SALVADOR TECHNOLOGIES

OT CYBER RESILIENCE PLATFORM

Technical Description

INTRODUCTION

Operational Technology (OT) and Industrial Control System (ICS) environments require predictable operation, minimal downtime, and strong resilience against cyberattacks, misconfigurations, and system failures. Many production systems run legacy software, operate continuously, and cannot be patched frequently.

Salvador Technologies provides the first cyber resilience platform engineered specifically for OT and ICS environments.

The platform ensures operational continuity by:

- Managing OT workstation and server recovery readiness
- Ensuring backup integrity through automated verification
- Enabling instant (under one minute) recovery to minimize downtime and maintain process stability

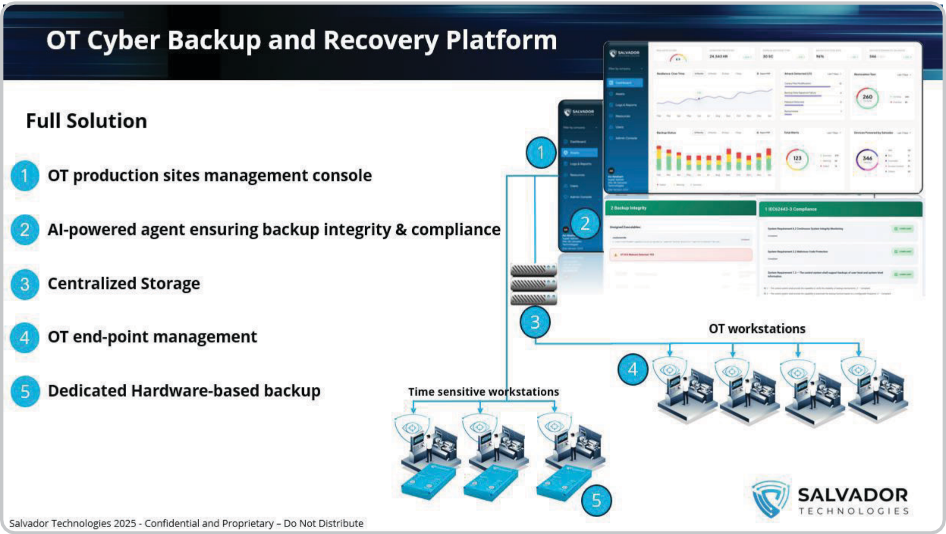
PLATFORM ARCHITECTURE

FIVE CORE COMPONENTS

1. OT Production Sites Management Console – Web Management Console (WMC)
2. Backup Integrity & Compliance – ML Fine-Tuned Models
3. Centralized Storage
4. OT Endpoint Management
5. Dedicated Hardware-Based Backup – Cyber Recovery Unit (CRU)

PRODUCT & COMPANY CERTIFICATIONS

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



OT Cyber Backup and Recovery Platform

Full Solution

1. OT production sites management console
2. AI-powered agent ensuring backup integrity & compliance
3. Centralized Storage
4. OT end-point management
5. Dedicated Hardware-based backup

Salvador Technologies 2025 - Confidential and Proprietary – Do Not Distribute

ADDRESSING OT / ICS COMPLIANCE

Salvador Tech supports IEC 62443-3-3 SR 7.1 RE(1)/RE(2) and SR 7.2, delivering automated, policy-based, air-gapped backups with integrity checks. These ensure that configurations and critical data remain trustworthy over time. Trusted restore workflows allow operators to rapidly recover full servers or specific configurations to a known-good state, maintaining system availability in alignment with SR 7.2.

Capabilities also align with NIST CSF 2.0 and NIS2 “Recover” requirements by enabling fast, deterministic restoration from verified backups, supported by:

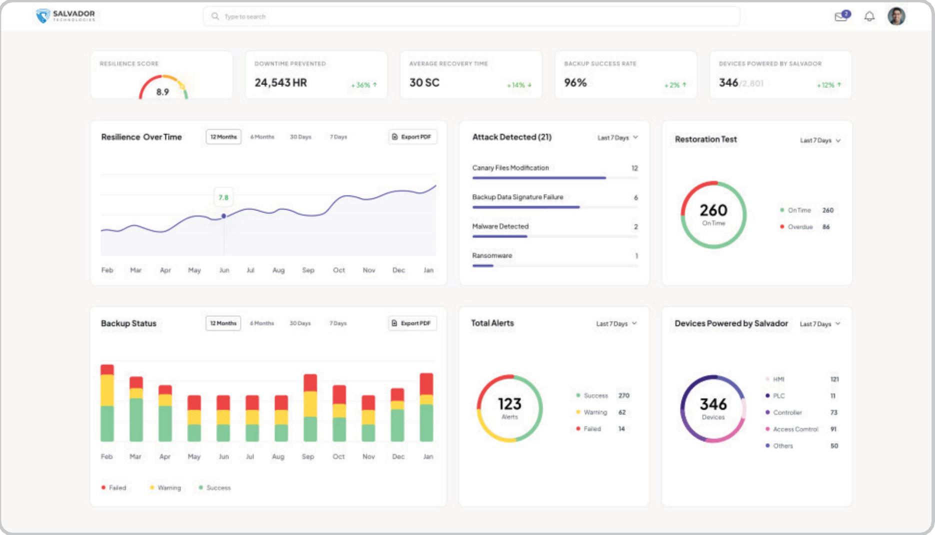
- Guided restoration recommendations
- Backup risk scoring
- Asset- and site-level reporting documenting recovery steps and clean snapshot sources

DETAILED COMPONENT BREAKDOWN

SALVADOR TECHNOLOGIES

WEB MANAGEMENT CONSOLE (WMC)

The WMC is the central control panel for multi-site industrial environments. It provides complete visibility into cyber resilience status across distributed OT environments.
A web-based interface for managing OT backup and recovery operations, it provides predefined configurations and streamlined workflows for routine protection and restoration tasks.
Administrators can register assets, configure backups, monitor health, and manage recovery processes across all connected sites.



→ KEY FUNCTIONS

- **Centralized monitoring:** Backup status, recovery posture, system health, and alerts across all assets and sites.
- **Scalable architecture:** Supports multiple sites, asset groups, centralized storage, and CRU devices.
- **Operational visibility:** Multi-site views showing backup coverage and system readiness.
- **Resilience scoring:** Calculates resilience scores per asset and per site.
- **Configuration management:** Includes backup policies and site-specific settings.
- **Notifications & alerts:** Email-based alerts for backup success/failure, delays, anomalies, and attack indicators.
- **Asset management:** Register, group, and manage endpoints, CRUs, and storage.
- **BitLocker key management:** Secure storage and retrieval for protected endpoints.
- **Flexible deployment:** Cloud-based or on-premises (VM-based) options.
- **Role-based access control:** For OT operations, engineering, and security teams.
- **SIEM integration:** Streams operational and security events via syslog.

→ WMC DEPLOYMENT OPTIONS

- **Cloud-based:** Salvador-hosted and fully managed. Requires only outbound HTTPS. Supports legacy machines.
- **On-premises:** Delivered as a preconfigured OVA VM. Defaults to HTTP; SSL certificates can be added for HTTPS.
- **Metadata-only processing:** Production data remains onsite.
- **Secure connectivity:** Outbound HTTPS only; no inbound connections required.

DETAILED COMPONENT BREAKDOWN

SALVADOR TECHNOLOGIES

BACKUP INTEGRITY & COMPLIANCE

Machine learning models validate backup usability and trustworthiness, essential in OT / ICS environments where backups themselves can become an attack target.

→ FUNCTIONALITIES

- **Metadata only:** Production data stays onsite.
- **Threat detection:** Identifies attempts to poison backups by altering files, configurations, or executables.
- **Early alerts:** Detects tampering, including BYOVD attacks targeting endpoint protections.
- **Compliance monitoring:** Continuous assessment against IEC 62443, NERC CIP, and internal policies.
- **Entropy analytics:** Identifies ransomware or encrypted data inside backups.
- **Integrity scoring:** Generates a backup integrity risk score and restoration recommendations.

→ INPUT DATA

- **File properties** (path, size, SHA256, timestamps, entropy indicators).
- **Differential analysis:** changes between backup versions.

→ BACKUP INTEGRITY ASSURANCE

- Detects OT-specific threats, e.g., manipulated engineering files.
- Confirms endpoint protections were active during backup.
- Compares current, previous, and baseline versions for drift, tampering, or encryption.
- Validates compliance with backup frequency and retention policies.

CENTRALIZED STORAGE

A repository for backup images used during recovery via the Salvador Recovery Environment.

→ STORAGE ROLE

- Stores system and workstation backups
- Enforces retention policies
- Provides images for the Recovery Environment

→ RECOVERY ENVIRONMENT

- Bootable via USB or PXE
- Connects to centralized storage to orchestrate recovery

→ DEPLOYMENT OPTIONS

- Customer-managed NAS (SMB protocol)
- Plug-and-play OVA virtual appliance
- Dedicated Dell PowerEdge R360 server

→ DEFAULT SERVER CONFIGURATION

- Dell R360, 48 TB usable (RAID 5)
- OS mirrored drives; redundant PSU
- OpenMediaVault OS
- 1 GbE NIC (optional 10 GbE)
- DHCP and static IP support

DETAILED COMPONENT BREAKDOWN

SALVADOR
TECHNOLOGIES

OT ENDPOINT MANAGEMENT SOFTWARE

A lightweight agent for managing backups and recovery operations with minimal performance impact. Supports Windows-based OS.

→ MINIMAL HARDWARE REQUIREMENTS

- 4 GB RAM
- 7200 rpm SATA / SSD / NVMe drive
- 512-byte sector size
- 320 MB minimum free space
- 1 GB for software & logs

→ SOFTWARE REQUIREMENTS

- NET 4.0

→ SUPPORTED OS

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

→ SETUP REQUIREMENTS

- Outbound HTTPS 443 (or HTTP 80)
- Salvador applications and storage whitelisted from EDR / XDR / DLP

CYBER RECOVERY UNIT (CRU)

Dedicated hardware device with built-in air-gap logic and triple-disk architecture.

→ HARDWARE REQUIREMENTS

- USB 2.0/3.X port
- SATA-based support for legacy OS
- Backup supports up to two physical hard drives
- Disk size ≤ CRU capacity

→ SPECIFICATIONS

- Three NVMe drives (1 TB / 2 TB / 4 TB) USB 3.2 Gen 2 (10 Gbps)
- Power consumption: 2.5W (USB 2.0),
- 4.5W (USB 3.X)
- Temperature: 0–40°C
- Humidity: 5–90% non-condensing IP50 rating
- Physical controls and LED indicators Dimensions: 105 × 57 × 17 mm
- Wall-mount option available

→ ISOLATION LOGIC ("TRUE AIR GAP")

- Only one disk is electrically connected at a time Baseline: Validated golden image,
- air-gapped after 24 hours
- Current: Latest backup Previous: Prior backup

→ BOOT SUPPORT

- USB boot for modern systems
- USB + SATA hybrid boot for legacy systems

→ ENCRYPTION

- Optional BitLocker encryption for Baseline, Current, Previous
- Keys managed per customer policy and WMC

→ MINIMAL REQUIREMENTS

- USB boot support enabled in BIOS / UEFI CRU whitelisted from AV / EDR

OTD BİLİŞİM
GLOBAL VAD

SALVADOR TECHNOLOGIES

SUMMARY

Most cybersecurity tools focus on detection and prevention. In OT environments, once systems are disrupted, recovery becomes the real battleground.
Salvador Tech delivers the first cyber resilience platform purpose-built for OT / ICS. It provides sub-minute restoration, integrity-verified system snapshots, and isolation-based recovery mechanisms to ensure operational continuity and minimal downtime.