UNISYS | Securing Your Tomorrow®

DELL Technologies TITANIUM PARTNER

HOW TO BECOME CYBER RECOVERY READY

Dell Technologies PowerProtect Cyber Recovery

Cyber Recovery Ready

Fast
Start your recovery immediately without having to wait for ransomware neutralization

Clean
Be confident that your recovery data is 99.5% free from ransomware reinfection

Secure
Maintain an isolated operation that enables management, replication, detection, recovery

To find out more, visit unisys.com

Are You Actually Ready for Ransomware?

The bad guys are constantly improving their tools, processes and backdoors to beat your defenses, stop your business and to exact an expensive ransom. Once they get inside your company, they map your network and operations, trick you into revealing your recovery systems, infect your back-ups and DR, and lock-down your most critical systems to force a ransom payment.

Statistically, it's a matter of time until they take control. And every hour, day, or week that your critical operations are locked-down is costing money and even jobs. This is not just a security issue, but a critical business continuance threat that is too important to disregard.

What's your plan when your domain server, data catalogs, and financial applications, are all polluted or locked? Can you restart fast enough to minimize financial impacts to your company?

Dell PowerProtect Cyber Recovery

Cyber recovery-ready means you can immediately access clean data, restore services and applications, and quickly get users back to work with minimal impact to your business after a ransomware lock-down.

The Dell EMC PowerProtect Cyber Recovery is the gold standard for rapid recovery operations, providing the fastest, cleanest, and most secure solution available to get your operations back on track despite a serious ransomware lockout. And do it without having to retool your network or security; without worrying about ransomware reinfections.

Key points of cyber recovery

- **Management:** direct operations, monitoring and recovery from a single-pane-of-glass in your remote SOC/NOC so recovery is rapid and seamless.
- **Replication:** automated daily copying of critical data into a cryptographically isolated and air-gapped vault where the data is retention-locked and immutable so you always have fresh clean copies of your data ready for recovery.

- **Detection:** automated file analysis detects and alerts on entropy (chaos in the data) deep in the files so you can quickly select the freshest clean files in your recovery without the threat of ransomware reinfections.
- **Recovery:** begin immediate recovery to restore critical services and get users back-to-work with pre-scripted operations, supported by Zero Trust cryptographic micro-segments that meet aggressive and predictable RTO objectives – so you can begin recovery without waiting to neutralize the ransomware.

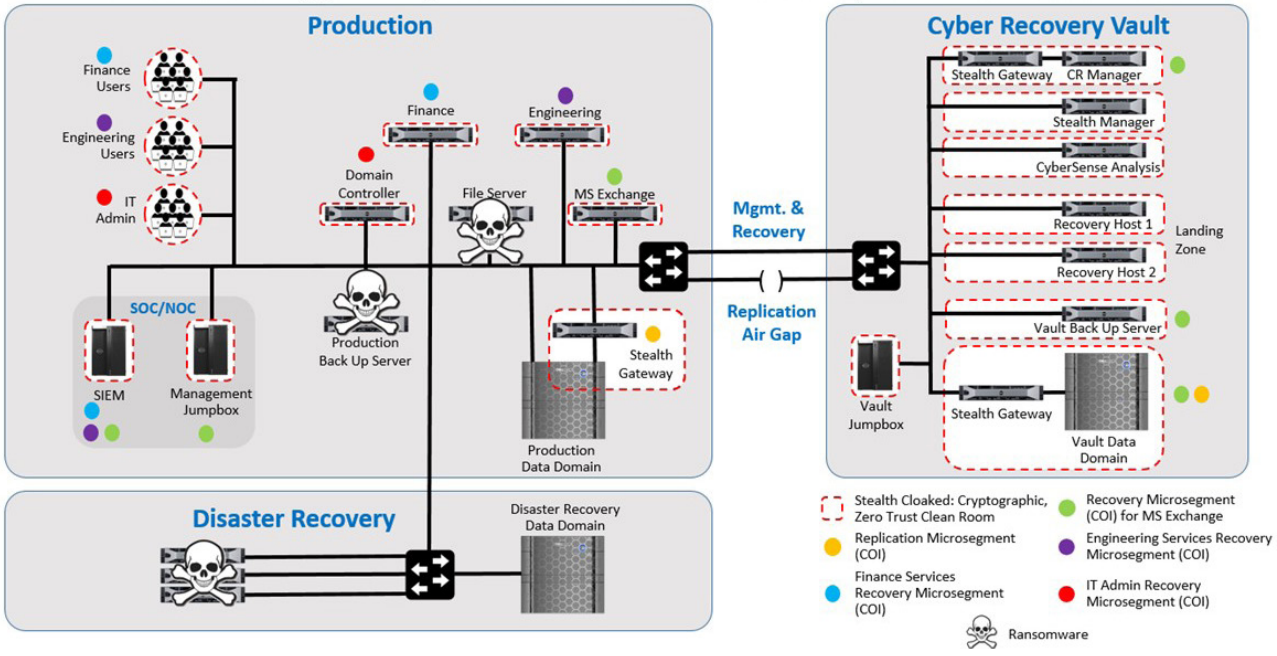
Complete Cyber Recovery Systems and Services

Here's what we provide to help you become a cyber recovery ready operation:

- **Preparation:** consulting specialists help design and build your recovery solution that includes a run book detailing virtually every decision, priority, and action required to restore operations. Plus, we'll help train, test and perform mock cyber recovery exercises so you'll be ready to recovery anytime ransomware strikes.
- **Systems:** complete compute, storage, security, back up, and networking systems to create an isolated and highly secure air-gapped cyber recovery vault.
- **Automation:** replicates critical data every day, or even multiple times a day, from production to the vault, where it's retention-locked for immutability, analyzed for corruption, and immediately reported to your cyber recovery operations.
- **Analysis:** CyberSense analytics machine-learning engine detects and flags levels of entropy, or chaos, deep in the replicated files that can escape Meta data analysis, so you will know that the files you chose to recover are clean and will not reinfect your operations.
- **Security:** Stealth™ Zero Trust micro-segmentation protects all vault systems with cryptographic cloaking and data encryption so they are isolated from ransomware. You can pre-script recovery micro-segments for your entire enterprise that remain passive until needed for a recovery, without additional hardware or licensing costs. In addition, Stealth integrates with your SIEM so you can detect suspicious behaviors and isolate endpoints in under 20 seconds.
- **Implementation:** our project management and technicians work with your IT team to stand-up, integrate, test, and assure operational excellence.
- **Services:** Unisys provides real-time monitoring, management, co-location, and recovery services so you can maintain a recovery-ready operation.

Cyber Recovery: Enabling Fast Restoral of Services and Users

Servers and user systems are protected by Stealth's cloaking cryptography so IT can quickly begin to restore services using pre-configured Zero Trust microsegments on day zero of a ransomware attack



For more information visit www.unisys.com