**BASIN BÜLTENİ**

**Çoklu bulut ortamlarının güvenliği için 3 şart**

**Fortinet’e göre, giderek karmaşıklaşan çoklu bulut ortamlarında üç temel gereksinimin karşılanması gerekiyor: entegrasyon, süreklilik ve birleştirilmiş yönetim**

Son yıllarda kurumların uygulamalar ve hizmetlerden altyapılara kadar tüm süreçlerde hızla buluta geçişi dijital dönüşüme damgasını vuruyor. Öte yandan, her geçen gün daha çok kurum, özellikle güvenlik endişesiyle bu eğilime mesafeli durmayı tercih ediyor. Kapsamlı, entegre ve otomatik siber güvenlik dünya lideri Fortinet (NASDAQ: FTNT), kurumların çoklu bulut ortamlarına güvenli bir geçiş süreci için üç kritik gereksinimi karşılamaları gerektiğini belirtiyor.

Konuyla ilgili görüş bildiren **Fortinet Bölge Teknoloji Direktörü Melih Kırkgöz** şöyle dedi: “Günümüzde giderek daha da karmaşık bir hal alan bulut ortamlarının güvenliğini sağlamak, belli bir altyapıda çalışabilen belli bir güvenlik çözümünü kullanmanın çok ötesinde bir yaklaşım gerektiriyor. Bulut ortamlarının güvenliğini sağlamak, karmaşık, çok bulutlu ortamların sunduğu hizmet ve işlevlerle, güvenlik araçlarının entegre edilebilmesinden geçiyor. Bu sebeple, bir güvenlik çözümünün belli bir bulut tabanlı uygulamanın kullanım senaryosuna uygun olup olmadığını görmek için genelde uygulanan kontrol listesi yaklaşımı yerine, etkin entegrasyon, süreklilik ve birleştirilmiş yönetimi kapsayan genel otomasyon desteği ve bulutlar arası yetenekliliklere dayalı bir yaklaşımın benimsenmesi önem arz ediyor.”

Fortinet, çoklu bulut ortamlarının güvenliği için kurumların şu üç konuyu önceliklendirmesini öneriyor:

**1) Entegrasyon**

Kurumların ilk olarak, kurulumunu yaptıkları farklı bulut platformlarında güvenlik çözümlerini entegre etmeleri gerekiyor. **Fortinet Bölge Teknoloji Direktörü Melih Kırkgöz**, bulut ortamlarının birbirlerinden kopuk bir şekilde var olmadığını belirterek, kurumların çok bulutlu, karmaşık ağlarda, ağ güvenliği çözümlerini sorunsuzca hayata geçirebilmeleri gerektiğini vurguluyor: “Bu tür karmaşık ortamlarda, güvenlik çözümlerinin otomatik ölçeklendirme, coğrafi yedeklilik ve otomasyon komut dizisi oluşturma gibi bulutta sunulan hizmetlerle entegre olması beklenir. Bunu, kurum içi araçların Ethernet girişleriyle entegre olmasına benzetebiliriz. Bu yeteneklerin, tehditleri tespit etmek, önlemek ve karşılık verebilmek için bir arada çalışan bir dizi ortak aracı kullanan çoklu genel bulut ortamları, özel bulut ortamları, SD-WAN, geleneksel veri merkezi ve şube ağlarında uyumlu bir şekilde hazır bulunabilmesi için entegrasyon hayati önem taşıyor.”

**2) Süreklilik**

Entegrasyon gerekliliğinin yanı sıra kurumlar, farklı platformlarda sürekli ve kesintisiz güvenlik yeteneklerine ve işlevlerine de ihtiyaç duyuyor. Kurumlar, kurum içi çözümlerinin sahip olduğu yeterliliklerin, webde, bulutta, SD-WAN/şubedeki araçlarda da aynı şekilde mevcut olmasını talep ediyor. Çünkü, yalnızca bu sayede, özellikle yasal düzenlemelerin öngördüğü kesintisiz güvenlik politikalarını, uygulamalarda planlı yamalama işlemlerini ve nerede kurulu olduğundan bağımsız olarak tüm uygulamaların sıfırıncı gün hassasiyetlerine karşı korunmasını sağlayabiliyor.

**3) Yönetim**

Üçüncü kritik gereksinim ise tüm ortamlarda uyumlu güvenlik yönetiminin tek bir yönetim katmanı üzerinden yürütülmesi. Kırkgöz bu gereksinimi şöyle açıklıyor: “BT ekipleri, kurdukları her cihaza dokunmak ve farklı bulut ortamlarında kullanılan tüm teknolojilerde uzman olmak zorunda kalmadan dağıtık güvenlik altyapılarını yönetebilmeli. Ekipler, nerede uygulandığına bakılmaksızın, aynı şekilde dağıtılabilen, uygulanabilen ve yürürlüğe konulabilen sade bir politikaya ihtiyaç duyuyor. Öte yandan, bu ekiplerin genişleyen saldırı yüzeyi ve artan riski daha iyi değerlendirebilmesi için tüm bu farklı ortamlarda kesintisiz vizibilite ihtiyacı da söz konusu. Bunun için de tüm bu farklı ortamlardaki aksiyonları tek bir yerden izleyebilmeleri çok önemli.” Buna ek olarak, her bulut ortamında farklı bir güvenlik çözümünün kullanılması, bu araçların yönetilmesi için daha çok siber güvenlik uzmanının istihdam edilmesini gerektiriyor. Bu sebeple, güvenlik yöneticilerinin hali hazırda aşina olduğu aynı arayüzü, yönetim aracını ve işlevselliğini kullanan bir çözümün benimsenmesi, güvenlik ekibinin hayatını kolaylaştırıyor ve kurumunun mevcut kaynaklarını kullanabilerek süreçlerini devam ettirmesini mümkün kılıyor.

**İlgili Kişi:**
Eray Çoşan Akkuş
Marjinal Porter Novelli
0 533 927 23 97
erayc@marjinal.com.tr

**Fortinet Hakkında**
Fortinet (NASDAQ: FTNT) dünya genelinde büyük ölçekli şirketlere, servis sağlayıcılarına ve kamu kurumlarına güvenlik sunar. Fortinet, her geçen gün artan sanal saldırılara karşı müşterilerine akıllı ve sorunsuz koruma sağlar, sınırların ortadan kalktığı ağların artan performans ihtiyaçlarını karşılar. Ağlardaki uygulamaların, bulut sistemlerinin ve mobil cihazların karşılaştığı en kritik güvenlik sorunlarına karşı performanstan ödün vermeden güvenlik sunan tek çözüm sadece Fortinet'in Security Fabric mimarisidir. Fortinet global çapta sevkiyatı yapılan en güvenilir çözümler alanında dünyanın bir numarasıdır ve dünya genelinde 360 binden fazla müşteri ticari faaliyetlerini korumak için Fortinet'e güvenmektedir. Daha fazla bilgi için: [http://www.fortinet.com](http://www.fortinet.com/), [Fortinet Blog](https://blog.fortinet.com/) sayfası veya [FortiGuard Labs](https://fortiguard.com/).