Fast, Local, & Complete Recovery from Ransomware Attacks

Maria E. Vachino
Resilience requires quick Recovery

- Bad actors move faster than defenses can be built ('Protect' will never be enough)
- Organizations must be confident they can quickly recover & restore operations and productivity, and do it in minutes or hours not days or months
- Cyntegra has made it our mission to make ransom payments a thing of the past
Today’s Recovery Options: Costly and Insufficient

**Prevention (will never be enough)**
- Asymmetric arms race – only one mistake can have catastrophic results
- Anti-virus, Patching, Whitelisting, and other best practices reduce attacks, but do not prevent them
- Attack signatures are created *after* disaster strikes someone

**Restore from Normal Backups**
- Backup can be encrypted by the same ransomware
- Does not restore customizations and configurations that allow users to operate efficiently
- Corporate networks unlikely to be available to access backups and don’t support ‘everyone-at-once’ restoration
- Useless if OS (operating system) is corrupted

**Pay the Ransom**
- Restoration not guaranteed
- Funds criminal activity and organizations
- Increasing legal risks
- Insurance may not cover the incident

**Rebuild the System**
- Often requires device replacement, which is time consuming and expensive
- Requires time-consuming in-person support
- All data may be wiped out
- Lost productivity
Infection **without** Cyntegra

- Whole system may be corrupted – including the Operating System
- Users with no access to:
  - Data
  - Applications
  - Network
  - Communications
- Catastrophic loss of productivity and processing
- Huge costs, lost revenue
Infection with Cyntegra’s protection

- Patented approach
- Recovery environment remains untouched
- Protected by a TPM
Recovery with Cyntegra

- **Fast** – minutes, not days/weeks
- **Local** – fully self-contained, no support required
- **Complete** – includes OS, data, customizations and configurations, histories, and favorites
Cyntegra: under the hood

- **Patented approach**
  - Developed by a seasoned team with over 100 years of combined cybersecurity and technology experience

- **Trusted hardware**
  - Opal 2.0 compliant drive
    - Read-only data ranges
    - Guaranteed Boot
  - Trusted Platform Module 2.0 (TPM)
    - Integrity verification
    - Secrets controlled by hardware, never software

- **Cyntegra management and recovery OS (CyntOS)**
  - Separate protected OS to manage backup and restoration
  - Does not interfere with, or rely on, main OS
  - Allows custom backup policy
Cyntegra: Deployment

- **On device**
  - Preferably baked-in at device build
  - Can be retroactively installed
  - Requires Opal compliant drive
  - Requires sufficient storage

- **cydecar**
  - Separate self-contained SSD and enclosure
  - Works with any existing windows system, even if low available native storage and non-Opal compliant drives
  - Requires initial config
  - Requires user to keep it available

- **Limited and intuitive end-user interaction**
  - Backups can be forced on power-on or power-off
  - Potential for automatic wake and backup
  - Restore requires power-cycle and simple menu-driven choices
Summary

- Mission driven
  - Making ransomware payments and business disruption a thing of the past

- Resilient and agile recovery capability
  - Fast
  - Local
  - Complete

- Patent-pending solution for servers, mobile devices, and industrial IoT
Cyntegra: leadership

**Maria Vachino**  
CEO

- Former Senior Cybersecurity Researcher and Strategist at Johns Hopkins Applied Physics Laboratory
- Former Technical lead for Department of Homeland Security Cybersecurity RD&T programs
- Former Director of Digital Identity at boutique consulting firm, Easy Dynamics
- Kantara Initiative Director at large
- UpSurge Baltimore Cybersecurity team
- Recognized expert in cybersecurity, digital identity, and blockchain

**Giles Watkins**  
Executive Chairman

- Former Partner with both EY and KPMG in Cyber Security and Technology Risk
- Led EY’s Tech M&A practice advising on over 500 deals
- Founded and led international Privacy consultancy, Concentium, subsequently sold to KPMG
- Former Board Member of the Open Identity Exchange and UK Country Leader for the International Association of Privacy Professionals
- Member of ISO standards committee for Blockchain and Distributed Ledger Technology

**David Challener, Ph.D.**  
Master Inventor

- Former Master Inventor at IBM with over 130 patents
- Original inventor of the patents underlying Cyntegra
- Author of ‘A Practical Guide to TPM 2.0’
- Chair of the Trusted Computing Group’s TPM WG
- Recognized Trusted Computing expert
- Independent Security Architect

**Russell Fink, Ph.D.**  
Engineering Consultant

- Cybersecurity professional with expertise in TPM and Opal technologies
- Co-inventor and engineering lead of the patented technology underlying Cyntegra

© Cyntegra ltd. All rights reserved
Questions?
The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.