**BASIN BÜLTENİ**

**Fortinet 2024 Bulut Güvenliği Raporu yayınlandı**

**2024 yılında kuruluşların çoğunluğu (yüzde 78) hibrit ve çoklu bulut stratejilerini tercih ediyor. Bu kuruluşların yüzde 43'ü bulut ve şirket içi altyapıdan oluşan bir hibrit kullanırken, yüzde 35'i çoklu bulut stratejisine sahip olduğu görülüyor**

Kurumlar daha fazla bulut uygulaması geliştirip dağıttıkça, güvenlik daha karmaşık hale geliyor. Birçok kuruluş, saldırı yüzeyini genişleten ve karmaşıklığı artıran hibrit veya çoklu bulut yaklaşımını benimsiyor. Güvenlik ekipleri genellikle çeşitli özel ve genel bulut iş yüklerini ve ortamlarını yönetmekte ve güvenliğini sağlamakta zorlanıyor. Çoklu bulutun benimsenmesinin birçok faydası olsa da birden fazla araçla uğraşmak yönetim karmaşıklığını artırıyor ve tüm bulut ortamlarında tutarlı güvenlik politikaları uygulamayı zorlaştırıyor ya da imkansız hale getiriyor. Daha da kötüsü, kuruluşlar bulut hizmetleri eklemeye devam ettikçe güvenlik karmaşıklığı seviyesi genellikle zaman içinde artıyor ve bu da daha fazla yönetim zorluğuna ve maliyete yol açıyor.

2024 Bulut Güvenliği Raporu, kurumların bulut ortamlarını korumada karşılaştıkları zorluklar ve öncelik verdikleri stratejiler hakkında bilgi edinmek amacıyla Cybersecurity Insiders tarafından Fortinet sponsorluğunda hazırlandı. Rapor, dünya çapında 927 siber güvenlik uzmanının katıldığı kapsamlı bir ankete dayanıyor ve bulut güvenliğini yönlendiren mevcut trendler hakkında içgörüler sunuyor.

**Hibrit ve çoklu bulut tercihi devam ediyor**

2024 yılında kuruluşların çoğunluğu (yüzde 78) hibrit ve çoklu bulut stratejilerini tercih ediyor. Bu kuruluşların yüzde 43'ü bulut ve şirket içi altyapıdan oluşan bir hibrit kullanırken, yüzde 35'i çoklu bulut stratejisine sahip. Bu rakamlar, kuruluşların yüzde 39'unun hibrit bulut ve yüzde 33'ünün çoklu bulut kullandığı iki yıl öncesine göre sadece küçük bir artışı temsil ediyor.

Yıllar süren hızlı benimsemenin ardından, pazar olgunlaştıkça bulut büyümesi yavaşladı. Bu noktada, heyecan dengesini bulmuş gibi görünüyor ve bulut bilişimin faydaları iyi anlaşılmış durumda. Bulut esnekliği ve çevikliğinden faydalanabilecek BT ihtiyaçları olan veya bulut ortamlarına özgü hizmetlere ihtiyaç duyan kurumlar projelerinde ilerleyebiliyor.

Çoğu kurum, güvenliğin bulut stratejilerine dahil edilmesi gerektiğinin de farkında. Bulutla ilişkili siber güvenlik zorlukları ve bulut ortamlarında gelişmiş güvenlik önlemlerine duyulan ihtiyaç, yapay zeka tabanlı yeni tehditler karşısında daha kritik hale geliyor. Aslında, kuruluşların yüzde 96'sı bulut güvenliği konusunda orta veya aşırı derecede endişeli olduklarını bildiriyor. Güvenlik açıkça bir önceliktir ve katılımcıların yüzde 61'i bulut güvenliği bütçelerinin önümüzdeki 12 ay içinde artacağını öngörüyor.

Kurumlar, günümüzün giderek bulut odaklı hale gelen ortamında hassas verileri korumak ve düzenleyici standartlara uymak amacıyla bulut güvenliği bütçelerini yüzde 37 oranında artırmayı planladıklarını bildiriyor.

**Teknik ve kaynak zorlukları devam ediyor**

Bulutun benimsenmeye devam etmesine rağmen, tutarlı çoklu bulut güvenliğinin uygulanmasında zorluklar devam ediyor. Güvenlik ve uyumluluk sorunları en büyük endişe kaynağı (yüzde 59) ve çoklu bulut stratejilerinin daha hızlı benimsenmesinin önünde bir engel teşkil ediyor. Kuruluşlar ayrıca teknik zorlukları (yüzde 52) ve kaynak kısıtlamalarını (yüzde 49) bulutun benimsenmesinin önündeki engeller olarak belirtiyor.

Karmaşık çoklu bulut altyapılarında görünürlük ve politika kontrolü elde etmek zor olabilir ve siber güvenlik becerileri açığı sorunu daha da karmaşık hale getiriyor. Bulut güvenliği uzmanlığına sahip kişilerin eksikliği ciddi bir sorundur ve katılımcıların yüzde 93'ü sektör genelindeki beceri eksikliğinden orta ila aşırı derecede endişe duyduklarını belirtiyor.

**Tek platform yaklaşımı kullanarak basitleştirme ve otomasyon**

Hibrit ve çoklu bulut ortamları karmaşık olduğundan, bunların güvenliğini sağlamak zor. Ancak kuruluşların büyük çoğunluğu (yüzde 95) tek bir gösterge tablosuna sahip birleşik bir bulut güvenlik platformunun, verilerin tüm bulut ayak izi boyunca tutarlı ve kapsamlı bir şekilde korunmasına yardımcı olacağını söylüyor.

Birden fazla farklı güvenlik sistemini yönetmenin verimsizliği ile uğraşmak yerine, tek bir entegre bulut güvenlik platformundan yararlanan güvenlik ekipleri, görünürlüğü artırmaya, tutarlı politika uygulaması sağlamaya ve siber güvenlik becerileri açığını azaltmaya yardımcı olabilecek daha basit entegrasyon, otomasyon ve azaltılmış yönetim ek yükünden yararlanıyor.

**Fortinet bulut güvenliği ile görünürlük ve kontrol kazanın**

Fortinet, bulut ortamları arasında ve genelinde tutarlı politikalar, merkezi yönetim ve uçtan uca görünürlük sağlayan birleşik bulut güvenliği çözümleri sunuyor. Tüm bulutlarda güvenlik otomasyonunun etkinleştirilmesiyle, uygulamaları her yerde tutarlı korumalarla güvenli bir şekilde oluşturulabiliyor, dağıtılabiliyor ve çalıştırılabiliyor. Fortinet bulut güvenlik çözümleri, genel ve özel bulutlar ile veri merkezleri arasında görünürlük ve kontrol sağlayarak güvenliği güçlendiriyor ve dağıtım karmaşıklığını azaltıyor.

**İlgili Kişiler:**     
Ceren Moral Aru

Marjinal Porter Novelli      
0533 921 43 53      
cerenm@marjinal.com.tr

Halit Yeşilbaş

Marjinal Porter Novelli

0538 376 17 10

[Hality@marjinal.com.tr](mailto:Hality@marjinal.com.tr)

**Fortinet hakkında**

[Fortinet](https://www.fortinet.com/?utm_source=website&utm_medium=pr&utm_campaign=boiler) (NASDAQ: FTNT), siber güvenliğin evriminde ve ağ ile güvenliğin yakınsamasında itici bir güçtür. İnsanları, cihazları ve verileri her yerde güvence altına alma misyonuyla bugün 50'den fazla kurumsal sınıf üründen oluşan en kapsamlı entegre portföy ile ihtiyacınız olan her yerde siber güvenlik sağlamaktadır. Yarım milyondan fazla müşteri, Fortinet'in sektörde en çok kullanılan, en patentli ve en çok onaylanmış çözümleri arasında yer alan çözümlerine güvenmektedir. Sektördeki en büyük ve en geniş eğitim programlarından biri olan [The Fortinet Training Institute](https://www.fortinet.com/nse-training?utm_source=website&utm_campaign=nse-training), siber güvenlik eğitimini ve yeni kariyer fırsatlarını herkes için ulaşılabilir kılmaya kendini adamıştır. Fortinet'in seçkin tehdit istihbaratı ve araştırma organizasyonu [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=website&utm_campaign=fortiguardlabs), müşterilere zamanında ve sürekli olarak en üst düzeyde koruma ve eyleme geçirilebilir tehdit istihbaratı sağlamak için önde gelen öğrenen makineler ve yapay zeka teknolojilerini geliştirip kullanmaktadır. Daha fazla bilgi için [https://www.fortinet.com](https://www.fortinet.com/), [Fortinet Blog](https://www.fortinet.com/blog?utm_source=website&utm_medium=blog&utm_campaign=blog), [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=website&utm_campaign=fortiguardlabs).