SALVADOR
TECHNOLOGIES

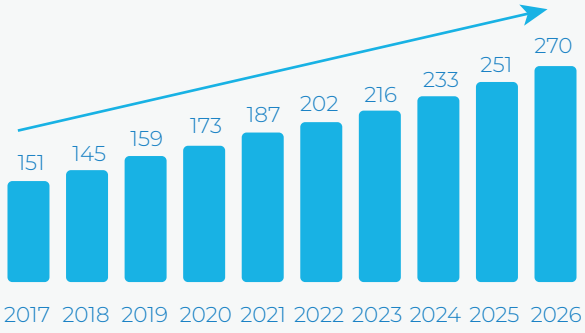
Revolutionizing Cyber-Attack Recovery Solution for ICS & OT Networks

OTD BİLİŞİM
GLOBAL VAD

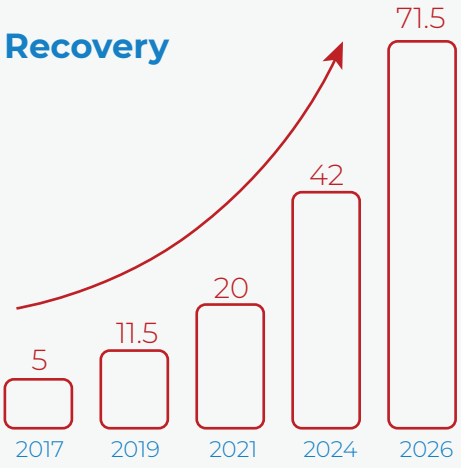
INTRODUCTION

In today's interconnected world, Industrial Control Systems (ICS) and Operational Technology (OT) networks are increasingly vulnerable to cyber threats. The industry 4.0 digital transformation evolution drives legacy isolated operational network, to be connected to the business network and beyond, over the internet. This evolution encourages increasing use of digital technologies including critical infrastructure operations and remote monitoring systems. With this connectivity, cyber risks rise and these cyber attacks impact on critical sectors such as manufacturing, maritime, and utilities can be devastating.

Embracing the Inevitable:
A Proactive Approach to Cyber Attack Recovery for Salvador Technologies



Security Investment (M$)



Ransomware Cost(B$)

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

The digital landscape is witnessing an alarming surge in the rate of cyber-attacks, necessitating a paradigm shift in our approach to cybersecurity. Indeed, dep efforts are invested in prevention and detection, but with the increasing ransomware attacks, it is plain to understand that it is no longer a question of "if" an organization will experience a cyber-attack, but rather "when."

This white paper emphasizes the importance of acknowledging this inevitability and outlines the critical measures that Salvador Technologies must undertake to ensure a swift and effective recovery in the aftermath of a cyber-attack.

THE NOVEL CYBER TECHNOLOGY: 30-SECOND RECOVERY

The emergence of a novel cyber technology presents a game-changing solution for cyber attack recovery in ICS and OT networks. This technology offers an unprecedented capability to recover a computer system, such as a PC, laptop, workstation, or server, within just 30 seconds from a cyber attack or a computer failure.

HOW DOES IT WORK?

The solution consists of

1. A Hardware unit connected to the PC, storing the data and protecting it from any corruption.

2. An agent software to perform dedicated data copy and anomaly inspection.

3. A Centralized Monitoring System to inform the user and display the status of each station.

In order to ensure operational continuity, the product should be set in advance, in a clean operational environment – after the computer is fully configured and contains no viruses.

In short, once a computer/HMI is attacked, you simply shut it down and boot from the Salvador Technologies' unit.

Hardware

The device is connected by a USB cable using the attached USB type-C (device end) to type-A (computer end) cable. The next generation will support SATA connection, to use the product in old operational system(OS) such as Windows XP and other systems that do not support boot from USB.

The system contains 3 NVMe disks – the fastest protocol for data transfer, up to 10Gbp/s. It allows running (boot) the computer from the device without compromising the computer's operation speed.

One disk – Factory Reset – is used to store the data configuration during installation. It is the fully operational version that is never exposed to the user.

The other two disks - Current and Previous – are used to continue full backups of the computer systems on a preconfigured frequency - daily, 2 days or 7 days.

The device is autonomous: in the backup mode, it will switch the target disk from Current to Previous every X days (X = 1 / 2 / 7).

The patented protection algorithm will not allow any external or internal control of this functionality from the computer. It means, that every X days, a different disk will be accessible to the user for backup of the data - other disks are electronically offline.

Using the on-device switches, you can change the functionality, frequencies, modes, and target disks. Physical isolation provides the most robust air- gap protection of the data.

The electrical consumption of the device is low (up to 1A, 5V), enabling it to be used with only one USB socket of USB 2.0 or USB 3.1/3.0. A full copy of the data will be stored on the device. It will include the bootable version of the OS, the drivers, software, configurations, and files.

As opposed to image backup, this allows you to boot directly from the device and work immediately (30 seconds - the time to reboot the computer) from a clean version of the data which was air-gapped (disconnected) at the time of the attack.

The Panel of the CRU

Recovery /Configure switches to change the mode; Recovery defines the data rate of data update, Configure indicates the currently available disk (current /previous /factory reset).

Protection against theft

The device can be physically mounted to a wall or a desk using the included wall mount, BitLocker encryption provides an additional method to secure data against malicious access. In case a DLP policy blocks external USB drives, you should exclude from the list. the device named “Salvador CRU”, or by using a unique

Specifications of CRU:

- USB ports: USB Type-C female
- USB 3.1 cable Type-C to Type-A male to male (included)
- Available capacity: 3 x NVMe drives - options: 512GB / 1TB / 2TB / 4T (PNs: CRU-512 / CRU-1000 / CRU-2000 / CRU-4000)
- Data transfer rate: 10Gbps USB - for USB 3.1/3.0 computers; Hi-Speed 480 Mbps - for USB 2.0 computers (backward compatibility)
- User interface - mode, backup frequency and backup version selection

  2 x buttons

  8 x LED indicators
- Dimensions (mm): 105 x 57 x 17
- Material: Aluminum body

Software Agent

Installing and using the agent is very easy – configure the source disk (the one you want to protect), and the data backup frequency (including the time and the day) – the frequency should be the same as configured on the Hardware device.

The agent will send status to the Management system to inform the user about any anomaly – such as backup status (performed on time), data integrity (intrusion, deletion, encryption), or suspicious activity on the workstation (in this case backup will automatically suspend until the user intervenes).

In the case of an advanced persistent threat (APT): the malware cannot be operated when the disk is disconnected as it is not located in an executable environment (no OS running). In case there is a suspicion for an APT, the device can be cleaned using a sanitization station (a sperate computer with forensic tools and anti-virus), the user can also boot from the “Factory Reset” version which is always offline and protected from the APT.

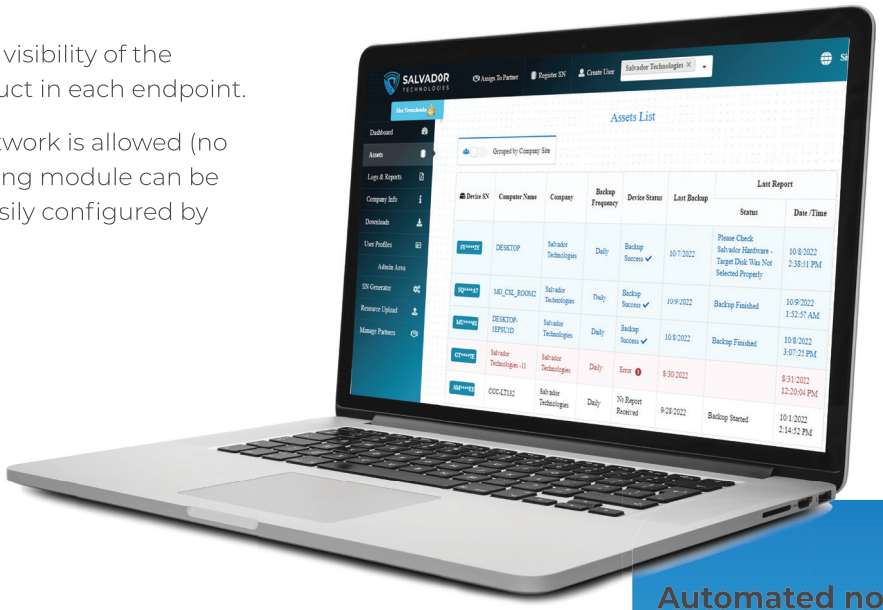
The Agent is also designed to disable the discovery of the disk (e.g., in “My Computer”) as an additional layer of protection on top of the hardware air-gap protection. Having physical separation of the NVMe disks, even if the first restore fails, enables you to have two more full copies of the data from a different time.

The software is very easy to use with less than 1 minute of installation USB 3.1 /3.0 & 2.0 interfaces.

Management module

The module allows complete visibility of the status of every installed product in each endpoint.

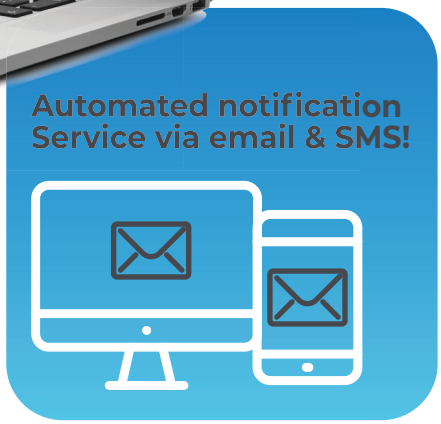
In case of only an internal network is allowed (no internet access), the monitoring module can be installed locally as VM and easily configured by the IT manager.



CRU reports backup status to Agent Software

Agent Software reports backup status and alerts to web monitoring system

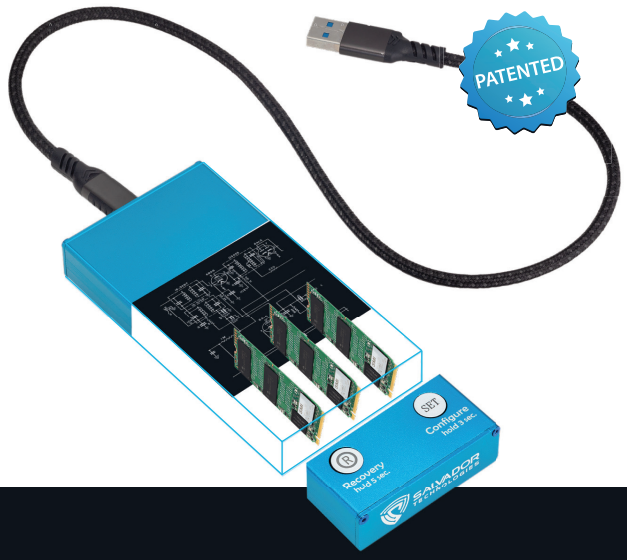
Full visibility of backup status through log in or personalized direct notifications



STRONGER THAN FIREWALL PROTECTION, AIRGAP

Air-gapping, a security measure that physically isolates a computer or network from external connections, plays a crucial role in cyber security. By preventing unauthorized access and reducing the risk of malware and ransomware attacks, air-gapping provides an additional layer of protection for critical systems and sensitive data. The concept of air-gapping is significant in safeguarding against cyber threats, as well as supporting the widely recognized 3-2-1 backup principle, as part of the organization backup, recovery, and operational continuity plan.

Implementing air-gapping as part of the 3-2-1 backup strategy enhances the resilience of organizations against cyber threats. In the event of a ransomware attack or data corruption, the air-gapped copy can be used to restore critical systems and recover valuable data quickly. This reduces downtime, mitigates financial losses, and ensures business continuity.



MAIN USE CASES

The primary use cases of this technology include Human-Machine Interfaces (HMIs), Supervisory Control and Data Acquisition (SCADA) systems, and other critical computer systems operating on Windows. While currently supporting Windows systems, future plans include support for Linux and other operating systems. The air-gapping approach ensures total isolation electromagnetically, electronically, and physically, providing a robust defense against malware, ransomware, and unauthorized access.

The solution is designed for Critical Infrastructures, Manufacturing, Energy, Building Management Systems (BMS) and Maritime.

Manufacturing | Medical | Maritime | BMS | Critical Infrastructures | Energy

About Salvador Technologies

Salvador Technologies provides breakthrough technological solutions for operational continuity and cyber-attack recovery, ensuring an easy validation of the backup integrity with an instant restoration test.

Our mission is to ensure operational continuity by providing unique tools and features to minimize the downtime and allow recovery from any scenario.