

Betriebskontinuität & Wiederherstellung von Cyberangriffen Für IKS & OT Systeme

OTD BİLİŞİM

GLOBAL VAD



SALVADOR
TECHNOLOGIES

• **Salvador Technologies** bietet eine einfache Überprüfung der Backup-Integrität mit sofortigen Wiederherstellungstests mit bahnbrechenden technologischen Lösungen für die Betriebskontinuität und die Wiederherstellung von Cyberangriffen.

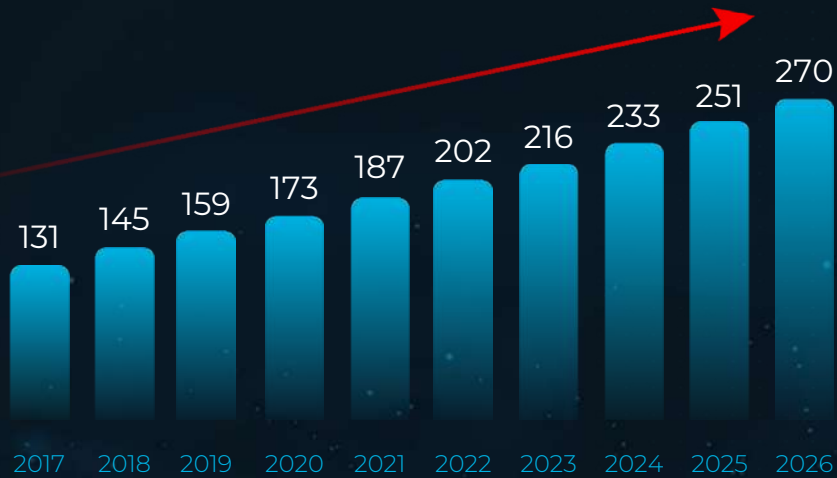
Unsere Mission ist es, die Betriebskontinuität mit einzigartigen Tools und Funktionen zu gewährleisten, um Ausfallzeiten zu minimieren und die Wiederherstellung nach jedem Szenario zu ermöglichen.

Die Expertise des Unternehmens basiert auf mehr als zehn Jahren Erfahrung in der Nationalen Cyber-Einheit und dem Elite-Geheimdienstkorps der IDF sowie auf der Leidenschaft, zur globalen Cybersicherheitsagenda beizutragen.

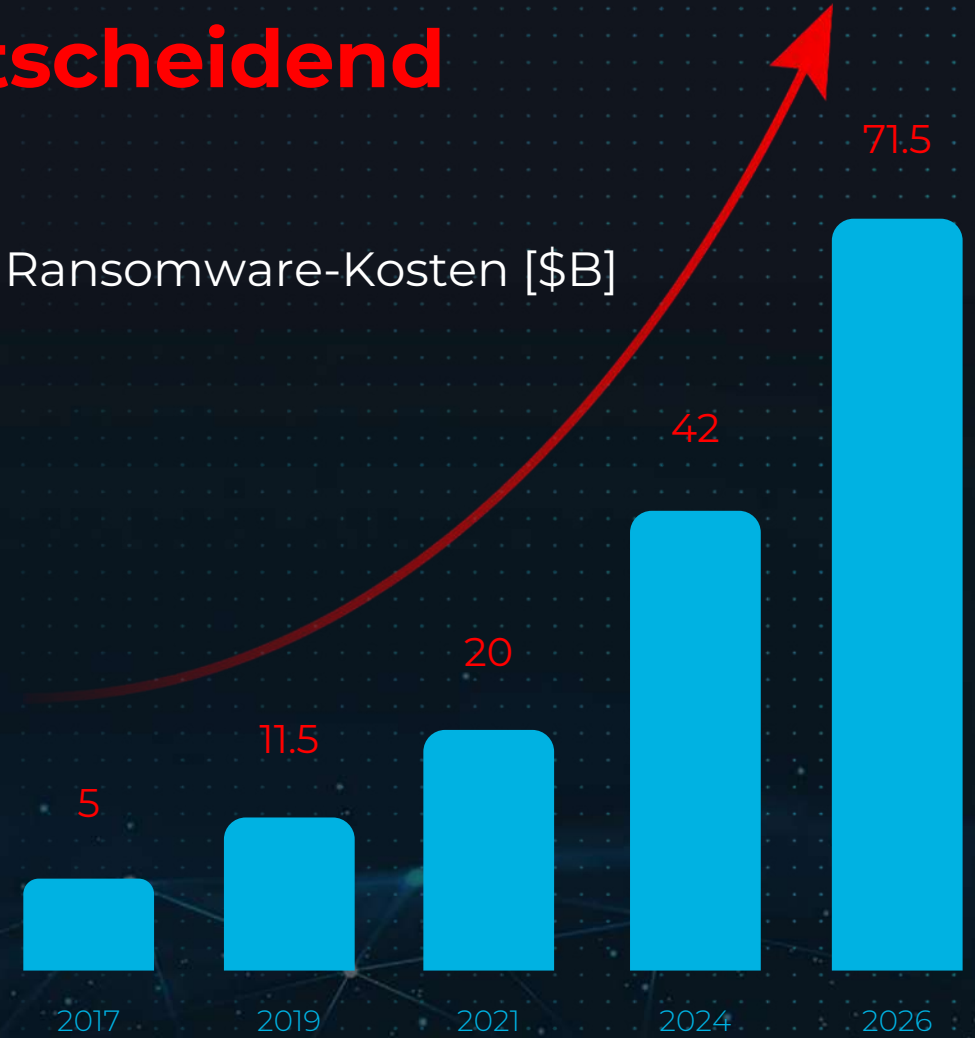
• **Angriff kommt immer vor Verteidigung**

Reaktion auf Vorfälle ist entscheidend

Investition in Sicherheit: [Mio. \$]



Ransomware-Kosten [\$B]



Hauptproblem: **Ausfallzeit**

Eines der größten Probleme in der OT- und Industriewelt



Kosten für Ausfallzeiten

\$260,000
pro Stunde*
(Durchschnitt von Gartner)



Manuelles und primitives Backup

Externe Festplatten,
Bänder



Langsame Wiederherstellung von Ransomware

20 Tage
Wiederherstellung,
aus einzige Quelle

Sonderfälle: Verlust

Ransomware kostet \$20,000 pro Minute

2 Wochen Ausfallzeit

1,3 Milliarden
Dollar



4 Tage Ausfallzeit

171 Millionen
Dollar



3 Monate Ausfallzeit

52 Millionen
Dollar



Haben sie einen plan für einen ungeplanten ausfallzeit?



• Unsere Angebote

Revolutionierte patentierte Luftspalt-Technologie, um sicherzustellen

- Der Vermeidung von Betriebsausfällen
- Sofortige Wiederherstellung
- Reduziertes Risiko von Datenverlust
- Einfache Validierung der Datenintegrität

3 Verteidigungsebenen



Luftspalt
Datenschutz für
Isolierter Bereich



Intelligenter
Agent



Kontinuierliche
Überwachung



30 sek.
und endlich ist alles wieder in
ordnung!

Luftspalt

Der algorithmus erlaubt **keine externe oder interne kontrolle** dieser funktionalität vom computer aus.

Das bedeutet, dass alle X tage eine andere festplatte für den benutzer zugänglich ist, um die daten zu sichern, **andere festplatten sind elektronisch offline.**

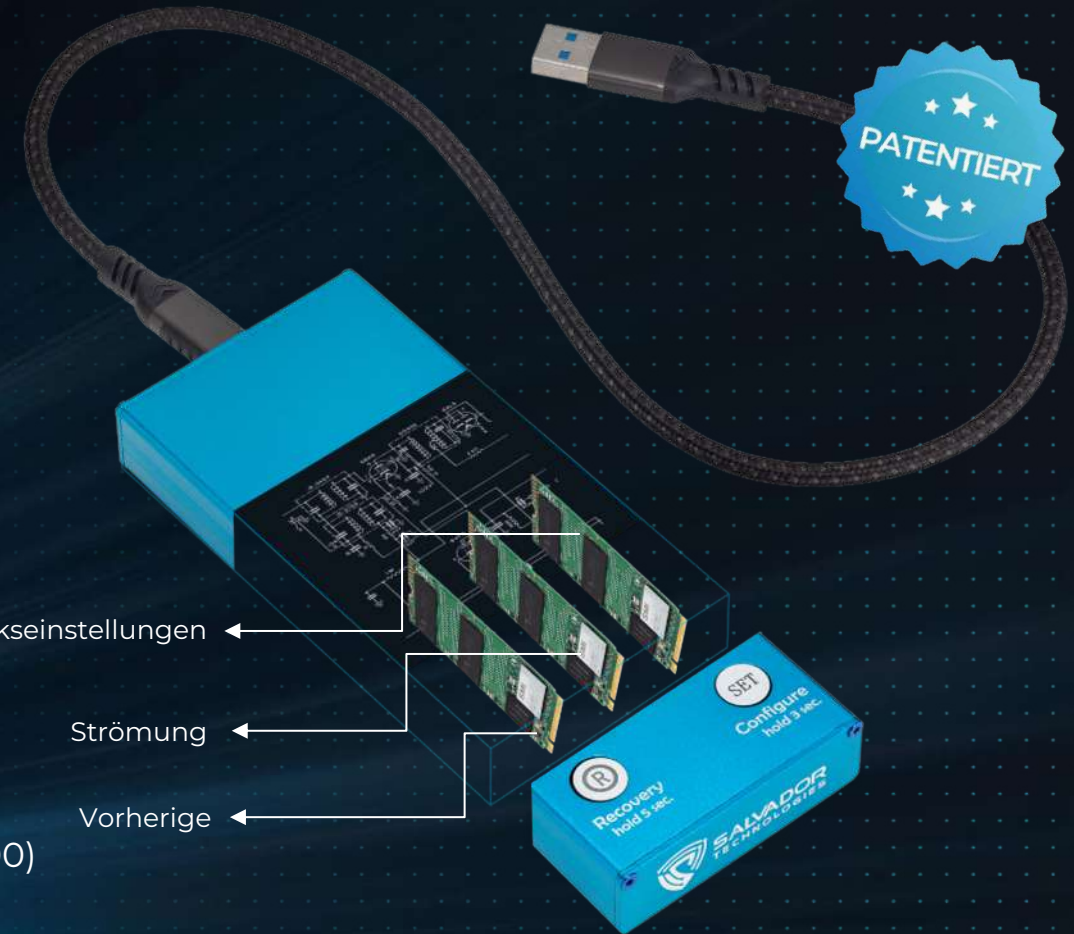
Verfügbare Kapazität: 3 x NVMe-Laufwerke

Optionen: 512 GB / 1 TB / 2 TB (PNs: CRU-512 / CRU-1000 / CRU-2000)

Zurücksetzen auf Werkseinstellungen

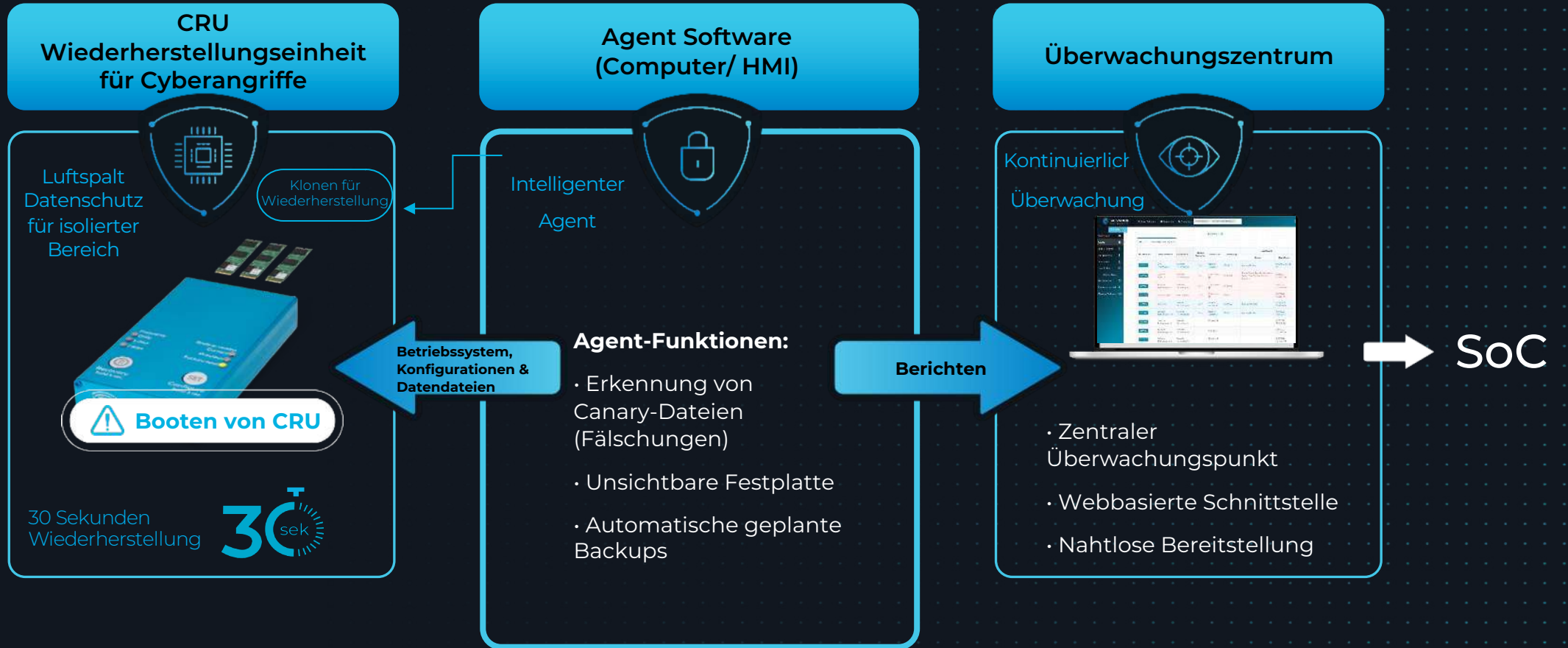
Strömung

Vorherige

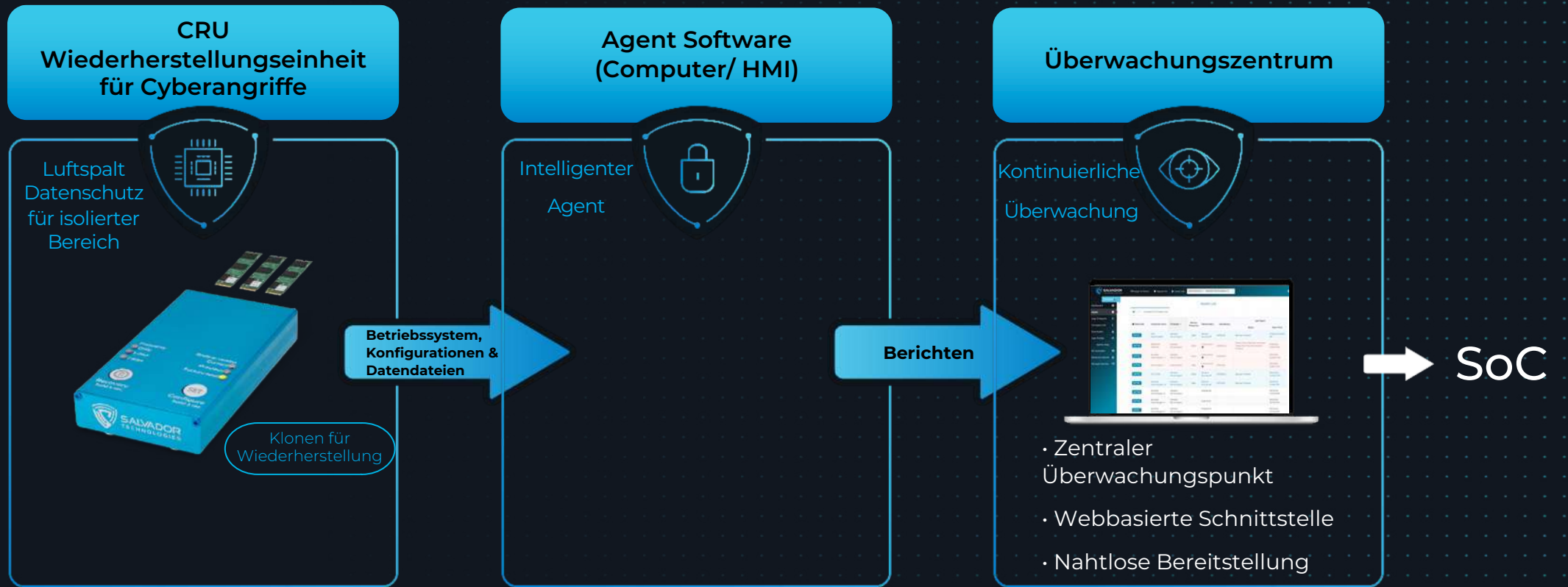


SCHRITT 1 –

Ausfallzeit? Starten Sie sofort neu!



SCHRITT 2 – Sie können während der Datenwiederherstellung weiterarbeiten



SCHRITT 3 – Zurück zur Normalität

CRU Cyber-Attack Recovery Unit

Luftspalt
Datenschutz
für isolierter
Bereich



The image shows a blue rectangular device with a silver top and bottom, labeled 'SALVADOR TECHNOLOGIES'. It has several ports on the front and a small display. Above it is a shield icon with a chip inside.

Agent Software (Computer/ HMI)

Intelligenter
Agent



Agent-Funktionen:

- Erkennung von Canary-Dateien (Fälschungen)
- Unsichtbare Festplatte
- Automatische geplante Backups



Starten von Computer

The image shows a shield icon with a padlock inside. Below the list is a button with a warning icon and the text 'Starten von Computer'.



Überwachungszentrum

Kontinuierliche
Überwachung



• Zentraler Überwachungspunkt
• Webbasierte Schnittstelle
• Nahtlose Bereitstellung

The image shows a shield icon with an eye inside. Below it is a laptop displaying a monitoring dashboard with various charts and data. Below the laptop are three bullet points.

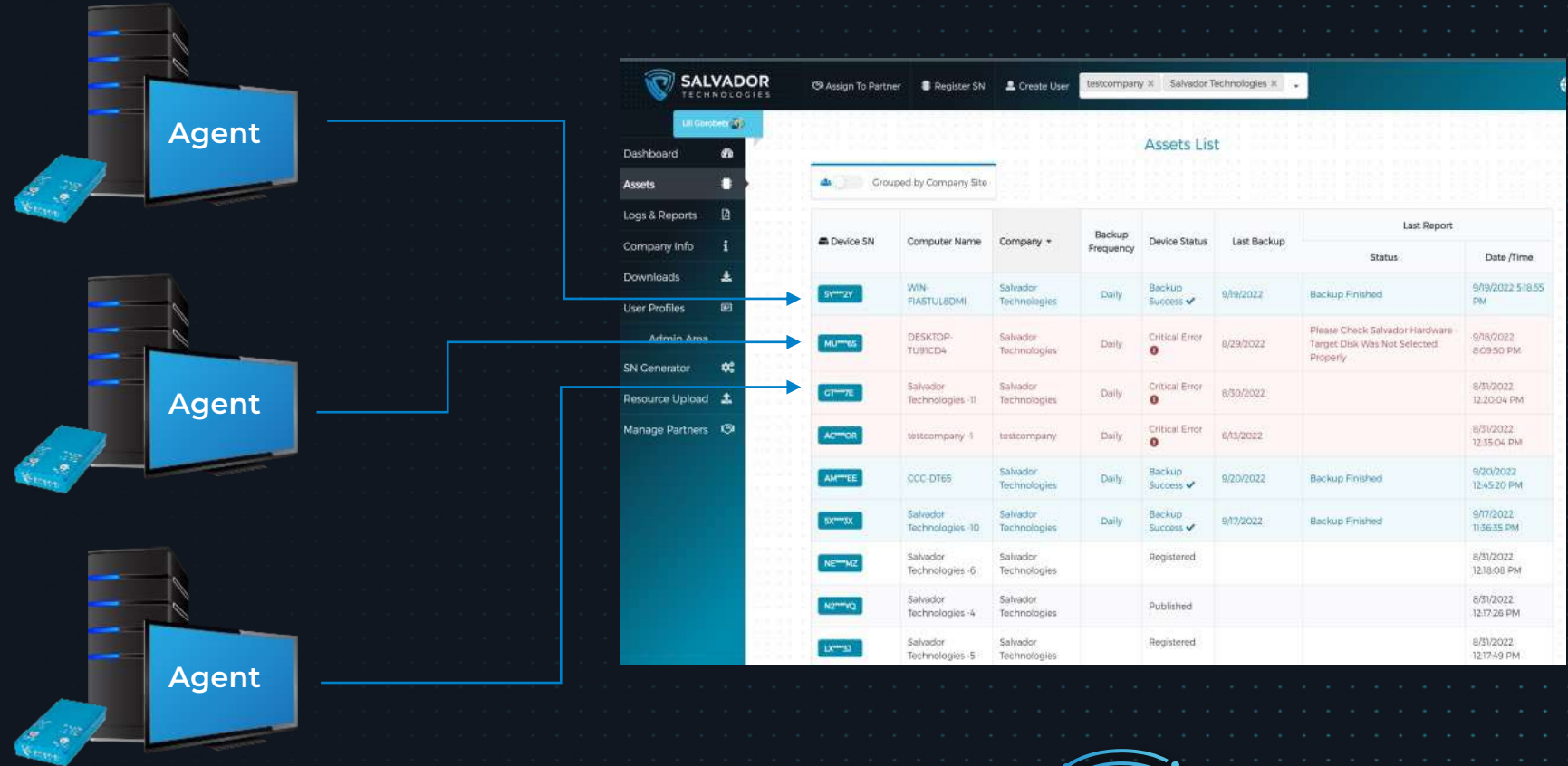


SoC

Volle Transparenz

Zentraler-Berichten des Backup-Status

- OK
- Meldung fehlt
- Angriff erkannt
- Hardware-Warnung



Computer-Systemumgebung

Die Integration des Überwachungssystems

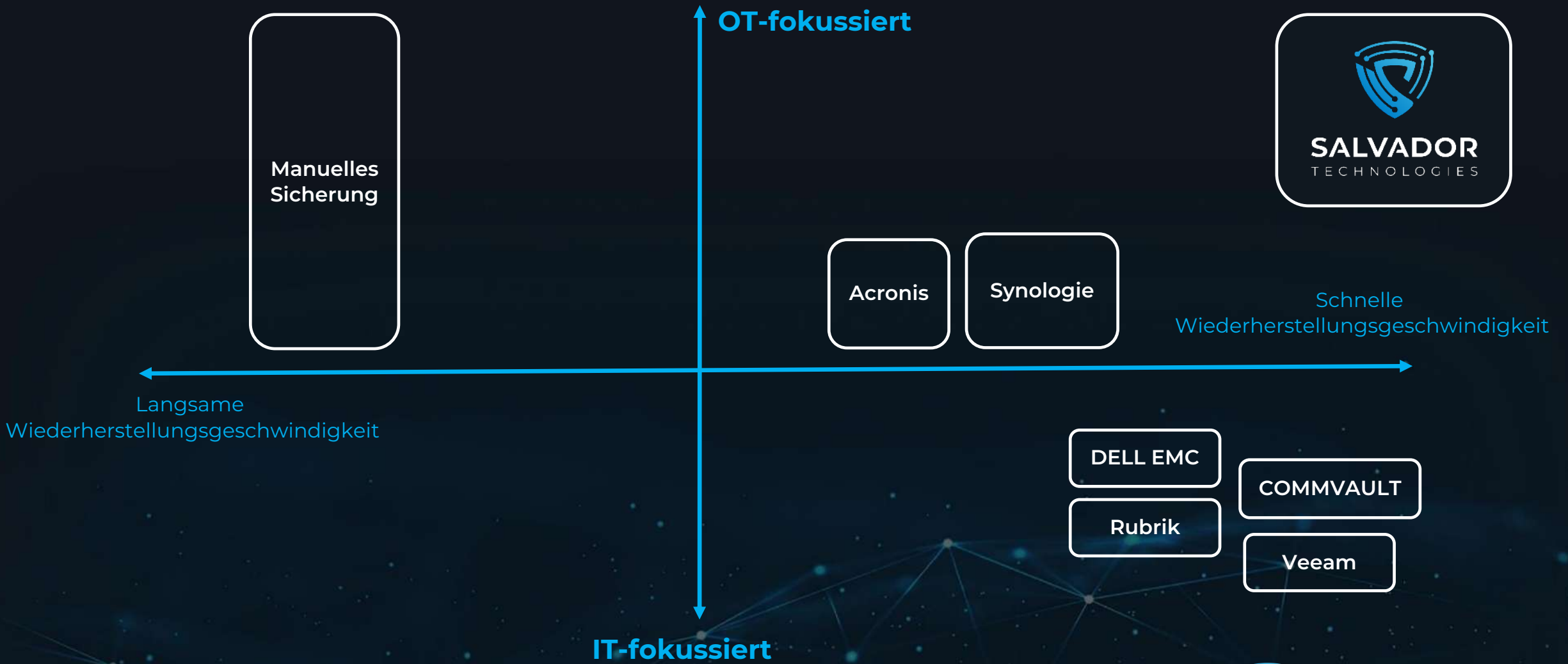




Unsere Tools zur Verhinderung von Datenverlust sind einfach zu bedienen - weniger als **1 Minute Installation**, um die Daten vor böswilliger Verschlüsselung zu schützen.

Es dauert nur **30 Sekunden**, um das System im Falle eines Cyberangriffs oder einer Systemstörung wieder in Betrieb zu nehmen.

Wettbewerbsvorsprung



Nehmen sie sich unserem schnell wachsenden kundenstamm in Europa und den USA teil



Herstellung



Medizin



Logistik



BMS



Kritische Infrastrukturen



Energie



Maritim



Herstellung von Chemikalien

Globale Mineralien - und Chemiehersteller, die Magnesium, Düngemittel, Brom für die Landwirtschaft und Lebensmittelindustrie liefern. Verbindungen wie Kalium, Phosphate und Calcium werden für verschiedene Anwendungen verwendet. Um die Produktion von Tonnen landwirtschaftlicher Produkte zu unterstützen, die weltweit vertrieben werden, betreibt Fabriken Hunderte von HMI-Stationen und Servern.

Die Notwendigkeit

Securing the continuity of operational servers responsible for management of the manufacturing processes, such as resource planning, monitoring, configuration, and real-time hazard recognition. Backup of Engineering workstation: Real-time Plant Control, product and operations traceability, Inventory Management.

Die Lösung

Deployment of Cyber Recovery Unit (CRU) on critical end-points, centralized servers responsible for ongoing operations of the factory. The CRU backups whole server with several virtual machines (VM) running on Windows 2012 Hyper-V platform.



Maritime Die Hafengesellschaft von Ashdod

Der Hafen von Ashdod, Israels größter Seehafen mit Frachtvolumen und ein wichtiges Tor für Waren und Fracht vom und zum Staat Israel, nahm 1965 seinen Betrieb auf.

Die Notwendigkeit

Betriebskontinuität kritische Eine Alternative zur vorherigen manuellen Backup-Methode, die physischen Zugang zu jeder Kranstation erforderte. Effiziente und häufige Backup aller operativen Systeme von Konfigurationsaktualisierungen für alle Endpunkter Ausrüstung - verschiedene Arten von Kränen, einschließlich Legacy-Systeme.

Die Lösung

Einmalige physische Installation auf der Kranstation, die automatische häufige Backups ermöglicht. Einsatz der Cyber Wiederherstellung Einheit (CRU) an kritischen Endpunkten: ABB HMI Terminalkran-Computersysteme basierend auf Window 10 und SIEMENS Window Server 2012 mit SIMOCRANE CMS (Kranmanagementsystem).



Logistik

- **UPS Logistikzentrum** Eigenständige Computer, die den kritischen Vorgang der Verpackungssortierung verwalten. Computer werden nicht überwacht und sind nicht gesichert. Wenn es nicht mehr funktioniert, werden Hunderte von Paketen in der Lieferung verzögert **[10 Einheiten]**



• Gebäudemanagementsystem

- **Gebäudemanagementsystem** eines großen Rechenzentrums:
Die Server, die für den Betrieb von Kühlsystemen,
Zugangskontrolle, Aufzügen verantwortlich **sind [10-50
Einheiten]**



• Kritische Infrastrukturen

- **Im Falle eines Ausfalls** eines Ammoniak-Kühlsystems muss der Bediener Dutzende von Endpoint-Controllern manuell überwachen. **[10-20 Einheiten]**
- **Wasserversorgungsanlagen** HMI (SCADA) Server, der die Wasserqualität überwacht und die Wasseraufbereitung von dicht besiedelten Gebieten in Israel steuert **[3-5 Einheiten pro Anlage]**

HÄUFIG GESTELLTE FRAGEN

Warum ist Ihre Wiederherstellung so schnell?

Unsere fortschrittliche Backup-Software erstellt ein vollständiges Duplikat des Systems, das das IT (Betriebssystem), Datendateien, Treiber und die eindeutige Benutzerkonfiguration enthält. Der Angreifer kann die Daten nicht erreichen, verschlüsseln oder löschen, da sie durch einen Luftspaltschutz gesichert sind. Dies ermöglicht es dem Benutzer, sofort neu zu starten und von Salvadors Festplatte zu arbeiten, ohne dass IT-Kenntnisse erforderlich sind, mit einem Klick auf eine Schaltfläche.

Irgendeine Lösung für Petabytes an Datenspeicherung?

Die meisten kritischen Assets können unsere Cyber Wiederherstellung Einheit(CRU)-Einheiten für die sofortige Wiederherstellung verwenden. Für Server mit großer Kapazität und private Clouds haben wir die Netzwerk Wiederherstellung Station (NRS), die auf dem DPU-Netzwerkadapter basiert. Dieses Produkt ist nicht durch die Kapazität Ihrer Daten beschränkt.

Wie vermeiden Sie ein Backup des Virus?

Wir führen eine kontinuierliche Überwachung der Daten sowohl des Computers als auch der Backup-Daten durch. Dies ermöglicht es uns, Angriffsversuche sofort zu erkennen und den Benutzer zu informieren, eine Aktion zu ergreifen.

Wie führe ich Wiederherstellungsübungen für mein Unternehmen durch?

Es ist einfach und erfordert nicht, dass Sie Ihre Workstation herunterfahren. Alles, was Sie tun müssen, ist, das Gerät von der Workstation anzuschließen und dann den Wiederherstellungsprozess auf einem anderen Computer testen (beim Booten vom Salvador-Gerät dauert der gesamte Vorgang ca. 30 Sekunden).

Wie geht man mit einem APT-Virus um?

Eine Kopie der Daten ist vor der Wiederherstellung nie zugänglich, um eine APT-Virusinfektion zu vermeiden. Die beiden anderen Kopien sind durch einen patentierten Offline-Schutzalgorithmus gesichert. Der Zugriff auf Daten in diesen Kopien ist zeitlich begrenzt und nur proprietäre salvadorianische Software ist erlaubt. Die Festplatten sind für das Betriebssystem.

unsichtbar.

Wie unterscheidet es sich von einem DR-System?

Ja. DR (Notfallwiederherstellung) wurde speziell für Datenverlust in Fällen wie Feuer, Wasser und physischem Diebstahl entwickelt. Dabei handelt es sich in der Regel um Online-Lösungen, die anfällig für Cyberangriffe sind. Salvadors Lösung basiert auf Luftspaltchutz-Speicher, um die Wiederherstellung nach Ransomware, Wiper-Malware und anderen Arten von Cyberangriffen zu ermöglichen.

Ich habe viele Endcomputer in meiner Organisation, wie kann ich Ihr Produkt bereitstellen?

Die Bereitstellung ist sehr einfach. Die Installation dauert weniger als eine Minute pro Station. Das bedeutet, dass Sie Hunderte von Systemen in wenigen Stunden bereitstellen können.

Wie führe ich eine Backup-Validierung durch?

Mit unserem benutzerfreundlichen Webüberwachungssystem können Sie den Status aller Workstations in einem einzigen Verwaltungspanel, in der Cloud oder vor Ort sehen (falls keine Internetverbindung besteht).

Lernen Sie unser Team kennen

Salvador Technologies team besteht aus 11 sehr erfahrenen fachleuten, jeder in seiner eigenen disziplin, missionsorientiert und mit großer sozialer Kompetenz!

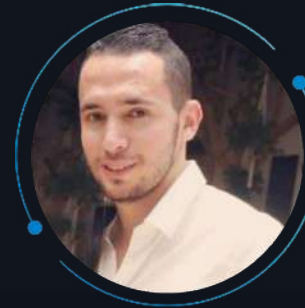
Das gesamte team engagiert sich für betriebskontinuität planung und teilt die leidenschaft, zur globalen cybersicherheitsagenda beizutragen.



Alex Yevtushenko

VORSITZENDE

Elektroingenieur,
Fachrichtung VLSI und
Technische Informatik



Oleg Vusiker

CTO

Elektrik- und
Elektronikingenieur mit
langjähriger Erfahrung in
der Nationalen Cyber-
Einheit



Amos Halfon

Vizepräsident Vertrieb
EMEA

29+ Jahre Erfahrung im Hi-
Tech-Vertrieb und Aufbau
globaler Märkte



Sharon Caro

Marketing -Leiter

15+ Jahre Erfahrung in
Geschäftsentwicklung,
Branding und globale Strategien



Ariel Maislos

Serienunternehmer
Investor (Anobit)



Prof. Hezy Yeshurun

Mitbegründer @ ForeScout
Prof. Emeritus @ TAU



Bruno Darmon

Vizepräsident Vertrieb
EMEA
@ Check Point



Gabriel Marcus

Cyber Architekt
@ Bandiskont



SALVADOR
TECHNOLOGIES

T: +90 216 912 10 05

✉ otd.salesgrp@onlineteknikdestek.com

www.onlineteknikdestek.com