SALVADOR
TECHNOLOGIES

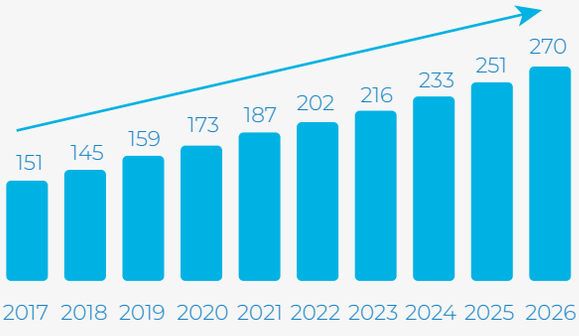
EKS ve OT Ağları için Siber Saldırı Kurtarma Çözümlerinde Devrim

OTD BİLİŞİM
GLOBAL VAD

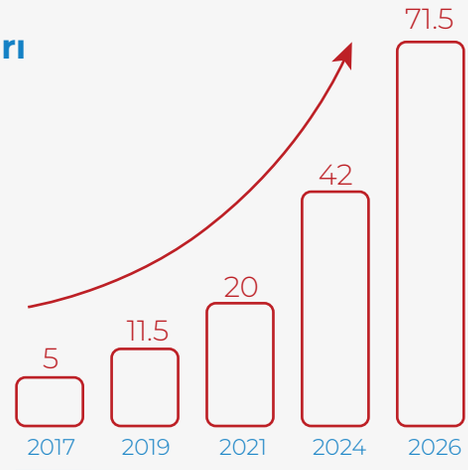
GİRİŞ

Günümüzün birbirine bağlı dijital dünyasında, Endüstriyel Kontrol Sistemleri (EKS) ve Operasyonel Teknoloji (OT) ağları giderek artan siber tehditlere karşı daha savunmasız hale gelmektedir. Endüstri 4.0 dijital dönüşüm süreci, geçmişte izole çalışan operasyonel ağların iş ağlarıyla ve internet üzerinden daha geniş dijital ekosistemlerle bağlantılı hale gelmesini sağlamaktadır. Bu dönüşüm, kritik altyapı operasyonları ve uzaktan izleme sistemleri de dâhil olmak üzere dijital teknolojilerin kullanımını teşvik etmektedir. Ancak bu bağlantılı yapı, beraberinde artan siber riskleri getirmekte ve bu tür saldırıların üretim, denizcilik ve kamu hizmetleri gibi kritik sektörler üzerindeki etkileri yıkıcı olabilmektedir.

Kaçınılmaz Olanı Benimsemek: Salvador Technologies İçin Siber Saldırı Kurtarmada Proaktif Yaklaşım



Güvenlik Yatırımı (M$)



Fidye Yazılımı Maliyeti (B$)

Stats based: www.databridgemarketresearch.com/reports/global-operational-technology-market

Dijital dünya, siber saldırıların oranında endişe verici bir artışa tanıklık ediyor ve bu durum, siber güvenliğe bakış açımızda köklü bir paradigma değişimini zorunlu kılıyor. Elbette önleme ve tespit alanlarında yoğun çabalar harcanmaktadır; ancak artan fidye yazılımı saldırılarıyla birlikte artık bir kuruluşun siber saldırıya uğrayıp uğramayacağı değil, ne zaman uğrayacağı sorusu gündemdedir.

Bu white paper, bu kaçınılmaz gerçeğin kabul edilmesinin önemini vurgulamakta ve Salvador Technologies'in, bir siber saldırı sonrasında hızlı ve etkili bir kurtarma sürecini garanti altına almak için atması gereken kritik adımları ortaya koymaktadır.

YENİ NESİL SİBER TEKNOLOJİ: 30 SANİYEDE KURTARMA

Yeni nesil bir siber teknolojinin ortaya çıkışı, EKS ve OT ağlarında siber saldırı sonrası kurtarma süreçlerinde oyunun kurallarını değiştiren bir çözüm sunmaktadır. Bu teknoloji, bir siber saldırı ya da sistem arızası sonrasında PC, dizüstü bilgisayar, iş istasyonu veya sunucu gibi bir bilgisayar sisteminin yalnızca 30 saniye içinde kurtarılmasını mümkün kılan benzersiz bir yetenek

NASIL ÇALIŞIR?

Çözüm şu bileşenlerden oluşur:

1.Donanım Ünitesi: Bilgisayara bağlı birim, verileri depolar ve olası bozulmalara karşı koruma sağlar.

2.Yazılım Aracısı (Agent): Özel veri kopyalama ve anomali denetimi gerçekleştiren yazılım bileşenidir.

3.Merkezi İzleme Sistemi: Kullanıcıyı bilgilendirir ve her istasyonun durumunu görüntüler.

Operasyonel sürekliliği garanti altına almak için ürün, bilgisayarın tamamen yapılandırıldığı ve virüssüz olduğu temiz bir çalışma ortamında önceden yapılandırılmalıdır.

Kısaca, bir bilgisayar veya HMI saldırıya uğradığında, cihazı kapatıp Salvador Technologies biriminden başlatmanız (boot etmeniz) yeterlidir.

Donanım

Donanım Cihaz, uç kısmı USB Type-C (cihaz tarafı) ve Type-A (bilgisayar tarafı) olan bir USB kablosu aracılığıyla bağlanır. Bir sonraki nesil versiyon, SATA bağlantısını destekleyecek şekilde tasarlanmıştır; böylece ürünü Windows XP gibi eski işletim sistemlerinde veya USB'den önyüklemeyi desteklemeyen sistemlerde de kullanmak mümkün olacaktır. Sistem, 10 Gbp/s'ye kadar veri aktarım hızı sunan en hızlı protokol olan 3 adet NVMe disk içerir. Bu yapı, bilgisayarın cihaz üzerinden çalıştırılmasına (boot edilmesine) olanak tanırken performans kaybı yaşanmasını önler.

Diğer iki disk — Current (Güncel) ve Previous (Önceki) — bilgisayar sistemlerinin önceden yapılandırılmış yedekleme sıklığına (günlük, 2 günde bir veya 7 günde bir) göre tam yedeklerini almaya devam etmek için kullanılır.

Cihaz tamamen otonom çalışır: yedekleme modundayken sistem, hedef diski her X günde bir (X = 1 / 2 / 7) otomatik olarak Current diskten Previous diske geçirir.

Patentli koruma algoritması, bu işlevin bilgisayardan dışarıdan veya içeriden hiçbir şekilde kontrol edilmesine izin vermez. Bu, her X günde bir yalnızca belirli bir diskin kullanıcı erişimine açık olacağı, diğer disklerin ise elektronik olarak çevrimdışı (offline) kalacağı anlamına gelir.

Cihaz üzerindeki fiziksel düğmeler aracılığıyla işlevleri, frekansları, modları ve hedef diskleri değiştirmek mümkündür. Bu fiziksel izolasyon, veriler için en güçlü “air-gap” korumasını sağlar.

Cihazın güç tüketimi düşüktür (en fazla 1A, 5V) ve yalnızca tek bir USB 2.0 veya USB 3.0/3.1 bağlantı noktası üzerinden çalışabilir. Cihaz, verilerin tam bir kopyasını depolar: buna önyüklenebilir işletim sistemi sürümü, sürücüler, yazılımlar, yapılandırmalar ve dosyalar dâhildir.

Geleneksel disk imajı yedekleme yöntemlerinden farklı olarak, bu teknoloji sayesinde cihazdan doğrudan önyükleme (boot) yapılabilir ve 30 saniye içinde, saldırı anında izole (air-gap) edilmiş temiz bir veri sürümünden çalışmaya devam edilebilir.

CRU Paneli

KURTARMA / YAPILANDIR anahtarları modu değiştirir; KURTARMA veri güncelleme sıklığını belirler, YAPILANDIR ise o an erişilebilir diski gösterir (Güncel / Önceki / Fabrika Ayarları).

Hırsızlığa Karşı Koruma

Cihaz, kutuya dâhil edilen duvar montaj aparatı kullanılarak duvara veya masaya fiziksel olarak sabitlenebilir. Ek olarak, BitLocker şifreleme özelliği, verileri kötü niyetli erişimlere karşı korumak için ilave bir güvenlik katmanı sağlar. Eğer kurumunuzda bir DLP politikası (Data Loss Prevention) harici USB sürücülerini engelliyorsa, “Salvador CRU” adlı cihazı bu yasaklı liste dışında bırakmanız gerekir. Alternatif olarak, her cihazın benzersiz seri numarasını (SN) kullanarak da bu istisnayı tanımlayabilirsiniz.

CRU Teknik Özellikleri

- USB Bağlantı Noktaları: USB Type-C (dişi)
- Kablo: USB 3.1 Type-C – Type-A (erkek – erkek) kablo (pakete dâhildir)
- Kapasite Seçenekleri: 3 x NVMe disk 512 GB / 1 TB / 2 TB / 4 TB (Parça numaraları: CRU-512 / CRU-1000 / CRU-2000 / CRU-4000)
- Veri Aktarım Hızı: 10 Gbps (USB 3.1 / 3.0 bilgisayarlar için) 480 Mbps (USB 2.0 bilgisayarlar için – geriye dönük uyumlu)
- Kullanıcı Arayüzü: Mod, yedekleme sıklığı ve yedek sürüm seçimi

  Kontroller: 2 adet buton

  LED Göstergeler: 8 adet
- Boyutlar (mm): 105 x 57 x 17

  Malzeme: Alüminyum gövde

Yazılım Aracısı

Agent'in kurulumu ve kullanımı son derece basittir. Koruma altına almak istediğiniz kaynak diski ve veri yedekleme sıklığını (gün ve saat dahil) belirlemeniz yeterlidir. Bu sıklık, donanım cihazında yapılandırılmış frekansla aynı olmalıdır. Agent, yönetim sistemine düzenli olarak durum bilgisi gönderir ve kullanıcıyı aşağıdaki anormallikler hakkında bilgilendirir:

Yedekleme durumu (zamanında gerçekleştirilip gerçekleştirilmediği), Veri bütünlüğü (yetkisiz müdahale, silme, şifreleme), İş istasyonunda şüpheli etkinlik (bu durumda yedekleme işlemi otomatik olarak durdurulur ve kullanıcı müdahalesi beklenir).

Gelişmiş Kalıcı Tehdit (APT) durumunda, kötü amaçlı yazılım disk bağlantısı kesildiğinde çalışamaz çünkü yürütülebilir bir ortamda (aktif işletim sistemi bulunmadığı için) etkin değildir. APT şüphesi halinde cihaz, temizlik istasyonu (adli bilişim araçları ve antivirüs yazılımları içeren ayrı bir bilgisayar) kullanılarak temizlenebilir. Ayrıca kullanıcı, her zaman çevrimdışı ve APT'ye karşı korumalı olan "Factory Reset" sürümünden sistemi başlatabilir.

Agent ayrıca, donanım temelli air-gap korumasına ek olarak diskin keşfedilmesini (örneğin "Bilgisayarım" altında görünmesini) engelleyecek şekilde tasarlanmıştır. NVMe disklerinin fiziksel olarak birbirinden ayrılmış olması sayesinde, ilk kurtarma başarısız olsa bile farklı zamanlardan iki tam veri yedeğine daha erişim mümkündür. Yazılım son derece kullanışlıdır ve 1 dakikadan kısa sürede kurulabilir. Hem USB 3.1 / 3.0 hem de USB 2.0 arayüzleriyle uyumludur.

Yönetim Konsolu

Modül, her uç noktada kurulu olan tüm ürünlerin durumuna ilişkin tam görünürlük sağlar.

Yalnızca iç ağ bağlantısının (internet erişimi olmadan) izin verildiği durumlarda, izleme modülü yerel olarak bir sanal makine (VM) üzerine kurulabilir ve BT yöneticisi tarafından kolayca yapılandırılabilir.

CRU, Yedekleme Durumunu Yazılım Aracısına (Agent Software) Raporlar

Yedekleme Durumunun, Giriş Yapılarak veya Kişiselleştirilmiş Doğrudan Bildirimlerle Tam Görünürlüğü

Giriş Yaparak veya Kişiselleştirilmiş Doğrudan Bildirimlerle Yedekleme Durumuna Tam Görünürlük

E-posta ve SMS ile Otomatik Bildirim Hizmeti!

OTD BİLİŞİM
GLOBAL VAD

GÜVENLİK DUVARI KORUMASINDAN DAHA GÜÇLÜ: AIR-GAP TEKNOLOJİSİ

Air-Gap (Fiziksel Ağ İzolasyonu), bir bilgisayarın veya ağın dış bağlantılardan fiziksel olarak izole edilmesini sağlayan bir güvenlik önlemidir ve siber güvenlikte kritik bir rol oynar. Bu yöntem, yetkisiz erişimi engelleyerek ve zararlı yazılım ile fidye yazılımı saldırı riskini azaltarak, kritik sistemler ve hassas veriler için ek bir koruma katmanı sunar. Air-gap yaklaşımı, yalnızca siber tehditlere karşı koruma sağlamakla kalmaz; aynı zamanda, kurumların yedekleme, kurtarma ve operasyonel süreklilik planlarının bir parçası olan, yaygın kabul görmüş 3-2-1 yedekleme prensibini de destekler.

3-2-1 yedekleme stratejisinin bir parçası olarak air-gap teknolojisinin uygulanması, kuruluşların siber tehditlere karşı dayanıklılığını önemli ölçüde artırır.

Bir fidye yazılımı saldırısı veya veri bozulması durumunda, air-gap ile izole edilmiş yedek kopya, kritik sistemlerin hızla geri yüklenmesini ve değerli verilerin kısa sürede kurtarılmasını sağlar. Bu yaklaşım, sistem kesintilerini en aza indirir, finansal kayıpları azaltır ve iş sürekliliğini garanti altına alır.

BAŞLICA KULLANIM ALANLARI

Bu teknolojinin temel kullanım alanları arasında İnsan-Makine Arayüzleri (HMI), Veri Toplama ve Gözetim Kontrol Sistemleri (SCADA) ve Windows tabanlı diğer kritik bilgisayar sistemleri yer almaktadır. Şu anda yalnızca Windows sistemleri desteklenmekle birlikte, gelecekte Linux ve diğer işletim sistemleri için de destek sağlanması planlanmaktadır. Air-gap yaklaşımı, elektromanyetik, elektronik ve fiziksel düzeyde tam izolasyon sağlayarak, kötü amaçlı yazılımlar, fidye yazılımları ve yetkisiz erişimlere karşı güçlü bir savunma mekanizması oluşturur. Bu çözüm özellikle kritik altyapılar, üretim tesisleri, enerji sektörü, bina yönetim sistemleri (BMS) ve denizcilik endüstrisi için tasarlanmıştır.

- Üretim
- Sağlık
- Denizcilik
- BMS
- Kritik Altyapılar
- Enerji

Salvador Technologies Hakkında

Salvador Technologies, operasyonel süreklilik ve siber saldırı sonrası kurtarma için yenilikçi teknolojik çözümler sunar. Sistem, yedekleme bütünlüğünün kolayca doğrulanmasını ve anında geri yükleme testiyle hızlı kurtarma süreçlerini garanti altına alır.

Şirketin misyonu, işletmelerin operasyonel sürekliliğini koruyarak, kesinti sürelerini en aza indiren ve her türlü senaryodan hızlı kurtarma olanağı sağlayan benzersiz araçlar ve özellikler sunmaktır.