İSTANBUL TİCARET ÜNİVERSİTESİ FEN BİLİMLERİ DERGİSİ

İstanbul Commerce University Journal of Science

http://dergipark.org.tr/ticaretfbd

Derleme Makale / Review Article

SIFIR GÜVEN AĞ ERİŞİM MİMARİSİNDE KULLANICI GÜVENLİĞİNİN SAĞLANMASI*

USER IN ZERO TRUST NETWORK ACCESS ARCHITECHTURE ENSURING SECURITY

Abbas BULUT[1] **Muhammed Ali AYDIN[2]** **Abdül Halim ZAİM[3]**

https://doi.org/10.55071/ticaretfbd.1102276

Sorumlu Yazar / Corresponding Author
abbasbulut@yahoo.com

Geliş Tarihi / Received
12.04.2022

Kabul Tarihi / Accepted
13.10.2022

Öz

Sıfır güven ağ güvenlik modeli, geleneksel ağ modeline ciddi bir alternatif haline gelmiştir. Bilindiği gibi ağ yapıları ilk kurulduğunda asıl amaç güvenliği sağlamak değildi. İnternetin yaygınlaşması, paylaşılan bilgi miktarının artması ve kolay ulaşılabilir olması bilgi güvenliği ile ilgili endişeleri hayatımıza sokmuştur. Sıfır güven bu noktada devreye girmiş ve "asla güvenme-her zaman doğrula" kavramıyla yepyeni bir anlayış getirmiştir. Kısa sürede kabul gören bu anlayış, şirketlerin giderek ağ yapılarını segmentlere ayırmalarına ve entegre ürünler geliştirmelerine neden olmuştur. Sıfır güven güvenlik modeli Kullanıcı, Veri, Cihaz, Uygulama ve Ağ trafiği bileşenlerinden oluşur. Bu bileşenlerden en önemlisi, kullanıcı olarak tanımlanan uç nokta cihazlarıdır. Çünkü siber saldırı bir uç noktada başlar ve hedefi bir uç noktada biter. Bu bağlamda makale, sıfır güven mimarisinde uç noktanın önemini ve Sıfır güven güvenlik platformunu son kullanıcıya genişletmenin faydalarını vurgulayacaktır.

Anahtar Kelimeler: Kullanıcı doğrulanması yetkilendirilmesi, kullanıcı erişim güvenliği, sıfır güven mimarisi, sıfır güven ağ mimarisi.

Abstract

The zero trust network security model has become a serious alternative to the traditional network model. As it is known, when the network structures were first established, providing security was not the main goal. The widespread use of the Internet, the increase in the amount of shared information, and easy accessibility have brought concerns about information security into our lives. Zero trust stepped in at this point and brought a brand new understanding with the concept of "never trust - Always verify". This understanding, which was accepted in a short time, gradually caused companies to segment their network structures and develop integrated products. Zero trust security model consists of User, Data, Device, Application and Network traffic components. The most important of these components is the end point devices, which are described as users. Because a cyber attack starts at an endpoint and its target ends at an endpoint. In this context, the article will emphasize the importance of the endpoint in zero trust architecture, and the benefits of extending the Zero trust security platform to the end user.

Keywords: Endpoint authentication and authorization, endpoint secure access, zero trust architechture, zero trust network architechture.

.

Bu yayın Abbas BULUT isimli öğrencinin İstanbul Ticaret Üniversitesi Fen Bilimleri Enstitüsü, Siber Güvenlik Programındaki Lisansüstü tezinden üretilmiştir.

[1]İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, İstanbul, Türkiye.
abbasbulut@yahoo.com, Orcid.org/0000-0003-2880-7861.

[2]İstanbul Üniversitesi-Cerrahpaşa, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, İstanbul, Türkiye.
aydinali@iuc.edu.tr, Orcid.org/0000-0002-1846-6090.

[3]İstanbul Ticaret Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, İstanbul, Türkiye.
azaim@ticaret.edu.tr, Orcid.org/0000-0002-0233-064X.

1. GİRİŞ

Geleneksel ağ mimarileri tasarlanırken asıl başarılması gereken, verilerin kaynaktan hedefe doğru "en hızlı nasıl ulaşabiliriz ?" konusu idi. Bu sebeple ağ sistemlerine yapılan yatırımlar veri iletim altyapısındaki değişime ve gelişime yapılan yatırımlardı. Bu yapılar ilk kuruldukları yıllarda nispeten izole sistemlerdi. Ağ kavramı yeni olduğu için dışardan gelebilecek saldırı tehditleri yoktu. Zaman içinde gelişen bilişim güvenliği kavramı sayesinde geleneksel ağ yapıları "güvenilen alan" (Trust) ve "güvenilmeyen alan" (Untrust) olarak iki kısma ayrıldı. Atak vektörleri yönü, dışardan içeri olacak şekilde tanımlandı. Güvenlik duvarı (Firewall) cihazlarının devreye girmesi ile iki kısma ayrılan ağ yapılarına, DMZ (De-Militarized Zone) alanı kavramı eklenmiş oldu. Bu şekilde dış dünyaya hizmet verebilecek sunucularımız oluşturuldu. Gelişimlere paralel olarak, merkez-ofis arasında IPSec VPN (IP Security Virtual Private Network), mobil kullanıcılar için SSL VPN (Secure Socket Layer Virtual Private Network) bağlantıları ile hibrid yapılar oluşturmaya başlandı. Bulut tabanlı (Cloud base) altyapı hizmetlerin gelişmesinden sonra sunucuların, uygulamaların dahi nerede olduğu bilinmeyen sanal yapılara kavuşuldu. Nesnelerin Interneti (IoT-Internet of Things) teknolojisinin gelişmesi çok daha birbirine bağlı ve bağımlı olan sistemleri oluşturdu. Bu devasa yapıyı sadece açık ağ sistemleri gibi düşünmek değil kapalı ağların da dahil olduğu işlevsel teknoloji (Operational Technology- OT) yapısı olarak da düşünmek gerekmektedir.

Günümüz pandemi şartları sebebiyle, dijital dönüşüm planları yapan firmaların tüm süreçlerini hızlandırmış oldu. İlerleyen zamanlarda tamamlamayı düşündükleri yapısal değişim daha erken gerçekleşti. Mevcut yapının değişimi doğal olarak, siber güvenlik yaklaşımını da değiştirmiş oldu. Dijitaleşme düzenine hızlı geçiş sürecinde, değişen 3 konu var.

1. Tam olarak uzaktan çalışma olmasa bile, artık hibrit yapılarda çalışmaya başlandı. Bu durum cihazların görünebilirliğinin azalmasına ve bağlanılan cihazların ne olduğunun tam olarak bilinmeyen bir yapıya dönüşmesine sebep oldu.
2. Firmaların bu süreçte kendi özel bulut (private cloud) yapılarını tamamen genel bulut (public cloud) yapısına geçirilme işlemi hızlanmış oldu. Her ne kadar bulut (cloud) yapısı ölçeklenebilirlik ve işlem gücü gibi olanaklarını sağlama kolaylığı vermese de, kullanılan yazılımların ne kadar güvenli olduğu konusu, yazılımlar içinde ek bilgi kaynağı olarak kullanılan üçüncü parti uygulamaların, hatta konteyner sistemlerinin güvenliği konusu tartışılmaya başlandı. Bu uygulamaların ve uygulamalar içinde barındırılan platformların (Amazon Web Services, Microsoft Azure v.s) güvenliği söz konusu olmaya başladı.
3. Hızla gelinen dijitalleşme ortamında telemetri verileri inanılmaz bir şekilde artmaya başladı. Çok fazla yerden daha çok log gelmeye başladı. Doğal olarak bu logların korelasyona tabi tutulup saldırıların analitik incelenmesi, saldırıya dakikalar içinde cevap verilebilme zorunluluğunu ortaya çıkarmıştır. Bu kadar log verisinin yönetilmesi için yapay zeka uygulamalarının kullanımı zorunlu olmuştur.

Ağ tasarımlarında güvenlik kavramı düşünülmediği için, katmanlarının arasına farklı güvenlik seviyelerinin kontrollerini yapan cihazlar yerleştirildi. Bu şekilde tüm yapının güvenliğinin sağlanılmaya çalışıldığını görüyoruz. Bu cihazların çoğu zaman birbirinden farklı üretici ürünleri olması, kontrollerinin tek bir noktadan yapılması zorlaştırmıştır. Bu sebeple, bilişim dünyasında (uygulama, yazılım, donanım) ve ağ altyapılarındaki gelişmeler ile siber saldırı vektörlerinin çok daha karmaşık, sofistike olduğu bir noktaya gelmiş bulunmaktayız.

Sıfır güven mimarisi (Zero Trust Architecture) aslında tam bu noktada yeni güvenlik stratejisi olarak devreye girmiştir. Bilinenin aksine, atak vektörlerinin içerden dışarı doğru tanımlanmasını önermektedir. Bu yaklaşım satın alınılabilecek bir ürün ya da servis değildir. Fakat ürün içine ya da yönetilen servislere katma değer olarak eklenebilecek bir mekanizmadır. Daha önceden bilinen

kavram olmasına rağmen, değişik yapılara uygulanabilmesi ile hızlı bir şekilde kabul gören bir strateji olmuştur. Şirketlerin giderek ağ yapılarını segmentlere ayırmalarına, birbiri ile entegre ürünler geliştirmelerine neden olmuştur.

Sıfır güven mimarisi ile yaşanan gelişmeler değişik yapılara entegre olan yeni kavramlar ortaya çıkmasına sebep olmuştur. Sıfır güven mimarisini bir şemsiye olarak düşünüldüğünde, sıfır güven ağ mimarisi (Zero Trust Network Architechture) bu yapılanmalardan birini teşkil etmektedir. Temel kavramlar olarak benzer olsalar bile, sıfır güven mimarisi ile sıfır güven ağ mimarisi aynı kavramlar değildir.

Sıfır güven ağ mimarisine bakıldığında genel olarak ana bileşenler,

- erişim yapan/yapılan cihaz tanımlanması ve kontrolü (device identification and control)
- erişim yapan kullanıcı tanımlaması ve kontrolü (user identification and control)
- profil kontrol (posture)
- uygulama geçiş kontroleri (application transaction controls)

Bu çalışmada, genel olarak sıfır güven ağ mimarisine dayalı kullanıcı erişim kontrollerinin nasıl yapıldığı incelenmiştir. Mevcut kullanılan bazı uygulamaların orta ölçekte firmalarda test edilmiş sonuçları da paylaşılmıştır.

Sıfır güven ağ mimarisi kullanıcı güvenliği noktasında, 3 temel husus üzerine inşa edilmiştir.

- asla güvenme - her zaman doğrula
- en az ayrıcalığı uygula
- her zaman ihlal varmış gibi düşün.

Stratejinin doğası gereği, veri girişlerinin yapıldığı alanlarda bir kontrol noktası oluşturulması esastır. Dolayısıyla gerek lokal üzerinden, gerek uzak erişimle merkezi veri alışverişi yapan tüm kullanıcı erişimleri kontrol edilmelidir. Güvenlik zincirindeki en zayıf halka insandır. Organize-odaklı siber saldırıların çoğu zaman bir uç noktada (end point) başlayıp yine bir uç noktada sonlanması sebebiyle, kullanıcı insiyatifini en aza indirip kontrollerini sağlıklı bir şekilde yapmak gerekir. Tecrübelere dayanarak ifade edilebilir ki, kullanıcı makinelerinde çoğu zaman antivirüs yazılımları ya da makine bazlı çalışan güvenlik duvarı yazılımları bulunmaktadır. Bu yazılımlar gelişen tehditlere karşı çoğu zaman etkisiz kalmaktadırlar.

Şekil 1. üzerinde, Ponemon Institute tarafından, 2020 yılı sonu itibariyle yayınlanan Uç Birim Güvenlik Riskleri" (*Endpoint Security Risks Status)* raporunda veri ihlallerinin sebep olduğu kullanıcılara olan etkileri görülebilir.

Şekil 1. Son Kullanıcıya Yönelik Saldırı Vektörleri

Bu alandaki çalışmalar incelendiğinde, mevcut yapılardan sıfır güven ağ mimarisine geçerken en önemli bileşenlerden olan kullanıcı kavramının değişim süreci incelenmemiş. Ayrıca sıfır güven ağ mimarisine geçtikten sonraki kullanıcı entegrasyonu ile çalışmaların sayısı çok fazla değildir. Yapılan çalışmaların içeriğinin genel olarak teorik olduğu görülmüştür. Bu çalışmanın iki amacı vardır. Birincisi literatürde yer almayan sıfır güven ağ mimarisi içerisinde, son kullanıcı güvenliğini sağlamaya yönelik boşluğu doldurmak, bir diğeri ise mevcut son kullanıcı ürünlerinin incelenmesi sonucu elde edilen verilerin yapay zeka destekli uygulamaların geliştirilmesinde model önermektir. Bazı ticari uygulama testleri birçok kuruluşların son kullanıcı bilgisayarlarında denenmiştir.

Bu çalışma devamında, Bölüm 2'de literatür araştırmalarına yer verilmiş, literatür değerlendirmeleri yapılmıştır. Bölüm 3 'de çalışmada kullanılan materyal ve metotların ne olduğu tartışılmıştır. Bölüm 4 kullanılan metotlarla ilgili kullanıcı makinelerinde yapılan testlerin analizi yer almıştır. Bölüm 5 de ise sonuç ve öneriler kısmı bulunmaktadır.

2. LİTERATÜR

Literatürde sıfır güven mimarisi, sıfır güven ağ mimarisinin bileşenlerinin kimlik doğrulaması, değişik cihazlar üzerinde uygulanışı ve cihaz doğrulamasının sağlanması ile ilgili bazı çalışmalar aşağıda aktarılmıştır.

Eidle ve ark. (2017), sıfır güven mimarisi ile organize olacak şekilde, TCP sessionlarının arasında TAC -Transport Access Control - denilen TCP connection ilk paketinde bir token gönderilmesi konusunu incelemiştir. Samaniego ve ark. (2018), tarafından çalışmada IoT cihazlarındaki artışın beraberinde getirdiği güvenlik risklerini ele alınmış, özellikle kimlik doğrulama alanında Blockchain yapısının kullanılmasını incelemiştir. Vanickis ve ark. (2020), gelişen IoT teknolojilerine paralel olarak IIoT (Industrial Internet of Things) sistemlerindeki gelişmelere değinmiş, bu tür ağlar için bir risk analizin belirlenememesi en büyük handikap olarak görülmüş, sıfır güven mimarisinin mikro segmentasyon özelliği ile risk analizi raporlarının çıkarılmasını incelemiştir. Chen ve ark. (2021), 5G nin sahip olduğu yüksek bant genişliği, düşük gecikme ve aynı anda birden fazla işlem yapabilme kapasitesinde olduğu için medikal alanda kullanılabilmesini incelemiş ayrıca 5g uyumlu akıllı medikal çözümlerde hasta ve hastane verilerinin lokal olarak on-prem den çıkıp bulut ortamına yönelmesi ile sıfır güven mimarisinden yararlanılması ihtiyacı doğurmasına değinilmiştir. Liu ve ark. (2020) usb ya da benzeri cihazlarla taşına bilginin daha güvenli olduğu düşünülmesinin dezavantajları anlatılarak, Elastik Stack açık

kaynak kodlu yazılım üzerinde sıfır güven modellemesinin yapılması ile birlikte biyometrik özelliklerin kimlik doğrulaması için kullanılabilmesi incelenmiştir. Tian ve Song (2021) sıfır güven mimarisinin "asla güvenme, her zaman doğrula" mottosuna ek olarak, "yazmak yok, okumak yok" kavramı ile birleştirip, veri gizliliğinin, bütünlüğünün gerçekleştirilmesini incelemiştir. Bu yöntemin birtakım eksiklikleri olduğu en önemli eksikliğinin ise sistemlere ilk güven değerinin 100 olarak verilmesi yani güvenilmesidir. Sonrasında davranışlara göre risk skorunun yeniden belirlenmesi, belli bir seviye indirilmesi sağlansa bile başlangıç değerinin başlı başına risk olduğu görülmüştür. Yang ve ark. (2021) son dönemlerde popüler bir konu olan IHA (insansız hava araçları)'nın sahtecilik saldırılarına karşı zayıf olduğu, kullanıcı tabanlı kimlik denetimleri gibi klasik doğrulama metotlarının kullanılması da klasik güvenlik zafiyetlerine açık olduğu ifade edilmiştir. IHA üzerinde bir ağ geçidinin kurulması ve IHA'lardaki diğer ağ geçitleri, yer istasyonundaki ağ geçitleri ile sıfır güven mimarisini kullanarak haberleşmesi incelenmiştir. Bu şekilde güvenilir kimliği, bu sistemin çalışabilmesinin garantisi olacağı düşünülmektedir. D'Silva & Ambawade (2021). Sıfır güven mimarisinin tüm OSI katmanları boyunca incelenip avantaj ve dezavantajlarını ifade edilmiş olup, sıfır güven mimarisinin temel bileşenlerinden olan mikro segmentasyonun kubernetes ortamlarına uygulanışı incelenmiştir. Patil ve ark. (2020) dağıtık yapılarda paylaşılan kullanıcı verilerinin izlenmesi, her bir düğüme erişen ve erişim isteği gönderen kullanıcıların kimlik doğrulamasının yapılması için sıfır güven mekanizması uygulanması incelenmiştir. Zhang ve ark. (2021) karma (mesh) topolojilerde güvenlik açısından tehlikeler oluşturmaya başladığına değinilmiştir. Ağların mikro segmentasyonu ile yürüyen sistemin ana parçalarını farklı farklı tutma yeteneği sağlaması incelenmiştir. Yang ve ark. (2018), Büyük veri (big data) teknolojisinin birçok güvenlik riskini beraber getirmekte olduğuna vurgu yapılıp, sıfır güven mimarisinin güvenlik mekanizması ile big data platformlarının üzerinde kullanıcı kimlik doğrulamalarının tanımlanması incelenmiştir. DeCusatis ve ark.(2016), TCP iletişiminde paket isteğine kimlik doğrulama tokenlarının yerleştirilerek ilk paket doğrulaması ile sıfır güven mimarisinin etkisini daha da arttıracağını öngörmüşlerdir. Bunun hem kurumsal bilgi hareketinde hem de bulut tabanlı uygulamalarda güvenlik kavramını derinlemesine incelemişlerdir. Amaral ve ark. (2021), uzun yıllardır bilinen "Siber Tedarik Zinciri (Cyber Supply Chain)" saldırılarına alınması gereken güvenlik önlemlerinin sıfır güven mimarisi ile nasıl entegre olması gerektiğini incelenmiştir. McCarry ve ark. (2021), daha önce test edilmemiş çoklu-bulut (Multi Cloud) ortamlarda sıfır güven mekanizmasının performansını kontrol edebilmek için Istio yazılımını kullanılmasını incelemişlerdir. Xiaojan ve ark.(2021), IoT (Internet of Things - nesnelerin interneti)'ler üzerinde devamlı kimlik kontrolünün yapılması, Erişim kontrol listelerinin tanımlanması konusunda sıfır güven mimarisinden faydalanılması incelenmiştir. Rocha ve ark. (2021), gelişmiş kalıcı tehditler (APT-Advanced Persistent Threats) saldırılarının çok uzun süreçli, emek ve bilgi gerektiren bir saldırı tipi olduğundan bahsedilmiş, APT saldırılarına karşı sıfır güven mimarisi kullanılması incelenmiştir. Dhar ve ark. (2021), IoT yapısının heterojen nitelikte olduğu için mevcut ağ güvenliği araçlarının yetersizliği ve IoT cihazlarına iletilen verileri tehdit eden çok sayıda atak vektörü olduğundan bahsedilmiştir. Bu şekilde yapılanma içerisinde sıfır güven ve block-zincir (block-chain) kullanımı ile IoT cihazlarının güvenliğini sağlanması incelenmiştir. Bertino & Brancik (2021), sıfır güven tasarımındaki zorluklarından özellikle mevcut yapıların geçişinin kolay olmadığı incelenerek analiz çalışmasının dikkatli yapılması konusu vurgulanmıştır. Zhang & Jiang (2021), Internet servis sağlayıcı (ISP) olan firmaların bulut teknolojisini kullanarak SaaS (Software As a Service) olarak sağladığı bu yapıların sıfır güven mimarisi ile kullanılması incelenmiştir. Bicakci ve ark.(2021), USB dongle gibi external cihazların veri taşınmasındaki risk olduğunu, kimlik doğrulamanın tercih edilmesi ve sıfır güven üzerindeki etkisini incelemişlerdir. Ali ve ark. (2021) medikal sistemler için yazılan uygulamaların 5G teknolojisi ile entegre olurken kullanıcı-cihaz, cihaz-cihaz doğrulaması için sıfır güven mimarisi kullanılması incelenmiştir. Koudai ve ark. (2021) Sıfır güven mimarisinin, çevre ağ yaklaşımının önüne geçip, kuruluş kaynaklarının korunması, yetkilendirme kararlarının dinamik verilip, dinamik erişim listeleri ile entegrasyonu incelenmiştir. Meng ve ark. (2022) tarafından incelenen ve China Communications Magazine dergisinde Ağustos 2022 yılında yayınlanan yazı içeriğinde,

Sıfır güven mimarisine farklı bir açıdan bakmayı düşünmüşlerdir. Yazarlara göre, sıfır güven mimarisinde cihazdan cihaza, kullanıcıdan kullanıcıya da uygulamaya sürekli kimlik doğrulama aşamasında bir güven yetkilisine güvenir. (Güven yetkilisi burada cihaz ya da kullanıcıların sertifika ile haberleştiği veri ile kullanıcı arasında bir katman olup, tüm session bazlı bağlantıların üzerinden geçtiği düğüm ya da sunucu olabilir). "Bu güven yetkilisinin güvenirliliğinden nasıl emin olabiliriz?" sorusuna cevap aranmıştır. Sıfır güven mimarisi içinde bu otoritenin yerine blok-zinciri (block-chain)'nin merkeziyetçi olmayan yapısının kullanılmasını incelemişlerdir. Hosney ve ark. (2022) sıfır güven mimarisindeki kimlik doğrulama işleminin BT yöneticilerine getirdiği iş yükünün yapay zeka algoritmaları kullanılarak çözülmesini incelemiştir. Chen ve ark. (2021) Bilgi işlem altyapılarında merkezi olmayan bir kimlik yönetiminin önemine vurgu yapılarak, blok-zinciri (block-chain) mimari çözümünü incelemiştir. Bunun için her nesneye bağımsız ve eşsiz kimlik numarası verilmesi tek yönlü akış şemaları incelenmiştir. Dobrowski & Pacyna (2022), Kuperberg (2020), kimlik yönetim sisteminin dağıtık yapısından dolayı yönetilmesinin zor olacağı belirtilmiştir. Tek noktadan kontrol için blok-zinciri (block-chain) tabanlı sistemlerin kullanılması incelemişlerdir. Kang ve ark. (2022). Tüm erişim listelerinin ve erişim ile ilgili sertifikaların korunduğu ana sunucunun güvenliğini sağlamak için sıfır güven ile entegre edilmesini incelemiştir. Wang ve ark.(2019) tarafından bulut sistemlerinde kullanıcı kimlik doğrulaması için Etherium Blok zinciri tabanlı kullanımını incelenmiştir. Wu ve ark. (2021), erişim kontrollleri ve kimlik yönetiminin fonksiyonlarının sıfır güven mimarisi içinde entegre çalıştırılabilmesi incelemişlerdir. Srour ve ark. (2006) eşlerarası ağ (P2P- peer to peer network)'ların merkezi bir yapısının olmaması sebebiyle oluşan güvenlik açıklıklarına, kendi geliştirdikleri itibar (reputation) servis algoritmasını incelemişlerdir. Fang & Guan (2022) iOS terminallerinin, sıfır güven mimarisini kullanarak, kurumsal kaynaklara erişimi incelenmiştir. Wu ve ark. (2021), Güç Nesnelerin İnterneti (Power Internet of Things) terminallerinin ihtiyaç duyduğu, kullanıcı doğrulaması (user authentication), cihaz doğrulaması (equipment trust), uygulama bütünlüğü (application integrity), veri akışı (flow baselines) işlemlerinin sıfır güven mimarisi ile entegrasyonu incelemişlerdir. Chen ve ark. (2021) Mobil internet hizmetlerinin karşılaştığı güvenlik sorunları incelenmiş, farklı perspektiflerden sıfır güven mimarisi ile entegrasyonu araştırılmıştır. Araştırmalar sonucu ortaya atılan çalışabilirlik alanı (framework) tablolarının gelişen ataklara karşı güncellenerek sıfır güven mimarisine uyarlanmasının ilerleyen çalışmalarda öncü olacağı belirtilmiştir. Syed ve ark. (2022). Sıfır güven mimarisini farklı senaryolar üzerine derinlemesine incelenmiştir. Mikro segmentasyon, kullanıcı ve cihaz doğrulaması konuları ayrıntılı incelenmiştir. Sheikh ve ark. (2021), mevcut kurumsal altyapı ve uygulamaların bulut ortamına taşınması ile sıfır güven mimarisinin bu yapıya uygunluğu incelenmişlerdir. Mikro segmentasyonun ağ ortamlarına uygulanmasını gerek sunucular arasında gerekse uygulamalar arasında geçiş sağlanırken etiketleme (tagged) metodunu incelemişlerdir. Sanal makineler üzerinde yaptıkları testlerde erişim sağlanan sunucu ya da uygulamanın karşılıklı beyaz liste (whitelist) eklenmesi ile ilgili bir çalışma yapılmış, kısmen başarı sağlanmış, nihai durum için gelecek çalışmalara vurgu yapılmıştır.

2.1. Literatür Taraması Sonuçları ve Literatürdeki Boşlukları

Literatür içerisinde çoğunlukla sıfır güven mimarisi/sıfır güven ağ mimarisini mevcut bir teknolojinin yanında o teknolojinin etkisini ve güvenirliliğini arttırmak için kullanılmıştır. Bulut ortamları için nadir olarak ara katman (middleware) yazılımlarını kullanmak zorunda kalınmış uygulamaların güvenliğini sağlama konuları işlenmiştir. Mevcut ağ sisteminin sıfır güven ağ mimarisine dönüştürülmesinde, analiz ve uzun süreli test çalışmalarının önemine vurgu yapılmıştır. Literatür taraması sonucunda, literatür boşlukları;

- Çalışmaların çoğunda popüler olan nesnelerin interneti (Internet of Things-IoT) geliştirilmesi için kullanılmıştır. Verinin tüm erişilebilir olduğu noktada bu çalışmalar yapılmalıdır.

- Çalışmalarda genel olarak sıfır güven ağ mimarisinin saf olarak kullanılmasına değinilmemiştir. Var olan sistemlere entegre olup sistemin güvenliği geliştirmek temel amaç şeklinde düşünülmüştür.
- Organizasyon ve özellikle bu araştırmanın konusu olan kullanıcı ile ilgili yönler araştırmacılar tarafında ihmal edilmiştir. (Aynı zamanda bunun uygulayıcılar tarafından da ihmal edildiği piyasa şartlarında gözlemlenmiştir.)

3. MATERYAL VE METODOLOJİ

Sıfır güven mimarisinin fonksiyonel olarak eyleme dönüşebilmesi için mevcut ağ mimarisinin yeni güvenlik stratejisine göre düzenlenmesi ya da sıfırdan başlangıç için bileşenlerin belirlenmesi gerekmektedir. Ortam olarak hazırlandıktan sonra güvenlik stratejisine uygun kullanıcı erişim güvenliği için metotlara değinilecektir.

3.1. Sıfır Güven Ağ Mimarisine Geçiş Hazırlıkları

Sıfır güven ağ tabanlı bir güvenlik sistemi kurmanın birden fazla yolu vardır.(Chambel, 2020)

- Kuruluş içerisinde kritik aktörlerin belirlenmesi:
  Sıfır güven ağ mimarisini hayata geçirebilmek için ilk yapılacak işlemlerden biri, kuruluşun faaliyet göstermesi için kurumsal konular hakkında bilgi sahibi olunması gerekmektedir. Geliştiriciler veya sistem yöneticileri gibi özel ayrıcalıklara sahip kullanıcılar, öznitelikler veya roller atanırken ek incelemeye ihtiyaç duyar. Pek çok eski güvenlik mimarisinde, bu hesapların tüm kurumsal kaynaklara erişim için kapsamlı izni olabilir. Sıfır güven mimarisi, geliştiricilere ve yöneticilere, erişim davranışı modellerini tanımlamak, günlükleri denetim eylemlerini kullanırken yeterli esnekliğe sahip olmalarına izin vermelidir.

- Kuruluşun sahip olduğu varlıkları tanımlama:
  Sıfır güven ağ mimarisinin temel gereksinimlerinden biri ağ ortamında bulunan ya da ağ ortamına bağlanan cihazları tanımlama ve yönetme becerisidir. Kurumsal varlıkları yönetme yeteneği, sıfır güven mimarisinin başarılı bir şekilde konumlandırılmasının anahtarıdır. Buna donanım bileşenleri (ör. dizüstü bilgisayarlar, telefonlar, IoT cihazları) ve dijital varlıklar (ör. kullanıcı hesapları, uygulamalar, dijital sertifikalar) dahildir. Kuruluşa ait altyapıda bulunan, yeni keşfedilen varlıkları hızlı bir şekilde tanımlama, kategorize etme ve değerlendirilmesine ihtiyaç vardır. Bu şekilde sıfır güven mekanizması kurumsal varlıklardan oluşan bir veri tabanını kataloglamanın ve sürdürmenin ötesine geçer. Aynı zamanda konfigürasyon yönetimi ve izlemeyi de içerir. Bir varlığın mevcut durumunu gözlemleyebilme yeteneği, erişim taleplerini değerlendirme sürecinin bir parçasıdır.

Kurumsal olmayan varlıklar ve kurumun sahip olduğu "gölge BT" olabildiğince kataloglanmalıdır. Bu bilgiler görülebilenleri (örneğin, MAC adresi, ağ konumu) ve yönetici veri girişi ile artırılmış her şeyi içerebilir. Elde edilen veriler sadece erişim kararları için değil, aynı zamanda kuruluş tarafından izleme günlüğü için de kullanılır. Gölge BT, bu kaynakların kuruluşa ait olması, ancak diğer kaynaklar gibi yönetilmemesi nedeniyle özel bir sorun teşkil eder. Belirli sıfır güven mimarisi yaklaşımları (esas olarak ağ tabanlı), bilinemeyen bu yüzden erişim politikalarına dahil edilemeyen sistemler yüzünden uygulanamaz hale gelebilir, çünkü sonradan tespit edilen her bileşenin mimariyi baştan düzenlemeye sebep olması kaosa sebep olabilir.

- Temel süreçlerin belirlenmesi ve yürütme süreci ile ilgili risklerin belirlenmesi:
  İş süreçleri, hangi kaynak erişim taleplerinin verildiği ve reddedildiğini bildirmelidir. Kesintiler büyük olasılıkla tüm organizasyonu olumsuz etkilemeyeceğinden, kuruluş sıfır güven mimarisine ilk geçiş için düşük riskli bir iş süreciyle başlamak isteyebilir. Yeterli deneyim kazandığında, daha kritik iş süreçleri aday olabilir. Bulut tabanlı kaynakları kullanan veya uzaktaki çalışanlar tarafından kullanılan iş süreçleri genellikle sıfır güven mimarisine geçiş için en iyi adaylardır. Kurumsal müşteriler, kurumsal çevreyi (perimeter) buluta yansıtmak veya müşterileri bir VPN aracılığıyla kurumsal ağa getirmek yerine, bulut hizmetlerini doğrudan talep edebilir. Planlayıcılar ayrıca, belirli bir iş süreci için sıfır güven mimarisini uygularken ortaya çıkabilecek performans, kullanıcı deneyimi ve olası artan iş akışı kırılganlığındaki potansiyeli de dikkate almalıdır

3.2 Sıfır Güven Mimarisi İçin Politikalar Oluşturmak

Sıfır güven mimarisine geçiş için iş akışını belirleme süreci birkaç faktöre bağlıdır:

- kuruluş için sürecin önemi,
- etkilenen denek grubu,
- iş akışı için kullanılan kaynakların mevcut durumu.

Varlık veya iş akışına yönelik riske dayalı varlık veya iş akışının değeri, NIST Risk Yönetimi Çerçevesi kullanılarak değerlendirilebilir.

Varlık veya iş akışı tanımlandıktan sonra, kullanılan tüm üst akış kaynaklarını (ör. Kimlik yönetim sistemleri, veri tabanları, mikro hizmetler), alt akış kaynakları (ör. Günlük kaydı, güvenlik izleme) ve varlıkları (ör. Varlık isimleri, hizmet hesapları) belirleyin veya iş akışından etkilenir. Daha sonra, işletme yöneticilerinin aday iş sürecinde kullanılan kaynaklar için kriter setini (kriterlere dayalı teknik yardım kullanılıyorsa) veya güven düzeyi ağırlıklarını (puan temelli teknik yardım kullanılıyorsa) belirlemeleri gerekir. Yöneticilerin değerlendirme aşamasında bu kriterleri göz önünde tutmaları gerekebilir. Politikaların etkili olmasını ancak kaynaklara erişimin tamamen engellememesini sağlamak gereklidir.

3.2.1. İlk kurulum aşaması ve izlenmesi

Kurumsal firmanın iş akışı ve SGM bileşenleri seçildikten sonra, ilk dağıtım başlayabilir. Kuruluş yöneticileri, seçilen bileşenleri kullanarak geliştirilen politikaları uygulamalıdır, ancak ilk başta bir gözlem ve izleme modunda çalışmak isteyebilirler. İlk yinelemelerinde çok az kurumsal politika seti tamamlanmıştır: önemli kullanıcı hesaplarının (ör. Yönetici hesapları) ihtiyaç duydukları kaynaklara erişimi reddedilebilir veya kendilerine atanmış tüm erişim ayrıcalıklarına ihtiyaç duymayabilir.

Yeni iş akışı, politikaların etkili ve uygulanabilir olduğundan emin olmak için bir süre yalnızca raporlama modunda çalıştırılabilir. Bu aynı zamanda kuruluşun temel varlık ve kaynak erişim talepleri, davranışları ve iletişim modellerini anlamasına da olanak tanır. Yalnızca raporlama, çoğu istek için erişimin verilmesi gerektiği anlamına gelir ve bağlantıların günlükleri ve izleri, geliştirilen ilk politika ile karşılaştırılmalıdır. Zorunlu tutulur ve günlüğe kaydedilir, ancak ilk dağıtımdan sonra erişim ilkeleri, iş akışının gerçek etkileşimlerinden veri toplamak için daha esnek olmalıdır. İş akışı için temel aktivite modelleri oluşturulduktan sonra, anormal davranış daha kolay tanımlanabilir. Daha yumuşak bir nitelikte çalışmak mümkün değilse, kurumsal ağ operatörleri günlükleri yakından izlemeli ve operasyonel deneyime dayalı olarak erişim politikalarını değiştirmeye hazırlıklı olmalıdır.

3.2.2. Mikro segmentasyon:

Geleneksel ağ yapılarında kullanıcıları ayırmak için vlan yapıları kullanılır. Bunlar her ne kadar bir güvenlik sınırı oluşturmak için yapılandırılsa bile, aslında teknolojik olarak bunu yapamazlar. Kötü niyetli bir saldırganın vlanlar arasında hareket etmesini önleyemezler. Mikro segmentasyon, ağ üzerinde kullanılan tüm kaynakları erişim kontrolü, güvenlik, şifreleme, paket yönlendirme gibi uygulama ile birleştirerek küçük düğümlere ayırmaktır (Rose ve ark., 2022). Sonuçta, her biri kendi güvenlik politikalarına ve erişim izinlerine sahip olan, erişimi yönetmede esnekliğe izin veren ve şirketlerin ağ içindeki bir tehdidin kontrolsüz yayılımını engellemesini sağlayan çok sayıda ayrılmış segmentasyon oluşur. Bu şekilde uyum ve performans sorunları çözülmüş olur (Rose ve ark., 2022).

3.2.3. Paralel anahtarlama altyapıları

Geleneksel anahtarlama altyapıları doğal olarak ağ üzerinde bir darboğazdır. Bu sebeple güvenli ve verimli ağlar oluşturmak konusunda bize kısıtlı bir yapı sunarlar. Bugün arkasında çok önemli fabric yapıları bulunan Birleşik Anahtarlar (Unified Switch) kullanılmaktadır. Ama asıl sorun anahtarlama altyapısının bilgiyi paralel ve çok çekirdekli (multi core) yapıda işleyememesidir. Zira İşlenen tüm paketlerin yapısı, hedefleri, öncelikleri farklı olacaktır.

Modern dizüstü bilgisayarlarında işletim sistemi merkezli çok çekirdekli yapılar kullandığını biliyoruz. Bu aynı zamanda birden fazla işlemi (process) dağıtık olarak aynı anda yapabilmeyi sağlar. Bu model core anahtarı birden fazla fabric yapıya bölerek verinin paralel işlenmesini amacıyla modern ağlarda da kullanılabilir. Böyle bir yapıda maliyet açısında daha ucuz core yapılar kurularak her bir işlem için mikro anahtarlama yapıları oluşturabilmeye ihtiyaç var.

3.2.4. Tek noktadan merkezi yönetim

Merkezi cihaz yönetimi “komut satırı” günlerinde çok pratik ve mümkün değildi. Şu anda kullanılan genel çözüm çok sayıda bileşenleri tek bir console ekranından yönetmek şeklindedir. Fakat çoğu zaman hedefe bakılmaksızın tüm trafiklerin bir yöne doğru aynalanması (mirroring-span) trafik sıkışıklığına sebep olabilir. Olması gereken ise bileşen altyapısındaki yönetim arayüzü performansını arttırmaktır. Bunun için uç noktalarda ağ öğelerinin her birinin bir her olayı kaydedip analiz edebilmesi ve gerekli trafiği ya da olması gereken logları merkezi bir yapıya yönlendirmesi önem arz etmektedir. Log üreten cihaz en yakın noktada olmak esastır.

3.2.5. Sıfır güven ağ mimarisini genişletmek

Yeterince güven kazandığında ve iş akışı politika belirlendiğinde, kuruluş istikrarlı operasyonel aşamaya girer. Ağ ve varlıklar hala izlenir ve trafik günlüğe kaydedilir. Ancak yanıtlar ve politika değişiklikleri şiddetli olmaması gerektiğinden daha düşük bir tempoda yapılır. İlgili kaynakların ve süreçlerin konuları ve paydaşları da operasyonları iyileştirmek için geri bildirim sağlamalıdır. Bu aşamada, kurumsal yöneticiler sıfır güven mimarisinin dağıtımının bir sonraki aşamasını planlamaya başlayabilir. İş akışı ve çözüm seti belirlenmeli ve ilk politikalar geliştirilmelidir. Bununla birlikte, iş akışında bir değişiklik olursa, çalışan mimarinin yeniden değerlendirilmesi gerekir. Yeni cihazlar, yazılımda yapılan önemli güncellemeler ve organizasyon yapısındaki değişiklikler gibi sistemdeki imzalı değişiklikler, iş akışı, ilke değişikliklerine neden olabilir. Gerçekte, işin bir kısmının zaten yapılmış olduğu varsayımı ile tüm süreç yeniden değerlendirilmelidir.

3.3. Metodoloji

Sıfır güven ağ mimarisi, sıfır güven güvenlik modelinin metodolojisidir. Bu modelin uygulanabilir, görülebilir halidir. Çalışmada işlenen sıfır güven ağ mimarisinde kullanıcı güvenliğinin sağlanması konusu iki metodolojik yaklaşımla ele alınmıştır. İlk adımda sıfır güven ağ mimarisindeki kullanıcı tabanlı erişim politikaları için kipling metodu anlatılmıştır. İkinci adımda ise Forrester sıfır güven ağ metodu anlatılmıştır.

3.3.1. Kipling metodolojisi

Kipling yöntemi, herhangi bir problemi bulmak adına Ne?, Nerede?, Ne zaman?, Nasıl?, Neden?, Kim? sorularını sorarak çözüm hakkında fikirlerimizin genişlemesine yardımcı olur. Bu metod güvenlik çerçevesi (security framework) olarak düşünüldüğünde erişim politikaların belirlenmesinde kullanılabilir. Kipling methodunun 5 adım modellemesini incelersek,

1. Korumanız gereken alanları belirlenmesi: atak arayüzleri (attack surfaces) devamlı gelişmekte ve genişlemektedir. Bu sebeple kuruluş için kritik verilerin neler olduğunu belirlemek, neyi korumamız gerektiğini bilmek açısından önemlidir.
2. Veri trafiği akışlarının haritalanması: kritik verilerin birbirleriyle girdiği etkileşim, ağ boyunca hareket etme şekli (şifreli/şifresiz) belirlenmelidir. Bu şekilde uygulamalar için etkili erişim politikaları yazılabilir.
3. Sıfır güven mimarisinin oluşturulması: kritik verileri belirleme ve veri akışlarının ilişkileri tanımlandıktan sonra, altyapı olarak gelişmiş güvenlik duvarları kullanılarak mikro segmentasyon alanları oluşturulabilir. (mikro segmentasyon, korunacak verilerin güvenli alanlar oluşturularak diğer verilerden ayrılmasıdır).
4. Erişim listelerinin oluşturulması: Bu metod üzerinde bir beyaz liste (white list) oluşturulması gerekiyor. Bu liste metodolojinin sorularına verilen cevaplarla oluşturulacaktır.
    a. Kim – Kaynağa kim erişecek?
    b. Ne - Korunması gereken alan (protect surface) içinde bulunan kaynaklara erişim için kullanılan uygulamalar nedir?
    c. Ne zaman - Kaynak erişimine ne zaman erişim sağlanacak?
    d. Nerede - gönderilen verinin hedefi nedir?
    e. Neden - veri paketi korunan alana neden erişmek istiyor?
    f. Nasıl – Korunan alana erişen uygulamalar bunu nasıl yapıyorlar?
5. Tüm yapının izlenmesi ve bakımının yapılması: ilk 4 adımda uygulanan mimarinin performans değerlendirilmesinin yapılması gerekir. İzleme sırasında elde edilen bazı bulgular sürece dahil edilip bakımı yapılmalıdır.

3.3.2. Forrester sıfır güven ağ metodolojisi

Kullanıcı adı ve şifre bilgisi, mevcut kullanıcıyı tanımlamaktan öte bazı kontroller gerektirir. Bu sebeple her kullanıcı bağlantı girişiminin yeniden değerlendirilmesi önem arz etmektedir. Bu metodoloji de sıfır güven mimarisinde kullanıcıların yapılandırılmasında dikkat edilecek hususlar aşağıdaki gibi sıralanabilir.

- Yetkili kullanıcılarınızı sadece uygulama seviyesinde değil, ağ seviyesinde de kontrol etmek gereklidir.
- Temel olarak single-sign-on yöntemi ile yetkili kullanıcı girişlerini tercih edebilirsiniz. Ortamda bulunan AAA (Authentication, Authorization, Accounting) sunucu ile entegre şekilde çalışabilirsiniz. Bu birden fazla kimlik bilgisi riskini ortadan kaldırır.
- Kullanıcı erişimlerinizi Multifactor authenticaton metotlarıyla güçlendirin. Çok faktörlü kimlik doğrulama (Multi Factor Authentication –MFA) katmanı kritik uygulamalarınıza

erişirken ekstra güvenlik sağlar. Özellikle dış dünyadan bağlanan kullanıcılar veya tanımlı olmayan cihazlarla bağlantı kurulduğunda iyi bir seçenek olabilir.

- Kullanıcı yetkilerini daraltmayı deneyebilirsiniz. Kaynak kullanımında etkinliği azaltmayacak şekilde kuralların belirlenmesi, belli bir zaman diliminde bağlanma, belli bir coğrafi konumdan bağlanabilme ya da erişim türünü belirlenmesi sağlanabilir. (kablolu, kablosuz SSL VPN vb.) Bu kontrollerin tümüne "ortam denetleme" (context inspection) adı verilir.
- Anomali tespiti yapılabilir. Bunun için çeştli loglama/SIEM çözümleri ile de çalışılabilir. Bu şekilde kullanıcının bağlanmasına izin verilmediği durum, başarısız kullanıcı girişimleri takip edilmelidir.
- Sıfır Güven Ağ mimarisinde en önemli kavramlardan biri de görünebilirliktir. Sisteme dahil olan her birim tanımlanmalı, aktivite raporları alınabilmeli, loglanabilmelidir. Bu amaca yönelik merkezi bulut tabanlı sıfır güven ağ teknolojileri daha çok rağbet görmektedir.

Şekil 2. de Forrester sıfır güven ağ modeli ana hatları gösterilmiştir.

Şekil 2. Forrester sıfır güven ağ modeli

4. BULGULAR VE YORUMLAR

Sıfır güven ağ mimarisinde kullanıcı güvenliğinden bahsedilmesi için, genel olarak bazı altyapıların kurulması gerekir. Sıfır güven güvenlik modelini yeni bir güvenlik stratejisi gibi düşünmek gerekmektedir. Bu strateji sıfır güven ağ mimarisinin tasarımı ile eyleme dönüşür.

Gelişmiş özellikli, davranış analizi yapan güvenlik duvarları, yerel ağların küçük parçalara ayrılıp her birinin çevre (perimeter) oluşturulması, erişim kurallarının tanımlanması ve uygulanması, vb. Ancak bir yandan atak vektörlerinin çoğalması, tehditlerin artması sebebiyle, bahsedilen metodolojilerin uygulandığı sektör ürünleri kullanarak aktif bir kuruluş için gerçekleştirdiğim test sonuçları aşağıdadır. Burada öncelikle kullanıcı erişimlerini kontrol etmek için yazılımların genel bir tanımı yapılmıştır.

- Uçbirim algılama ve yanıt yazılımları (Endpoint Detection and Response EDR): Geleneksel antivirüs çözümlerinde güvenlik ürünü devamlı aktif ve potansiyel olarak imzaları ve atak yüzeyleri bilinen güvenlik tehditlerine yönelik tedbirler ve önlem uygular. Diğer taraftan EDR ise daha çok sezgisel özellikleri kullanarak geleneksel antivirüs çözümlerini atlatmaya yönelik yazılmış, belki de daha önce hiç görülmemiş tehditleri algılayabilir.
- Genişletilmiş algılama ve yanıt yazılımları (Extended Detection and response XDR): XDR "birden fazla güvenlik ürününü tüm lisanslı bileşenleri birleştiren uyumlu bir güvenlik işlemleri sistemine yerel olarak entegre eden SaaS tabanlı, satıcıya özgü güvenlik tehdidi algılama ve olay müdahale aracı" olarak tanımlanabilir.

Temel perspektiften bakılırsa her iki (EDR,XDR) çözümün amacı veri görünürlüğü, veri analitiği ve tehdit istihbaratının ortak kullanımı ile otomatik tehdit algılama, yanıt sağlamak için tasarlanmış sistemler olarak da tanımlanabilir. EDR birden fazla uçbirimin bilgilerini toplayıp bunları korele edip ilişkileri anlamaya çalışır. XDR ise EDR kapsamının ötesine giderek uçbirim ile birlikte, bu uçbirimin bağlı bulunduğu sunucu sistemleri ile ilişkisini de analiz eder.

- Yönetilen algılama ve yanıt (Managed Detection and Response MDR): MDR bir teknoloji değildir. Yönetilebilir bir servis olarak kuruluşların uçbirim güvenliği ihtiyacını karşılamaya yönelik hizmettir. Saldırları sürekli izlemek için gerekli uzmanlığa sahip olmayan kuruluşlara büyük değerler sağlar. MDR belli güvenlik hedefleri olan ve bunların sonuçlarının olduğu bir sistem ile tanımlanır.

Kullanıcı erişim güvenliğini test etmek amacıyla, EDR hizmeti veren firma ürünlerini inceledim. Bu ürünlerin yeni versiyonları kullanıcı tarafında sıfır güven mekanizmasını ele alacak şekilde genişlemişlerdir.(Çoğu üretici firmanın EDR ürünü bulunmaktadır, XDR desteği ise çok az üretici firma tarafından desteklenmiştir). Çeşitli parametrelere göre değerlendirmeler Tablo 1 de ifade edilmeye çalışılmıştır.

Tablo1. Kullanıcı Güvenliği Çözümlerinin Karşılaştırılması

Kategori	**Fortinet EDR**	**Checkpoint Harmony**	**SentinelOne EDR**
Üreticinin Pazar yaygınlığı	Fortintet -Türkiye Next Generation Firewall konusunda en yaygın üretici durumundadır. Orta ve Küçük işletmelerde lider konumdadır.	Checkpoint pazardaki en eski firewall üreticisidir. Pazarda ciddi kayıp yaşamasına rağmen, hala üst segment müşteriler için tercih sebebidir.	Türkiye de çok yaygın olmayan bir markadır.
Diğer Güvenlik Ürünleri ile Entegrasyon	EDR ürününün doğal olarak Fortinet -Security Fabric yapısı ile fortinet ürünlerine entegrasyonu var. siğer üreticiler ile API desteğine ihtiyaç duyuyor.	Ürünün chekcpoint cihazları ile uyumu var. Diğer ürünler için API desteği gerekir.	RestFul API desteği var. Diğer ürünlerle bu şekilde konuşabilir.
Ürünün Koruma Yeteneği	Erişim ayarlarında şüpheli (suspicious) engelleme seçeneği mevcut.Dış dünyaya bağlantı açıldığında bağlantıyı açan uygulamanın tanınmadığını belirleyebilir ve engelleme yapabilir.Bu bakımdan diğer ürünlerin çözümlerinden üstün performans sağladığı görüldü. Ek olarak sandboxing işleminin en net fark edildiği ürün olması da diğer avantajıdır.	Checkpoint Harmony test edilen zararlı yazılımları daha çalıştırmadan önce tespit edip silme işlemi gerçekleştirmiştir. Tespit edilen yazılımların sınıflandırılması isabetlidir. Meterpreter payload ı çalıştırılmadan önce engelleyip silmiştir. Ürün üstünde gelen forensic analiz modülünün çoğu zaman başarılı sonuç verdiği görülmüştür. Davranışsal analiz raporlarının başarılı olduğu gözlemlenmiştir.	Kurulu olduğu sistem üzerinde diğerlerine göre daha az kaynak kullanıldığı gözlemlendi. Tespit edilen zararlıların hangi tekniği kullandığı tutarlı bir şekilde verilmiş. Sadece zararlı dosyaları değil, zararlı dosyaların kullandığı zararsız dosyaları da karantinaya aldığı gözlemlendi. Rapor formatı: csv dir. Ajan kurulu makinelerde log toplaması, remote shell session ı alma vb. birçok aksiyona imkan vermektedir. Threat Hunting (her an saldırı anında olduğunu düşünme ve buna uygun aksiyon alma) özelliği mevcut. Analizlerin grafiksel görünümü diğerlerine göre artı bir özellik olarak görülmüştür.

Yönetim Kolaylığı	En büyük dezavantajı ise dashboard yapısı olduğu söylenilebilir. Tespit edilen zararlının grafik olarak incelenmesi kolay değil. Dashboard ekranı kullanıcı dostu değil.	Yönetimi en kolay çözümlerden biridir. Zararlı tespitinin evant graph içinde bulunabilmesi ve analiz edilmesi kolaydır. Kullanıcı ajan ara yüzü diğerlerine göre daha iyidir.	Bu ürünün ara yüzü checkpoint ürünündeki kadar iyi olmasa bile kullanım kolaylığı performansı iyidir. Kullanıcı dağıtımının kolay olması yönetilebilirliğini arttırmaktadır.
Cihaz Kaynak Kullanımı	Ürünün belirteçlerinde vaat edilen kaynak kullanım oranlarını sağlayamaması bir sorundur.	Kaynak kullanımını orta düzeydedir. Donanımı çok düşük makine haricinde performans sorunu çıkarmayacaktır.	Test edilen çözümler arasında en düşük kaynak kullanımı SentinelOne EDR dır. Aynı anda process sayısı çok azdır.

Ürünlerin kullanıcı tarafında yapılan teknik analizi ise Tablo 2 de ifade edilmiştir.

Tablo 2. Ürün Teknik Analiz

Teknik Yetenekler	**Alt Özellik**	**Fortinet EDR**	**Checkpoint Harmony**	**SentinelOne EDR**	**Acronis**
EPP (Endpoint protection)		Çok İyi	Çok İyi	Çok İyi	Orta
EDR / XDR Endpoint Detection and Response / Extended Detection and Response	Mitre Att&CK	Zayıf	Çok İyi	Çok İyi	yok
	Incident Detail	orta	Çok İyi	Çok İyi	yok
	Remedation	İyi	Çok İyi	İyi	İyi
	Network Events	Çok İyi	iyi	iyi	yok
	Ransomware Protection	Çok İyi	Çok İyi	Çok İyi	Çok İyi
	Execution Files Prevention	İyi	iyi	Çok İyi	Kötü
	Exfiltration Prevention	Çok İyi	orta	orta	yok
	XDR	var	yok	var	yok
	Threat Hunting	iyi	iyi	Çok İyi	yok
VA/Scoring (Vulnerability Analysis/Scoring)		orta	yok	iyi	Çok İyi
Inventory	Software	var	var	var	var-sorunlu
	Hardware	var	var	var	var
Device Control		var	var	var	var
Patching		yok	yok	yok	var
Backup & Recovery		yok	yok	yok	var
White Label		var	var	var	var
Forensic Capability		Çok İyi	Çok İyi	Çok İyi	yok
Threat Intelligence (Tehdit İstihbaratı)		Çok İyi	Çok İyi	İyi	İyi
URL Filtering		yok-ayrı web servisi olarak bulunmaktadır.	var	yok	var
Browser Protection		yok	var	yok	yok
Mail Security		yok-ayrı mail servisi olarak bulunmaktadır.	var	yok	var-çalışmıyor
Mobile Threat Defence (MTD)		var	var	yok	yok
Network Security Plug-in		var	var	yok	yok
Sandboxing		var	var	yok	yok
Remote Management		yok	yok	var	var

Kullanıcı ve bilgisayarları sadece kuruluş içerisinde değil, kuruluş dışında da koruma altında olurlar. Sıfır güven ağ mimarisinde, uygulamaların birbiriyle etkileşimi, cihazlar doğrulanması çok önemli olsa da en kritik konu kullanıcı erişimleridir. Atak bir şekilde başlar ama son kullanıcı makinesinde son bulur. Atak yüzeyi engellenmesi, ağ üzerinde yatay harekete engel olur. Bu çalışmadaki asıl amaç ise kullanıcı erişimlerini kontrol edip güvenliğini sağlamak, giriş noktasında saldırganı etkisiz hale getirmektir.

5. SONUÇ VE ÖNERİLER

Sıfır güven ağ mimarisini uygulamak, altyapı veya süreçlerin toptan değiştirilmesinden ziyade bir yolculuktur. Bir kuruluş, en yüksek değerli veri varlıklarını koruyan sıfır güven ilkelerini, süreç değişikliklerini ve teknoloji çözümlerini aşamalı olarak uygulamaya çalışmalıdır. Çoğu kuruluş, devam eden BT modernizasyon girişimlerine yatırım yapmaya devam ederken belirsiz bir süre için hibrit bir sıfır güven/ çevre (perimeter) tabanlı mod da çalışmaya devam edecektir. Sıfır Güven ilkelerine dayalı bir mimariye geçmeyi içeren bir BT modernizasyon planına sahip olmak, bir kuruluşun küçük ölçekli iş akışı geçişleri için yol haritaları oluşturmasına yardımcı olabilir. Kuruluşun bu stratejiye nasıl geçtiği, mevcut siber güvenlik duruşuna ve operasyonuna bağlıdır. Artan tehditler, çoğalan atak ara yüzleri firmaların kendi güvenlik stratejisini değiştiremeden kullanıcılarının bundan zarar görmesine neden olmuştur. En azından kullanıcı operasyonlarında sıfır güven ağ mimarisine uygun olabilecek koruma yazılımları geliştirmişlerdir. Geleneksel yapıların dışında önerilen metodolojinin kullanılması ile saldırgan faaliyeti daha başlamadan bertaraf edilmiştir. Örneğin oltalama (ransomware) ataklarına karşı yaptığım testlerde, %100 başarı elde edilmiştir.

Yakın bir zamana kadar sıfır güven mimarisinin tam anlamıyla ağ ortamlarına uygulanacağını düşünülmemektedir. Ağ güvenlik stratejisini değiştirebilmek için altyapının, uygun olarak hazırlanması gerektiği düşünülmektedir. Peki geçiş esnasında nasıl bir koruma sağlamalıdır? Testlerinin yapıldığı ürünlerin lokal ortamda hizmet veren karşılığı olsa da, tamamen merkezi olarak bulut ortamında kullanılan yapıların bu süreç içerisinde, maliyet ve gelişmiş BT güvenlik personeli açısından daha çok tercih edileceği düşünülmektedir.

Gelecek çalışmalarda, kullanıcı güvenliğinin sağlanması adına elde edilen verilerin, yapay zeka uygulamalarının geliştirilmesinde kullanılacağı düşünülmektedir.

Yazarların Katkısı
Yazarların makaleye katkıları eşit orandadır.

Teşekkür
Makaleyi değerlendiren hakemlere değerli katkılarından dolayı teşekkürü bir borç bilmekteyiz.

Çıkar Çatışması Beyanı
Herhangi bir çıkar çatışması bulunmamaktadır.

Araştırma ve Yayın Etiği Beyanı
Yapılan çalışmada araştırma ve yayın etiğine uyulmuştur.

KAYNAKÇA

Assunção, P. (2019, January, 16-16). A zero trust approach to network security, *Proceedings of the Digital Privacy and Security Conference*. Portugal, 65-72. https://doi.org/10.11228/dpsc.01.01.007

Belal A., Mark A., Gregory & Li, S. (2021, Nov, 24-26). Uplifting Healthcare cyber resilience with a multi-access edge computing zero-trust security model, *31st International Telecommunication Networks and Applications Conference (ITNAC),* Australia, 192-195. https://doi.org /10.1109/ITNAC53136.2021.9652141

Bicakci, K., Uzunay, Y. & Khan, M. (2021, December, 2-3). Towards zero trust: the design and ımplementation of a secure end-point device for remote working, *14th International Conference on Information Security and Cryptology*, Ankara, Türkiye, 28-33. https://doi.org/10.1109/iscturkey53027.2021.9654298

Camphell, M. (2020). Beyond zero trust: Trust is a vulnerability. *Computer*, 53(10), 110-113. https://doi: 10.1109/MC.2020.3011081

Chen, B., Qiao, S., Zhao, J., Liu, D. Shi, X., Lyu, M., Chen, H., & Lu, H. (2021, July, 1-1). A security awareness and protection system for 5g smart healthcare based on zero-trust architecture, *IEEE Internet of Things Journal*, 8(13), China. https://doi.org/10.1109/jiot.2020.3041042

Chen, R., Shu, F., Huang, S., Huang, L., Liu, H., Liu, J., & Lei, K. (2021). BIdm: A Blockchain-Enabled Cross-Domain Identity Management System, *Journal of Communications and Information Networks*, 6(1), 44-58.

Chen, L., Dai, Z., Chen, M., & Li, N.(2021, May, 29-30) *Research on the security protection framework of power mobile ınternet services based on zero trust.* 6th International Conference on Smart Grid and Electrical Automation (ICSGEA), China, 65-68. https://doi.org/10.1109/ICSGEA53208.2021.00021.

Dabrowski, M., & Pacyna, P. (2022, January, 14-16). *Blockchain-based identity discovery between heterogenous identity management systems.* 6th International Conference on Cryptography Security and Privacy (CSP), Poland, 131-137. https://doi.org/10.1109/CSP55486.2022.00032

Dayna, E., Si Ya N., De Cusatis C., & Sager, A. (2017). Autonomic security for zero trust networks, *National Science Foundation under CCDNI Integregation (Area 4): Application Aware Software Defined Networks for Secure Cloud Services*, NY-USA. 288-293. https://doi.org/10.1109/uemcon.2017.8249053

DeCusatis, C., & Liengtiraphani, P., (2016, Nov, 18-20). *Implementing zero trust cloud networks with transport access control and first packet authentication*. IEEE International Conference on Smart Cloud, USA. 5-10. https://doi.org/10.1109/smartcloud.2016.22

Dhar, S., & Bose, I., (2021). Securing Iot devices using zero trust and blockchain, *Journal of Organization Computing and Electronic Commerce*, 31(1), 18-34. https://doi.org/0.1080/10919392.2020.1831870

D'Silva, D., & D. Ambawade, D., (2021, April, 02-04). *Building a zero trust architecture using kubernetes.* 6th International Conference for Convergence in Technology (I2CT), Pune, India. 1-8. https://doi.org/10.1109/I2CT51068.2021.9418203

Elisa Bertino, E., & Brancik, K., (2021, Aralık, 10-14). *Services for zero trust architectures - a research road- map.* IEEE International Conference on Web Services (ICWS), USA, 14-20. https://doi.org/10.1109/ICWS53863.2021.00016

Fang, W., & Guan, X., (2022, March, 04-06). *Research on iOS Remote security access technology based on zero trust.* IEEE 6th Information Technology and Mechatronics Engineering Conference (ITOEC), China. 238-241. https://doi.org/10.1109/ITOEC53115.2022.973-4455

Hatayema, K., Kotani, D., & Okabe, Y. (2021, March, 22-26). *Zero Trust Federation: Sharing Context under User Control towards Zero Trust in Identity Federation*, PerFlow 2021: International Workshop on Persavive Information Flow, Kyoto, Japan, 514-519. https://doi.org/10.1109/PERCOMWORKSHOPS51409.2021.9431116

Hosney, E., Abdel Halim, I.T., & Yousef, A.H. (2022, Mart, 09-10). *An artificial intelligence approach for deploying zero trust architecture (zta)*, 5th International Conference on Computing and Informatics (ICCI), Egypt, 343-350. https://doi.org/10.1109/ICCI54321.2022.9756117

Kang, C., Li, E., Li, Y., Wang, L., Liu, Y., & Han, Z. (2022, May, 27-29). *Dynamic access control architecture distribution master station based on extended trust evaluation*. IEEE 5th International Electrical and Energy Conference (CIEEC), China, 506-510. https://doi.org/10.1109/CIEEC54735.2022.9846041

Kuperberg, M. (2020). Blockchain-based ıdentity management: A survey From the enterprise and ecosystem perspective, *IEEE Transactions on Engineering Management*, 67(4), 1008-1027.

Liu, J.,Wang, H., Xian, M., & Kong,C., (2020, December, 25-27). *A small LAN zero trust network model based on elastic stack*, 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), China. 1075-1078. https://doi.org/10.1109/ICMCCE51767.2020.00236

Melo, T., Amaral, S. & Gondim, J.J.C, (2021, Nov, 18-19). *Integrating zero trust in the cyber supply chain security*, 6th Workshop on Communication Networks and Power Systems (WCNPS 2021), Brasil. https://doi.org/10.1109/WCNPS53648.2021.9626299

Meng, L., Huang, D., An, J., Zhou, X., & Lin,F. (2022). A continuous authentication protocol without trust authority for zero trust architecture, *China Communications Magazine*, 19(8), 198-213.

Patil, A., Karkal, G.,Wadhwa, J., Sawood, M., & Reddy, K.D, (2020, Dec, 10-13). *Design and implementation of a consensus algorithm to build zero trust model*. IEEE 17th India Council International Conference (INDICON), India. https://doi.org/10.1109/indicon49873.2020.9342207

Rodigari, S., O'Shea, D., McCarthy, P., McCarry, M., & McSweeney, S., (2021, Sept, 5-10). *Performance analysis of zero-trust multi-cloud.* IEEE 14th International Conference on Cloud Computing, Ireland. 730-732. https://doi.org/10.1109/cloud53861.2021.00097

Rocha, B.C., Melo, L.P. & Sousa Jr, R.T., (2021, Nov, 18-19). *Preventing APT attacks on LAN networks with connected IoT devices using a zero trust based security*. 6th Workshop on Communication Networks and Power Systems (WCNPS), Brasil https://doi.org/20.2209/wcnps53648.2021.926270

Rose, S., Borchert, O., Mitchell, S. & Connelly, S. (2020), Zero trust architecture, special publication (NIST SP), *National Institute of Standards and Technology*, Gaithersburg, MD, Stafford. https://doi.org/10.6028/NIST.SP.800-207

Samaniego, M. & Deters, R. (2018, July, 2-7). *Zero-trust hierarchical management in IoT*. IEEE International Congress on Internet of Things, Canada, 88-94. https://doi.org/10.1109/ICIOT.2018.00019

Sheikh, N., Pawar M., & Lawrence,W., (2021, May, 10-13). *Zero trust using Network Micro Segmentation.* IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 1-6, https://doi.org/10.1109/INFOCOM-WKSHPS51825.2021.9484645

Srour, L., Kayssi, A., & Chelab, A.(2006, September, 1-1). *Reputation-based algorithm for managing trust in file sharing networks.* 2006 Securecomm and Workshops, Lebanon. 1-10, https://doi.org/10.1109/SECCOMW.2006.359538.

Syed, N. F., Shah, S. W., Shaghaghi,A., Anwar, A., Baig, Z., & Doss,R.,(2022). Zero trust architecture (ZTA): A comprehensive survey, *IEEE Access*, 57143-57179, https://doi.org/ 10.1109/ACCESS.2022.3174679.

Tao,Y., Lei, Z., & Ruxiang, P., (2018, Dec, 11-13). *Fine-grained big data security method based on zero trust model,* 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), China, 1040-1045. https://doi.org/10.1109/ICPADS.2018.00140

Tian, X., & Song, H., (2021). A zero trust method based on BLP and BIBA model, *2021 14th International Symposium on Computational Inteeligence and Design (ISCID)*, 96-100. https://doi.org/10.1109/ISCID52796.2021.00031

Vanickis, R., Jacob, P., Lee, B., & Dehghanzadeh, S. (2020, June, 21-22). *Access control policy enforcement for zero-trust networking.* European Union's Horizon 2020 research and Innovation programme under grant agreement 700071, Ireland.

Wang, S., Pei, R., & Zhang, Y., (2019). EIDM: A ethereum-based cloud user identity management protocol, *IEEE Access Multidisciplinary | Rapid Review | Open Access Journal*, 7, 115281-115291. https://doi.org/10.1109/access.2019.2933989

Wu, G.Y.,Yan, H.W., & Wang, Z.J.,(2021, Aug, 13-15). *Real identity based access control technology under zero trust architecture.* International Conference on wireless Communications and Smart Grid (ICWCSG), China, 18-22. https://doi.org/ 10.1109/ICWCSG53609.2021.00-011

Wu, K., Shi, J.,Guo, Z., Zhang, Z., & Cai,J. (2021, June, 25-27). *Research on security strategy of power ınternet of things devices based on zero trust.* International Conference on Computer Engineering and Application (ICCEA), China, 79-83. https://doi.org/0.1109/ICCEA53728.2021.00023

Xiaojan, Z., Liandong, C., Jie, F., Xiangqun,W., & Qi,W. (2021, Jan, 8-10). *Power IoT security protection architecture based on zero trust framework.* IEEE 5th International Conference on Cryptography, Security and Privacy, China, 166-170. https://doi.org/10.1109/csp51677.2021.9357607

Yang, D., Zhao,Y.,Wu, K., Guo, X., Peng, H. (2021, October 29 - November 1). *An efficient authentication scheme based on zero trust for UAV swarm.* 2021 International Conference on Networking and Network Applications (NaNA), China, 356-360.
https://doi.org/10.1109/NaNA53684.2021.00068

Zhang, F & Jiang, X., (2021, March, 26-28). *The zero trust security platform for data trusteeship,* 2021 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE), China, 1014-1017. https://doi.org/10.1109/AEMCSE51986.2021.00207

Zhang, P., Tian, C.Shang, T., Liu, L., Li, L.,Wang,W., & Zhao,Y. (2021, May, 14-16). *Dynamic access control technology based on zero-trust light verification network model*. IEEE 3rd International Conference on Communications, Information System and Computer Engineering (CISCE), China, 712-715.