CSO

Microsoft Security

SPONSORLU İÇERİK

Sıfır Güven güvenliği: **İlk kullanıcılarımızdan çıkarılan dersler**

CSO Microsoft Security

İçindekiler

CSO Microsoft Security

Giriş

Son iki yılda yaşanan aksaklıklar, geleneksel BT ve güvenlik modellerini sarstı. Sonuçta, ilginç bir kavram olarak değerlendirilen Sıfır Güven güvenliği hızla modern kurumsal güvenliğin temeli haline geldi.

Foundry tarafından yapılan yeni araştırma, kurumların %52'sinin Sıfır Güven mimarisini denemekte olduğunu veya kurduğunu ve %15'lik başka bir kısmın Sıfır Güven modellerini araştırdığını ortaya koyuyor. Bu stratejiyi benimseyenler kurulumlarından, müşteri verilerinin daha iyi korunması, karmaşıklığın azaltılması ve kurumsal kaynaklara güvenli, güvenilir erişim sağlanması dahil olmak üzere sayısız fayda gördüklerini söylüyor.

Bu e-kitapta, CISO'ların kurumlarını çok sayıda saldırı vektöründen kaynaklanan çok sayıda riske karşı korumalarına yardımcı olmak için Sıfır Güven stratejisinin önemini vurgulayan Foundry araştırmasının sonuçları incelenecektir. Ayrıca, yolculuklarına başlayanlar için Sıfır Güven'in nasıl uygulanacağına dair rehberlik de sunulmaktadır.

Anket hakkında

Foundry, Sıfır Güven'in benimsenmesinde mevcut durumu araştırmak için Şubat ve Mart 2022'de ABD'deki kurumlarla anket yaptı. Ankete katılanların 500'den fazla çalışanı olan bir kurumda BT yöneticisi veya üstü bir pozisyonda bulunması ve siber güvenlik ürün ve hizmetlerinin satın alınmasında bir role sahip olması gerekiyordu.

23 soruluk ankete toplam 250 katılımcı yanıt verdi.

CSO Microsoft Security

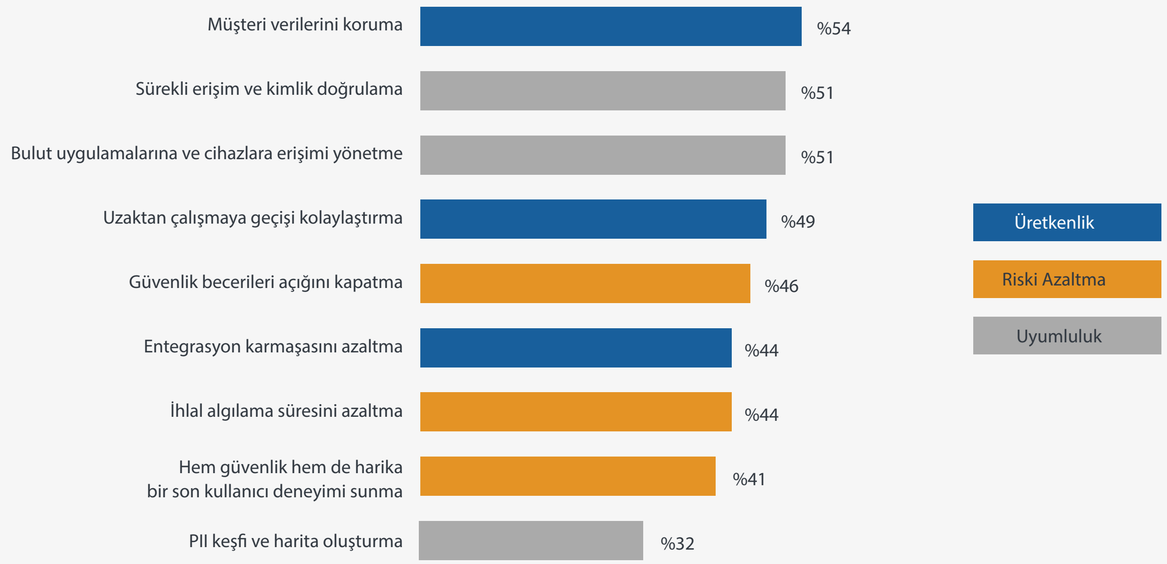
Sıfır Güven burada ve değer sağlıyor

BT ve güvenlik yöneticileriyle yapılan ayrıntılı görüşmelerin yanı sıra anket sonuçlarından da Sıfır Güven'in çoğu kurumda en çok ilgilenilen konu olduğu açıkça görülmektedir. Farklı Sıfır Güven bileşenlerini kuranlar bunun faydasını hemen görmektedir.

Sıfır Güven'i uygulayan çoğunluktaki katılımcılar (%87), mimarinin uygulama, benimseme ve entegrasyon için orijinal hedeflerine ulaştığını, hatta hedeflerinin üzerine çıktığını söylüyor.

Küresel bir perakende kurumunun BT direktörü, "[Sıfır Güven] bizim için standart bir çalışma prosedürü haline geldi. Daha önce bulunduğumuz yola geri döneceğimizi hiç sanmıyorum" diyor. (Katılımcılara güvenlik planları hakkında serbestçe konuşmaları karşılığında kimliklerini gizli tutma seçeneği sunuldu.)

Sıfır Güven'in uygulanmasından bu yana elde edilen faydalar



%12 oranında katılımcı *tüm* bu faydaları elde ettiğini belirtti

Kaynak: Zero Trust Adoption Survey, Mart 2022, Foundry. Base: 250

CSO Microsoft Security

Ankete katılanların yaklaşık %44'ü Sıfır Güven'in, tümleşik bir güvenlik mimarisi uygulamanın doğal bir sonucu olarak ortaya çıkan karmaşayı azalttığını da bildirdi. 3.500 çalışanı olan bir çağrı merkezi kurumunun CISO'su, "Bir çerçeve ile uğraştığınız ve bu çerçeve içinde çalıştığınız için işler daha karmaşık hale gelmiyor" diyor.

17.000 çalışanı olan bir finansal hizmetler kurumun Başkan Yardımcısı ve CISO'su, kurumunun Sıfır Güven'in bir parçası olarak uyguladığı çok faktörlü kimlik doğrulamanın çalışanlar tarafından çok beğenildiğini söylüyor: "Aslında çalışan memnuniyetini artırdı çünkü artık kurum tarafından sağlanan makinelerini açmak ve bir VPN istemcisi kullanmak zorunda değiller; kaynaklara her yerden ulaşabiliyorlar."

CISO, en az ayrıcalıklı erişim kavramının da aynı şekilde yarar sağladığını belirtiyor ve sözlerine şöyle devam ediyor: "Bu ayrıcalıklı erişim sisteminin uygulanması sayesinde sistem yöneticilerinden kaynaklanan yıkıcı hata sayısı azaldı. Sistem yöneticileri, ayrıcalıklarını belirli şeyler ve belirli zaman dilimleri için alıyor, bu da hata yapma olasılıklarının daha düşük olması anlamına geliyor."

Perakende kurumundaki BT yöneticisi, kimlik avı ve diğer siber saldırıların giderek daha yaygın hale gelmesi göz önünde bulundurulduğunda Sıfır Güven'in faydalarını şu şekilde özetliyor: "Bu tür araçlara sahip olmasaydık muhtemelen kötü bir durumda ve şu anda birilerine Bitcoin ile ödeme yapıyor olurduk."

CSO Microsoft Security

Sıfır Güven kurulumuna yön veren unsurlar

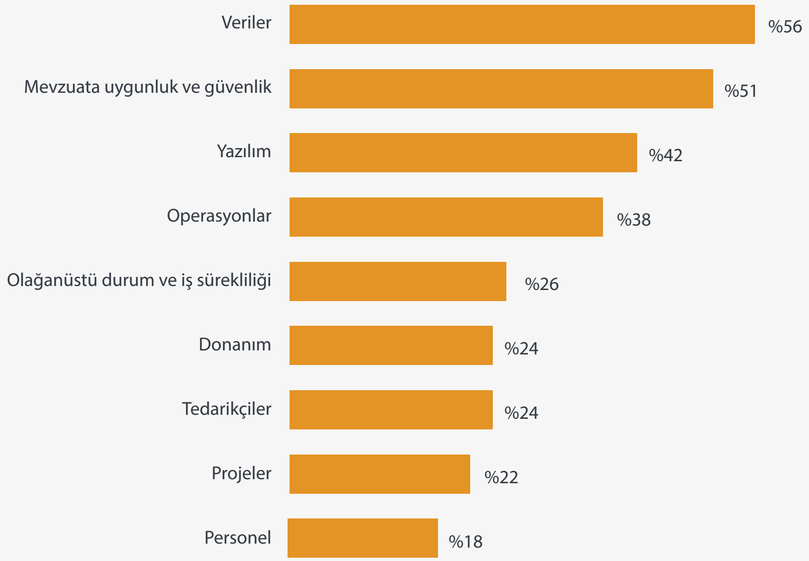
Olayların bir araya gelmesi, kurumları en azından Sıfır Güven mimarisini düşünmeye itiyor. Listenin başında çok sayıda kaynağa yönelik çok sayıda tehdide karşı riskleri yönetme ihtiyacı yer almaktadır. Ankete katılanlar, bir yıl boyunca karşılaştıkları güvenlik olaylarını, üçüncü taraf bireylerden veya kurumlardan kaynaklanan güvenlik açıklarına bağlı bir dizi nedenle ilişkilendirdi. Belirtilen diğer nedenler şunlar oldu:

- Beklenmedik kurumsal riskler
- Hizmetlerin veya sistemlerin hatalı yapılandırılması
- Kötü amaçlı, bilinçli içeriden düzenlenen saldırılar
- Kimlik avı saldırısı kurbanları dahil, kötü amaçlı olmayan kullanıcı hataları
- Güvenliği ihlal edilmiş kimlikler
- Yamasız yazılımlar
- Çalınan kimlik bilgileri

Bu olaylar, verilerin yol açtığı çeşitli risklere neden olur.

Birçok kurum için geleneksel çevre tabanlı güvenlik modellerinin modası geçmişti. Pandemi nedeniyle uzaktan çalışmaya ani geçiş, Sıfır Güven'i benimseme planlarını hızlandırdı. Daha fazla uygulamayı ve BT altyapısını buluta taşıdıkları için birçok kurum zaten bu yöne yönelmişti ancak pandemi fazladan bir sarsıntı sağladı.

Siber güvenlik tehditlerinden en çok etkilenen kategoriler



Kaynak: Zero Trust Adoption Survey, Mart 2022, Foundry. Base: 250

CSO Microsoft Security

Örneğin, 1.700 çalışanı olan bir tıbbi teknoloji kurumunun CISO'su, bulutun ve pandeminin, Sıfır Güven'in benimsenmesinde itici güç olduğunu ve gelecekteki işyeri modeli ne olursa olsun Sıfır Güven'in kendilerine güvenli bir temel sağladığını söylüyor.

“Bulut tabanlı bir kurum olmamız ve çevremizi güvence altına alabilmemizin gerekmesi itici unsurlardı,” diyor ve ekliyor: “Aynı zamanda, pandemi sırasında, becerikli bir uzaktan işgücü sağlamamız gerekiyordu. [Sıfır Güven] emlak ayak izimizi önemli ölçüde azaltmamıza imkan tanıdı ve büyük olasılıkla en azından %60 oranında sanal uzak kurum olarak devam edeceğiz.”

CSO Microsoft Security

Tehditler hiç azalmıyor

Uyumluluk ihtiyaçları da daha sağlam güvenlik modelleri için bir itici güç sağladı. 290.000 çalışanı olan bir finansal hizmetler kurumun küresel bilgi güvenliğinden sorumlu Kıdemli Başkan Yardımcısı, "Düzenleyiciler bizi izliyor ve güvenlik çerçevemizi iyileştirmeye devam etmemizi bekliyor," diyor.

Bazı kurumlar, yanlış nedenlerle spot ışıklarının kendilerine çevrilmesine yol açacak yüksek profilli bir veri ihlalini önlemek için proaktif bir şekilde Sıfır Güven yönünde adımlar atmıştı. 3.500 çalışanı bulunan bir yüksek öğretim kurumunun CIO'su şunları söylüyor: "Proaktif olmak ve hakkınızda haberlerin çıkmamasına çalışmak önemliydi. Bizimkine benzer büyüklükteki diğer yerel kurumların uzun bir süre kapanmasına neden olan bazı gerçek korku hikayeleri var."

Diğerleri de zaten ciddi bir siber güvenlik olayı yaşadı ve bu da onları güvenlik stratejilerini hızla yeniden gözden geçirmeye sevk etti. 6.000 çalışanı olan bir sigorta şirketi, kurumsal ağını iki hafta boyunca kapatan bir fidye yazılımı saldırısına maruz kaldıktan sonra, Sıfır Güven'i benimseme emri doğrudan CEO'dan geldi. Kurumun BT geliştirmeden sorumlu Başkan Yardımcısı, "Uygulamayı son derece hızlı yaptık," diyor ve ekliyor: "Başlangıçta sadece en iyi uygulamalara uyuyorduk, fidye yazılımı saldırısından sonra gerçekten çok hızlandı."

Bulut tabanlı bir katalizör

Büyük bir finansal hizmetler kurumunun Başkan Yardımcısı ve CISO'su, daha fazla bulut tabanlı kaynağın benimsenmeye başlanması ve kullanıcıların daha mobil hale gelmesi nedeniyle ekibinin birkaç yıl önce yeni bir güvenlik mimarisine duyulan ihtiyacı fark ettiğini söylüyor.

"Geçmişte güvendiğimiz geleneksel kale ve hendek güvenlik mimarisinin bizi gelecekte saldırganlardan korumayacağını fark ettik" diyor.

Bu gerçek, 2020'nin başlarında, kurumun önceki yıl içinde bir saldırganın içeriye sızdığını ve tespit edilmeden ortamda yanal olarak hareket ettiğini keşfetmesiyle çok net bir şekilde ortaya çıktı. "Kaynakları bulundukları yerde koruyabileceğimiz ve bu kaynakların kullanımını doğrulayabileceğimiz yeni bir mimariye ihtiyacımız vardı ve Sıfır Güven, bunu yapmak için tasarlanmış bir mimari."

CSO Microsoft Security

Sıfır Güven'i benimsemenin önündeki engeller

Birçok kurum için Sıfır Güven, güvenlik yapısı, süreç ve zihniyet olarak temel bir değişim gerektirir. Bu durum, Sıfır Güven stratejisini benimsemeden önce üstesinden gelmeleri gereken bazı engelleri açıklamaktadır.

Çağrı merkezi CISO'su, sunucu, ağ ve veritabanı ekiplerinin her birinin kendi web sunucularına ve araçlarına sahip olduğunu açıklayarak, "Kurum içinde çok sayıda farklı silo ile karşılaşmaya başlamıştık" diyor. "Bu bizi çıkmaza soktu çünkü herkesin nereye gideceği ve bir işin nasıl yapılacağı konusunda farklı fikirleri vardı."

Sıfır Güven'in benimsenmesini engelleyen nedir?

Kaynak: Zero Trust Adoption Survey, Mart 2022, Foundry. Base: 250

CSO Microsoft Security

Microsoft'ta Sıfır Güven konusunda kıdemli ürün pazarlama müdürü olan Anthony Mocny'ye göre, bu tür sorunları ortaya çıkarmak Sıfır Güven'in olumlu bir yan etkisi olabilir. Mocny, "Bir mimari olarak Sıfır Güven, teknoloji sütunları içinde yaşayan güvenlik ekibi silolarını yıkmak ve ekiplerin birlikte uyumla çalışmasına yardımcı olmak için tasarlandı" diyor ve ekliyor: "Bu, ekiplerin birlikte çalışma biçimi açısından kültürel bir değişim geçirmesi anlamına da gelebilir."

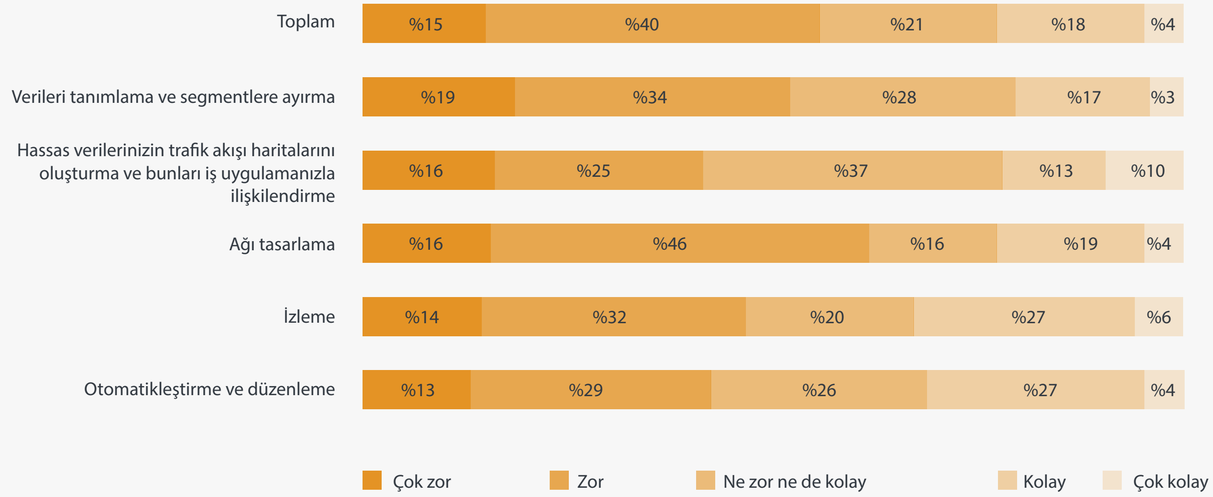
Finansal hizmetlerden sorumlu Başkan Yardımcısı/ CISO için eski uygulamalar, Sıfır Güven'e giden yolda üstesinden gelinmesi gereken bir engeldi. Bu konuda, "Modern kimlik doğrulama teknolojisiyle güçlendirilmeleri gerekiyor" diyor ve ekliyor: "Ne kadar eski olduklarına bağlı olarak, bu çok kolay bir şey olmayabilir."

CSO Microsoft Security

Kurulum ile ilgili zorluklar

Kurumlar Sıfır Güven yolculuğuna çıktıklarında, çeşitli uygulama zorlukları da ortaya çıkabilir. Ankete katılanların yarısından fazlası (%56), Sıfır Güven uygulamasının zor veya çok zor olduğunu onayladı. Özellikle:

Sıfır Güven uygulaması ne kadar zorlu?



Kaynak: Zero Trust Adoption Survey, Mart 2022, Foundry. Base: 168

CSO Microsoft Security

Ayrıntılı görüşmelerde segmentasyon ve mikro segmentasyonla ilgili zorluklar sıklıkla gündeme geldi.

Finansal hizmetlerden sorumlu Başkan Yardımcısı/CISO, "Ağınızı ayrı ana bilgisayarlara bölüyorsunuz" diyor. "Bu, tüm trafiği görebilmeniz ve ayrı ayrı her makineye kadar denetleyebilmeniz için dahili ağdaki her bir ana bilgisayar arasına küçük bir güvenlik duvarı yerleştirmek gibi. Bunun büyük güvenlik avantajları var ancak uygulanması çok zor çünkü artık on binlerce güvenlik duvarını yönetmeniz gerekiyor."

Trafik akışı haritaları oluşturmak, bir aydan daha uzun sürecek başka bir süreç olabilir. 5.000 çalışanı olan bir yayıncılık ve medya kurumunun CTO'su için, korumaları gereken kritik veri, uygulama ve ağ hizmetlerini tanımladıktan sonra şunları söylüyor: "Ağ boyunca işlem akışlarının haritasını oluşturduk ve bunları bilgi grupları olarak anlamaya çalıştık. [Daha sonra] bu bilgilerin bölümlerini ve ağı gerçekte nasıl geçtiğini, hatta tekil bilgi paketlerine kadar segmentlere ayırdık." Bu noktada kurum, her bir trafik akışı türüne Sıfır Güven kurallarını uyguladı. "Ayrıca ağımızı izlemek ve sürdürmek için yeni yetenekler geliştirdik."

Zorluklara rağmen, birçok katılımcı Sıfır Güven'in nihayetinde günlük operasyonları basitleştirdiğine inanıyor. Küresel bilgi güvenliğinden sorumlu finansal hizmetler Kıdemli Başkan Yardımcısı, geleneksel teknolojilerle "değişiklik yapmak günler alıyor; bunları tüm donanım ve yazılım bileşenlerine yaymanız gerekiyor ve bunun için çok fazla kaynak kullanıyoruz. "Sıfır Güven'e baktığımızda, uzun vadede mimari karmaşayı gerçekten en aza indiriyor ve aynı tür işleri yapmak için ihtiyaç duyduğumuz çalışan sayısını azaltıyor" diyor.

Sıfır Güven'i uygulamak için en iyi uygulamalar

Sıfır Güven mimarisini uygulayan kurumların sayısı arttıkça, bu kurumlar diğerlerinin izlemesi için yol haritaları ve en iyi uygulamalar da geliştiriyor. Bir kurulum planlarken dikkate alınması gereken beş noktayı burada görebilirsiniz.

Başlangıçta çok fazla yüklenmeyin

Bir Sıfır Güven stratejisinin haritasını çıkarmak, bu adımı yalnızca ağlar, veriler, uygulamalar, kimlikler, uç noktalar ve altyapı genelindeki kuralları ve korumaları gözden geçirme zorunluluğu gibi geniş bir bağlamda görüyorsanız göz korkutucu olabilir. Yüksek öğretim CIO'su, "Başlangıçta sadece tırmanacağımız bu devasa dağa bakıyorduk ve bunu gerçekten yapıp yapamayacağımızı sorguladık. "Tek yapmanız gereken her seferinde bir adım atmak" diyor.

CIO ve ekibi, sonunda "parayı takip et" yaklaşımını benimsedi ve finans ve bordro uygulamalarının ayrı bir ağ üzerinde bölümlere ayrılmasına öncelik verdi.

Mocny'ye göre, korunması gereken en kritik varlıkları belirlemek sağlam bir yaklaşım. "İlk etapta Sıfır Güven'i uygulama nedeninize dikkat edin"diyor.

Şüphe duyduğunuzda, çok faktörlü kimlik doğrulaması ile başlayın

Güvenlik yığınına öncelik verirken, birçok CISO ve güvenlik tedarikçisi, başlangıçta kimlik doğrulama ve diğer kimlik tabanlı korumalara odaklanmanızı önerir. Mocny bu konuda, "Aklınızda bir başlangıç noktası yoksa çok faktörlü kimlik doğrulama bakmak için iyi bir yer" diyor. Microsoft, çok faktörlü kimlik doğrulamanın kimlik tabanlı saldırıların %90'ından fazlasını önleyebileceğini tahmin ediyor.

Finansal hizmetlerden sorumlu Başkan Yardımcısı/CISO da buna katılıyor. "Kimlik doğrulama, Sıfır Güven mimarisini uygulamanın temel bir unsuru. Son kullanıcının kimliğini doğrulayamazsanız diğer bileşenlerin hiçbiri işe yaramaz, o yüzden biz de oradan başladık."

Daha sonra, finansal hizmetlerden sorumlu Başkan Yardımcısı/CISO, uzaktan çalışanları desteklemede hemen fayda sağlayan ağ oluşturma bileşenini ele aldı. Ekip, kurumun geneli kolayca görülmediği için mikro segmentasyonu yolculuğun ilerleyen zamanlarına bıraktı. Başkan Yardımcısı/CISO, "İşiniz bittiğinde çok daha güvende oluyorsunuz ancak kimse farkı bilmiyor" diyor.

CSO Microsoft Security

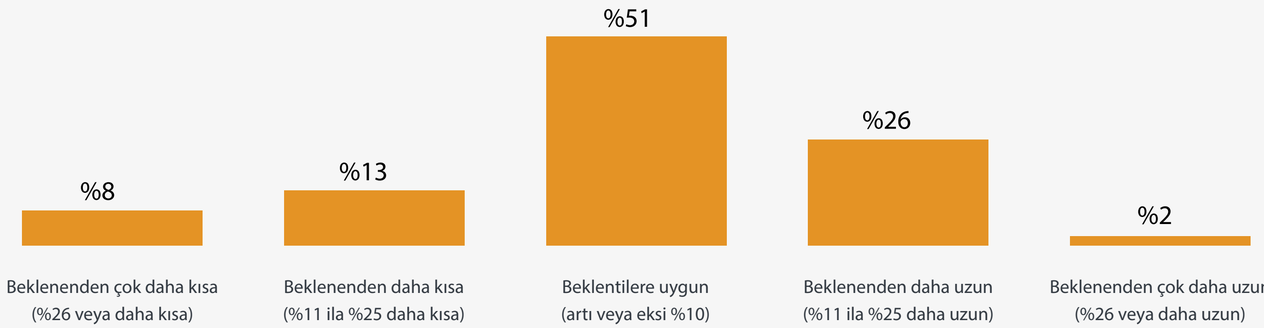
Zaman çizelgeleri konusunda gerçekçi olun

CISO'ların Sıfır Güven kurulumları hakkında gerçekçi beklentiler belirlemesi önemlidir. Finansal hizmetlerden sorumlu Başkan Yardımcısı/CISO, "Sıfır Güven mimarisini uygulamak bir proje değil, bir program. Bu çok büyük bir değişiklik. Bunu doğru yapmak çok sayıda projeyi içerir ve muhtemelen yıllarca sürer; Sıfır Güven mimarisini hızla ve kolayca uygulamanın bir yolu yok" diyor.

Finans alanındaki diğer Kıdemli Başkan Yardımcıları da aynı fikirde. "Bu sürecin biteceğini hiç sanmıyorum çünkü her zaman yeni teknolojiler geliştiriliyor, sürekli olarak yeni malware'ler ortaya çıkıyor, her zaman yeni tehditler oluyor" diyor.

Ankete katılanların çoğunluğu (%72) kurulum zaman çizelgelerinin ya yolunda gittiğini ya da planlanandan önce ilerlediğini söylerken, geri kalan katılımcılar uygulamanın beklenenden daha uzun sürdüğünü söylüyor.

Sıfır Güven, zaman çizelgesi hedeflerinize uyuyor mu?



Kaynak: Zero Trust Adoption Survey, Mart 2022, Foundry. Base: 168

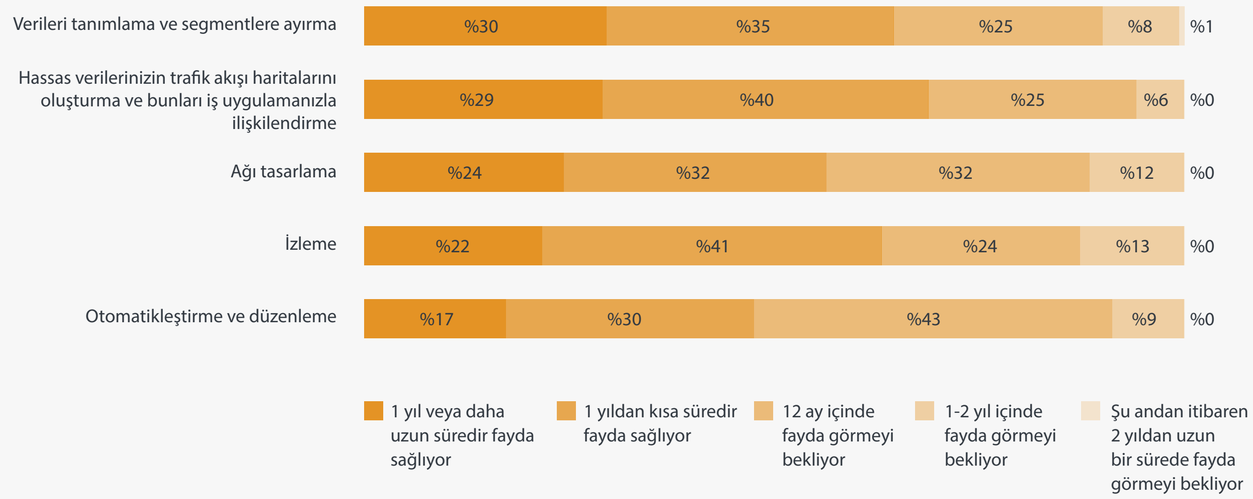
CSO Microsoft Security

İlerledikçe ölçüm yapın

Sıfır Güven kurulumu devam ederken, CISO'lar ilerlemeyi ölçmek için yol boyunca kilometre taşları oluşturabilir ve oluşturmalıdır. Ankete katılanların yaklaşık üçte ikisinin, bir yıl içinde projelerinden birçok açıdan fayda elde ettiklerini ve yaklaşık yüzde 25'inin veya daha fazlasının, verileri tanımlama ve segmentlere ayırma, trafik akışlarının haritasını oluşturma ve ağı tasarlama gibi temel etkinliklerde 12 ay içinde fayda elde etmeyi beklediğini söylemesi iyi bir işarettir.

Mocny, "Sıfır Güven, saldırıların değişen doğasına karşı savunmanız gereken sürekli değerlendirme nedeniyle bir yolculuktur" diyor. "İyileştirmeler için her zaman tetikte olun."

Sıfır Güven'den fayda sağlamak için zaman çizelgesi



Kaynak: Zero Trust Adoption Survey, Mart 2022, Foundry. Base: 103

CSO Microsoft Security

Sadece teknolojiye değil, insanlara odaklanın

Sıfır Güven güvenlik modelinin geniş kapsamı, modeli kurmakla görevli BT ve güvenlik ekipleri de dahil olmak üzere her çalışanı etkiler. Bu nedenle, herhangi bir büyük teknoloji projesinde olduğu gibi, sorunsuz ve başarılı bir kullanıma sunma süreci sağlamak için kurulumların yeni süreçlerle ve değişiklik yönetimi uygulamalarıyla senkronize olduğundan emin olmak önemlidir.

Mocny, "Teknolojideki değişikliğe ek olarak kültürel bir değişiklik de var. "Ağ mimarları veya kimlik uzmanları dahil olmak üzere güvenlikle ilgilenen birden fazla ekibiniz varsa bu ekiplerin birlikte çalışma şeklini de değiştirmeniz gerekir. Teknolojinin birlikte uyumlu bir şekilde çalışmasını sağlamak için siloları yıkmanız gerekir" diyor.

Siloları ortadan kaldırmak, tüm bu disiplinlerdeki ekiplerin pilot uygulama ve kavram kanıtı (POC) projelerine sıkı bir şekilde dahil olmasını içerir. Yaklaşık 2.000 çalışanı olan bir telekomünikasyon kurumunun BT sistem yöneticisi, kurulum sırasında, kimlik doğrulaması yapamayan hizmetler ile bunları oluşturan ve aniden "güvenilmez" hale gelen diğer hizmetlerin yanı sıra kullanılamayan bazı sistemler dahil, birkaç tek hata noktasıyla uğraştıktan sonra bu dersi almıştı.

Sistem yöneticisi, "Bir hizmeti kurmak domino etkisi yaratabilir ve diğerlerinin de çökmesine yol açabilir. Artık, kurulumdan önce çok daha dikkatliyiz. Daha fazla POC süresi tanıyoruz, daha fazla inceleme ve konunun uzmanlarıyla daha fazla mimari değerlendirme yapıyoruz" diyor.

Sıfır Güven Yatırım Getirisi

2021 yılında hazırlanan **Forrester Consulting Total Economic Impact™ çalışması** Microsoft Sıfır Güven çözümlerinin maliyet tasarruflarını ve sağladığı iş avantajlarını ölçmektedir. Forrester'ın görüştüğü beş kuruma dayanan bir karma kurum, Microsoft ile bir Sıfır Güven mimarisi uygulayarak üç yıllık %92'lik bir yatırım getirisi elde etmiştir.

Bu karma kurum ayrıca, uç nokta yönetimi, antivirüs ve kötü amaçlı yazılımdan koruma çözümleri dahil olmak üzere Sıfır Güven kapsamında gereksiz hale gelen güvenlik araçlarına olan ihtiyacı ortadan kaldırarak çalışan başına ayda ortalama 20 USD tasarruf sağlamıştır.

CSO Microsoft Security

Sıfır Güven yolunda neredesiniz?

Anketin gösterdiği gibi Sıfır Güven güvenlik modelinin faydaları, CISO'ların ve güvenlik ekiplerinin karşılaştığı bazı kurulum zorluklarına göre açık bir şekilde daha ağır basmaktadır. Bu zorlukları iyi düşünülmüş bir planla karşılamak, kurumunuzun hızla korumaları iyileştirmesine, riski azaltmasına ve kurum genelinde değer sunmaya başlamasına yardımcı olabilir.

Kurumunuzun Sıfır Güven olgunluk düzeyini değerlendirmek ve daha pratik kurulum kaynakları görmek için Microsoft'un **Sıfır Güven olgunluk modeli değerlendirmesini** tamamlayın.