UYGULAMA MERKEZLİ DÜNYADA F5 NETWORKS ZERO TRUST YAKLAŞIMI

F5 Networks “Zero Trust” Yaklaşımı

"Zero Trust", bir işletmenin daha ileri gitmesine ve daha güvenli olmasına yardımcı olabilecek güçlü bir stratejidir. Son yıllarda yeni bir konsept olmasa da çok fazla gündem olmaya başladı. Dünyanın dört bir yanındaki şirketler COVID-19 krizi sırasında nasıl çalışacakları ve nasıl tepki verecekleriyle boğuşurken, bu kavram her zamankinden daha anlamlı ve önemli bir hale geliyor.

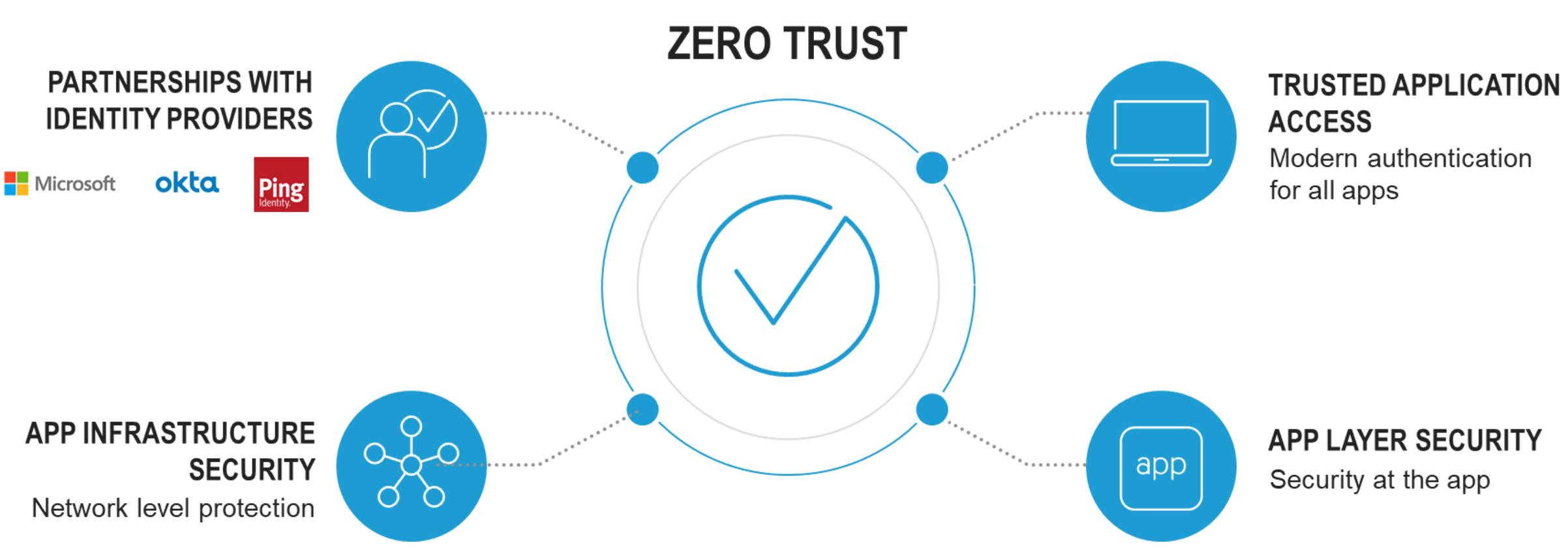
Geleneksel ağ güvenliğini sağlamak artık yeterli değil. Çoklu bulut sistemlerinde, devreye alınan uygulamaların ve mobil iş gücünün artmasıyla, perimeter security (ağ çerçevesinin) güvenliği neredeyse tamamen ortadan kalktı.

Zero Trust, tanımlanmış bir çevre içinde güvenilir bir ağ fikrini ortadan kaldırır. Bugün, en az ayrıcalıklı kullanıcı erişimini uygulamanız ve mümkün olduğunca incelemeniz, saldırganların zaten ağda olduğunu ve ağda saklandığını varsaymanız ve kontrol noktalarından daha fazla bağlam ve görünürlük elde etmeniz gerekir. Zero Trust'ı etkinleştirmek için kuruluşların "Güven ama Doğrula" yaklaşımından vazgeçmesi ve şu üç ilkeye bağlı kalması gerekir:

- **Asla güvenme**
- **Daima doğrula**
- **Sürekli olarak gözlemle**

Hiçbir üretici, Zero Trust için gereken unsurları tek başına sağlayamazken, F5 Networks sağlam uygulama güvenliği portföyü ile değer katabilir ve Zero Trust mimarisinde dört temel kontrol noktasını güvence altına alabilir. Özellikle:

- **Uygulamalara erişen uç noktalar: Güvenilir uygulama erişim çözümleri tüm uygulamalar için modern kimlik doğrulaması sağlar.** ***(trusted app access)***
- **Ağ altyapısı: F5 Networks, ağı korumaya yardımcı olacak uygulama altyapısı güvenlik çözümlerine sahiptir.** ***(application infrastructure security)***
- **Uygulamalar (uygulamalar ister bulutta, ister şirket içinde, SaaS tabanlı veya tamamen yönetiliyor olsun): F5 Networks, uygulama içinde veya yakınında güvenlik sağlamak ve uygulama yığınını korumak için Layer 4'ten 7'ye kadar uygulama katmanı güvenlik çözümleri sunar.** ***(application layer security)***
- **Kimlik hizmeti: F5 Networks' ün, Microsoft, Okta ve Ping ile iş ortaklıkları var. Güvenilir uygulama erişim çözümlerini, bu Hizmet Olarak Kimlik** ***(IDaaS)*** **sağlayıcıları ile entegre ederek, birleşik, güvenli bir erişim deneyimi sunmak için bulut tabanlı, SaaS ve kritik ve özel uygulamalar arasındaki kimlik boşluğunu kapatmaya yardımcı olur.**



Eğer, F5 Networks'ün sunduğu "zero trust" modelinin firmanız için etkilerini ve yararlarını daha yakından incelememiz gerekirse;

Güvenli Uygulama Erişimi (APM)

Uygulama erişimi söz konusu olduğunda, kuruluşlar sitelerine erişen herkesin kötü amaçlı bir aktör olduğunu varsaymalıdır. Erişimle ilgili ihlaller artmaya devam ederken, F5 Labs'e göre erişimle ilgili ihlaller 2018'de% 47 iken, 2019'da % 52 ile oldu.

F5 BIG-IP Erişim Politikası Yöneticisi (APM), kullanıcıların ve uygulamalarının nerede olduğuna bakılmaksızın uygulamalara, API'lere ve verilere erişimi güvence altına alır, basitleştirir ve merkezileştirir. Kimliğe Duyarlı Proxy (IAP) ile APM, her uygulama erişim talebini güvence altına alan, ayrıntılı bağlama dayalı bir Zero Trust modeli doğrulaması uygular. Ayrıca uygulama oturumu boyunca her bir kullanıcının cihazını, konumunu ve erişimini sürekli olarak izler.

Birincil değer önerileri şunlardır:

- **SSO (Single Sign On) ile benzersiz bir kullanıcı deneyimi ve uygulama ister şirket içinde ister bulutta olsun, tüm uygulamalara erişmede ortak bir kullanıcı deneyimi.**
- **Zero Trust mimarisinde daha güvenli uygulamalar.**
- **Hibrit ortamlar için ortak bir mimari ve birden çok bulutta ortak politika uygulanabilmesi.**

F5 Networks, Shape'in eklenmesi ve sahtekarlık yapan kötü aktörleri belirleme becerisiyle, artık iyi kullanıcıları daha iyi belirleyebiliyor ve kullanıcının bir parola girmesi gereken nokta sayısını azaltabiliyor. Bu, kullanıcının şifreleri unutmadan hizmetlere daha fazla erişim sağlamasına olanak tanırken, helpdesk destek maliyetlerini düşürür ve güvenlik eşiğini arttırır.

Uygulama Altyapısı Güvenliği (SSLO)

Zero Trust yaklaşımını başarıyla uygulamak için, uygulamaların müsaitliğinin ve güvenliğinin sağlanması önemlidir, bu yüzden ağ altyapısı da oldukça önemlidir. Ağınızı etkileyebilecek diğer bir alan da şifrelenmiş tehditlerdir.

Şifreleme artık yeni normaldir. F5 Labs araştırmasına göre, sayfa yüklemelerinin % 91'i SSL/TLS ile şifrelenmiştir. Saldırganlar, güvenlik denetimlerini atlamak için artık şifreleme kullanmaktadırlar. Kuruluşlar, gelen şifrelenmiş trafiğin kötü amaçlı yazılım barındırdığını varsaymalıdır. Aynı şekilde, giden şifrelenmiş trafiğin dışarı sızabilecek hassas bilgiler içerdiğini de varsaymamız gerekir.

F5 SSL Orchestrator, ağınızdaki şifrelenmiş trafik tehlikelerini çözer. Gelen / giden; SSL / TLS trafiğinin düzenlenmesi için özel bir çözümdür ve şifreleme kontrolünü merkezileştirir. Şifrelenmiş trafikte saklanan kötü amaçlı yazılımları açığa çıkararak kör noktaları ortadan kaldırır ve çalınan verilerin dışarı sızmasını engeller.

Uygulama Katmanı Güvenliği – (ASM)

Günümüz uygulama dünyasında, bir kuruluşun en önemli araçlarını web&mobil uygulama ve API'ler oluştururken, en savunmasız oldukları yerde burasıdır. F5 Labs araştırmasına göre, şirket başında ortalama 983 uygulama düşmektedir. Tek bir kuruluş tarafından yönetilmesi gereken bu kadar çok uygulama, saldırganlar için çok cazip bir hedeftir. Uygulamaların her biri değerli verilere açılan birer kapı olabileceğinden, uygulamaların güvenliğini aktif bir şekilde aşarak delmeye çalışırlar. Zero Trust stratejinizin bir parçası olarak uygulamaları sürekli korumak çok önemlidir.

F5 Networks, tüm uygulamalarınızı Sıfır Güven mimarisi ile koruyabilir. Advanced WAF ve Essential App Protect gibi WAF çözümleri, OWASP Top 10 veya SQL / PHP enjeksiyonları gibi yaygın güvenlik açıklarını ve istismarları karşı önlemeye yardımcı olur.

F5 Networks WAF çözümleri, uygulamaların durumunu sürekli olarak izlemek için davranış analizi özelliği ile, Layer 7 DoS saldırılarına karşı da koruma sağlar. Saldırganların kullanıcı hesaplarına yetkisiz erişimini önlemek için kimlik bilgileri korumasını da sağlar. Ayrıca, artan API kullanımıyla, uygulamalarınızı API saldırılarına karşı koruyabilir.

F5 Networks, WAF ve API güvenlik çözümleriyle uygulama güvenlik açıklarınızı korurken, Shape ile hesap çalma dolandırıcılığı, login atakları ve yeni hesap dolandırıcılığını tespit etme ve önlemede katkı sağlar.

F5 Networks, tüm bu korumaları Zero Trust stratejisine uygun olacak şekilde, on-premise, as-a service veya Silverline ve Shape Security aracılığıyla tamamen yönetilebilir bir hizmet olarak sunulabilmektedir.