OpsGuard

SECURE PATCH OPERATIONS & ORCHESTRATION

Kritik Sunucu Ortamları için Güvenli Patch Operasyonu ve Orkestrasyon

ÜRÜN TANITIMI

GÜNDEM

Bugün Neler Konuşacağız

01

Sorun

Sunucu bakımında kritik sektörlerin karşılaştığı ortak risk

02

Çözüm

OpsGuard'ın konumu ve mimarisi

03

Nasıl Çalışır

Bir operasyonun uçtan uca yolculuğu

04

Ayrıştırıcı Özellikler

Rakiplerin sunmadığı 6 yetenek

05

Kanıtlanmış Sonuçlar

Gerçek ortamlarda doğrulanmış ölçek

06

Sonraki Adım

Pilot ve demo süreci

TEK CÜMLEDE

OpsGuard Nedir?

Kritik sunucu ve servis ortamlarında patch, reboot ve zafiyet operasyonlarını; güvenlik kurallarıyla koruyan, iş servisini önceliklendiren ve her adımı kanıtla belgeleyen orkestrasyon platformu.

Mevcut Otomasyonun Üzerinde

AWX / Ansible altyapısını değiştirmez, güvenlik ve karar katmanı ekler

Kapalı Ağ Dahil Her Ortamda

İnternete tamamen kapalı, regüle ortamlarda çalıştığı doğrulanmıştır

Tek Panelden Yönetim

Envanter, zafiyet, patch planı ve uyumluluk — tek ekranda

NEDEN BU ÜRÜN VAR

Sunucu Bakımı, Sessizce Büyüyen Bir Risk

- Yüzlerce sunucuda patch, reboot ve zafiyet takibi büyük ölçüde manuel yürütülüyor — “hangi sunucu ne zaman güncellendi” sorusu güvenilir şekilde cevaplanamıyor.
- Tek bir yanlış adım büyük hasara yol açabiliyor: aynı hizmetin iki düğümünün aynı anda düşmesi, birincil veritabanının beklenmedik reboot alması, disk alanı yetersiz bir sunucuya patch atılması.
- Denetim ekipleri sorduğunda elde imzalı bir kanıt yok — “kim, ne zaman, hangi onayla, hangi sonuçla güncelledi” sorusu belgelenemiyor.
- Zafiyet tarayıcıları (Nessus, Wazuh vb.) sorunu buluyor; ama “şimdi hangi sunucuyu, ne zaman güvenle yamalayabilirim” sorusuna cevap vermiyor. Bulgu ile aksiyon arasında bir uçurum var.
- **Sonuç: patch operasyonları ya aşırı temkinli ve yavaş, ya da toplu ve kontrolsüz yürütülüyor — ikisi de kritik iş için risklidir.**

NEDEN ŞIMDI

Baskı Her Yönden Artıyor

Regülasyon Baskısı

ISO 27001, NIS2 ve sektörel denetimler artık “yaptık” değil, “yaptığımızı kanıtlıyoruz” diyebilmeyi şart koşuyor.

Büyüyen Saldırı Yüzeyi

Her gün yeni CVE/USN bülteni yayınlanıyor; hangisinin kendi ortamını etkilediğini hızlı ve doğru tespit etmek zorlaşıyor.

Kısıtlı IT Kaynağı

Ekipler aynı anda hem hız hem güvenlik istemek zorunda; manuel süreçler bu ikisini birlikte veremiyor.

Kesintinin Maliyeti

Kritik bir servisin planlı bakımda beklenmedik şekilde düşmesi, patch'i geciktirmekten çok daha pahalıya mal oluyor.

ÇÖZÜM

OpsGuard Mimarisi — Üç Katman

MOTOR

AWX / Ansible

Sunuculara gerçekten bağlanan, komutu çalıştıran, kanıtlanmış otomasyon altyapısı. Zaten kullandığınız yatırım korunur.

BEYİN

OpsGuard Katmanı

Her operasyondan önce/sonra "bu güvenli mi, sırası doğru mu, kanıtı var mı?" sorusunu otomatik sorar ve uygular.

ARAYÜZ

Tek Panel

Envanter, zafiyet, patch planı, uyumluluk ve raporlama — operasyon ve yönetim aynı ekranda buluşur.

"AWX işi yapar, OpsGuard işin doğru ve kanıtlanabilir yapılmasını garanti eder."

NASIL ÇALIŞIR

Bir Operasyonun Uçtan Uca Yolculuğu

1 Keşif

Sunucular otomatik envantere alınır; web/DB/LB gibi iş rolleri tespit edilir.

2 Ön Kontrol

Disk, bağlantı, repo ve servis durumu düzenli ve otomatik olarak taranır.

3 Güven Skoru

Operasyon öncesi 0-100 puan: hazır / uyarı / onay gerekli / engellendi.

4 Guardrail Kontrolü

Riskli senaryolar (örn. aynı servisin iki düğümü aynı anda) sistemce engellenir.

5 Kademeli Uygulama

Test → az kritik → kritik sırayla, dalga dalga; bir dalga başarısızsa süreç durur.

6 Kanıt Paketi

İmzalı, değiştirilemez rapor: kim, ne zaman, ne onayladı, sonuç ne oldu.

Rakiplerin Sunmadığı Yetenekler

Güven Skoru

Confidence Score

Her operasyon öncesi tek bakışta 0-100 puan + gerekçe (disk, bağlantı, repo, geçmiş başarı, servis, bakım penceresi).

"Bu sunucuya şimdi dokunmalı mıyım?" sorusuna saniyeler içinde, verilere dayalı bir cevap.

İş Servisi Farkındalığı

Business Service Awareness

Sunucuyu değil, servisi korur: aynı servisin iki düğümü aynı anda düşmez, birincil veritabanı ayrı ele alınır.

Patch operasyonu, iş sürekliliğini asla tehlikeye atmaz — endpoint araçlarının veremediği bir güvence.

Operasyonel Guardrail'lar

Guardrails

Riskli kararları sistem otomatik engeller: üretimde otomatik reboot yasak, kritik kümede %50 sınırı gibi kurallar kodludur.

İnsan hatası, kural ihlaline dönüşemeden önce sistem tarafından durdurulur.

Rakiplerin Sunmadığı Yetenekler

Kanıt Paketi

Evidence Pack

Her operasyon sonunda hash imzalı, değiştirilemez rapor: kim onayladı, ne kontrol edildi, sonuç ne oldu.

Denetim günü panikle rapor hazırlamak yerine, hazır ve doğrulanabilir kanıtla karşılarsınız.

Arıza İstihbaratı

Failure Intelligence

Geçmiş hataları otomatik örüntüye çevirir: “bu hata son 30 günde 14 sunucuda, ana sebep X, önerilen aksiyon Y.”

Aynı hatayı tekrar tekrar elle araştırmak yerine, sistem kök nedeni size gösterir.

OpsGuard Risk Skoru

Risk Score

Zafiyet ciddiyeti × sunucu kritikliği × ortam × istismar riski × maruziyet süresi = gerçek operasyonel risk sıralaması.

CVSS puanının ötesinde: “önce hangi sunucuyu yamalamalıyım” sorusunun gerçek cevabı.

ZAFIYET YÖNETIMI

Bulgudan Aksiyona: Vulnerability Center

- Nessus, Wazuh gibi tarayıcılardan gelen bulgular + NVD zenginleştirmesi (CVSS, KEV, önem derecesi) tek merkezde birleşir.
- Bir güvenlik bülteni (USN/CVE) yayınlandığında, sistem hangi sunucularınızı etkilediğini otomatik eşler — paket ve sürüm bazında.
- Etkilenen sunucular tek bir bakım planında toplanır; plan sadece hedeflenen paketleri günceller, kapsam dışına asla taşmaz.
- **Agentless ön kontrol, tarayıcının YERİNE geçmez — tarayıcının bulduğunu yönetilebilir, izlenebilir bir aksiyona çevirir.**

GERÇEK SENARYO (ANONİMLEŞTİRİLMİŞ)

Kritik bir SSH güvenlik bülteni yayınlandı. OpsGuard, bülteni etkilenen 49 sunucuyla otomatik eşledi ve tek bir bakım planı oluşturdu. Sadece ilgili paketler güncellendi — bulgudan aksiyona geçiş dakikalar içinde tamamlandı, kapsam dışı hiçbir paket dokunulmadı.

YÖNETIŞIM VE UYUMLULUK

Regülasyona Hazır Bir Yapı

- **Never-Auto-Reboot ilkesi: üretim sunucuları hiçbir zaman insan onayı olmadan otomatik olarak yeniden başlatılamaz.**
- Kural bazlı guardrail'lar: kritik/birincil sistemlerde ek manuel onay zorunlu kılınabilir; kritik kümede aynı anda %50'den fazla sunucu güncellenemez.
- Kademeli (ring) yayılım: test ortamından kritik üretime doğru sırayla ilerler; bir aşama başarısız olursa süreç otomatik durur.
- Kanıt paketi bütünlüğü: her rapor SHA-256 hash ile imzalanır — sonradan değiştirilip değiştirilmediği denetçi tarafından doğrulanabilir.
- **Sonuç: “patch yaptık” demek yerine, ne zaman/kim/hangi onayla/hangi sonuçla yapıldığını kanıtlayabilirsiniz.**

PAZARDAKI KONUM

OpsGuard Neden Farklı

Kamuya açık bilgilere dayalı, yaklaşık bir karşılaştırma — kesin özellik seti için ilgili sağlayıcıyla teyit edilmelidir.

Yetenek	Uç Nokta Yama Araçları	JetPatch (waves/approval)	OpsGuard
Hazır olma değerlendirmesi	Kısmi	Var	**Var + gerekçeli skor**
Dalga / kademeli yayılım	Sınırlı	Var	**Var**
Onay iş akışı	Sınırlı	Var	**Var**
İş servisi farkındalığı	Yok	Belirsiz / sınırlı	**Var**
İmzalı kanıt paketi	Yok	Belirsiz / sınırlı	**Var**
CVE-ötesi risk skorlama	Yok	Belirsiz / sınırlı	**Var**
Otomatik rol/servis keşfi	Yok	Belirsiz / sınırlı	**Var**

KAPSAM NETLİĞİ

Entegre Oluruz, Kopyalamayız

OpsGuard, kritik sunucu/servis ortamları için bir patch orkestrasyon platformudur — genel amaçlı bir BT yönetim paketi değildir. Aşağıdaki alanlarda bilinçli olarak rekabet etmiyoruz; mevcut araçlarınızla entegrasyon sunuyoruz.

Uzak Masaüstü	Yedekleme	Helpdesk / Ticketing	Genel Amaçlı RMM	Antivirüs / EDR
MDM	Şifre Kasası	Ağ İzleme	Yazılım Mağazası	Genel Varlık Yaşam Döngüsü

Odağımız: patch, reboot ve zafiyet operasyonlarını en kritik ortamlarda en güvenli şekilde yönetmek.

KANITLANMIŞ ÖLÇEK

Gerçek Ortamlarda Doğrulandı

Fintech / Ödeme Sektörü

Üretim ortamında canlı çalışıyor. Kritik iş sürekliliği gereksinimi olan bir ortamda, guardrail ve onay mekanizmalarıyla günlük operasyon.

80+ Sunuculuk Kapalı Ağ

İnternete tamamen kapalı, regüle bir ortamda uçtan uca kuruldu ve doğrulandı — offline kurulum yeteneği gerçek ölçekte kanıtlandı.

Sürekli Referans Ortamı

Günlük otomatik ön kontrol, haftalık envanter senkronu ve zafiyet taraması kesintisiz çalışıyor.

Not: Müşteri gizliliği nedeniyle ortamlar anonimleştirilmiştir; talep halinde referans görüşmesi düzenlenebilir.

DAĞITIM MODELI

Kurulum Kolaylığı, Ölçeklenebilirlik

- **Tek script ile standart kurulum — mevcut AWX/Ansible altyapınızın üzerine oturur, yeniden yazım (rip-and-replace) gerektirmez.**
- İnternete kapalı / regüle ortam desteği: kurulum, kapalı ağda gerçek ölçekte doğrulanmıştır.
- Çoklu müşteri (multi-tenant) mimarisi: MSP'ler tek platformdan birden fazla müşteriyi ayrı ayrı yönetebilir.
- Standart, tekrarlanabilir kurulum: her yeni ortam aynı yöntemle, tutarlı şekilde devreye alınır.

“Mevcut otomasyon yatırımınızı çöpe atmıyoruz — üzerine güvenlik ve kanıt katmanı ekliyoruz.”

NEDEN BU EKIP

Ürünü İnşa Eden ve Kendi Ortamında Kullanan Ekip

- **OpsGuard, kritik müşteri ortamlarında yıllardır işletilen AWX/Ansible otomasyon tecrübesinin üzerine inşa edildi.**
- Ekip, OpsGuard'ı kendi operasyonunda da kullanıyor (dogfooding) — her yeni yetenek, önce gerçek ortamlarda doğrulanıyor.
- Sürekli geliştirme: ürün, gerçek sahadan gelen geri bildirimlerle düzenli olarak güçlendiriliyor.
- Kapalı ağ, regüle ortam ve MSP çoklu-müşteri senaryolarında elde edilen tecrübe, kurulum ve devreye alma sürecini hızlandırıyor.

Hazır mısınız?

“Patch'i sadece yapmıyoruz — güvenle, kanıtlanabilir şekilde ve doğru sırayla yapıyoruz.”

Don't Just Patch. Patch Safely.

Demo Talep Edin

30 dakikalık canlı gösterim ile OpsGuard'ı kendi senaryonuzda görün.

Pilot Ortamı Kuralım

Kendi ortamınızda, sınırlı kapsamda, riske girmeden değerlendirin.

www.opsguard.net