

Kurumlar için Bulut Güvenliđi Başlangıç Kılavuzu



Forcepoint

Broşür

İçindekiler:

- 01 Ortama Genel Bakış: Bulut Güvenliđi ve Buluta Aktarma
- 02 Bulut Kullanmanın Doğru Yolu
- 03 Buluta İliřkin Sorunlar ve Öneriler
- 04 Buluta Bađlı bir Dünyada Başarıya Ulařmak

Ortama Genel Bakış: Bulut Güvenliği ve Buluta Aktarma

Bulutun gitgide yaygınlaştığını düşünüyorsanız, haklısınız. Peki bulutun bu kadar hızlı yayılmasını sağlayan nedir? Aslında, tüketim çılgınlığıdır. Evet, B2C yani e-ticaret'ten bahsediyoruz.

İnsanların her gün bulut üzerinden gerçekleştirdikleri tüketimler, şirketlerin bulutu benimseme ve koruma şekillerine yön vermekte.

Bulut güvenliği, insan merkezli bir süreçtir.

Bulut, anında erişim demektir.

Ve bir beklentidir.

Hepsi sürekli ve kesintisiz şekilde birbirine bağlı olan içeriklere, uygulamalara ve cihazlara sürekli erişim sağlayan bulut, günlük yaşamımızın ayrılmaz bir parçasıdır. Bulut, modern insanın bilinçsiz olarak yaptıklarının ve çalışma şeklinin içine işlemiş durumda. Dolayısıyla, iş yerlerinde de aynı beklenti söz konusu. İhtiyaç duyduğunuz şeyleri, ihtiyaç duyduğunuz anda kullanmak istiyorsunuz. Ayrıca, verimliliğinizi kısıtlamayan, tam tersine artıran, akıcı bir deneyim istiyorsunuz. Bulutla verimliliği nasıl artırabilirsiniz? Daha az kaynakla nasıl daha çok iş yaparsınız? Çünkü bulut gerçekte kolaylık demektir. Ama aynı zamanda da bir güvenlik açığıdır.

Nihayetinde, çalışanlarınız da tüketicilerdir. Kurumların faaliyetlerini, verilerini ve çalışanlarını koruma şekli, günlük yaşamımızda sahip olduğumuz beklenti ve deneyimle eşleşmelidir. Güvenlik uygulamaları da evrim geçirerek bu akıcılığa izin verirken aynı zamanda da bu özgürlük ve kolaylıkla birlikte gelen ve kapsamı gittikçe genişleyen tehditlere karşı koruma sağlamalıdır.

Bu, bulutun genel görünümüdür. Peki ama eylemlere ilham veren ve kurumların bir bütün olarak bulut ve güvenlik yaklaşımlarını yeniden değerlendirmesine neden olan özel koşullar nelerdir? Bu koşullardan bazıları:

- O365'in benimsenmesi ve uygulanmasıyla başlayan dijital dönüşüm yolculuğu
- EHR veya ERP sistemleri gibi eski ve özel uygulamaların buluta taşınması
- Ofis dışında, kurumsal ağın ve diğer savunmaların kapsamının ötesinde çalışan insanlar
- Şirket merkeziyle aynı güvenlik seviyesine ihtiyaç duyan tesisleri içeren yüksek oranda dağıtık bir ortamda çalışan ve tüm bunları her tesiste pahalı ve donanım ağırlıklı bir yatırım yapmadan ve trafiği merkeze geri yönlendirmeden yapması gereken küresel işletmeler
- Optimizasyon çabaları - güvenlik sistemlerinin birleştirilmesi, ekiplerin iş akışlarının kolaylaştırılması veya sermaye ve operasyon harcamalarının azaltılması
- Altyapının AWS ve Azure gibi halka açık bulutlara taşınması

Bulut Kullanmanın Doğru Yolu

Bulut güvenliği, farklı insanlar için farklı şeyler ifade eder. Üstelik, sürekli ve hızla değişen bir kavramdır. Peki, bu değişime nasıl ayak uyduracaksınız? Yaklaşımınızın bütünsel ve etkili olduğundan nasıl emin olacaksınız? Kurumunuzun başarılı bir şekilde korunabilmesi için, bulut güvenliğinin kapsayıcı olması gerekir.

Bulutun ana bileşenlerini düşünelim:



Buluttaki veriler



Buluttaki kullanıcılar



Buluttaki uygulamalar



Bulutta bağlantı



Buluttaki altyapı



Bulutta güvenlik

Temelde, bulut güvenliğinin amacı da budur. Güvenlik açıklarının önlenmesi ve kullanıcıların ve verilerin güvende tutulması için bulutun tüm bileşenleri değerlendirilmeli, yönetilmeli ve korunmalıdır. Bulut güvenliğinin tek bir sabit tanımı olmasa da “bulutu” kullanmanın doğru bir yolu vardır.

Peki, bu yol neye benzer?

Kurumlar, buluta bağlanmak ve bulut güvenliğini sağlamak için şunları yapmalıdır:

- Her kullanıcının web içeriğine ve bulut uygulamalarına her yerden ve her cihazdan güvenli erişmesini sağlamak
- Bulut güvenliği stratejisini belirlemek için kurum çapında görünürlük ve kontrol sağlamak
- Buluta gelen ve buluttan giden tüm verileri korumak
- Trafiği geriye yönlendirmeden kurumların ve kullanıcıların doğrudan buluta bağlanmasını sağlamak
- Altyapıyı ve iş akışını optimize etmek
- Sıfır gün saldırıları dahil olmak üzere gelişmiş tehditlere karşı koruma sağlamak

Harika, artık ne yapmanız gerektiğini biliyorsunuz ama bunu nasıl yapacaksınız? Pek çok kurum, bazı temel özelliklere sahip olan farklı ürünlere veya bulut güvenliğinin belli unsurlarından sorumlu olan farklı ekiplere sahip olabilir. Ancak, her güvenlik kurumunun kaçınmak istediği şey, birbirine entegre olmayan ve birbirleriyle iletişim kurmayan birden fazla özel amaçlı ürünü uygulayarak zaten yoğun olan güvenlik ekiplerinin iş yükünü aşırı düzeye çıkarmaktır.

Kurumların gerçekten ihtiyaç duyduğu şey, farklı satıcılardan gelen ilgisiz ürünler değil, tek bir çözümdür. Elbette kontrol sağlamak için görünürlük sağlama ihtiyacı veya ağ dışındaki kullanıcıları korumak için şirket içi web güvenliğini buluta taşıma ihtiyacı gibi bağımlılıklar mevcuttur. Bulut güvenliği, ideal haliyle, veri, web erişimi, bulut erişimi ve bulut verileri ve bağlantıları kapsayan birleşik bir çözümdür. Güvenlik ekibinizin sorun yaşadığı tüm noktaların ve güvenlik açıklarının ortadan kaldırılmasını sağlar. Çözümleri ister bir, ister üç satıcıdan tedarik ediyor olsunlar, kurumlar temel ticari hedeflerine ulaşmak için ellerindeki çözümlerin, istedikleri çözümlerin ve bu çözümleri istedikleri yerin uyumlu olmasını sağlamak zorundadır.

Bulutla İlişkin Sorunlar ve Öneriler

Verilerin buluta taşınması büyük bir iştir ve bu konuda endişeleriniz varsa, kesinlikle yalnız değilsiniz. Sahiplik ve kontrolü nasıl sürdürürsünüz? Tehditleri uzak tutmaya nasıl devam edebilirsiniz? Gerekli performansı nasıl sağlarsınız?

En çok sorulan bu sorulardan bazılarına cevap verelim.



Gecikme

Kapsama alanı, gecikmenin azaltılması açısından kritiktir. Dünya çapında pek çok PoP içeren geniş kapsamlı bir ayak izi, düşük gecikme sürelerinin yanı sıra içerik yerelleştirme gibi verimlilik artışı sağlayan diğer faydaları da beraberinde getirir. **1. Kademe ağlar ve 4. Kademe veri merkezleri**, gecikmeye karşı hassas uygulamalar için ideal kapsam, yedekleme, bağlantı ve kaliteyi sağlar.



Görünürlük

Göremediğiniz şeyi koruyamazsınız. Ayrıca, neleri etkileyeceğini bilmeden değişiklik yapamaz veya politika belirleyemezsiniz. **Bulutta sunulan bir web ağ geçidini bir güvenlik duvarıyla** eşleştirmek, politika uygulama ve gölge BT kontrolü dahil olmak üzere tüm kullanıcı ve konumlar için tutarlı bir görünürlük ve uygulama becerisi sağlar. **CASB** işlevleri de, riskleri anlamak ve kullanıcıları ve verileri korumak için hem onaylanmış hem de onaylanmamış uygulama kullanıcılarının bulutta neler yaptığının görünmesini sağlayarak, kurumların korunmasına yardımcı olur.



Uygunluk

Yalnızca dahili olarak denetlenen uygunluğa değil, program sertifikalarına güvenin. Kurumunuz için önemli standartlar, muhtemelen aşağıdakileri içerecektir:

- **ISO 27018** - Kişisel Bilgileri (PII) yöneten standart
- **ISO 27001** - geliştirme, kalite güvencesi, dağıtım ve destek faaliyetleri için çok merkezli bir sertifika
- **CSA** - bulut ortamında yazılım güvenliğini ve süreçler arası faaliyetleri yöneten (ve GDPR Davranış Kurallarına dayanan) bir sertifika
- **SOC2** - veri merkezi testlerine ve işletme verimliliğine ek olarak güvenlik, kullanılabilirlik, işleme bütünlüğü, gizlilik ve mahremiyetle ilgili finansal olmayan raporlamaya odaklanan bir sertifika



Veri Bağımsızlığı

Bulutun fiziksel sınırları olmasa da coğrafi sınırların getirdiği yasal sonuçlardan muaf değildir. Dijital veriler, verilerin bulunduğu ülkenin kanunlarına tabidir. Kurumunuzun **faaliyet gösterdiği bölgelerde bulunan bulut veri merkezlerinin kullanılması**, hem performans hem de yerel kanun ve düzenlemelere uyulması açısından esastır.



Veri Kaybı

En başarılı yaklaşım, birleşik bir yaklaşımdır. Entegre **veri koruma çözümleri** sayesinde şirket içindeki güvenlik önlemlerinizi İnternet, e-posta, uç nokta, ağ ve bulutu kapsayacak şekilde genişletebilirsiniz. Bulutta bekleyen ve hareket halindeki verileri korumak için mevcut veri koruma politikalarınızdan faydalanın.



BYOD (Kendi Cihazını Getir)

Günümüzde çalışanlar yönetilen ve yönetilmeyen cihazlarda çalıştırılan onaylanmış ve onaylanmamış bulut uygulamalarına bel bağlamaktadır. Ağ çevre savunmaları ve uç nokta koruması, uzaktan ve hareket halindeki çalışan kullanıcıları korumak için yeterli değildir. Çalışanlara güvenlik açığı yaratmadan tercih ettikleri cihazları kullanmaları konusunda esneklik tanımak için **ayrıntılı güvenlik politikalarını** kullanarak yönetilen cihazlarla BYOD (kendi cihazını getir) arasında ayırım yapmanız gerekir. **Genişletilmiş kontroller**, hem iş hem de kişisel amaçlar için şirket cihazlarını kullanan uzaktan çalışan kişiler için güvenlik sağlar.



Daha Azı İle Yetinmeyin

Daha çevik, verimli, vb. olmak isteyen şirketler, bulut konusunda genellikle "kervan yolda düzelir" yaklaşımını benimsemektedir. Ancak bu yaklaşımla genellikle güvenlik ve etkinlikten taviz verilir. Örneğin, URL filtreleme, tek başına güvenlik sağlamaz; benzer şekilde, tekrarlı bir DNS çözümü de tam bir web ağ geçidinin yerini tutamaz. Bir çözümün tek bir ögesiyle tam koruma sağlayamazsınız. Ayrıca, mümkün olduğunca azıyla yetinme yaklaşımı, güvenliğin proaktif olmak yerine reaktif olmasına neden olur. Şirketiniz dijital dönüşüm yol haritasını oluştururken, **güvenlik ve ağ oluşturma birliktedir** **çalıştığından ve planınızda ikisine de yer verdiğinizden** emin olun — böylece iş hedeflerinize uygun şekilde çalışmalarını sağlayarak fazla mesai yapmak zorunda kalmazsınız.

Buluta Bağlı bir Dünyada Başarıya Ulaşmak

Başlangıçta, bulut güvenliğinin insana bağlı bir süreç olduğunu belirtmiştik. Bu yüzden de insan merkezli olması gerekiyor.

Bulut sayesinde, **yeni güvenlik çemberi insanlar.**

Dünyanın her yerindeki kullanıcıların, ortakların ve müşterilerin şirketinizin verilerine eriştiği bir ortamda, verileri koruyan yapay duvar artık yeterli olmuyor.

Ağ içerisindeki kullanıcıları güvenilir, dışındakileri ise güvenilmeyen olarak gruplandıran eski, altyapı merkezli güvenlik artık anlamını kaybetmiş durumda.

Koşulsuz güven, güvenlik sisteminizin bir parçası olamaz.

Ayrıca, güvenlik sisteminiz, dijital dönüşüm açısından bir aksesuar değil, ayrılmaz bir parça niteliğindedir.

İşte, güvenliği hızlandırmanızı ve korumanızı sağlayacak bazı temel prensipler:



Buluta Geçerken Acele Etmeyin

Roma bir günde kurulmadı. Dolayısıyla, buluta geçişiniz de bir gecede gerçekleşmeyecektir. Pek çok işletme hibrit BT/çoklu bulut ortamlarında faaliyet göstermekte ve bu durum yakın gelecekte de böyle olmaya devam edecek. Güvenli web ağ geçidinizin, işletmenizin şimdi ve gelecekte buluta doğru şekilde geçmesini sağlayacak esnek kullanım seçenekleri sunduğundan emin olun. Böylece, kurum çapında güvenliği koruyarak buluta kendi koşullarınızda ve hazır olduğunuzda geçiş yapabilirsiniz.



Sınırlarınızı Genişletin

Bulut, ağ ve uç nokta güvenliğinizi, şirketinizin sürekli değişen ihtiyaçlarını karşılayacak şekilde genişletin. Modüler güvenlik özelliklerine sahip düşük donanımlı, birleşik bir platform, dağıtık bir yapıya sahip kurumlara, yeni teknolojik gelişmelerden faydalanmak, kör noktaları önlemek ve tesisler arasında güvenli ve yönetilebilir bağlantılar kurmak için gereken genişletilebilirlik ve çeviklik özelliklerini sağlar.



Sıfır Güven, Tam İçgörü

Asla güvenme, her zaman doğrula", Sıfır Güven çerçevesinin ana sloganıdır, bu doğrultuda kurumunuzun verileri korunurken, o verilere kullanıcı ve cihaz etkileşimleri bazında sağlanan erişim değerlendirilir. Bu, "kim" ve "nasıl" sorularının yanıtını anlamanızı sağlar. "Neden" sorusuna yanıt bulduğunuzda ise farkındalığın ötesine geçer ve sorunları önlemeye başlarsınız. Niyeti anlamak için sürece davranış analizini de dahil edin.



Genişletilebilir bulut güvenliği yolculuğunuzda bir sonraki adıma hazır mısınız?

› [İş Gücünü Her Zaman ve Her Yerde Koruyun](#) adlı e-kitabımızı inceleyin.



forcepoint.com/contact

Forcepoint hakkında

Forcepoint, dijital dönüşüm ve büyüme sağlarken kurumları koruması için güvenilen, kullanıcı ve veri koruma alanında lider siber güvenlik şirkettir. Forcepoint'in uyumlu çözümleri, insanların verilerle etkileşime girme şekillerine gerçek zamanlı olarak uyum sağlar ve erişim güvenliği sağlarken, çalışanların değer üretmesine de imkan tanır. Genel merkezi Teksas, Austin'de bulunan Forcepoint, dünya çapında binlerce müşteri için güvenli ve güvenilir ortamlar yaratmaktadır.