# Cyber Recovery Unit – CRU-V2B

## Product Description

The CRU (Cyber Recovery Unit) device can recover a computer system, such as a PC, laptop, workstation or server, in 30 seconds from a cyber-attack or a computer failure. The primary use cases are HMI, SCADA, BMS and other critical computer systems based on Windows operational system; Linux, Ubuntu, macOS to be supported in the future.


### The solution consists of

1. A Hardware unit to store the data and protect it from any corruption.
2. A Software Agent 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 installed in advance (before an attack happens). If possible, we advise, performing the first installation (Factory Reset version) on a clean operational environment – after the computer is fully configured and contains no viruses (i.e., before internet connected). We suggest installing on the most critical workstations in the organization – thus, that requires continuous operation and fast recovery.

### 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 OS (Operational System) 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. The 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 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 moment of the attack.

+972-73-2209-444 info@salvador-tech.com www.salvador-tech.com

# Cyber Recovery Unit – CRU-V2B
## Product Description

### The Panel of the CRU

Backup/Recovery switches to change the mode, Recovery defines the data rate of data update, Recovery indicates the currently available disk (current / previous / Baseline).

### 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 SN for every single device.


## Software Agent:

Installing the software agent on the workstation is necessary for the data copy to function. Future versions will include agentless capabilities. Admin rights should be used for the installation process only.

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).

Hackers cannot easily attack or disable the agent; however, if this happens the data on the device will not be affected only updated and the user will be notified via the monitoring system.

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 Baseline version which is always offline and protected from the APT.

Another role of the agent is 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.

For systems that prohibit third-party installation, we are developing an agentless solution in parallel to obtaining cooperation and approval from relevant associations.

+972-73-2209-444 info@salvador-tech.com www.salvador-tech.com

# Cyber Recovery Unit – CRU-V2B
# Product Description

SALVADOR TECHNOLOGIES

## Management module:

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

As a standard used in Salvador Technologies' cloud, easily accessible on web browser: https://support.salvador-tech.com

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.

### 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

### Typical Applications & Features

- Critical infrastructures systems, HMI workstations, building Management Systems and production machines
- Standalone systems, Servers, laptops and workstations
- High speed up to 350MB/s
- Less than 1 minute of installation
- USB 3.1 /3.0 & 2.0 interfaces

## About Salvador Technologies

Salvador Technologies provides security failover technology for cyber-attack recovery in ICS & OT. The recovery solution bypasses standard recovery protocols of downtime and forensics and regains operations within an astonishing 30-second timeframe.

The company's expertise is based on more than ten years of experience in the National Cyber Unit and elite intelligence corps of the IDF and on the passion for contributing to the global cyber security agenda.

+972-73-2209-444 info@salvador-tech.com www.salvador-tech.com