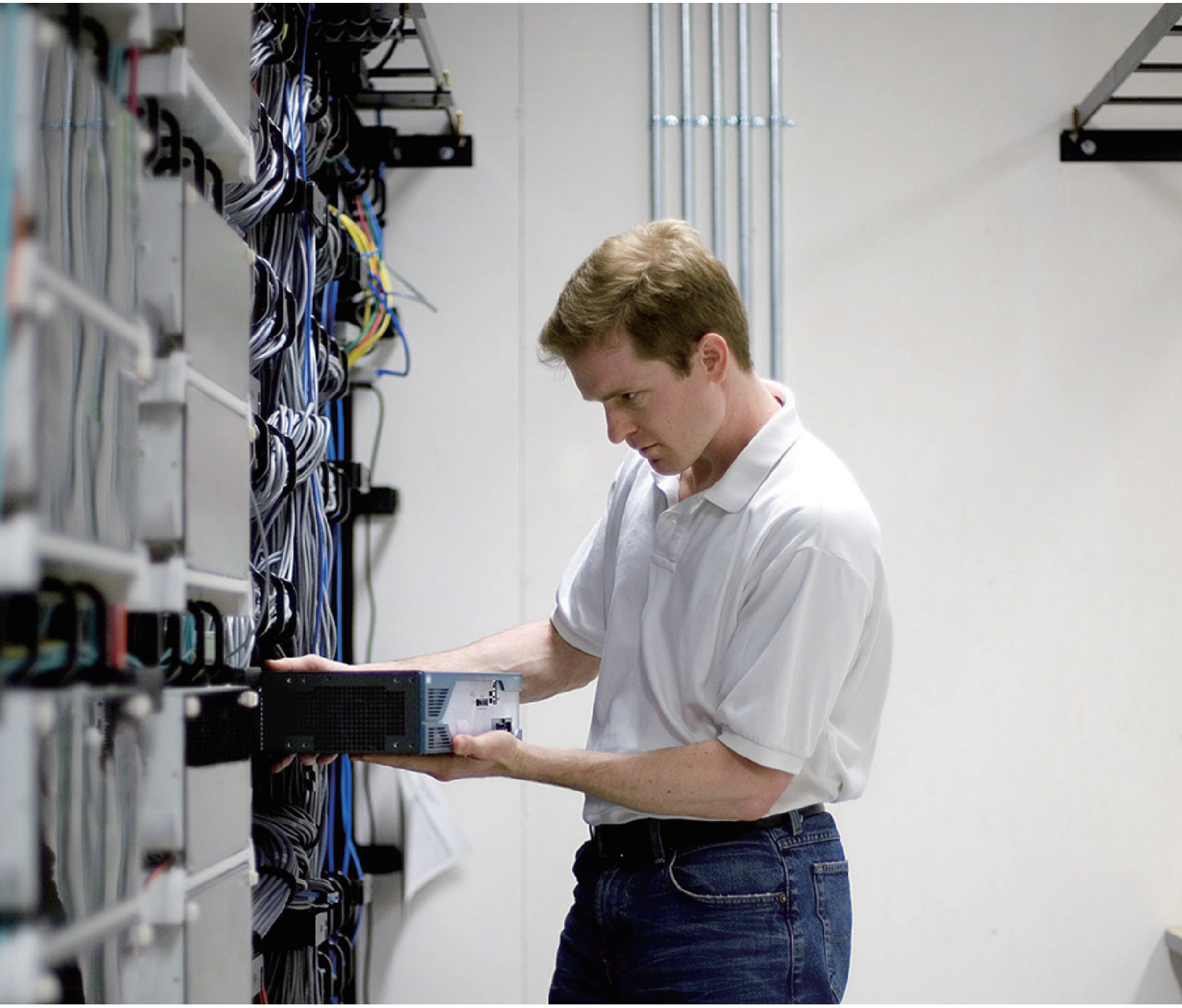
Ağ Ucunuzu Akıllı Hale Getirin ve Yarının İhtiyaçlarını Bugünden Karşılayın



Yönetici Özeti

Yeni dijital iş gerçekliğinde, ağ ucu hiç bu kadar önemli olmamıştı. Çoğunlukla gözden kaçan ağ kenarı, dijital başarının gerçekleşmesinde veya kaybedilmesinde temel taşıdır. Ağ ucunuzda meydana gelen her şeyi göz önünde bulundurun:

- Ağ ucu, güvenilir olmayan kötü amaçlı cihazların sızmasına karşı ilk savunma hattıdır.
- Hedef kitlelere, çoğunlukla büyük yatırımlar yapılmış, uygulamaları ve servisleri dağıtan kanaldır.
- Geniş çaplı dağıtık kuruluşları bağlayan stratejik ağ geçididir.
- Kuruluşunuz ve müşterileriniz arasındaki köprüdür.
- Yeni Nesnelerin İnterneti (IoT) cihazlarının bağlandığı ve yönetildiği noktadır.
- İşletmenizde neler olduğunu gerçekten anlamanız için en ideal yerdir.

Ağ ucu bazen tüm ağ çözümlerinin esasen aynı olduğuna inanılarak kurulur. Cisco bunu reddeder ve yeni dijital işletmenin uçta büyük istihbarata ihtiyaç duyduğuna inanır.

Biz, iş başarısını destekleyen çözümler ve stratejik işlevler sunarız. Cisco, yeni dijital ağ ucunu şunlara odaklanarak destekler:

- Kenardaki çok önemli kaynakları varlıkları savunma. Kuruluşlar, ağı hem bir sensör hem de muhafız gibi geliştirerek ağ ihlallerinin %99,2'sini engelleyebilirler. Bu, korumayı ve müdahale hızını artırmak için daha kapsamlı sezgisel veriler sunularak da yapılabilir.
- 1200'ün üzerindeki uygulamayla, sekiz kat daha hızlı yönlendirme ve görünürlük ile uygulama ve cihaz farkındalığı sağlama. Bu, Apple ile yapılan stratejik bir iş ortaklığı ve Wi-Fi yenilikleri ile mümkün hale getiriliyor.
- İşletmeniz kablosuz LAN, LAN ve WAN ile ilgili bir yazılım tabanlı bir yaklaşımla büyüdükçe ağınızı hızlı şekilde adapte etme. Bu, yazılımı donanımdan ayırarak ve WAN ucunu sanallaştırarak kurulum maliyetlerini %79 oranında azaltır.
- Gelecekteki talepleri karşılamak için standartlara dayalı, programlanabilir bir temel oluşturarak tasarlanan bir platform yeni işlevleri ihtiyaç duyulduğunda hızlıca ekleyebilir.
- Daha iyi iş kararları için perakende satıştan konaklamaya kadar daha detaylı ve hızlı sezgisel veriler sunma, konum verilerinde bir metreye varan ayrıntı düzeyi elde etme.

Günümüzde, kuruluşlar dijital dönüşüm yolculuklarını yaparken tüm kuruluşlarda değişikliği sanal olarak harekete geçirmek için ağ çok önemlidir. Bu dönüşüm yolculuğu, kuruluşlara üretkenliği artırma, müşterilerle daha iyi bağ kurma ve önemli fikri mülkiyet haklarını ve varlıkları korumaları konusunda yardımcı olacaktır.

Ağ ucunun bu dönüşümde çok önemli bir rolü vardır ve çekirdek ve veri merkezi ağları ile kıyaslandığında belki de en geniş sorumluluk kümesinin ağırlığını taşır. Şekil 1'de gösterildiği gibi her ağ katmanını karşılaştırırken, ağ ucunun kampüste geniş bir sorumluluk alanı vardır. Bu şube içinde geçerlidir.

Şekil 1. Ağ Katmanları ve Bunların İşlevleri

Ağ Ucunun Rolü

Dijital dönüşüm, ağ ucunu daha önce hiç olmadığı kadar önemli hale getirmiştir. Ağınızın ucunda meydana gelen her şeyi göz önünde bulundurun:

- **Ağ ucu ilk savunma hattıdır.** Bu uç, ihtiyacınız olan şeylere erişebilme becerinizi sınırlamadan politikanın uygulandığı ve doğrulandığı yerdir. Erişim doğru şekilde yönetilmezse, işletmeniz sızmaya veya tehdit artışına kolayca yem olabilir ve tehdit alanı büyürken tehlikeli şekilde büyür. Cihaz, aygıt yazılımı ve hatta işletim sistemi bile tamamen istismar edilecek noktalardır.
- **Büyük yatırımlar yapılan uygulamaları dağıtan kanaldır.** Ağ ucu, önceliklendirmenin yapıldığı yerdir. Uçtaki kötü bir deneyim uygulamanın yatırım geri dönüşünü azaltarak daha yavaş benimsenmesine neden olur.
- **Geniş çaplı dağıtık kuruluşları bağlayan stratejik bir ağ geçididir.** Çalışanlarınıza, iş ortaklarınıza ve müşterilerinize olması gerektikleri her yerde kusursuz bir deneyim sunmak en önemlisidir. İkinci sınıf bir ağ, esas hedef kitlelere normalin dışında servis seviyeleri sunacaktır.
- **Kuruluş ve müşterileri arasındaki köprüdür.** Bir perakende satış veya konaklama işinin parçasıysanız, vasatın altında bir erişim müşterilere kişisel bir düzeyde bağlanma becerinizi engelleyecek ve markanızı olumsuz yönde etkileyecektir.
- **Artan IoT cihazı taleplerini güçlendirmek ve desteklemek için üretilmiştir.** Ağ ucu, operasyonların iyileştirilmesi, maliyetlerin azaltılması ile tüm sektörleri dijital çağa sanal olarak taşıyarak fiziksel ortama uyarlanır. Uçta doğru işlevler olmadan kuruluşlar maliyet azaltma ve operasyonel etkinlik açısından geride kalabilir.
- **Burası, işletmenizde neler olduğunu gerçekten anlamanız için en ideal yerdir.** Dağıtılmış bir ağda, yalnızca uç, verileri ve analizleri uçtan toplayarak tüm veri trafiğini görür. Kullanıcılar, uygulamalar, cihazlar ve tehditler ile ilgili veriler, çalışanları desteklemek, riski ve maliyeti azaltmak ve hedef kitleye bilgi dağıtmak için daha iyi iş kararları almaya yardımcı olan öngörüler sağlayabilir. Doğru bir seviyede tutarlı veri ayrıntısı olmadan, bu veriler çarpık ve güvenilmez hale gelir.

Ucun metalaştırılması iyi bir şey midir?

Birçok uç çözümü, uç ağı cihazları kurmak ve doğrudan sektör standartlarına göre tasarım yapmak için kullanıma hazır bileşenlere bel bağlayarak metalaştırmaya başvurur. Bu çoğunlukla, bileşen üreticilerinin kullanıma hazır hale getirdiği tasarımları kullanarak donanımın mühendislik ve üretim maliyetlerini azaltmak için yapılır. Bu da ucun metalaştırılmasına yol açar. Bu yaklaşım maliyeti ve yönetimi, büyüme ve güvenlikle ilgili önemli yenilikleri sunmanın üzerinde tutarak işletmenizi daha büyük risklere açık hale getirir.

Risk nedir?

Bileşenlere ve tasarımlara yalnızca cihaz üreticilerinin kullanımına sunulmaz; onlar kendilerini ağa sızma peşinde olan insanların ellerinde bulabilirler. Ağa bağlı her cihaz, ağa sızılabilecek bir noktadır. Günümüzün kuruluşları, iş başarısını artırmak için ağlarındaki mobil ve Nesnelerin İnterneti (IoT) cihazlarının sayısını artırmaya bel bağlamaktadır. Kuruluşlar, kenardan başlayıp veri merkezine giden trafiğin her adımında trafiği denetlemeye ve yeniden denetlemeye devam ederek, erişim güvenliğine hitap eden çözümler aramaya ihtiyaç duyuyor.

Yeni bir iş gereksinimi doğduğunda ağı yeniden tasarlamak zorunda kalma riski de vardır. Kullanıma hazır çözümler, çok sayıda mevcut kullanım durumunu karşılamak için tasarlanır ancak esneklik ve özelleştirme açısından sınırlıdır. Bu çözümler ağınızın öngörülemeyen büyümesi açısından da sınırlıdır. Ağ platformunun, günümüzün hızlı ilerleyen dijital dünyasına uyum sağlaması gerekmektedir.

Kullanıma hazır birçok çözüm, bir dizi temel ihtiyaç ve işlev kümesi sunmak için önemli olan sektör standartlarına doğrudan uyacak şekilde oluşturulur. Ancak bu standartlar değişebilir. Standart süreci çoğunlukla uzun sürer ve cihaz üreticilerinin, uygulama geliştiricilerinin ve kullanıcı taleplerinin oranı sürekli olarak değişmektedir. Standart tabanlı bir yaklaşım kullananlar, daha yüksek kullanıcı beklentilerini karşılamak söz konusu olduğunda kendilerini geride kalmış bulabilir. Bir çözümün standardı karşılayarak başlayabildiği ancak gerekmesi durumunda sonradan bu standartlardan da üstün ek işlevler geliştirebilme kapasitesine sahip olması gereken zamanlar vardır. Bunlar, daha iyisinin yapılmasının ve kabul edilmesinin yıllar sürebileceği standartlarla sınırlanmadan dijital dünyanın yeni taleplerini karşılar.

Ayrıca cihaz bütünlüğünün tehlikeye düşme riski de vardır. Kötü amaçlı kuruluşlar, cihazlar dünyanın dört bir yanına nakledilirken onları ele geçirip bileşenlerini değiştirirler. Örneğin hassas verileri almak için işlemcileri söküp başka bir aygıta takabilir veya monitörler entegre edebilirler.

Gerçek Maliyet Nedir?

Ucun metalaştırılması çoğunlukla mühendislik ve üretim maliyetlerini azaltmak için yapılır ve bazı çözümlerin daha düşük bir fiyata satılabilmesine olanak verir. Bununla birlikte, maliyeti ölçerken sadece sermayeye, hatta işletim maliyetine bakmakla kalmayıp riskle ilişkili maliyete de bakmamız gerekir. Her kuruluş farklıdır, bu nedenle herkesi temsil edilecek gerçek maliyetleri belirlemek mümkün değildir. Ancak şunu göz önünde bulundurun:

- Bir güvenlik ihlalinin maliyeti. Birçok kuruluşun fikri mülkiyet hakkı ve varlıkları onun ekmek kapısıdır. Yanlış ellere geçtiklerinde başınıza gelebilecekler nelerdir? Kötü amaçlı kuruluşlar fikri mülkiyetleri fidye isteyerek, şantaj yaparak ve bunları daha yüksek fiyat veren bazı kişilere satarak paraya dönüştürme konusunda inanılmaz iyilerdir. Bazı çalışmalar tıbbi kayıtlar için kayıt başına 40,00 ABD doları fidye istendiğini ortaya koymuştur. Binlerce kayıtla, hastanelerin kendilerine ait olanı yeniden almak için çok fazla para kaptırma kıskacına düşme ihtimali vardır.
- Çalışanlar tarafından benimsenmemiş bir kritik iş uygulamasının maliyeti. Birçok kuruluş bütçelerinin büyük bir kısmını üretkenliği artıran yeni uygulamalara ve sistemlere ayırırlar. Çalışanların bu uygulamalar ve sistemlerle ilgili deneyimleri kötüyse kullanmayı bırakırlar ve yatırım geri dönüşü hayal olur.
- Kaçırılmış bir fırsatın maliyeti. Bir perakende satış veya ağırlama kuruluşunun parçasıysanız, müşterileri mobil cihazları üzerinden bağlıyorsunuzdur. Ancak müşterileriniz bağlanma konusunda sıkıntı yaşarsa, kuruluşunuz bu müşteriyle bağlanma ve istenen davranışı etkileme fırsatını kaçırır.
- Yetersiz görünürlüğün maliyeti. Ağ ucu kullanıcılar, onların cihazları, kullandıkları uygulamalar, nereye gittikleri ve hatta potansiyel tehdidin nerede olduğu ile ilgili çok sayıda bilgi barındırır. Bu görünürlük olmadan kuruluşunuz, kullanıcıların ortamla nasıl etkileşimde bulunduğunu, bilgilere nasıl eriştiğini ve kullandığını öğrenmek için sayısız saatler geçirebilir ve hatta erkenden yatıştırılabilecek potansiyel bir tehdidi gözden kaçırabilir.

Cisco Uçta İstihbarat Sunar

Cisco, ucu metalaştırmak yerine farklı bir yaklaşımın avantajından yararlanır. Biz, kuruluşları dijital çağa geçirmeye yardımcı olmak için konumlandırılmış yenilikler geliştirmeye büyük ölçüde yatırım yaptık. Daha yüksek düzeyde uygulama ve cihaz farkındalığını desteklemek ve daha derin ve daha hızlı öngörüler sunmak için kritik varlıkları savunmaya titizlikle odaklandık. Cisco, işletmeniz büyüdükçe uyum sağlamanıza ve gelecekte gerçekleşecek her şeye hazırlanmanıza yardımcı olur. Bunu en başından benzersiz işlevler oluşturarak veya gerçek ortamda test edilmiş bileşenlerin işlevlerini iyileştirerek yaparız. Cisco, hem bugün hem de gelecekteki ağ kenarı taleplerini karşılamanıza yardımcı olan işlevler sunar.

Kenardaki Kritik Varlıkları Savunma

Ağ ucu kullanıcıların ve cihazların bağlandığı yer olduğu için, burası yetkisiz veya kötü amaçlı erişimlerin bir numaralı noktasıdır. Ağa neyin alındığını belirlemek ve kontrol etmek için ağ ucunun güvenilir olması gerekir.

Uç güvenliğinin metalaştırılması, kullanıma hazır güvenliğin çalıştığı varsayılırsa etkin olacaktır. Bu doğruysa bilgi hırsızlığı, fidyeciliği veya şantajcılığı neden hızla büyüyüp 1 trilyon dolarlık bir sektöre dönüşmektedir?

Mevcut uç güvenliği yaklaşımları işe yaramamaktadır. Cisco, bir cihazın ağa erişmesine ve ağda gezinmesine izin vermeden önce durumunu öğrenmenin yanı sıra ne ve kim olduğunu bilen yenilikçi teknolojilere sahip bir piyasa lideridir.

Cisco müşterileri için çok sayıda Cisco® ağ ucu güvenlik yeniliğini ve nasıl kullanıldığını burada bulabilirsiniz:

- **Cihaz ve kullanıcı kimliği ve durumu**. Cisco kenar cihazları, en kapsamlı kenar profil sorgulama teknolojilerini entegre eder. Ek olarak, Cisco AnyConnect® Güvenlik Aracısı, üretim ağına erişime izin vermeden önce bir tutum ve politika uyum durumu denetimi yapar. En doğru uç noktası kimliği, yetkisiz, sağlıksız (kötü amaçlı yazılım bulaşmış) cihazları, temiz ve yetkili olduğu kanıtlanana kadar ağdan tamamen uzak tutar.
- **Tehdit puanı ile değişen erişim ayrıcalıkları**. Cisco Identity Services Engine ile entegrasyon yapılarak, kullanıcılar ve cihazlar STIX tehdidi veya CVSS güvenlik açığı puanları değiştikçe kendi erişim ayrıcalıklarına sahip olabilir. STIX ve CVSS, güvenlik tehditlerinin ve güvenlik açıklarının önem derecesini açıklayan ifadelerdir.
- **Yazılım tanımlı bölümlendirme entegrasyonu**. Sanal LAN'lar ve erişim kontrol listeleri (ACL) ile bölümlendirmeyi oluşturmak ve yönetmek genellikle zordur ve bölümlendirme IoT operasyonlarında temel haline geldikçe daha da zorlaşacağı kanıtlanmıştır. Cisco kenar cihazları, yüksek performanslı erişim noktasından veri merkezindeki bir uygulamaya kimlik ve bölümlendirme sağlayan ASIC'in yanı sıra işletim sisteminde yerleşik olan Cisco TrustSec® yazılım tanımlı bölümlendirme ile birlikte teslim edilir.
- **Muhafız Olarak Ağ**. Bu yazılım tabanlı bölümlendirme, erişimi denetlemek ve tehditleri zapt etmek için güvenlik politikasının anlık ve tutarlı şekilde desteklenmesine olanak veren kenar cihazlarında yerleşiktir. Identity Services Engine ile entegrasyon halinde çalışan Cisco Stealthwatch ve Cisco Security Technology Associate teknolojileri, bir tehdidi zapt etmek için politikayı başlatabilir. Üstelik tüm bunları tek bir kontrol ekranından veya bir üründen yapar.
- **Sensör Olarak Ağ**. NetFlow ve Cisco Stealthwatch'ın yorumu ile uçtan uca gelişmiş görünürlük edinin.
  Tüm Cisco kenar cihazlarında Flexible NetFlow olmadığı için, anormal davranışları keşfetmek için uçtan uca görünürlüğe sahip olabilirsiniz. Metalaştırma teknolojileri ile, kullanıcıların ağa geldiklerinde neler yaptıklarını ve İnternet'te neler yaptıklarını gösteren davranışlara gözünüz kapalı olur.
- **Stealthwatch Learning Network entegrasyonu**. Bu yenilik, tüm şube cihazlarının davranış verilerini paylaşmasına ve nelere izin verildiği, neyin onu daha hızlı, daha kolay ve daha ölçeklenebilir hale getirdiği konusunda daha sezgisel olmasına olanak verebilir.
- **Sıfır dakikada defcon politikası uygulama**. Bu, sıfır gün saldırısı veya hızla yayılan bir bilgisayar korsanlığı olayı gibi yıkıcı olaylara müdahale eden önayar politikalarına sahip olabileceğiniz anlamına gelir. Tek bir düğmeye basarak, tehdit savuşturuluncaya kadar tüm iletişimleri kısıtlamak veya durdurmak üzere ağdaki her cihaz için erişim politikası değişikliklerini başlatabilirsiniz.

- **IoT uç noktası kimliği ve otomatik bölümlendirme**. Cisco kenar cihazlarındaki sorgular günümüzdeki tıbbi IoT cihazlarının en büyük koleksiyonunu belirlemeye yardımcı olur ve bu teknoloji diğer birçok sektöre yayılmaktadır. Identity Services Engine gibi gelişmiş teknolojilerin entegrasyonu ile, ağ kenarı cihazları en yoğun uç noktalarını daha iyi belirleyip otomatik olarak bölümlendirebilir ve bunları saldırıdan korumak için otomatik olarak ayrı ağ segmentlerine ekleyebilir. Böylece bir çalışan bir cihazı ağa dahil ettiğinde cihaz belirlenir, sınıflandırılır ve onun ilgili ve güvenli ağ segmentine yerleştirilir.
- **Tehdidi hızlı şekilde kontrol altına alma**. Cisco kenar cihazları Identity Services Engine ve TrustSec ile entegre olur. Böylece bir Cisco veya teknoloji iş ortağı bir saldırı tespit ettiğinde, tehdit eden kenarı bir BT komutu ile ya da otomatik olarak bir ağ segmentine alabilir. Tehditler daha hızlı tespit edilir ve kontrol altına alma için anında müdahale edilir.
- **Şifrelenmiş trafikte kötü amaçlı yazılım tespiti**. Saldırganlar ağa erişmek için tespit edilmemiş daha fazla yöntem buldukça, Cisco, kötü amaçlı yazılımı belirlemek için bizim ağı inceleme becerimizi kullanır, hatta şifrelenmiş trafikte bile.
- **Bulut, kötü amaçlı yazılım ve fidye yazılım koruması**. Cisco Umbrella for Branch ile entegrasyon, Cisco kenar cihazlarını Cisco'nun Fidye Yazılım Çözümünün önemli bir parçası haline getirmiştir. Umbrella, çalışanların şüpheli, tehlikeli veya kötü amaçlı web sitelerine erişmesini önler. Kötü amaçlı yazılım ve fidye yazılım robotlarının, normalde çalışmak için ihtiyaç duydukları ana dosyalara erişmesini de önler.
- **Mobil çalışan koruması**. Mobil çalışanlar, çoğunlukla uzaktayken internete serbestçe eriştikleri için kötü amaçlı yazılımların muhtemelen en yaygın sızma noktalarıdır. Cisco Gelişmiş Kötü Amaçlı Yazılım Koruması ve Cisco Umbrella for Mobility ile, ağ dışındayken güvende kalmak için VPN'li Cisco AnyConnect güvenlik ajanının sayısı artırılabilir. VPN üzerinden birçok Cisco kenar cihazına bağlanmaya da olanak verir. Bu tek ajanlı mobil cihaz güvenliğinin hiçbiri bir meta ortamında çalışmayacaktır.
- **Ağ cihazı bütünlüğü**. Saldırganların, sistemlere sızmak ve müdahale etmek için salt uygulamalardaki ve işletim sistemlerindeki güvenlik açıklarını kırmak dışında birden fazla yolu vardır. Donanımlara ve yazılımlara ağ cihazları üzerinden saldırırlar, böylece ağ cihazını emniyete almak güvenlik açısından çok önemlidir. İşletim sistemlerinde ve uygulamalarda olduğu gibi, ağ cihazının güvenlik açıkları muhtemelen keşfedilmeye devam edecektir. Cisco, Cisco müşterilerinin güvenilir bir ağda çalışmaya devam edebilmesine yardımcı olmak amacıyla, yazılım ve donanım geliştirme için geri çekilme testiyle eksiksiz hale getirilmiş en sıkı kuralları kullanır.

Daha Detaylı Veriler ve Daha Hızlı Öngörüler

Cisco kenar cihazları; kullanıcılar, onların kullandıkları cihazlar ve eriştikleri uygulamalar hakkındaki öngörüler ile, işletmenizde gerçekte neler olduğu konusunda bir bilgi hazinesi olarak hizmet verir. Değişikliklere ve ihtiyaçlara otomatik olarak uyarlamak için ağdaki cihazları anlama ve öğrenme becerisine sahiptir. Daha doğru iş kararları alınmasını sağlamak amacıyla, kullanıcıların ortamla nasıl etkileşimde bulunduğunu daha iyi anlamak için konum tabanlı veriler sunar ve tehditlerin işletmeye nasıl sızdığını öğrenmek için tehdit soruşturmaları yapabilir.

Cisco IOx Fog Computing ile kenar, ister tesiste ister bulutta olsun, bu verilerin işleneceği en ideal yere karar vererek kuruluşun performansının artmasına ve maliyetlerin düşmesine olanak sağlar. Cisco Connected Mobile Experiences (CMX) uygulamasında bulunan konum analiz araçları, kullanıcıların ortamla nasıl etkileşimde bulunduğunun gerçekçi bir görünümünü sağlamak üzere ayrıntılı Wi-Fi ve Bluetooth Low Energy (BLE) destekli konum analizleri sunar.

Perakende satış, konaklama ve eğitim gibi işletmeden tüketiciye (B2C) hizmet veren kuruluşlar, Wi-Fi + BLE ile bir metreden az konum doğruluğuna ulaşabilmişler ve doğrudan gelir artışları elde etmişlerdir. Hyatt Regency'nin oda haricinde elde ettiği %20 gelir, müşterinin konaklama süresinde üç kat artış ve Stary Browar'da müşteri deneyiminde %80 iyileşme bazı örnekler arasında verilebilir. Tüm bu kazanımlar kişiselleştirilmiş mobil deneyimler sunulurken edinilmiştir.

Ek olarak, Cisco Prime™; son kullanıcıların, onların cihazlarının ve ağda kullanılan uygulamaların 360 derecelik bir görünümünü sunar. Bu, daha iyi bir ağ planlamaya, uygulamanın benimsenme düzeyini ölçmeye ve maliyetleri düşürmeye olanak sağlar.

İşletme Otomasyon Aracılığıyla Büyüdükçe Uyarlayın

Yönetilecek kullanıcı, cihaz ve konum sayısı arttıkça, sahip süreçleri ve yeni servisleri sıfır gün ve ilk gün özellikleriyle otomatik hale getirmek daha büyük bir gereksinim haline gelmiştir. Kablolu ve kablosuz erişim alanında, özel uygulama erişimine sahip entegre devrelerde (ASIC'ler) çalışan ayrıştırılmış yazılım tabanına sahip bir kampüs ve veri merkezi yapısı şunlara olanak sağlar:

- Daha iyi ölçeklendirme
- Servis güvencesi
- Güvenlik
- Hem fiziksel hem de sanal cihazlar, uygulamalar ve kullanıcılar için başka servisler

Ağ sanallaştırma, ağ ve politika yönetimini kullanıcı türüne göre hızlı şekilde başlatır ve uygulamaları özelleştirir ve tehditleri daha hızlı kontrol altına alır. Yeni uzak konumları herhangi bağlantı türü üzerinden günler yerine dakikalar içinde güvenle kurmak için merkezi hale getirilmiş bir yaklaşımdır.

Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM), uçta hiç dokunmadan kurulum için merkezi olarak kontrol edilen tak ve çalıştır (PnP) ve kolay servis kalitesinde (QoS) işlevler sunar. Kritik uygulamalarınız için dinamik uygulama önceliklendirmeye olanak da verir.

Cisco, özelleştirme için yazılımın olanak verdiği çevikliği sunar. Kuruluşunuza, güçlü entegre yazılım ve donanım platformları üzerinden, WAN ve erişim ucunda kendisini gösterecek olan önemli avantajlar sunabiliriz. WAN'a uyarlanmış bileşenler arasında hızlı ASIC ve bulut yönetim yazılımı, Cisco Kurumsal Ağ İşlevlerini Sanallaştırmayı (Kurumsal NFV) bir gerçeğe dönüştürür. Burada ağ servislerini aylar yerine dakikalar içinde açabilirsiniz. Kurumsal NFV; bilgi işlem, depolama alanı, ağ ortamı altyapısı, yönetim ve güvence olanakları sunar. Böylece şubede karmaşayı azaltabilir ve talep üzerine uçta yeni servisleri etkinleştirebilirsiniz.

APIC-EM PnP ile kuruluşların kurulum maliyetlerinde %79 azalma ve APIC-EM Intelligent uygulamalarıyla sağlamanın %85 daha hızlı olduğu görülmüştür.

Her tür sahadan bağlanan çok fazla sayıda kullanıcı ve cihazla, ağ ucu büyük kampüslerde ve küçük uzak sahalarda olabilir. Otomatikleştirilmiş PnP özelliklerine sahip küresel topoloji görünümleri, anahtar, yönlendirici veya erişim noktası gibi bir ağ cihazının kurulum ya da yükseltme maliyetini düşürür. Denetleyicideki ek uygulamalar, kritik iş trafiğini kritik olmayan bant genişliği kullanıcılarına karşı hızlıca koruyarak ağ çapında QoS sağlanmasına olanak verir. Intelligent WAN (IWAN) uygulaması gibi özelleştirilmiş uygulamalar sağlama, izleme ve güvenlik sorunlarını giderme, şifreleme, yol seçimi ve uygulama görünürlüğü ve WAN üzerinden kontrol olanağı verir.

İlaveten, Cisco ONE™ Yazılımı, ucunuz için yazılım satın almanın esnek bir yolunu sunar. Ürün ömrünün her aşamasında Cisco ONE Yazılımı, ağınızda satın alma, yönetim ve yükseltme işlemlerini kolaylaştırmaya yardımcı olur. Yatırımınız süregelen yeniliklerle, fiziksel ve sanal makineler güncellemeleriyle ve yükseltmeleriyle büyüdükçe güçlü bir yatırım geri dönüşünün farkına varın.

Uygulama ve Cihaz Farkındalığı

Cisco, daha iyi bir mobil deneyim sunmak için mobil cihaz sektör lideri Apple ile iş ortaklığı yapan tek satıcıdır. İki şirketin bu stratejik ortaklığı, optimum yönlendirme üzerinden en iyi Wi-Fi deneyimi sunmak üzere ağ zekasını destekler. Başka bir deyişle, iş yerinde çalışanların üretkenliğini artıran Apple iOS cihazlarındaki kritik iş uygulamaları için bir sürat şeridir.

Kuruluşlar sekiz kat daha hızlı yönlendirme ve %66 daha güvenilir Wi-Fi araması, SSID sayısının azalmasından dolayı ağ yönetimi için çalışan sayısında %50 azalma bekleyebilir ve son kullanıcılar iOS cihazının pil ömründen %30 oranında tasarruf sağlayabilirler.

Uzun yıllardır Cisco, mevcut standardın ötesine geçen Wi-Fi yenilikleri sundu ve sonraki standart için kanıt noktaları olarak hizmet verdi. Cisco Aironet® kablosuz teknolojisi; yayın araçlarını, cihaz performansını ve uygulama deneyimini iyileştiren yüksek yoğunluklu deneyim yenilikleri sunar. Cisco, radyo kullanılabilirliğini sınırlamadan Wi-Fi ağının performansını optimize eden Flexible Radio Assignment teknolojisine de öncülük etmiştir. Bu beceri, kablosuz erişim noktalarının, ani kablosuz bant genişliği taleplerini belirlemeye olanak verir ve bu ihtiyacı karşılamak için kablosuz ağı otomatik olarak uyarlar. Bu, çok sayıda kullanıcının bir araya geldiği ve kablosuz bant genişliği için savaştığı alanlarda çok önemlidir.

Dijital işletme, üretkenliği artırmak ve müşterilerle sıkı bağlar kurmak için kullandığı uygulamalara dayalıdır. Cisco, kablolu ve kablosuz uçta uygulamaları algılayan Uygulama Görünürlüğü ve Denetimi sunar. Biz, kablolu veya kablosuz LAN'ınız üzerinden dağıtımı optimize ederken WAN'ınız üzerinde en iyi yolu seçmek için akıllı yol denetimini kullanırız. Böylece kullanıcılarınız olası en iyi uygulama deneyiminin keyfini çıkarır.

Kuruluşlar 1200'ün üzerindeki uygulama için detaylı uygulama görünürlüğüne sahip olur ve kritik iş uygulamalarını APIC-EM ve Cisco Prime Altyapısına sahip bir düğmeyi tıklayarak önceliklendirebilir.

Ucun, kullanıcı deneyimini fiziksel alanda kontrol etme ve iyileştirme becerisi vardır. Cisco Digital Ceiling, aşağıdakileri içeren birden fazla bina ağını birleştirerek IoT avantajlarını artırır:

- Aydınlatma
- Isıtma ve soğutma
- IP video
- IoT sensörleri
- Güvenli ve akıllı bir ağ platformu üzerinden çok daha fazlası

Bir Digital Ceiling, çalışanlar için yeni deneyimlerin ve yeteneklerin önünü açar ve tesislerin işletme masraflarını düşürür.

Gelecekte Hüküm Sürecek Her Şey İçin Tasarlanmıştır

Gelecek akılda bulundurularak standart tabanlı, modele göre programlanabilme işlevine sahip bir Cisco IOS-XE işletim sistemi olmadan tasarlanan Cisco uç nokta cihazları, ortamda, işletmede veya sektörde değişiklikler oldukça yeni işlevler eklenecek şekilde ağı hazırlar. Bu, uç ağını açık, programlanabilir ve genişletilebilir hale getirir.

Uç, cihaz cihaz özelleştirme modelinden, bölümlendirmenin ve erişim denetiminin bir ağ yapılandırmasına eklendiği tam politika otomasyonlu bir çözüme geçiş yapmaktadır. Gelecekte, ağların doğrudan sağlanması gerekmeyecektir. Politikayı basit bir amaç olarak ifade edebileceksiniz. Dahası, ister tesislerde ister bulutta olsun hangi kullanıcıların veya grupların belirli ayrıcalıklı uygulama veya veri gruplarına erişeceğini belirleyebilirsiniz. Ağ, halen izlemeye, sorun gidermeye, iyileştirmeye veya belirli trafiğe ek servisler uygulamaya olanak verirken, bu politikayı desteklemek için otomatik olarak sağlanacaktır.

Ayrıca uç tamamen programlanabilir hale gelmektedir. Orkestrasyon çözümleri; standart model destekli API'lar, Python komut dizini veya diğer Linux tarzı araçlar kullanılarak uçla arayüz bağlantısı oluşturabilir. Bu, çevikliğe ve özelleştirmeye daha önce hiç görülmemiş şekilde olanak vererek, modern yazılım geliştirme yöntemlerine entegrasyonu daha kolay hale getirir.

Ağ Ucunda Sürekli Yenilik

Bağlanılabilirliğin önemli fırsatlar sunarak çıkış yapması beklenirken, şirketler bu dönüşümün ağ altyapılarında ve verileri yönetme ve analiz etme becerilerinde köklü değişiklikler gerektireceğini anlamaya başlamaktadır. Biz, ağ altyapısında yeniliği, altyapı yönetimini ve verilerden eyleme geçirilebilir fikirler elde etmek için analiz araçlarını destekleyerek bu dönüşüm boyunca yol göstermekteyiz.

Cisco, tepkisel sorun gidermeyi proaktif hale getirmeye ve çözüm süresini günlerden dakikalara düşürmeye odaklanmaktadır. Bunu ağdaki her cihazı bir sensör ve dağıtık bir veri işleme öğesi olarak görerek yapacağız. Makine öğrenmesi aracılığıyla eyleme geçirilebilir sezgisel veriler oluşturmak üzere uçtaki cihazlardan veriler alıp, veri işlemeyi veri kaynağının daha yakınına kurarak analizleri hattın hızında yapabiliriz.

Kurulu en büyük sisteme ve özel ASIC çözümlerine sahip olan Cisco, analiz araçları için optimize edilmiş donanımları ve yazılımları tasarlamak için biçilmez kaftandır. Kurulu sistemin gücünden yararlanır. Tek bir ağda kablolu ve kablosuz ağın bir araya getirilmesi , sorun ister uçta meydana gelmiş olsun ister olmasın, uçtaki zekanın sorunları saniyeler içinde gidermenize yardımcı olabileceği anlamına gelir. Ayrıca zamanla potansiyel sorunları oluşmadan bile gidermek demektir. Bu, ileride istenen ağ ve uygulama performansı için BT departmanlarının servis düzeyi anlaşması (SLA) sunmasına yardımcı olacaktır.

Sonuç

Ağ ucuna bu kadar fazla bel bağlanırken, kablolu ve kablosuz LAN ve WAN'ın metalaştırılması, güvenlik ihlallerine, üretkenlik ve gelir kaybına, fırsatların kaçırılmasına ve yetersiz görünürlüğe yol açabilecek riskler ortaya çıkarır. Cisco ağ ucu, uçta yüksek değerli zeka sunarak kuruluşların kullanıma hazır, standartlarla sınırlı bir yaklaşımın ötesine geçmesine olanak sağlar.

Bu yaklaşım kuruluşlara şu olanakları sunar:

- İşletmeyi güçlü bir ilk savunma hattı ile koruma
- Uygulamaları hedef kitlelere güvenle sunma
- Çalışanlara her yerden kusursuz bir deneyin sunma
- Yeni gelir akışları yaratmak için müşterilerle bağ kurma
- IoT cihazlarını daha iyi yönetme ve fiziksel ortamı optimize etme
- İşletmenizde gerçekte neler olduğunu anlamak için optimum görünüm sağlama

Daha Fazla Bilgi İçin

Daha fazla bilgi edinmek için, http://www.cisco.com/c/en/us/solutions/enterprise-networks/unified-access/index.html adresindeki Cisco Tümleşik Erişim Teknolojisi sayfamızı ziyaret edin.

C11-737691-00 08/16