# Bulut Güvenliği: Azure ve AWS Platformlarında Güvenlik Mekanizmaları

Bulut Tabanlı Sistemlerde Erişim Süreçleri ve Güvenlik Çözümleri

EYLÜL KAY

# Proje Amacı, Hedefleri ve Kapsamı

Bu proje, bulut tabanlı sistemlerde kullanılan güvenlik mekanizmalarını incelemek, erişim süreçlerini anlamak ve güvenlik sorunlarına çözüm önerileri sunmak amacıyla gerçekleştirilmiştir. Özellikle Microsoft Azure ve Amazon Web Services platformları üzerinde durulmuştur.

## Proje Amacı

Bulut tabanlı sistemlerde kullanılan güvenlik mekanizmalarını incelemek, bu mekanizmalara erişim süreçlerini anlamak ve karşılaşılan güvenlik sorunlarına çözüm önerileri sunmaktır. Özellikle Microsoft Azure ve Amazon Web Services (AWS) platformları üzerinde detaylı analiz yapılmıştır.

## Beklenen Sonuçlar

- Azure ve AWS güvenlik mekanizmalarının detaylı analizi
- Erişim süreçlerinde yaşanan yaygın problemler ve çözüm önerileri
- DevOps entegrasyonu ve IDS/IPS kullanımına dair kapsamlı bilgiler

## İzlenecek Yol

- Bulut platformlarının seçimi (Azure ve AWS)
- Güvenlik mekanizmalarının belirlenmesi (IAM, RBAC, MFA, şifreleme, ağ güvenliği, loglama, IDS/IPS, DevOps entegrasyonu)
- Azure ve AWS'de karşılaşılan problemler ve çözüm önerilerinin araştırılması
- Rapor ve sunum dosyalarının oluşturulması

# Microsoft Azure: Bulut Bilişim Platformunun Özellikleri

Microsoft Azure, Microsoft tarafından sunulan bir bulut bilişim platformudur. Kullanıcılara altyapı (IaaS), platform (PaaS) ve yazılım (SaaS) hizmetleri sağlar. Kurumsal güvenlik, Microsoft ekosistemiyle uyumluluk ve hibrit bulut desteği ile öne çıkar.


## Azure Ne İşe Yarar?

- Uygulama barındırma (Web, mobil, API)
- Veritabanı yönetimi (SQL, NoSQL)
- Makine öğrenmesi ve yapay zeka servisleri
- Depolama (Blob, File Storage)
- Ağ hizmetleri (VPN, Firewall, Load Balancer)
- Güvenlik (Azure Active Directory, MFA, RBAC)
- DevOps entegrasyonu (Azure DevOps, CI/CD)

## Azure Nasıl Kullanılır?

- Azure portal üzerinden kaynak oluşturulur (VM, Database, App Service)
- Azure CLI veya PowerShell ile yönetim yapılabilir
- API ve SDK desteği ile uygulamalara entegre edilir

## Azure Neden Tercih Edilir?

- Microsoft ekosistemiyle uyumlu (Windows Server, Office 365, Active Directory)
- Kurumsal güvenlik ve uyumluluk sertifikaları
- Global veri merkezleri ağı
- Hibrit bulut desteği (On-prem + Cloud)

# AWS: Pazar Lideri Bulut Hizmetleri Platformu

AWS, dünya çapında en yaygın kullanılan bulut platformudur. 200'den fazla tam özellikli hizmet sunar ve milyonlarca müşteriye hizmet verir. Güvenlik, ölçeklenebilirlik ve esneklik konularında sektör standardı belirler.

## AWS Nedir?

Amazon Web Services (AWS), Amazon tarafından sunulan en büyük bulut bilişim platformudur. Pazar liderliği konumunda ve en geniş servis yelpazesine sahiptir. IaaS, PaaS ve SaaS hizmetleri sunar.

## AWS Ne İşe Yarar?

- Compute (EC2 sanal sunucular)
- Depolama (S3, Glacier)
- Veritabanı (RDS, DynamoDB)
- Makine öğrenmesi (SageMaker)
- Ağ hizmetleri (VPC, Route 53)
- Güvenlik (IAM, GuardDuty, WAF)
- Sunucusuz mimari (Lambda)

## AWS Nasıl Kullanılır?

- AWS Management Console üzerinden servisler yönetilir
- AWS CLI ile komut satırından işlem yapılır
- SDK'lar ile uygulamalara entegre edilir

## AWS Neden Tercih Edilir?

- Pazar lideri, çok geniş servis yelpazesi
- Esnek fiyatlandırma (kullandıkça öde)
- Global erişim ve yüksek ölçeklenebilirlik
- Güçlü güvenlik ve uyumluluk

# Bulut Ortamında Çok Katmanlı Güvenlik Mimarisi

Bulut ortamında bir kaynağa erişim, sadece kimlik doğrulama ile bitmez; çok katmanlı bir güvenlik süreci vardır. Bu süreci yedi temel aşamada inceleyebiliriz ve her katman birlikte kapsamlı bir güvenlik sağlar.

**1 Kimlik Doğrulama (Authentication)**

Kullanıcının gerçekten iddia ettiği kişi olduğunu doğrulama. Azure AD, AWS IAM ve MFA kullanımı.

**2 Yetkilendirme (Authorization)**

Kullanıcının hangi kaynaklara hangi düzeyde erişebileceğini belirleme. RBAC ve IAM Policy ile en az yetki prensibi.

**3 Ağ Güvenliği Kontrolü**

Erişim isteğinin güvenli bir ağ üzerinden geldiğini doğrulama. IP kısıtlamaları, NSG, firewall ve VPN kullanımı.

**4 Veri Şifreleme Kontrolü**

Verinin hem aktarımda hem depolamada korunması. TLS/SSL, Azure Key Vault ve AWS KMS ile anahtar yönetimi.

**5 Güvenlik Politikaları ve Uyumluluk**

Kurumsal politikaların uygulanması. Azure Policy ve AWS Config ile otomatik düzeltme mekanizmaları.

**6 İzleme ve Loglama**

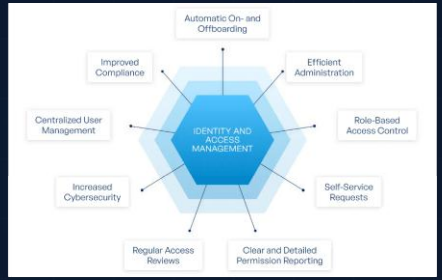
Erişim aktivitelerinin kaydedilmesi ve analiz edilmesi. Azure Monitor, CloudTrail ve SIEM entegrasyonu.

**7 Tehdit Algılama ve Önleme**

Şüpheli aktiviteleri tespit etme ve engelleme. IDS/IPS, Azure Defender ve AWS GuardDuty.

**Özet Güvenlik Akışı**

Kimlik Doğrulama → Yetkilendirme → Ağ Güvenliği → Şifreleme → Politikalar → İzleme → IDS/IPS




# Kimlik Doğrulama: Kullanıcı Kimliğinin Doğrulanması

Kimlik doğrulama (Authentication), kullanıcının gerçekten iddia ettiği kişi olduğunu doğrulama sürecidir. Bulut ortamında güvenliğin ilk ve en kritik adımıdır. Azure ve AWS, güçlü kimlik doğrulama mekanizmaları ve protokolleri sunmaktadır.

## Azure'da Kimlik Doğrulama

- Azure Active Directory (Azure AD): Merkezi kimlik yönetimi ve kullanıcı giriş sistemi
- OAuth 2.0 ve SAML: Modern kimlik doğrulama protokolleri desteği
- Federasyon ve SSO: Tek oturum açma (Single Sign-On) imkanı
- Conditional Access: Koşullu erişim politikaları (IP, cihaz, konum bazlı)

## MFA (Çok Faktörlü Kimlik Doğrulama)

- Şifre + SMS kodu
- Şifre + Authenticator uygulaması
- Biometrik kimlik doğrulama
- Donanım token kullanımı

## AWS'de Kimlik Doğrulama

- IAM Kullanıcıları: AWS Identity and Access Management ile kullanıcı yönetimi
- Federated Login (SSO): SAML 2.0 ve OpenID Connect desteği
- Temporary Security Credentials: Geçici güvenlik kimlik bilgileri kullanımı
- AWS Cognito: Uygulama kullanıcıları için kimlik yönetimi

# Yetkilendirme: Erişim Haklarının Belirlenmesi

Amaç: Kullanıcının hangi kaynaklara ve hangi düzeyde erişebileceğini belirlemek. Kimlik doğrulandıktan sonra, kullanıcının hangi işlemleri yapabileceği yetkilendirme mekanizmaları ile kontrol edilir.

## Azure'da Yetkilendirme (RBAC)

**Rol Tabanlı Erişim Kontrolü (RBAC):** Azure'da yetkilendirme RBAC ile yönetilir.

**Rol →** Belirli izinleri tanımlar (Reader, Contributor, Owner)

**Atama →** Rol, bir kullanıcıya veya gruba atanır

**Kapsam →** Rol hangi kaynakta geçerli? (Subscription, Resource Group, Resource)

*Örnek: "Virtual Machine Contributor" rolü ile sadece VM'leri başlatma, durdurma ve yönetme izni verilir, ancak VM silme yetkisi yoktur.*

## AWS'de Yetkilendirme (IAM Policy)

**IAM Policy:** AWS'de yetkilendirme IAM Policy ile yönetilir.

**Policy →** JSON formatında izinler tanımlanır (s3:GetObject, ec2:StartInstances)

**Atama →** Policy, kullanıcıya, gruba veya role atanır

**Effect →** Allow veya Deny ile izin veya red kararı verilir

*Örnek: "s3:PutObject" izni ile sadece S3 bucket'a dosya yükleme yapılabilir, ancak dosya silme veya bucket ayarlarını değiştirme yetkisi yoktur.*

## En İyi Uygulama: En Az Yetki Prensibi (Least Privilege)

**Tanım:** Kullanıcıya görevini yapabilmesi için minimum gerekli izinler verilir. Fazla yetki verilmesi güvenlik risklerini artırır.

**Neden Önemli?** Fazla yetki → Veri sızıntısı, yanlış yapılandırma, kötüye kullanım riski artar.

- Gereksiz izinleri kaldır: Kullanıcının ihtiyaç duymadığı yetkileri verme
- Zaman sınırlı yetki: Azure PIM (Privileged Identity Management) ile geçici yetki ver
- Düzenli gözden geçirme: Rol ve policy'leri periyodik olarak incele
- Koşullu erişim: IP, cihaz, oturum süresi bazlı kısıtlamalar uygula

# Ağ Güvenliği Kontrolü: Güvenli Ağdan Erişim Doğrulaması

Amaç: Erişim isteğinin güvenli bir ağ üzerinden geldiğini doğrulamak ve yetkisiz veya riskli bağlantıları engellemek. Ağ güvenliği, IP kısıtlamaları, sanal ağ güvenlik grupları, firewall kuralları ve VPN gibi mekanizmalarla sağlanır.

### IP Kısıtlamaları

Mantık: Belirli IP adreslerinden veya IP aralıklarından gelen erişimlere izin verilir.

Azure: Conditional Access Policies ile IP bazlı erişim kısıtlaması

AWS: IAM policy içinde Condition kullanılarak IP kısıtlaması (aws:SourceIp)

### Sanal Ağ Güvenlik Grupları

Azure NSG: Sanal makineler ve alt ağlar için inbound/outbound kuralları tanımlar. Örnek: RDP (3389) sadece şirket IP'lerinden izinli

AWS Security Groups: EC2 instance'lar için inbound/outbound kuralları. Örnek: SSH (22) sadece belirli IP aralığından izinli

### Firewall Kuralları

Azure Firewall: Uygulama ve ağ seviyesinde trafik filtreleme, URL bazlı erişim kontrolü

AWS WAF: HTTP/HTTPS trafiğini filtreler, SQL Injection ve XSS saldırılarına karşı koruma sağlar

### Ekstra Güvenlik ve En İyi Uygulamalar

- VPN veya Özel Bağlantı: Azure ExpressRoute ve AWS Direct Connect ile şirket ağı ile bulut arasında özel, şifreli bağlantı sağlanır
- Zero Trust Yaklaşımı: Her bağlantıyı doğrula, hiçbir ağı otomatik güvenli kabul etme
- IP Whitelisting: Sadece güvenilir IP'lere izin ver
- VPN Zorunluluğu: Özellikle yönetici erişimleri için VPN kullanımını zorunlu kıl
- Düzenli Denetim: NSG ve Security Group kurallarını periyodik olarak gözden geçir

# Veri Şifreleme Kontrolü: Depolama ve Aktarım Güvenliği

Amaç: Verinin hem depolama sırasında (At Rest) hem de aktarılırken (In Transit) korunmasını sağlamak. Şifreleme, yetkisiz erişime karşı kritik bir savunma katmanıdır ve veri ihlallerini önler.

## At Rest (Depolamada Şifreleme)

Tanım: Veriler disk, veritabanı veya depolama alanında şifrelenir.

**Azure'da:**

- Azure Storage Encryption: Blob, File, Queue, Table verileri AES-256 ile şifrelenir
- Disk Encryption: VM diskleri BitLocker veya DM-Crypt ile şifrelenir
- SQL TDE: Veritabanı dosyaları otomatik şifrelenir

**AWS'de:**

- S3 Encryption: Server-Side Encryption (SSE) ile AES-256 veya KMS anahtarları
- EBS Encryption: EC2 diskleri şifrelenir
- RDS Encryption: Veritabanı instance'ları şifrelenir

## In Transit (Aktarımda Şifreleme)

Tanım: Veri ağ üzerinden taşınırken şifrelenir.

**Nasıl Yapılır?**

- TLS/SSL Protokolleri: HTTPS bağlantıları ile veri aktarımı güvence altına alınır
- HTTPS Zorunluluğu: Tüm API ve web trafiği şifreli olmalı

**Azure'da:**

- Azure Front Door: TLS yönetimi ve SSL sertifikaları
- Application Gateway: End-to-end SSL şifreleme

**AWS'de:**

- ELB (Elastic Load Balancer): SSL sertifikaları ile trafik şifreleme
- CloudFront: CDN üzerinden HTTPS zorunluluğu

## Anahtar Yönetimi

Amaç: Şifreleme anahtarlarının güvenli şekilde saklanması ve yönetilmesi kritik öneme sahiptir.

**Azure Key Vault:**

- Anahtar, sertifika ve gizli bilgileri güvenli şekilde saklar
- HSM (Hardware Security Module) desteği
- Erişim kontrolü ve denetim logları

**AWS KMS (Key Management Service):**

- Anahtar oluşturma, rotasyon ve erişim kontrolü
- AWS CloudHSM ile donanım tabanlı anahtar yönetimi
- Otomatik anahtar rotasyonu desteği

## En İyi Uygulamalar

- Müşteri Yönetimli Anahtarlar (CMK): Anahtar kontrolünü müşteriye bırak, daha fazla güvenlik ve uyumluluk sağla
- Anahtar Rotasyonu: Belirli aralıklarla anahtarları değiştir, güvenlik riskini azalt
- Şifreleme Zorunluluğu: Tüm depolama ve veri aktarımında şifreleme politikası uygula
- Uyumluluk: GDPR, ISO 27001, HIPAA gibi standartlara uygun şifreleme kullan
- Şifrelenmemiş Veri Yasakla: Policy ile şifrelenmemiş kaynak oluşturulmasını engelle

# Güvenlik Politikaları: Kurumsal Standartların Uygulanması

Amaç: Kurumsal güvenlik standartlarının (ISO 27001, GDPR, HIPAA vb.) bulut ortamında uygulanmasını sağlamak. Politikalar, bulut kaynaklarının belirli kurallara uymasını sağlar ve otomatik denetim ve düzeltme mekanizmaları ile uyumluluk sürekli kontrol edilir.

## Politika Tanımlama

Politikalar, bulut kaynaklarının belirli kurallara uymasını sağlar.

**Azure Policy:** Kaynak oluşturma ve yönetim sırasında kurallar uygular

- Deny: Uygunsuz kaynak oluşturulmasını engelle
- Audit: Uygunsuz kaynakları raporla
- Append: Kaynağa ek ayar uygula
- Örnek: Tüm VM'lerde disk şifreleme zorunlu

**AWS Config:** Kaynak konfigürasyonlarını sürekli izler

- Uyumsuzluk durumunda uyarı veya düzeltme
- Örnek: S3 bucket'ların public olmaması

## Uyumluluk Denetimi

**Azure:** Azure Security Center → Uyumluluk raporları (ISO, GDPR, HIPAA)
**AWS:** AWS Config + Security Hub → Uyumluluk durumunu gösterir
Düzenli raporlama ve otomatik kontrol mekanizmaları ile uyumluluk sürekli izlenir.

## Otomatik Düzeltme (Remediation)

Mantık: Uyumsuz kaynak tespit edildiğinde otomatik düzeltme yapılır

**Azure:**

- DeployIfNotExists: Eksik ayarı otomatik ekle
- Modify: Mevcut kaynağı düzenle

**AWS:**

- AWS Systems Manager Automation: Uyumsuz kaynakları düzeltir

## Örnek Senaryo: VM Disk Şifreleme Politikası

**Durum:** Şirket politikası gereği tüm VM diskleri şifrelenmeli

**Azure:** Azure Policy ile "Disk Encryption" zorunlu politikası oluşturulur, DeployIfNotExists efekti ile eksik şifreleme otomatik eklenir

**AWS:** AWS Config ile EBS şifreleme kontrol edilir, uyumsuz diskler AWS Systems Manager Automation ile şifrelenir

**Sonuç:** İnsan hatası minimize edilir, uyumluluk otomatik sağlanır

</head>

# İzleme ve Loglama: Güvenlik Aktivitelerinin Kaydı

Amaç: Bulut ortamında gerçekleşen erişim aktivitelerini kaydetmek, analiz etmek ve anormal davranışları tespit etmek. İzleme ve loglama, güvenlik olaylarının tespiti, denetim ve uyumluluk için kritik öneme sahiptir.

## Azure'da İzleme ve Loglama

**Azure Monitor**

Uygulama, altyapı ve ağ performansını izler. Log Analytics ile detaylı sorgular yapılır ve metrikler toplanır.

**Azure Security Center (Defender for Cloud)**

Güvenlik durumunu izler, tehdit algılama ve öneriler sunar. Güvenlik açıklarını tespit eder.

## AWS'de İzleme ve Loglama

**AWS CloudTrail**

API çağrılarını kaydeder (kim, ne zaman, hangi kaynağa erişti?). Uyumluluk ve denetim için kritik bir araçtır.

**AWS CloudWatch**

Performans ve operasyonel metrikleri izler. Alarm ve otomatik aksiyonlar tanımlanabilir.


## SIEM Entegrasyonu

Amaç: Logları merkezi bir yerde toplayıp analiz etmek, anomali tespiti yapmak.

Araçlar: Azure Sentinel (Microsoft'un bulut tabanlı SIEM çözümü), Splunk (log analizi ve korelasyon)

- Azure Monitor veya AWS CloudTrail logları SIEM'e aktarılır
- Korelasyon kuralları ile şüpheli aktiviteler tespit edilir

## En İyi Uygulamalar

- Logları merkezi bir yerde topla ve güvenli şekilde sakla
- Anomali tespiti için makine öğrenmesi tabanlı analiz kullan
- Gerçek zamanlı uyarılar oluştur ve otomatik yanıt mekanizmaları kur
- Uyumluluk için logları belirli süre sakla (örneğin 90 gün veya daha fazla)

# IDS: Saldırıları Tespit Etme Mekanizması

## IDS (Intrusion Detection System) Nedir?

IDS, ağ trafiğini ve sistem aktivitelerini izler, şüpheli davranışları tespit eder. Log analizi, imza tabanlı veya davranış tabanlı tespit yöntemleri kullanılır. Örneğin, bir kullanıcı kısa sürede çok sayıda başarısız giriş yaparsa alarm oluşturur. Bulut ortamında IDS genellikle uyarı üretir, ancak aksiyon almaz.

## Tespit Yöntemleri

### İmza Tabanlı Tespit

Bilinen saldırı imzalarını tanır ve tespit eder. Saldırı desenleri veritabanında kayıtlıdır. Hızlı ve doğru tespit sağlar ancak yeni saldırıları tespit edemez.

### Davranış Tabanlı Tespit

Anormal davranışları tanır. Normal kullanıcı davranışlarından sapmaları tespit eder. Yeni saldırıları tespit edebilir ancak yanlış pozitif oranı yüksek olabilir.

### Anomali Tabanlı Tespit

Normal davranıştan sapmaları tespit eder. Makine öğrenmesi ve istatistiksel analiz kullanır. Bilinmeyen tehditleri tespit edebilir.

### Azure'da IDS

- Microsoft Defender for Cloud: Sanal makineler, veri tabanları ve ağ trafiği için tehdit analizi yapar
- Davranış Tabanlı Anomali Tespiti: Makine öğrenmesi ile anormal davranışları tespit eder
- Azure Sentinel: SIEM ve SOAR yetenekleri ile merkezi tehdit tespiti
- Öneriler ve Raporlama: Tespit edilen tehditlere yönelik öneriler sunar

### AWS'de IDS

- AWS GuardDuty: Makine öğrenmesi ile anormal davranışları tespit eder ve sürekli izleme sağlar
- VPC Flow Logs: Ağ trafiğini analiz eder ve şüpheli aktiviteleri tespit eder
- CloudTrail: API aktivitelerini izler ve anormal erişimleri tespit eder
- Threat Intelligence: Tehdit istihbaratı ile bilinen kötü amaçlı IP'leri tespit eder

# IPS: Saldırıları Engelleme Mekanizması

## IPS (Intrusion Prevention System) Nedir?

IPS, IDS'nin bir adım ötesi; saldırıyı otomatik olarak engeller. Şüpheli trafiği otomatik olarak bloklar. Örneğin, SQL Injection denemesi tespit edilirse HTTP isteği engellenir. Bulut ortamında IPS, tehditleri gerçek zamanlı olarak etkisizleştirir ve güvenlik ihlallerini önler.

## Engelleme Yöntemleri

### Trafik Filtreleme

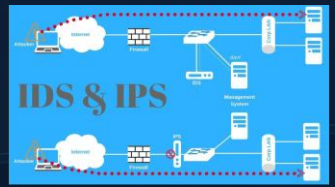
Şüpheli trafiği engelle. Kötü amaçlı IP'lerden gelen istekleri otomatik olarak bloklar. Firewall kuralları ile entegre çalışır.

### Oturum Sonlandırma

Şüpheli bağlantıyı kes. Anormal aktivite tespit edildiğinde kullanıcı oturumunu otomatik olarak sonlandırır.

### Otomatik Yanıt

Saldırıya otomatik olarak yanıt ver. Lambda fonksiyonları veya Azure Automation ile anında aksiyon alınır.





## Azure'da IPS

- Azure Firewall + WAF: Web uygulamalarını SQL Injection, XSS gibi saldırılara karşı korur ve otomatik olarak engeller
- Microsoft Defender for Cloud: Otomatik düzeltme aksiyonları ile tehditleri etkisizleştirir
- Threat Intelligence: Tehdit istihbaratı ile proaktif koruma sağlar ve bilinen kötü amaçlı IP'leri bloklar
- Azure DDoS Protection: DDoS saldırılarına karşı otomatik koruma ve trafik filtreleme

## AWS'de IPS

- AWS WAF (Web Application Firewall): Web saldırılarını engeller, SQL Injection ve XSS gibi tehditleri otomatik bloklar
- Network ACLs: Ağ seviyesinde trafik engelleme ve güvenlik kuralları uygulama
- GuardDuty + Lambda Integration: Otomatik yanıt mekanizmaları ile tehditleri hızlı şekilde etkisizleştirir
- AWS Shield: DDoS saldırılarına karşı otomatik koruma ve trafik yönetimi

## IDS vs IPS: Temel Fark

IDS: Tespit eder ve uyarı verir (pasif)
IPS: Tespit eder ve otomatik engeller (aktif)

Bulut ortamında her ikisi de birlikte kullanılır ve kapsamlı güvenlik sağlar.

# DevSecOps: Güvenliğin CI/CD Pipeline Entegrasyonu

## DevSecOps Nedir?

DevOps + Security = DevSecOps. Güvenliği yazılım geliştirme sürecinin her aşamasına entegre etme yaklaşımıdır. "Security as Code" prensibi ile güvenlik testleri ve otomatik taramalar CI/CD pipeline'larına dahil edilir. Böylece güvenlik açıkları erken tespit edilir ve düzeltilir.

## CI/CD Pipeline'larında Güvenlik Testleri

### SAST

Statik Kod Analizi: Kaynak kodda güvenlik açıklarını tarar. SQL Injection, XSS gibi açıkları tespit eder.

### DAST

Dinamik Kod Analizi: Çalışan uygulamada güvenlik açıklarını tarar. Runtime sırasında test eder.

### Bağımlılık Taraması

Kullanılan kütüphanelerdeki güvenlik açıklarını tarar. CVE veritabanı ile kontrol eder.

### Konteyner Taraması

Docker image'larında güvenlik açıklarını tarar. Base image ve layer güvenliğini kontrol eder.

### Azure DevOps Güvenlik

- Azure Pipelines: CI/CD pipeline'larında güvenlik testleri
- Azure Security Center: Kod kalitesi ve güvenlik analizi
- Dependency Check: Bağımlılıkların güvenlik açıklarını tarar
- Azure Key Vault: Gizli bilgilerin güvenli yönetimi

### AWS DevSecOps

- AWS CodePipeline: CI/CD pipeline'larında güvenlik testleri
- AWS CodeBuild: Güvenlik taramaları ve testler
- Amazon Inspector: EC2 instance'larında güvenlik açıklarını tarar
- AWS Secrets Manager: Gizli bilgilerin güvenli yönetimi

### En İyi Uygulamalar

- Güvenlik testlerini otomatikleştir
- Her commit'te güvenlik taraması yap
- Güvenlik açıkları bulunursa pipeline'ı durdur
- Güvenlik raporlarını düzenli incele
- Güvenlik eğitimini geliştirme ekibine ver
- Shift-Left yaklaşımı benimse

# Azure VM Erişim Senaryosu: Çok Katmanlı Güvenlik Uygulaması

## Senaryo: Kullanıcı Azure'da Bir VM'ye Erişmek İstiyor

Bir şirket çalışanı, Azure'da barındırılan bir sanal makineye (VM) RDP üzerinden bağlanmak istiyor. Bu erişim sırasında yedi katmanlı güvenlik süreci devreye girer ve her katman kullanıcının kimliğini doğrular, yetkilerini kontrol eder ve erişimi loglar.

### 1 Kimlik Doğrulama (Authentication)

**Azure AD:** Kullanıcı kimliğini doğrular. Kullanıcı adı ve parola ile giriş yapılır, MFA (Multi-Factor Authentication) ile ek güvenlik sağlanır. Azure AD, kullanıcının kimliğini doğruladıktan sonra bir token üretir.

### 2 Yetkilendirme (Authorization)

**Azure RBAC:** Kullanıcının VM'ye erişim yetkisi olup olmadığını kontrol eder. "Virtual Machine Contributor" rolü gibi roller atanır. Kullanıcının rolü yoksa erişim reddedilir.

### 3 Ağ Güvenliği (Network Security)

**NSG (Network Security Group):** RDP trafiğine izin verilip verilmediğini kontrol eder. Sadece belirli IP adreslerinden gelen RDP isteklerine izin verilir. Uygun kural yoksa bağlantı engellenir.

### 4 Veri Şifreleme (Encryption)

**TLS/SSL:** RDP bağlantısı TLS ile şifrelenir. VM'deki veriler Azure Disk Encryption ile korunur. Şifreleme anahtarları Azure Key Vault'ta güvenli şekilde saklanır.

### 5 Güvenlik Politikaları (Policies)

**Azure Policy:** VM'nin güvenlik standartlarına uygun olup olmadığını kontrol eder. Disk şifreleme zorunlu mu? Güncellemeler yapılmış mı? Uyumsuzluk varsa uyarı verilir veya erişim engellenir.

### 6 İzleme ve Loglama (Monitoring)

**Azure Monitor:** Kullanıcının VM'ye erişimi loglanır. Kim, ne zaman, hangi IP'den erişti? Anormal aktivite tespit edilirse uyarı oluşturulur ve güvenlik ekibine bildirilir.

### 7 Tehdit Algılama (Threat Detection)

**Azure Defender:** Şüpheli aktiviteleri tespit eder. Beklenmedik bir IP'den giriş yapılıyorsa veya anormal komutlar çalıştırılıyorsa alarm üretilir. Gerekirse erişim otomatik olarak engellenir.

### ✓ Sonuç: Erişim Başarılı

Tüm katmanlar başarıyla geçildiğinde kullanıcı VM'ye erişir. Her adım loglanır ve denetim için kaydedilir. Herhangi bir katmanda sorun olursa erişim reddedilir ve güvenlik ekibine bildirim gönderilir.

## Öğrenilen Dersler ve Faydalar

- Çok Katmanlı Koruma: Tek bir katman başarısız olsa bile diğer katmanlar güvenliği sağlar
- Otomatik Denetim: Her erişim kaydedilir, uyumluluk raporları otomatik oluşturulur
- Proaktif Tehdit Tespiti: Anormal davranışlar gerçek zamanlı tespit edilir ve engellenir
- Minimum Yetki Prensibi: Kullanıcılar sadece ihtiyaç duydukları kaynaklara erişebilir
- Uyumluluk: Güvenlik standartlarına (ISO 27001, GDPR) otomatik uyum sağlanır

# AWS S3 Dosya Yükleme Senaryosu: Erişim Kontrolü

## Senaryo

Bir kullanıcı AWS S3 bucket'a dosya yüklemek istiyor. Yedi katmanlı güvenlik süreci devreye girer ve her aşamada farklı güvenlik kontrolleri yapılır.

### 1. Authentication (Kimlik Doğrulama)

**AWS IAM + MFA:** Kullanıcı AWS Console'a giriş yapar, IAM kullanıcı adı ve şifre ile kimlik doğrular. MFA (Multi-Factor Authentication) ile ek güvenlik katmanı sağlanır.

### 2. Authorization (Yetkilendirme)

**IAM Policy:** Kullanıcının S3 bucket'a dosya yükleme yetkisi kontrol edilir. IAM policy'de "s3:PutObject" izni olmalı. Yetkisiz kullanıcılar engellenir.

### 3. Network Security (Ağ Güvenliği)

**VPC Endpoint + Security Groups:** S3'e erişim VPC Endpoint üzerinden yapılır, internet'e çıkmadan güvenli erişim sağlanır. Security Groups ile trafik filtrelenir.

### 4. Encryption (Şifreleme)

**S3 SSE + TLS:** Dosya yükleme sırasında HTTPS (TLS) ile aktarım şifrelenir. S3'te depolandığında Server-Side Encryption (SSE-S3 veya SSE-KMS) ile şifrelenir.

### 5. Policy Control (Politika Kontrolü)

**S3 Bucket Policy + AWS Config:** Bucket policy ile public erişim engellenir. AWS Config ile bucket'ın şifreleme ve erişim ayarları sürekli kontrol edilir.

### 6. Monitoring & Logging (İzleme ve Loglama)

**CloudTrail + CloudWatch:** Dosya yükleme işlemi CloudTrail'de loglanır (kim, ne zaman, hangi dosya). CloudWatch ile anormal aktiviteler izlenir ve alarm oluşturulur.

### 7. Threat Detection (Tehdit Algılama)

**GuardDuty + Macie:** GuardDuty anormal S3 erişimlerini tespit eder. Macie yüklenen dosyalarda hassas veri (PII, kredi kartı) tarar ve uyarı verir.

## Sonuç ve Faydalar

- Çok Katmanlı Koruma: Her katman farklı bir güvenlik kontrolü sağlar
- Otomatik Denetim: AWS Config ve CloudTrail ile sürekli izleme
- Veri Güvenliği: Hem aktarımda hem depolamada şifreleme
- Uyumluluk: GDPR, HIPAA gibi standartlara uygun
- Hızlı Müdahale: Anomali tespiti ile anında aksiyon

# Azure ve AWS Güvenlik Araçlarının Karşılaştırması

| | Azure | AWS |
|---|---|---|
| **Kimlik Doğrulama ve Yetkilendirme** | **Azure Active Directory (AAD):** Kimlik yönetimi, SSO, MFA<br>**RBAC:** Rol tabanlı erişim kontrolü<br>**Conditional Access:** Koşullu erişim politikaları | **AWS IAM:** Kimlik ve erişim yönetimi, MFA<br>**IAM Policies:** Detaylı erişim kontrolü<br>**AWS Organizations:** Merkezi hesap yönetimi |
| **Ağ Güvenliği** | **Azure Firewall:** Yönetilen bulut güvenlik duvarı<br>**NSG (Network Security Groups):** Ağ trafiği filtreleme<br>**Azure DDoS Protection:** DDoS saldırı koruması | **AWS WAF:** Web uygulama güvenlik duvarı<br>**Security Groups & NACLs:** Ağ erişim kontrolü<br>**AWS Shield:** DDoS saldırı koruması |
| **Veri Şifreleme ve Anahtar Yönetimi** | **Azure Key Vault:** Anahtar ve sertifika yönetimi<br>**Azure Storage Encryption:** AES-256 şifreleme<br>**Disk Encryption:** VM disk şifreleme | **AWS KMS:** Anahtar yönetim servisi<br>**S3 Encryption:** Server-side ve client-side şifreleme<br>**EBS Encryption:** Disk şifreleme |
| **İzleme ve Loglama** | **Azure Monitor:** Performans ve log izleme<br>**Log Analytics:** Merkezi log analizi<br>**Azure Sentinel:** SIEM ve SOAR çözümü | **AWS CloudWatch:** Metrik ve log izleme<br>**AWS CloudTrail:** API aktivite kaydı<br>**AWS Security Hub:** Merkezi güvenlik yönetimi |
| **Tehdit Algılama ve Önleme** | **Microsoft Defender for Cloud:** Tehdit algılama ve koruma<br>**Azure WAF:** Web uygulama güvenlik duvarı<br>**Threat Intelligence:** Tehdit istihbaratı entegrasyonu | **AWS GuardDuty:** Tehdit algılama servisi<br>**AWS WAF:** Web uygulama güvenlik duvarı<br>**Amazon Inspector:** Güvenlik açığı değerlendirmesi |
| **Uyumluluk ve Politika Yönetimi** | **Azure Policy:** Politika tanımlama ve uygulama<br>**Compliance Manager:** Uyumluluk raporlama<br>**Blueprints:** Standart yapılandırma şablonları | **AWS Config:** Kaynak konfigürasyon izleme<br>**AWS Audit Manager:** Uyumluluk denetimi<br>**Service Control Policies:** Organizasyon seviyesi politikalar |

# Yaygın Güvenlik Sorunları ve Çözüm Önerileri

## 1. Yanlış Yapılandırma (Misconfiguration)

**Problem:**

S3 bucket'ları public açık, güvenlik grupları çok geniş, şifreleme kapalı. Bulut ortamında en yaygın güvenlik açığıdır.

**Çözüm:**

- Azure Policy ve AWS Config ile otomatik kontrol
- Infrastructure as Code (IaC) kullan
- Düzenli güvenlik denetimleri yap

## 2. Yetkisiz Erişim

**Problem:**

Zayıf kimlik doğrulama, aşırı geniş yetkiler, MFA eksikliği. Kullanıcılar gerekenden fazla yetkiye sahip.

**Çözüm:**

- MFA zorunlu hale getir
- Least Privilege prensibini uygula
- RBAC ile rol tabanlı erişim kontrolü
- Düzenli erişim gözden geçirmeleri yap

## 3. Veri İhlalleri

**Problem:**

Şifrelenmemiş veri, yetersiz erişim kontrolü, veri sızıntısı. Hassas veriler korumasız bırakılıyor.

**Çözüm:**

- Tüm verileri şifrele (at rest ve in transit)
- DLP (Data Loss Prevention) araçları kullan
- Veri sınıflandırması yap
- Erişim loglarını düzenli incele

## 4. Eksik İzleme ve Loglama

**Problem:**

Loglar toplanmıyor, uyarılar yok, anomali tespiti eksik. Güvenlik olayları fark edilmiyor.

**Çözüm:**

- Azure Monitor ve CloudTrail'i aktif et
- SIEM entegrasyonu kur
- Gerçek zamanlı uyarılar oluştur
- Anomali tespiti için ML kullan

## 5. Uyumsuzluk (Compliance)

**Problem:**

GDPR, ISO 27001, HIPAA gibi standartlara uyumsuzluk. Yasal yükümlülükler yerine getirilmiyor.

**Çözüm:**

- Azure Security Center ile uyumluluk raporları
- AWS Config ile sürekli uyumluluk kontrolü
- Düzenli denetim ve raporlama

## 6. Güvenlik Açıkları ve Yamalar

**Problem:**

Güncel olmayan sistemler, yamalanmamış güvenlik açıkları, eski kütüphaneler kullanımı.

**Çözüm:**

- Otomatik yama yönetimi kur
- Bağımlılık taraması yap
- Vulnerability scanning araçları kullan

# Bulut Güvenliğinde En İyi Uygulamalar

1

### Çok Katmanlı Güvenlik Yaklaşımı (Defense in Depth)

Tek bir güvenlik katmanına güvenme. Kimlik doğrulama, ağ güvenliği, şifreleme, izleme ve tehdit algılama gibi birden fazla katman kullan. Her katman bir önceki katmanı destekler.

2

### En Az Yetki Prensibi (Principle of Least Privilege)

Kullanıcılara ve servislere sadece ihtiyaç duydukları minimum yetkileri ver. RBAC ve IAM ile detaylı erişim kontrolü uygula. Gereksiz yetkilendirme güvenlik riskini artırır.

3

### Şifreleme Zorunluluğu (Encryption Everywhere)

Tüm verileri hem depolamada (At Rest) hem de aktarımda (In Transit) şifrele. Azure Key Vault ve AWS KMS ile anahtar yönetimi yap. Şifrelenmemiş veri oluşturulmasını politikalarla engelle.

4

### Sürekli İzleme ve Loglama (Continuous Monitoring)

Tüm aktiviteleri logla ve merkezi bir yerde topla. Azure Monitor, CloudTrail ve SIEM araçları kullan. Gerçek zamanlı uyarılar oluştur ve anormal davranışları hızlıca tespit et.

5

### Otomatik Güvenlik Testleri (DevSecOps)

Güvenlik testlerini CI/CD pipeline'larına entegre et. SAST, DAST, bağımlılık taraması ve konteyner taraması yap. Güvenlik açıklarını erken tespit et ve düzelt.

6

### Düzenli Güvenlik Denetimleri (Regular Audits)

Güvenlik yapılandırmalarını düzenli olarak gözden geçir. Uyumluluk raporlarını incele ve iyileştirmeler yap. Penetrasyon testleri ile güvenlik açıklarını proaktif şekilde tespit et.

7

### Güvenlik Eğitimi ve Farkındalık (Security Training)

Geliştirme ve operasyon ekiplerine düzenli güvenlik eğitimi ver. Phishing, sosyal mühendislik ve güvenli kodlama pratiklerini öğret. İnsan faktörü güvenliğin en zayıf halkasıdır.

8

### Yedekleme ve Felaket Kurtarma (Backup & DR)

Düzenli yedekleme yap ve felaket kurtarma planı oluştur. Yedekleri farklı bölgelerde sakla. Ransomware saldırılarına karşı korunmak için yedekleri test et ve geri yükleme sürecini dene.

9

### Uyumluluk ve Politika Yönetimi (Compliance)

Kurumsal güvenlik standartlarını (ISO 27001, GDPR, HIPAA) bulut ortamında uygula. Azure Policy ve AWS Config ile otomatik uyumluluk kontrolü yap. Uyumsuzlukları otomatik düzelt.

10

### Zero Trust Yaklaşımı (Never Trust, Always Verify)

Hiçbir kullanıcıya veya cihaza varsayılan olarak güvenme. Her erişim talebi doğrulansın. MFA, koşullu erişim ve sürekli kimlik doğrulama kullan. Ağ konumuna değil, kimliğe güven.

# Sonuç: Çok Katmanlı Yaklaşım ve Sürekli İyileştirme

## Bulut Güvenliğinde Başarının Anahtarı

Bulut güvenliği, **tek bir araç veya teknoloji ile sağlanamaz**. Azure ve AWS platformlarında güvenlik, **çok katmanlı bir yaklaşım** gerektirir. Kimlik doğrulama, yetkilendirme, ağ güvenliği, şifreleme, politika yönetimi, izleme ve tehdit algılama katmanları birlikte çalışarak kapsamlı koruma sağlar. Her katman bir öncekini destekler ve tek bir katman başarısız olsa bile diğerleri güvenliği sürdürür.

### Çok Katmanlı Güvenlik

Defense in Depth prensibi ile yedi katmanlı güvenlik süreci uygula. Her katman farklı bir kontrol noktası sağlar ve birlikte kapsamlı koruma oluşturur.

### Otomasyon ve DevSecOps

Güvenliği yazılım geliştirme sürecine entegre et. CI/CD pipeline'larında otomatik güvenlik testleri yap ve insan hatasını minimize et.

### Sürekli İzleme

Tüm aktiviteleri logla, SIEM araçları ile merkezi analiz yap. Gerçek zamanlı uyarılar oluştur ve anormal davranışları hızlıca tespit et.

### Eğitim ve Farkındalık

Ekibi sürekli eğit. Güvenlik sadece teknik bir konu değil, kültürel bir yaklaşımdır. İnsan faktörü güvenliğin en zayıf halkasıdır.

### Uyumluluk ve Politika

Kurumsal güvenlik standartlarını (ISO 27001, GDPR, HIPAA) otomatik uygula. Azure Policy ve AWS Config ile sürekli uyumluluk sağla.

### Sürekli İyileştirme

Güvenlik hiç bitmeyen bir süreçtir. Düzenli denetimler yap, yeni tehditlere karşı hazırlıklı ol ve güvenlik süreçlerini sürekli geliştir.

## Temel Mesaj

Azure ve AWS, güçlü güvenlik araçları sunar ancak bu araçların doğru yapılandırılması ve etkin kullanılması kritik öneme sahiptir. Bulut güvenliği, teknoloji, süreç ve insanların birlikte çalıştığı bütünsel bir yaklaşım gerektirir. Proaktif olun, otomasyona yatırım yapın ve güvenliği her zaman öncelik haline getirin.

**"Güvenlik bir hedef değil, sürekli bir yolculuktur."**