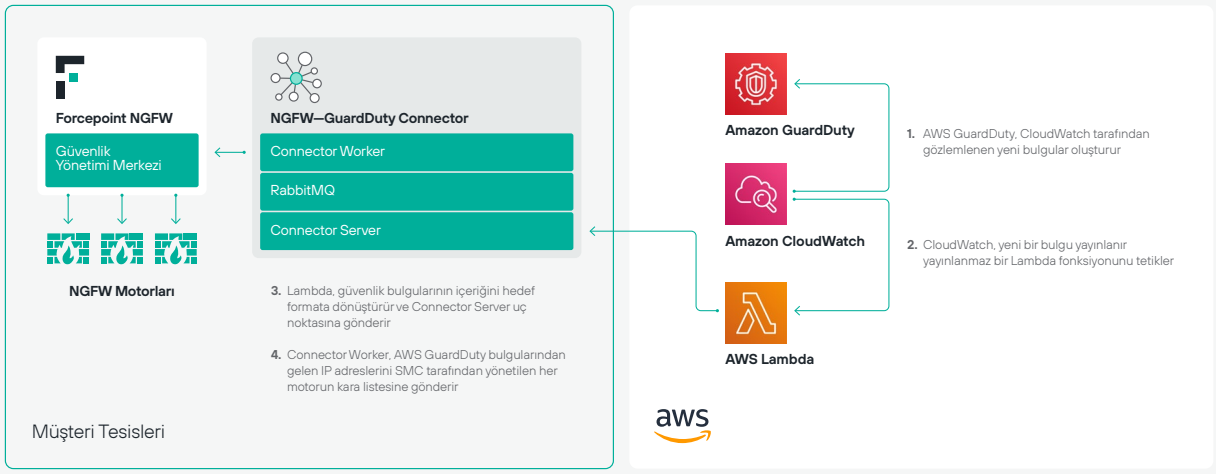


Transit Ağ Geçidi Entegrasyonu

Yedek bir Forcepoint Yeni Nesil Güvenlik Duvarı setinin EC2 kurulumları olarak kullanılmasını sağlar, bir AWS Transit Ağ Geçidi kurar ve AWS Lambda fonksiyonlarını kullanarak NGFW motorlarını mevcut bir Forcepoint Güvenlik Yönetimi Merkezine bağlar. Buluttaki NGFW motorlarıyla Transit Ağ Geçidi arasında yedek IPSEC tünelleri oluşturulur ve Forcepoint Güvenlik Yönetimi Merkezi tarafından yönetilen güvenlik politikaları AWS'deki NGFW motorlarına uygulanarak Transit Ağ Geçidinden geçen trafik güvenlik altına alınabilir.

- → Şirket içi ağlarda ve AWS'de güvenlik politikalarının tutarlı şekilde uygulanmasını sağlar
- → Özelleştirilmiş kurulumlara izin veren kişiselleştirilebilir parametrelere sahip tek bir AWS CloudFormation şablonu kullanarak tüm teknoloji yapısının kurulumunu otomatik hale getirir

Kılavuzu Edinin

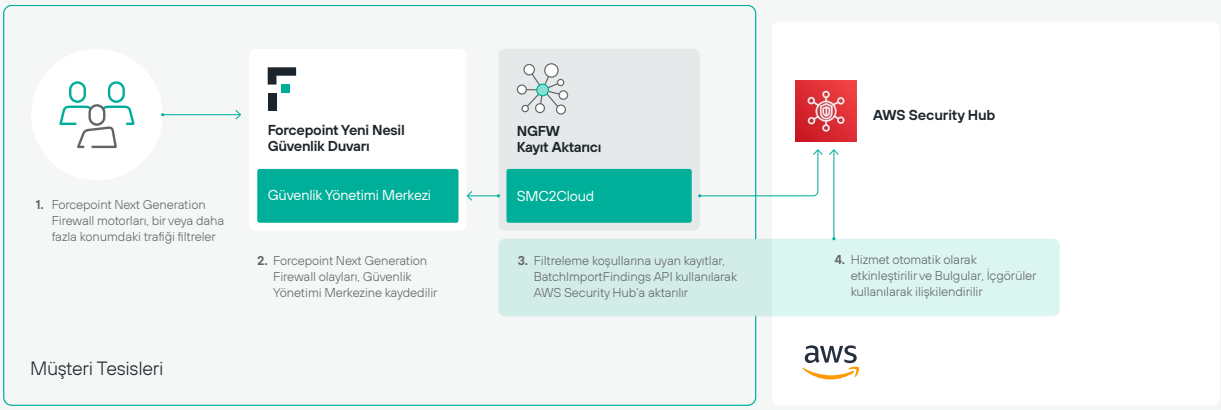


Amazon GuardDuty Entegrasyonu

GuardDuty, AWS müşterilerine AWS Cloud'da sürekli tehdit tespiti için akıllı ve uygun maliyetli bir seçenek sunar. Hizmet, potansiyel tehditleri tespit etmek ve önceliklendirmek için makine öğrenimi, anormal durum tespiti ve entegre tehdit analizi özelliklerinden faydalanır. Forcepoint NGFW entegrasyonu, güvenlik bulgularının Amazon GuardDuty'den gerçek zamanlı olarak içeri aktarılmasını otomatik hale getirir.

- → Şirket içinde yer alan ve NGFW tarafından korunan kullanıcı, uygulama ve hizmetler, kurumun AWS ayak izini hedef alan tehditler konusunda sağlanan ek görünürlükten faydalanır
- → Ardından, Amazon GuardDuty tarafından tespit edilen kötü amaçlı kaynaklara ait IP adresleri kurum sitelerinde kurulmuş olan tüm NGFW motoru filosunda kara listeye alınır
- → Ortak tehdit bilgileri sayesinde daha etkili koruma sağlar

Kılavuzu Edinin



AWS Security Hub ile Birlikte Çalışabilme

AWS Security Hub, tüm AWS hesaplarınızın güvenlik durumuyla ilgili konsolide bir görünüm sağlar. Forcepoint'in AWS Security Hub ile entegrasyonu, kullanıcıların her nerede olursa olsun en hassas verilerinizle nasıl etkileşime girdiğini görmenizi sağlar.

- → Müdahale sürelerini hızlandırmak için, Forcepoint NGFW'deki olay kayıtlarını otomatik ve gerçek zamanlı olarak AWS Security Hub'a aktarın.
- → NGFW tarafından korunan tüm konumlarda görünürlüğü artırmak için, güvenlik bulgularını diğer kaynaklarla ilişkilendirin
- → Kurumunuz için en önemli olan konulara öncelik vermek için, önem derecesi ve tür gibi pek çok farklı alanda gruplama yaparak verileri kolayca derleyin

Kılavuzu Edinin Bir Demo Planlayın