

3-200

HİZMET
KATALOĞU · 2026

Kubernetes, DevSecOps, MLOps ve Yapay Zekâ Güvenliği

Kurulumdan yönetime, model geliştirmeden güvenli kullanıma: modern uygulama ve yapay zekâ altyapıları için uçtan uca teknoloji hizmetleri.

DEVSECOPS / KUBERNETES · OPENSIFT / MLOPS · KUBEFLOW / YAPAY ZEKÂ GÜVENLİĞİ

Genel bakış

Dört hizmet, bütünleşik bir teknoloji yaklaşımı

Modern uygulama ve yapay zekâ altyapılarını kuruyor, işletiyor ve güvenli kullanımı destekliyoruz. Hizmetler birlikte veya tek tek alınabilir.

01

DevSecOps & CI/CD

Güvenlik taramaları, statik kod analizi ve uyumluluk kontrollerini pipeline'a entegre ederek her deploy'u otomatik denetleyen süreçler.

GITLAB CI · JENKINS · ARGO CD · TEKTON · SONARQUBE

02

Kubernetes / OpenShift

Production seviyesinde cluster kurulumu; kimlik yönetimi, izleme, gelişmiş ağ, çoklu cluster yönetimi ve felaket kurtarma entegrasyonları.

RKE2 · KUBEADM · OPENSIFT · CILIUM · VELERO

03

MLOps / Kubeflow

GPU kaynak yönetiminden model eğitime, deney takibinden production'a alma sürecine kadar tüm ML yaşam döngüsü tek platformda.

KUBEFLOW · KSERVE · KATIB · MLFLOW · NVIDIA MIG

04

Yapay Zekâ Güvenliği ve Kullanım Denetimi

Geliştirdiğimiz ürün, kurumsal yapay zekâ kullanımını denetler; hassas bilgilerin kurum dışına aktarılmasını önlemeye yönelik koruma sağlar.

Araç ve platform örnekleri

DevSecOps: GitLab CI · Jenkins · Argo CD · Tekton · SonarQube / Kubernetes: RKE2 · Kubeadm · OpenShift · Cilium · Velero / MLOps: Kubeflow · KServe · Katib · MLflow · NVIDIA MIG

Neden container tabanlı altyapı?

- VM'e kıyasla daha yüksek kaynak verimliliği; donanım ve lisans ihtiyacı azalır
- Otomatik yeniden başlatma, otomatik ölçekleme ve kesintisiz güncelleme
- Standartlaşmış deploy süreçleri; insan hatasına bağımlılık azalır
- Ekipler altyapı yerine ürüne odaklanır

Kimler için uygun?

- Birden fazla mikro servis işleten yazılım ekipleri
- Sık deploy çıkan ürün ekipleri
- Altyapı maliyetini optimize etmek isteyen kurumlar
- DevOps / DevSecOps olgunluğunu artırmak isteyenler
- ML / yapay zeka projeleri yürüten veya planlayan birimler
- Yapay zekâ kullanımını denetlemek ve kurumsal bilgilerini korumak isteyenler

MALİYET AVANTAJI VM tabanlı altyapıdan Kubernetes'e geçişte, pek çok kurumun deneyimine göre altyapı maliyetlerinde %40-70 arasında tasarruf sağlanabilmektedir.

DevSecOps danışmanlığı

DevSecOps; geliştirme (Dev), güvenlik (Sec) ve operasyon (Ops) süreçlerini tek bir entegre pipeline altında birleştiren bir metodoloji ve kültürdür. Güvenlik kontrollerini yazılım geliştirme döngüsünün en başından itibaren otomatize ederek hız ve güvenliği aynı anda sağlar.

KOD → BUILD → STATİK ANALİZ → GÜVENLİK TARAMASI → UYUMLULUK KONTROLÜ → DEPLOY

Her commit ve her deploy, pipeline içinde otomatik olarak denetlenir.

Ne katar?

- Güvenlik taramaları, statik kod analizi ve uyumluluk kontrolleri pipeline'a entegre edilir; her deploy otomatik denetlenir
- Tüm deploy süreçleri standart hale gelir, insan hatasına bağımlılık azalır
- Geliştirici ekipler altyapı ile uğraşmak yerine ürüne odaklanır
- Güvenlik, sürecin sonunda değil en başında devreye girer

Ne sunuyoruz?

- Sıfırdan DevSecOps pipeline kurulumu; kurumun kendi altyapısında ya da cloud'da
- Mevcut pipeline'ların yönetimi, optimizasyonu ve geliştirilmesi
- Yeni araç ve entegrasyonların eklenmesi
- Kurulum veya devir sonrası ekip eğitimi
- Ticket bazlı teknik destek

01 · CI/CD ARAÇLARI VE ENTEGRASYON

CI/CD araçları ve entegrasyon

Ekibimizin aktif deneyime sahip olduğu ve sıklıkla kurguladığı bileşenler. Bunlarla sınırlı değiliz; kurumun mevcut altyapısına veya talebine göre farklı CI/CD araçlarıyla da entegrasyon sağlıyoruz.

GitLab CI/CD

Kaynak kod ve pipeline entegrasyonu

Jenkins

Geniş ekosistemli otomasyon sunucusu

Argo CD

GitOps tabanlı continuous delivery

Tekton

Cloud-native CI/CD pipeline

SonarQube

Kod kalitesi ve güvenlik açığı analizi

GitHub Actions

GitHub repoları için yerleşik CI/CD

Azure DevOps

Kurumsal Microsoft ekosistemi

TeamCity · Bamboo

Kuruma özel araç tercihleri

Drone CI

İhtiyaca göre entegrasyon

ESNEK ARAÇ SEÇİMİ

Spesifik bir araç seti talep edilmesi halinde o araca yönelik kurulum, konfigürasyon ve entegrasyon desteği de verilir.

Kubernetes / OpenShift danışmanlığı

Kubernetes, containerized uygulamaları otomatik olarak deploy eden, ölçekleyen ve yöneten endüstri standardı bir orkestrasyon platformudur. OpenShift ise Red Hat'in kurumsal ihtiyaçlara yönelik geliştirdiği Kubernetes dağıtımıdır.

Ne katar?

- Kaynak kullanım verimliliği artar; donanım ve lisans maliyetleri düşer
- Uygulama çökerse otomatik yeniden başlatma; kesinti süresi minimuma iner
- Trafik artınca otomatik ölçekleme, azalınca kaynak iadesi
- Rolling update ile kesintisiz yeni versiyon
- Standart deploy süreçleri; insan hatasına bağımlılık azalır
- Ekipler altyapı yerine ürüne odaklanır

Ne sunuyoruz?

- Sıfırdan kurulum; kurumun kendi altyapısında (fiziksel veya sanallaştırma üzerinde) ya da cloud'da
- Mevcut ortamlar için sağlık analizi (cluster audit), güvenlik değerlendirmesi ve performans iyileştirme
- Yeni entegrasyonların eklenmesi
- Kurulum veya devir sonrası ekip eğitimi; ekibin sistemi bağımsız yönetebilmesi hedeflenir
- Ticket bazlı teknik destek

Kubernetes'e geiş ve kullanım alanları

Kimler için uygun?

- Birden fazla mikro servisi ayakta tutması gereken yazılım ekipleri; sık deploy ıkan rn ekipleri
- Altyapı maliyetlerini optimize etmek ve DevOps / DevSecOps olgunluęunu artırmak isteyen şirketler
- Startup'tan byk lekli kurumsal yapılara kadar her lekte

VM'den Kubernetes'e geiş

VM tabanlı mimarilerde her uygulama, iřletim sistemi katmanıyla birlikte ayrı bir sanal makinede alışır. Kubernetes'te uygulamalar container olarak aynı node kaynaklarını paylařır; sunucu başına uygulama yoęunluęu artar. Pek ok kurumun deneyimine gre altyapı maliyetlerinde %40-70 arasında tasarruf elde edilebilir.

Kamu kurumları için

Cumhurbaşkanlıęı Dijital Dnřm Ofisi koordinasyonunda hazırlanan Kamu Bulut Biliřim Stratejisi, bulut ve konteyner tabanlı esnek leklenen yapılara geiřte donanım kaynaklarında %50'ye varan maliyet kazancı ngrmektedir.

- Yerli veri merkezlerinde kurulacak altyapılar KVKK uyumluluęu ve veri egemenlięi gereksinimlerini karřılar
- Aık kaynak yapısı sayesinde lisans maliyeti oluřmaz
- Otomatik lekleme, self-healing ve standart deploy sreleriyle operasyon iř yk azalır

Gelişmiş entegrasyonlar

Production ortamındaki bir Kubernetes cluster'ında bulunması gereken temel entegrasyonlar. Talebe göre daha spesifik entegrasyonlar da gerçekleştirilebilir.

Kimlik ve erişim yönetimi

- LDAP / Active Directory: RBAC kurumsal dizinle ilişkilendirilir; kubectl ve dashboard erişimi LDAP üzerinden doğrulanır
- Keycloak: OIDC kimlik sağlayıcı; SSO, çok faktörlü doğrulama ve merkezi oturum yönetimi
- HashiCorp Vault: Secret'lar şifreli saklanır, Pod'lara güvenle enjekte edilir; Git'e veya image'a gömülmez

İzleme ve uyarı

- Prometheus: node, pod, container ve kontrol düzlemi metrikleri; yeni servisler otomatik keşfedilir
- Grafana: hazır ve özel dashboard'lar
- Alertmanager: CPU/bellek baskısı, crash-loop, disk doluluğu kuralları; Slack, PagerDuty, e-posta veya webhook bildirimi
- OpenTelemetry / Jaeger ile opsiyonel distributed tracing

Ağ, çoklu cluster ve felaket kurtarma

Gelişmiş ağ: Cilium (eBPF)

- L3/L4/L7 network policy; HTTP method, gRPC servisi veya DNS adı bazında mikro-segmentasyon
- Daha düşük gecikme, daha yüksek throughput
- Hubble ile gerçek zamanlı ağ akışı izleme
- Opsiyonel WireGuard ile şifreli node-to-node iletişim
- ClusterMesh ile cluster'lar arası servis keşfi ve policy

Çoklu cluster yönetimi

- Open Cluster Management: birden fazla cluster'ın yaşam döngüsü, policy dağıtımı ve uygulama teslimatı tek merkezden
- OpenShift ortamlarında Red Hat ACM: GitOps (Argo CD) ile merkezi konfigürasyon dağıtımı ve drift tespiti

Felaket kurtarma (Disaster Recovery)

AKTİF-PASİF

Primary cluster yükü taşır, standby cluster hazır bekler. Velero ile düzenli etcd ve PV snapshot'ları, ikincil lokasyona replikasyon. Failover'da GSLB DNS ağırlığı standby'a kaydırılır.

AKTİF-AKTİF

İki veya daha fazla cluster eş zamanlı trafik taşır. Stateful bileşenler için çapraz replikasyon (PostgreSQL, Kafka MirrorMaker 2). Sağlık ve coğrafi yakınlığa göre GSLB ile dinamik dağıtım (F5, Cloudflare, k8gb).

Her iki senaryoda da DNS düzeyinde health-check tabanlı failover ve weighted routing kurulur; kurumun mevcut load balancer altyapısına (F5 GTM/DNS, Citrix ADC vb.) veya cloud DNS servisine entegre edilir.

MLOps / Kubeflow

Makine öğrenmesi yaşam döngüsü tek platformda

Kubeflow, Kubernetes üzerine kurulu bir ML platformudur. Veri bilimcilerin ve ML mühendislerinin model geliştirme, eğitim ve production'a alma süreçlerini tek yerden yönetmesini sağlar. Altta bir Kubernetes cluster'ı gerekir; kurumda yoksa kurulum hizmete dahil edilir.

Ne katar?

- GPU kaynakları otomatik tahsis edilir, israf önlenir
- Model denemeleri izlenebilir ve karşılaştırılabilir
- Pipeline'lar zamanlanır, izlenir, tekrarlanabilir çalışır
- Model geliştirmeden production servisine kadar tüm süreç tek platformdan yönetilir
- Veri bilimciler altyapı yerine model geliştirmeye odaklanır

İki aşamalı kurulum

Aşama 1 · Production-ready Kubernetes: GPU/CPU node pool'ları, NVIDIA device plugin ve MIG, RWX storage, CNI/Ingress, RBAC ve namespace stratejisi, GPU metrikli izleme

Aşama 2 · Kubeflow: kurulum ve bileşen entegrasyonu

Kubeflow bileşenleri ve araçlar

Kubeflow bileşenleri

Jupyter Notebook

Namespace başına izole, kotalı notebook ortamı

Kubeflow Pipelines

Python SDK ile DAG tabanlı ML iş akışları

KServe

REST/gRPC inference; canary ve A/B testi

Katib

Otomatik hiperparametre arama

Training Operator

TFJob, PyTorchJob ile dağıtık eğitim

Central Dashboard

Tek arayüz, OIDC ile kimlik doğrulama

Sık entegre edilen araçlar

- MLflow — Deney takibi ve model registry
- Apache Airflow — Karmaşık iş akışı zamanlama
- Apache Spark — Spark on Kubernetes ile büyük veri
- Kafka — Gerçek zamanlı veri akışı
- MinIO — S3 uyumlu artifact ve veri depolama
- Feast — Feature store; training-serving skew'ini önler

GPU altyapısı

GPU tarafında

CUDA / cuDNN	CUDA / cuDNN ve NVIDIA container toolkit yapılandırması
MIG	A100 / H100 GPU'ları izole bölümlere ayırarak farklı ekiplerle paylaşım
NVIDIA RAPIDS	GPU hızlandırmalı veri hazırlama
GPU as a Service	Fiziksel GPU yoksa KVKK uyumlu, yurt içi veri merkezlerinden GPU'lu sunucu kiralanıp cluster'a bağlanır

04 · YAPAY ZEKÂ GÜVENLİĞİ

Yapay zekâ güvenliği

Kullanım denetimi ve kurumsal veri koruma

Yapay zekâ araçlarının iş süreçlerinde kullanılması, hassas kurumsal bilgilerin dış sistemlere aktarılması riskini beraberinde getirir. Geliştirdiğimiz ürün, yapay zekâ kullanımını denetleyerek kurumun belirlediği kapsamda hassas bilgilerin kurum dışına aktarılmasını önlemeye yönelik koruma sağlar.

Ne katar?

- Yapay zekâ kullanımında kurumsal denetimi güçlendirir.
- Hassas bilgilerin dış sistemlere aktarılması riskini azaltır.
- Çalışanların yapay zekâ araçlarından kontrollü biçimde yararlanmasını destekler.

Hizmetlerimizle nasıl bütünleşir?

01 Kubernetes / OpenShift

Uygulamaların ve yapay zekâ platformlarının çalışacağı altyapıyı kuruyor, ölçekliyor ve yönetiyoruz.

02 MLOps / Kubeflow

Model geliştirme, eğitim, deney takibi ve kullanıma alma süreçlerini yönetiyoruz.

03 DevSecOps & CI/CD

Yazılım geliştirme ve dağıtım süreçlerine otomatik güvenlik kontrolleri ekliyoruz.

04 Yapay zekâ kullanım denetimi

Geliştirdiğimiz ürünle kullanım aşamasında kurumsal bilgilerin korunmasını destekliyoruz.

05 · HİZMET MODELİ

Hizmet modeli

Nasıl çalışıyoruz?

İhtiyacınıza göre sıfırdan kurulum yapıyor ya da mevcut sistemlerinizi devralıp geliştiriyoruz. Kurulumu sizin altyapınızda ya da cloud ortamında gerçekleştirebiliyoruz.

01 Kurulum

Sıfırdan DevSecOps pipeline, Kubernetes / OpenShift veya Kubeflow altyapısı; on-prem, sanallaştırma üzerinde ya da cloud'da.

02 Yönetim ve danışmanlık

Mevcut ortamlar için cluster audit, güvenlik değerlendirmesi, performans optimizasyonu ve yeni bileşen entegrasyonları.

03 Eğitim

Kurulum veya devir sonrası ekibe yönelik Kubernetes / OpenShift ve Kubeflow eğitimi; ekibin sistemi bağımsız yönetebilmesi hedeflenir.

04 Destek

Kurulum ve kullanım sürecinde karşılaşılan hatalar için ticket bazlı destek.

05 Yapay zekâ güvenliği ve kullanım denetimi

Geliştirdiğimiz ürünün kurumun yapay zekâ kullanım senaryolarına göre devreye alınması ve kullanım kapsamının belirlenmesi.

ESNEK KAPSAM

DevSecOps, Kubernetes / OpenShift, MLOps / Kubeflow hizmetleri ve yapay zekâ güvenliği ürünümüz birlikte veya ayrı ayrı sunulabilir. Yalnızca MLOps talep edilirse ve kurumda Kubernetes ortamı yoksa, kurulum hizmetle birlikte kapsama dahil edilir.

FİRMA ADI

3 200 Teknoloji ve Yazılım A.Ş.