



**SALVADOR
TECHNOLOGIES**

OT CYBER RESILIENCE PLATFORMU

Teknik Açıklama

GİRİŞ

Operasyonel Teknoloji (OT) ve Endüstriyel Kontrol Sistemi (EKS) ortamları; öngörülebilir operasyon, minimum kesinti süresi ve siber saldırılara, yanlış yapılandırmalara ve sistem arızalarına karşı güçlü dayanıklılık gerektirir. Birçok üretim sistemi legacy yazılımlar üzerinde çalışır, kesintisiz operasyon yürütür ve sık sık patch uygulanamaz.

Salvador Technologies, özellikle OT ve EKS ortamları için tasarlanmış ilk Cyber Resilience platformunu sunmaktadır.

Platform, Operasyonel Sürekliliği şu şekilde sağlar:

- OT iş istasyonları ve sunucular için Recovery Readiness yönetimi
- Otomatik doğrulama ile Backup Integrity sağlanması
- Kesinti süresini en aza indirmek ve proses stabilitesini korumak için anında (bir dakikanın altında) kurtarma sağlanması

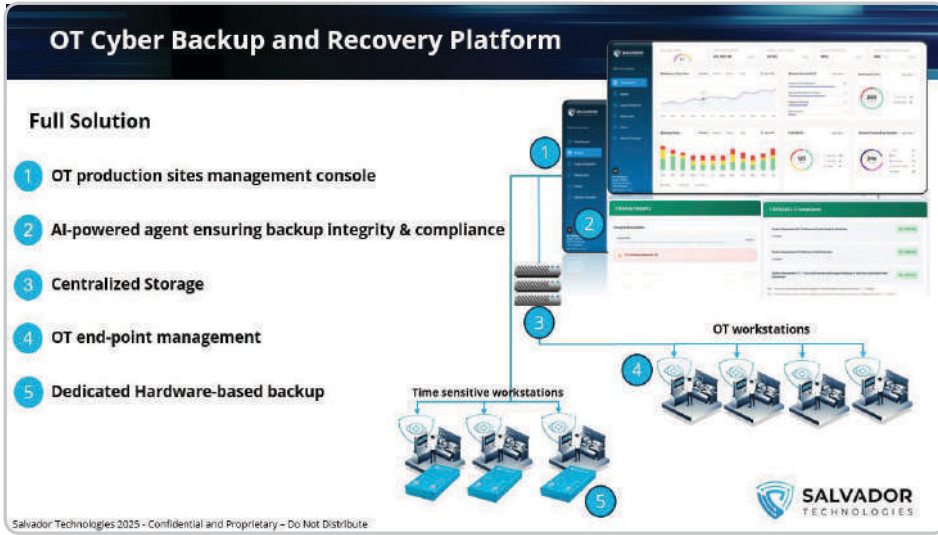
PLATFORM MİMARİSİ

BEŞ TEMEL BİLEŞEN

- 1 OT Üretim Sahaları Yönetim Konsolu – Web Management Console (WMC)
- 2 Backup Integrity ve Compliance – ML Fine-Tuned Modeller
- 3 Merkezi Depolama
- 4 OT Endpoint Yönetimi
- 5 Dedicated Hardware-Based Backup – Cyber Recovery Unit (CRU)

ÜRÜN VE ŞİRKET SERTİFİKASYONLARI

- ISO 27001
- FCC 047CFR, CE EN55032 / EN55035, EN / IEC 62368, VCCI-CISPR 32



OT / EKS UYUM GEREKSİNİMLERİNİN KARŞILANMASI

Salvador Tech, IEC 62443-3-3 SR 7.1 RE(1)/RE(2) ve SR 7.2 gereksinimlerini destekleyerek, otomatik, politika tabanlı ve air-gapped yedeklemeler ile bütünlük kontrolleri sunar. Bu sayede konfigürasyonların ve kritik verilerin zaman içinde güvenilirliğini koruması sağlanır. Trusted restore iş akışları, operatörlerin tam sunucuları veya belirli konfigürasyonları bilinen güvenli bir duruma hızlı şekilde geri yüklemesine imkân tanır ve SR 7.2 ile uyumlu biçimde sistem erişilebilirliğinin korunmasını sağlar.

Yetkinlikler ayrıca, doğrulanmış yedeklerden hızlı ve deterministik geri yükleme imkânı sağlayarak NIST CSF 2.0 ve NIS2 "Recover" gereksinimleriyle de uyumludur ve şu unsurlarla desteklenir:

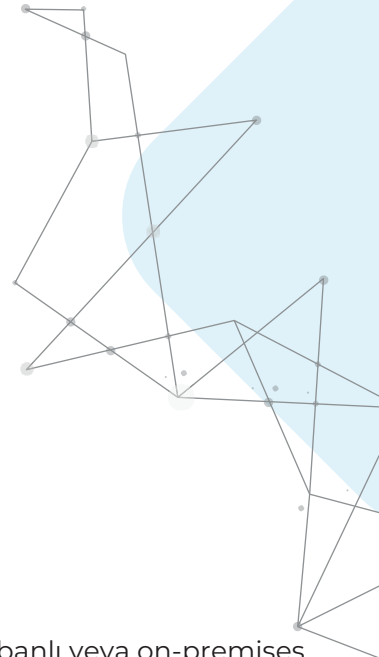
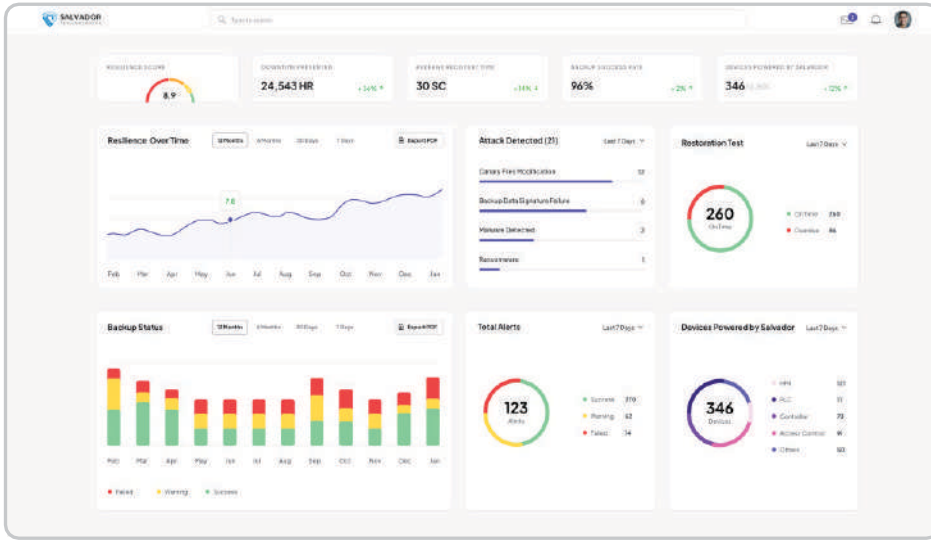
- Yönlendirmeli restore önerileri
- Backup risk skora
- Recovery adımlarını ve temiz snapshot kaynaklarını doküman eden varlık ve saha seviyesinde raporlama



WEB MANAGEMENT CONSOLE (WMC)

WMC, çoklu saha endüstriyel ortamlar için merkezi kontrol panelidir. Dağıtık OT ortamları genelinde Cyber Resilience durumuna ilişkin tam görünürlük sağlar. OT backup ve recovery operasyonlarının yönetimi için web tabanlı bir arayüz sunar; rutin koruma ve restore görevleri için ön tanımlı konfigürasyonlar ve sadeleştirilmiş iş akışları sağlar.

Yöneticiler; varlıkları kaydedebilir, yedeklemeleri yapılandırabilir, sistem sağlığını izleyebilir ve bağlı tüm sahalarda recovery süreçlerini yönetebilir.



→ TEMEL FONKSİYONLAR

- **Merkezi izleme:** Tüm varlık ve sahalarda genelinde backup durumu, recovery durumu, sistem sağlığı ve alarmların izlenmesi.
- **Ölçeklenebilir mimari:** Birden fazla saha, varlık grubu, merkezi depolama ve CRU cihazlarını destekler.
- **Operasyonel görünürlük:** Backup kapsama alanı ve sistem hazır olma durumunu gösteren çoklu saha görünümüleri.
- **Resilience skorumla:** Varlık ve saha bazında resilience skorlarının hesaplanması.
- **Konfigürasyon yönetimi:** Backup politikaları ve saha bazlı ayarların yönetimi.
- **Bildirimler ve alarmlar:** Backup başarı/başarısızlık durumları, gecikmeler, anomaliler ve saldırı göstergeleri için e-posta tabanlı uyarılar.
- **Varlık yönetimi:** Endpoint'lerin, CRU'ların ve depolama birimlerinin kaydedilmesi, gruplanması ve yönetimi.
- **BitLocker anahtar yönetimi:** Korunmalı endpoint'ler için güvenli anahtar saklama ve geri alma.

- **Esnek dağıtım:** Cloud tabanlı veya on-premises (VM tabanlı) seçenekler.
- **Rol tabanlı erişim kontrolü:** OT operasyon, engineering ve güvenlik ekipleri için.
- **SIEM entegrasyonu:** Operasyonel ve güvenlik olaylarını syslog üzerinden iletir.

→ WMC DAĞITIM SEÇENEKLERİ

- **Cloud tabanlı:** Salvador tarafından barındırılır ve tamamen yönetilir. Yalnızca outbound HTTPS gerektirir. Legacy makineleri destekler.
- **On-premises:** Önceden yapılandırılmış OVA VM olarak sunulur. Varsayılan olarak HTTP kullanır; HTTPS için SSL sertifikaları eklenebilir.
- **Yalnızca metadata işleme:** Üretim verisi sahada kalır.
- **Güvenli bağlantı:** Sadece outbound HTTPS; inbound bağlantı gerektirmez.



BACKUP INTEGRITY VE COMPLIANCE

Machine learning modelleri, backup'ların kullanılabilirliğini ve güvenilirliğini doğrular; bu, backup'ların kendisinin dahi saldırı hedefi hâline gelebildiği OT / EKS ortamlarında kritik öneme sahiptir.

→ FONKSİYONLAR

- **Yalnızca metadata:** Üretim verisi sahada kalır.
- **Tehdit tespiti:** Dosya, konfigürasyon veya çalıştırılabilir dosyaları değiştirerek backup'ları zehirlenme girişimlerini tespit eder.
- **Erken uyarılar:** Endpoint korumalarını hedef alan BYOVD saldırıları dahil olmak üzere manipülasyon girişimlerini algılar.
- **Uyumluluk izleme:** IEC 62443, NERC CIP ve kurum içi politikalara karşı sürekli değerlendirme yapar.
- **Entropi analitiği:** Backup'lar içindeki ransomware veya şifrelenmiş veriyi tespit eder.
- **Integrity skoruması:** Backup Integrity risk skoru ve restore önerileri üretir.

→ GİRDİ VERİSİ

- **Dosya özellikleri** (yol, boyut, SHA256, zaman damgaları, entropi göstergeleri).
- **Diferansiyel analiz:** Backup versiyonları arasındaki değişiklikler.

→ BACKUP INTEGRITY GÜVENCESİ

- OT'ye özgü tehditleri tespit eder (örneğin, manipüle edilmiş engineering dosyaları).
- Backup sırasında endpoint korumalarının aktif olduğunu doğrular.
- Mevcut, önceki ve referans versiyonları karşılaştırarak sapma, manipülasyon veya şifreleme durumlarını analiz eder.
- Backup sıklığı ve saklama politikalarına uyumluluğu doğrular.



MERKEZİ DEPOLAMA

Salvador Kurtarma Ortamı üzerinden kurtarma sırasında kullanılan backup imajları için bir depolama alanıdır.

→ DEPOLAMA ROLÜ

- Sistem ve iş istasyonu yedeklerini saklar
- Saklama politikalarını uygular
- Kurtarma ortamı için imaj sağlar

→ KURTARMA ORTAMI

- USB veya PXE üzerinden önyüklenebilir
- Kurtarma süreçlerini yönetmek için merkezi depolamaya bağlanır

→ DAĞITIM SEÇENEKLERİ

- Müşteri tarafından yönetilen NAS (SMB protokolü)
- Tak-çalıştır OVA sanal appliance
- Özel Dell PowerEdge R360 sunucu

→ VARSAYILAN SUNUCU KONFIGÜRASYONU

- Dell R360, 48 TB kullanılabilir alan (RAID 5)
- İşletim sistemi için mirror diskler; redundant PSU
- OpenMediaVault işletim sistemi
- 1 GbE NIC (opsiyonel 10 GbE)
- DHCP ve statik IP desteği





OT ENDPOINT YÖNETİM YAZILIMI

Minimum performans etkisiyle backup ve recovery operasyonlarını yönetmek için tasarlanmış hafif bir agent'tir.

→ MİNİMUM DONANIM GEREKİNİMLERİ

- 4 GB RAM
- 7200 rpm SATA / SSD / NVMe disk
- 512-byte sektör boyutu
- Minimum 320 MB boş alan
- Yazılım ve log'lar için 1 GB

→ YAZILIM GEREKİNİMLERİ

- NET 4.0

→ DESTEKLENEN İŞLETİM SİSTEMLERİ

- Windows XP (SP3), 7 (SP1), 10, 11
- Windows Server 2003–2022

→ KURULUM GEREKİNİMLERİ

- Outbound HTTPS 443 (veya HTTP 80)
- Salvador uygulamaları ve depolama bileşenlerinin EDR / XDR / DLP sistemlerinde whitelist'e alınması



SİBER KURTARMA BİRİMİ (CRU)

Yerleşik air-gap mantığına ve üçlü disk mimarisine sahip, belirli bir amaca özel donanım cihazıdır.

→ DONANIM GEREKİNİMLERİ

- USB 2.0/3.X portu
- Legacy işletim sistemleri için SATA tabanlı destek
- Backup, en fazla iki fiziksel sabit disk destekler
- Disk boyutu ≤ CRU kapasitesi

→ TEKNİK ÖZELLİKLER

- Üç NVMe disk (1 TB / 2 TB / 4 TB)
- USB 3.2 Gen 2 (10 Gbps)
- Güç tüketimi: 2.5W (USB 2.0), 4.5W (USB 3.X)
- Çalışma sıcaklığı: 0–40°C
- Nem: %5–90 yoğuşmasız, IP50 koruma sınıfı
- Fiziksel kontrol düğmeleri ve LED göstergeler
- Boyutlar: 105 × 57 × 17 mm
- Duvara montaj seçeneği mevcuttur

→ İZOLASYON MANTIĞI ("GERÇEK AIR GAP")

- Aynı anda yalnızca bir disk elektriksel olarak bağlıdır
- Referans: Doğrulanmış golden image,
- 24 saat sonra air-gap'e alınır
- Mevcut: En son backup
- Önceki: Bir önceki backup

→ BOOT DESTEĞİ

- Modern sistemler için USB boot desteği
- Legacy sistemler için USB + SATA hibrit boot desteği

→ ŞİFRELEME

- Referans, Mevcut ve Önceki için opsiyonel BitLocker şifreleme
- Anahtarlar, müşteri politikası ve WMC üzerinden yönetilir

→ MİNİMUM GEREKİNİMLER

- BIOS / UEFI üzerinde USB boot desteğinin etkinleştirilmiş olması. CRU'nun AV / EDR sistemlerinde whitelist'e alınmış olması



ÖZET

Çoğu siber güvenlik aracı tespit ve önlemeye odaklanır. OT ortamlarında ise sistemler kesintiye uğradığında asıl mücadele recovery aşamasında başlar. Salvador Tech, OT / EKS için özel olarak tasarlanmış ilk Cyber Resilience platformunu sunar.

Bir dakikanın altında restore imkânı, Integrity doğrulamalı sistem snapshot'ları ve izolasyon tabanlı recovery mekanizmaları sağlayarak Operasyonel Süreklilik ve minimum kesinti süresi sağlar.

