



SALVADOR
TECHNOLOGIES



Operational Continuity Platform For OT / ICS Computer Systems

Full & Fastest Recovery from Cyber Attacks and Computer Systems Failures



info@salvador-tech.com

Challenge

US charges Kaseya hacker and seizes \$6M from REvil ransomware gang



Image Credits: Bryce Durbin / TechCrunch

The U.S. Department of Justice (DOJ) has charged a 22-year-old Ukrainian citizen linked to the REvil ransomware gang for orchestrating the July ransomware attack against U.S. technology firm Kaseya. It has also seized more than \$6 million in ransom tied to another member of the notorious ransomware group.

During a news conference on Monday, U.S. Attorney General Merrick Garland announced that Yaroslav Vasinskiy was arrested last month in Poland at the request of the U.S. government and is currently being held in custody.

Queensland's CS Energy has its corporate systems infected by ransomware

Infection occurred on Saturday.

Queensland energy generator CS Energy's corporate IT systems are being impacted by a ransomware infection.

The company said in a [statement](#) that the infection had not impacted its Callide and Kogan Creek power stations, and that it is continuing to generate and dispatch electricity into the national electricity market (NEM).



IKEA, victime d'une cyber-attaque



Els Bellens
Els Bellens est redactrice chez Data News.

Le géant du meuble IKEA est aux prises avec une cyber-attaque exploitant des mails d'hameçonnage ('phishing') internes pour toucher les collaborateurs. IKEA a confirmé l'attaque.



Hackers Breached Colonial Pipeline Using Compromised Password

By William Turton and Kartikay Mehrotra
4 June 2021, 22:58 GMT+3

The hack that took down the largest fuel pipeline in the U.S. and led to shortages across the East Coast was the result of a single compromised password, according to a cybersecurity consultant who responded to the attack.



Hackers gained entry into the networks of Colonial Pipeline Co. on April 29 through a virtual private network account, which allowed employees to remotely access the company's computer network, said Charles Carmakal, senior vice president at cybersecurity firm Mandiant, part of FireEye Inc., in an interview. The account was no longer in use at the time of the attack but could still be used to access Colonial's network, he said.

MEDIAMARKT VITTIMA DI RANSOMWARE IN GERMANIA E OLANDA: MEDIAMARKT NON SEMBRA COLPITA

Di Francesco Santini | 8 Novembre 2021, Ore 16:32

Gli attacchi ransomware continuano a essere l'arma prediletta dai cybercriminali per colpire specialmente grandi aziende e società. Dopo avere visto nel dettaglio l'attacco ai danni della SIAE, ora è il momento di trattare l'offensiva contro il rivenditore europeo MediaMarkt in Germania e nei Paesi Bassi. È interessata anche Mediaworld?

I primi report provengono dal portale olandese RTL Nieuws che avrebbe ottenuto informazioni da dipendenti del gigante della vendita al dettaglio di elettronica di consumo in Europa. Essi avrebbero condiviso alcune



Specific Cases



Ransomware cost
\$20,000 per minute



\$1.3 billion
2 weeks downtime

tsmc

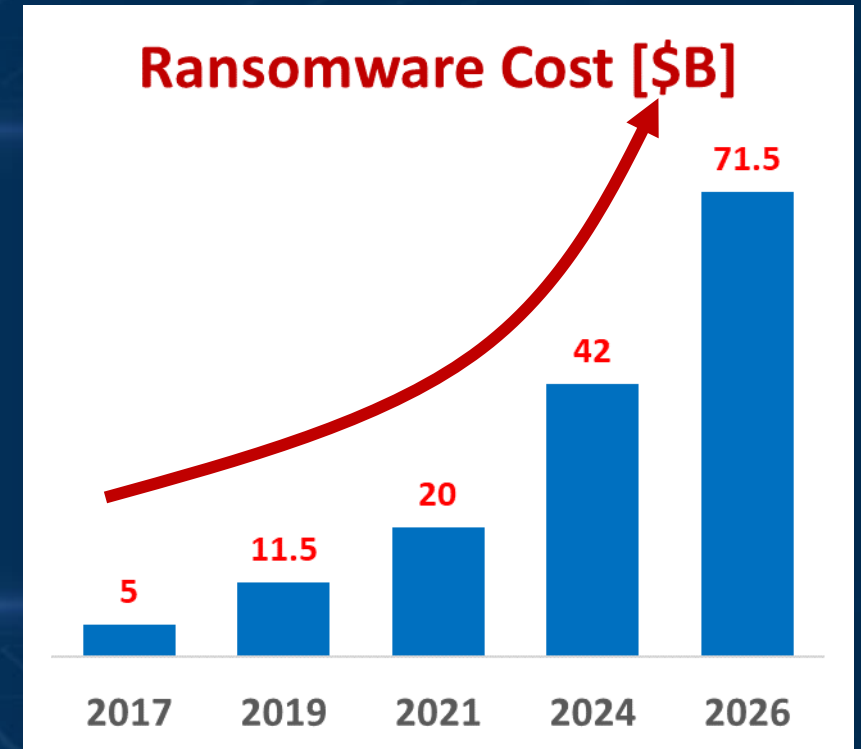
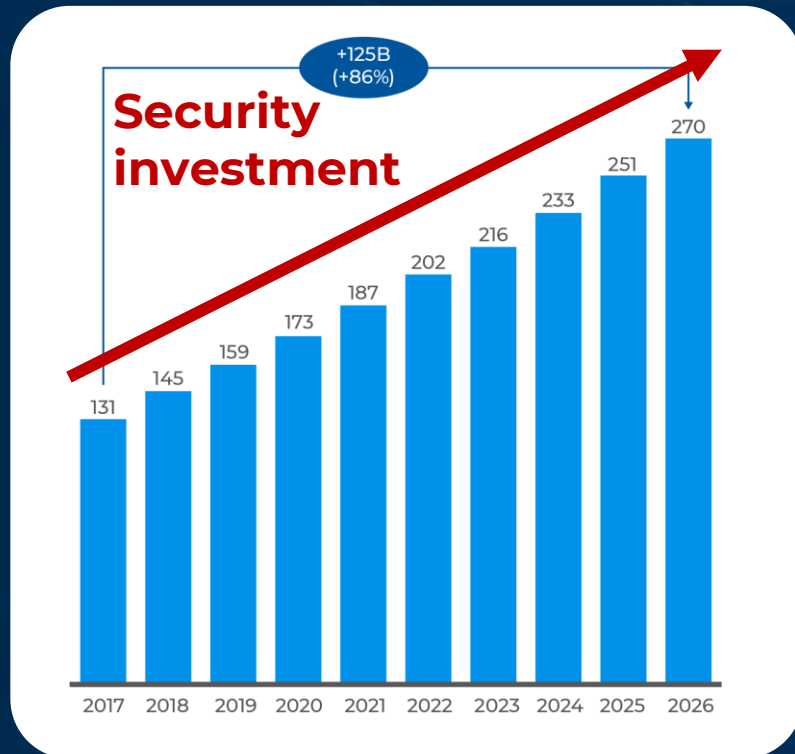
\$171 million
4 days downtime



\$52 million
3 months downtime

The offense is always one step ahead of the defense

Incident response is **critical**



<https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031>



Salvador Technologies Is The Solution

3 Layers of Defense



**Air Gap
Protection**



**Innovative
Software Agent**



**Continuous
Monitoring**

Invisible to the attackers

+



30

Seconds Recovery

CISA & FBI

“Ensure backups are **up to date**
and stored in an **easily retrievable**
location that **air-gapped**
from the organizational network”



www.bleepingcomputer.com - 11.07.2021



NIST SP 800-82

- Verify the backups for reliability and integrity
- Include testing of the restoration process

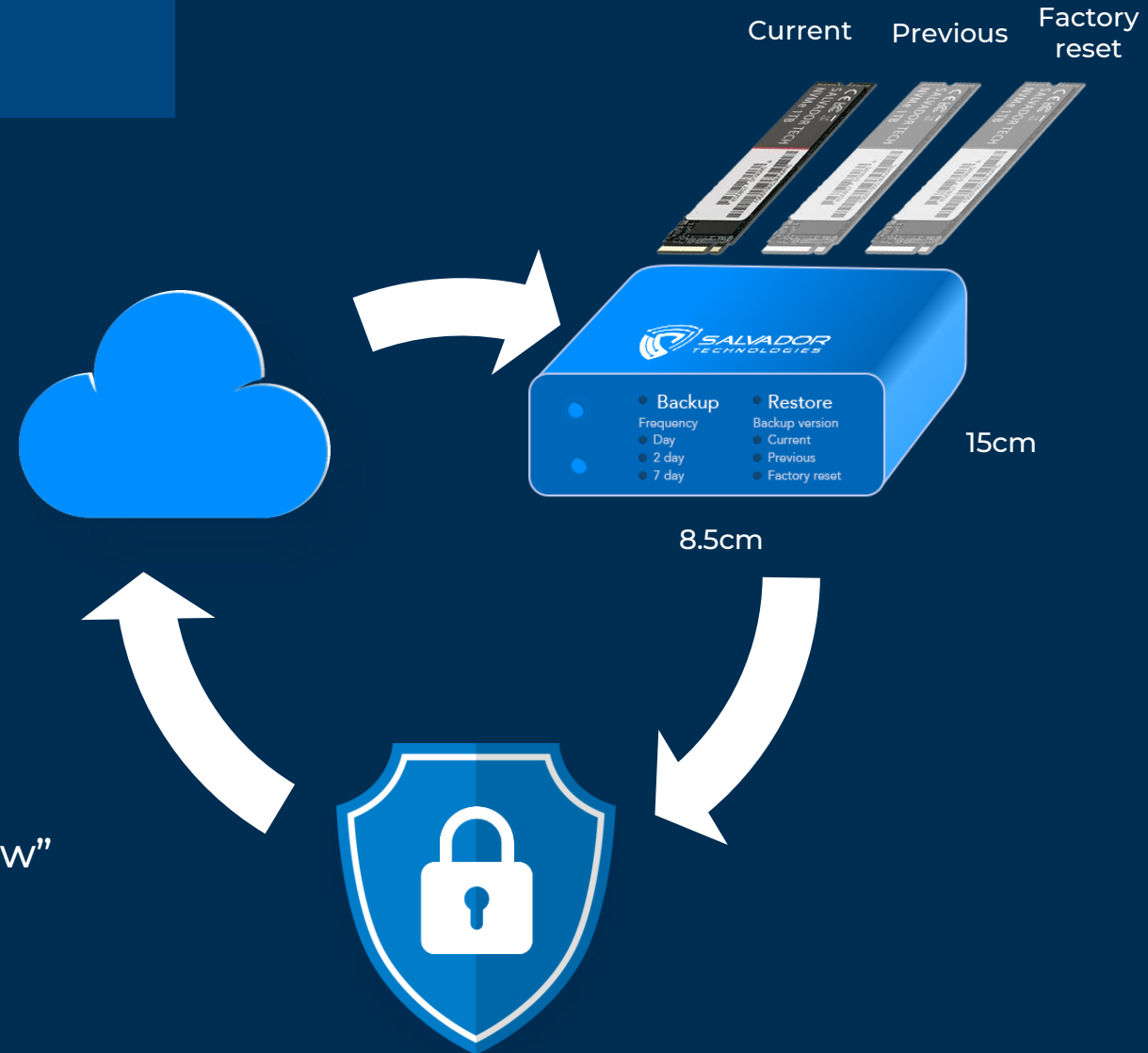
**You must use modern OT/ICS
backup & recovery methods to
meet the compliance requirements**



SALVADOR
TECHNOLOGIES

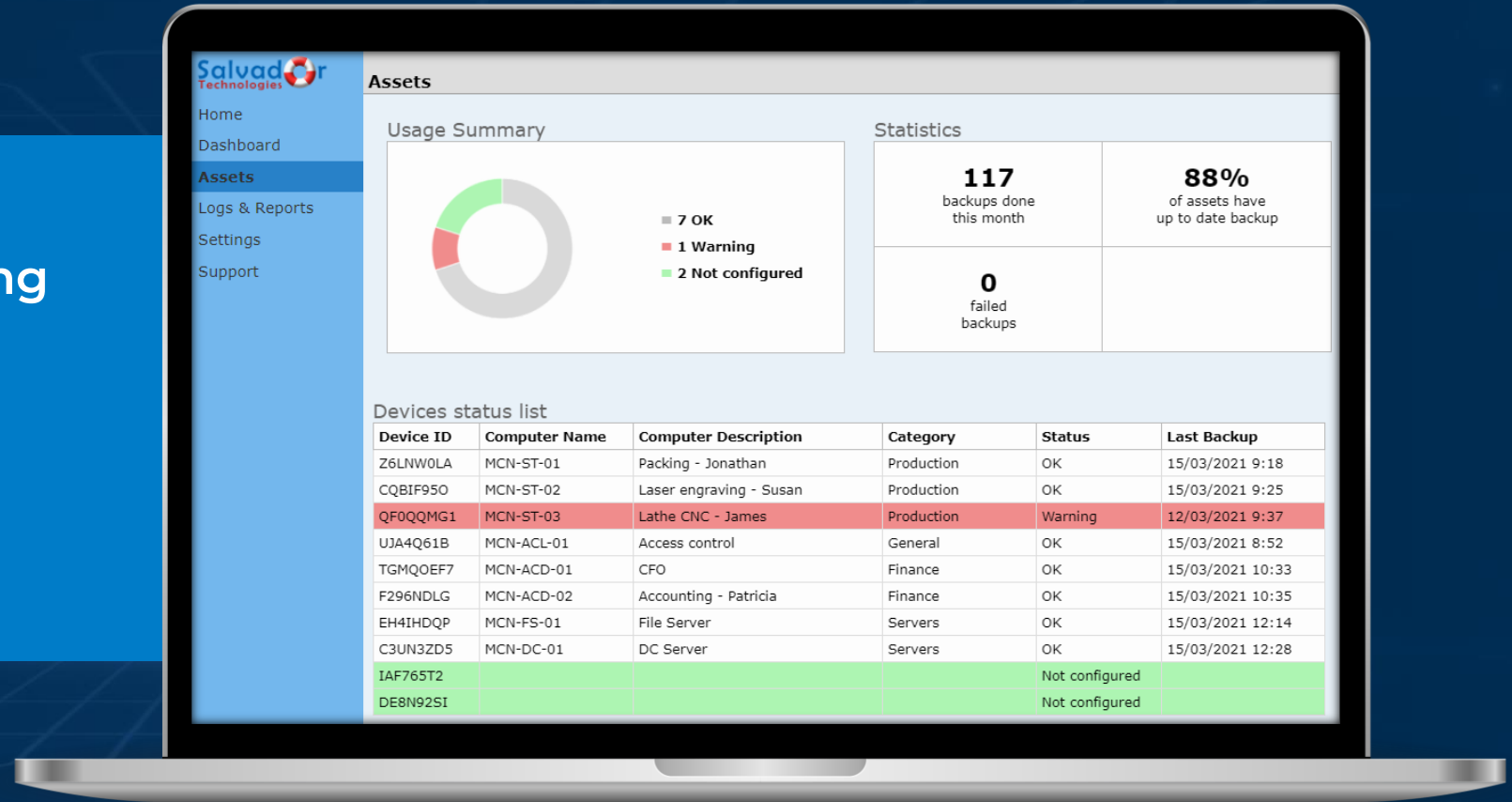
Instant Recovery Unit

- ✓ Full recovery from cyber-attacks and IT failures
- ✓ 30 seconds recovery agnostic to disk size
- ✓ 2 Minutes installation
- ✓ Offline protection of the backup data (air gap)
- ✓ Simple – press one button for the recovery
- ✓ Restoration tests can be done instantly
- ✓ Innovative machine-learning-based “backup window”



OT Backups Monitoring

- ✓ Single point of monitoring
- ✓ Web based interface
- ✓ Seamless deployment



Revolutionize the OT World

VEEAM

COMMAVAULT 

...



In IT environment
Instant **disaster** recovery of VMs
But not applicable for OT

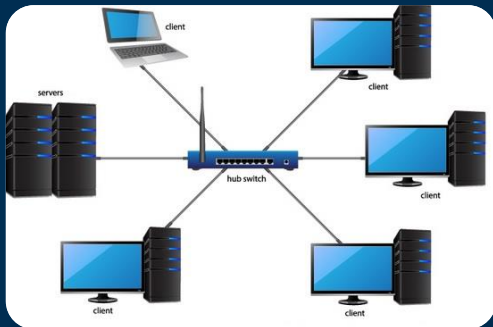


You need
our **OT** instant recovery
solution

Salvador Technologies Is The Solution

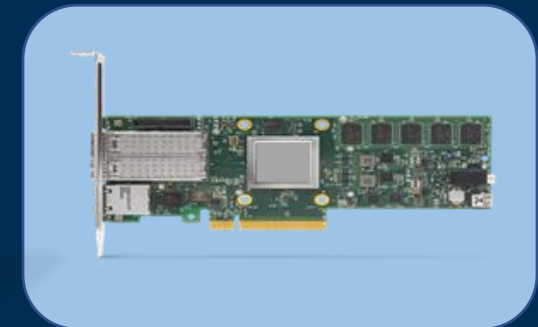
SME

- Workstations and Servers
- Critical infrastructures
- Stand alone systems
- Legacy backward compatibility



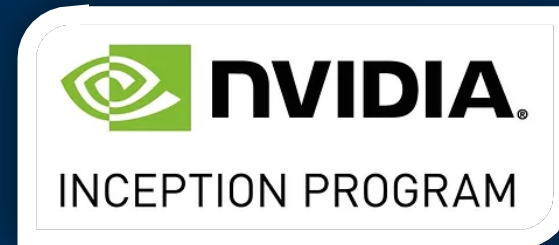
Large Scale Networks

- Production lines
- Large facilities
- Healthcare network
- Datacenters














NRS Centralized Recovery

- ✓ Centralized recovery solution for a large-scale networks
- ✓ Detection of malicious corruption in backup files (deletion / encryption) at the early stage of the attack
- ✓ Protected runtime environment using NVIDIA Bluefield2 DPU
- ✓ Detection of double extortion ransomware
- ✓ Dramatically reducing systems RTO (recovery time objective)
- ✓ Automated recovery using PXE protocol
- ✓ Air-gapped protection of backup data
- ✓ Up to 200GB/s NVMe-oF



Salvador - Category Leader in Recovery

Parameters \ Products	Salvador Technologies	Manual Backup (+software)	NAS + Backup Software	Cloud	
Recovery speed	30 sec.	Hours-days	Days-weeks	Weeks	
Offline protection	✓	✓	-	-	
Corruption detection	✓	-	-	-	
Up to date data	✓	-	✓	✓	
Simplicity of use (recovery automation)	✓	-	-	-	
IT Focused	-	-	✓	✓	
OT Focused	✓	✓	-	-	
Companies		 	 	 	   

3-2-1-1-0 Backup Strategy



- 3 copies of data
- 2 different storage media
- 1 copy is off-site

- **1 copy offline (air gapped)**
- **Recoverability & zero errors**

Long Term Vision

IT



SIEM

Backups
Monitoring

Device ID	Computer Name	Computer Description	Category	Status	Last Backup
25LW02LA	HCN-PT-01	Packing - Jarubun	Production	OK	15/10/2021 0:18
C0001950	HCN-PT-02	Laser engraving - Sultan	Production	OK	15/10/2021 0:25
00000201	HCN-PT-03	Laser CNC - Sime	Production	Warning	15/10/2021 0:37
00000118	HCN-ACC-01	Access control	General	OK	15/10/2021 0:32
00000187	HCN-ACC-01	CDS	Finance	OK	15/10/2021 10:20
00000102	HCN-ACC-02	Accounting - Patricia	Finance	OK	15/10/2021 10:25
00000101	HCN-PS-01	File Server	Services	OK	15/10/2021 12:14
00000103	HCN-ACC-01	DC Server	Services	OK	15/10/2021 12:28
00000172				Not configured	
00000191				Not configured	



NRS Centralized
Recovery Station

OT

- 24 hours operation
- Max production efficiency
- Legacy software



PLCs or RTUs
Feeds data to
SCADA system



HMI/SCADA Panel View
Supervise and control from
an operational terminal



PLCs or RTUs
Feeds data to
SCADA system



HMI/SCADA Computer
Supervise and control
from a workstation

Innovative Software

- ✓ Immediate recovery
- ✓ Autonomous response to attack
- ✓ APT (Advanced Persistent Threat) remediation
- ✓ Full visibility of the current backups status
- ✓ Early detection of backup corruption
- ✓ Files honeypots
- ✓ Statistical & cryptographic analysis



Main Use Cases

- ✓ HMI Industrial Computers
- ✓ BMS – Building Management Systems
- ✓ Logistics centers
- ✓ Energy production infrastructure
- ✓ Stand alone computer systems
- ✓ Cyber incident response team
- ✓ Medical equipment
- ✓ Critical infrastructures
- ✓ But not only...

2 digits customers already trust us
We have channel partners in Israel
and main EU countries



Case Studies

- ✓ Large chemical production facility: edge computer systems of engineering stations [20-30 units]
- ✓ Building management system of large datacenter facility: The computers responsible for the operation of cooling, access control, elevators [10-50 units]
- ✓ UPS logistics center: stand-alone computers managing the critical operation of packaging sorting. Computers are not monitored and are not secured. If it stops working, hundreds of packages will be delayed in the delivery [10 units]
- ✓ Water Supply Plants: HMI (SCADA) server that monitors water quality and controls the water treatment of densely populated areas in Israel [3-5 units each plant]
- ✓ Ammonia refrigeration system: in case of downtime the operator needs to manually monitor dozens of end-point controllers. [10-20 units]
- ✓ And more...

[*] - # of potential units



SALVADOR
TECHNOLOGIES

WORLD'S FASTEST RECOVERY FROM CYBER - ATTACKS

Contact us now

info@salvador-tech.com