Cyber Recovery Capabilities Protect the Most Critical Data

Government and transportation agencies are among the five most cyberattacked industries over the past five years, and attackers are increasingly targeting backup data. Most backup systems are not designed to recover from cyberattacks, but the Unisys Stealth with Dell EMC Cyber Recovery solution is different. It adds an additional level of protection and lowers the overall risk.

Cyber Recovery Capabilities Protect the Most Critical Data

Government and transportation agencies are among the five most cyberattacked industries over the past five years, and attackers are increasingly targeting backup data. Most backup systems are not designed to recover from cyberattacks, but the Unisys Stealth with Dell EMC Cyber Recovery solution is different. It adds an additional level of protection and lowers the overall risk.

Unisys Stealth® with Dell EMC PowerProtect Cyber Recovery

Dell EMC recently created a powerful cyber recovery solution that uses innovative Dell EMC automation, workflow and security analytics tools. This solution employs a backup and recovery data appliance called Dell EMC Data Domain to provide secure and scalable high-speed data backup storage, archiving and data recovery. Unisys Stealth® is a software suite that transforms an existing network—both on-premises and in the cloud—into a zero-trust network without requiring changes to existing networks or applications.

- Stealth™ principles are simple: trust no user or device (inside or outside the private network) and grant as little access as possible (based upon reliable identification).
- Stealth is a “defense-grade” solution that uses identity-based microsegmentation. Network microsegments can be defined and managed using an identity management system such as Active Directory or LDAP.
- Stealth creates a cryptographic wrapper around the Dell EMC Cyber Recovery vault so it’s virtually invisible to hackers and malware and only allows access to authorized devices.

THREATS COME IN MANY FORMS

Ransomware, cryptojacking, targeted attacks, malicious PowerShell scripts and “living off the LAN” are just a few examples of attacks that can:
- Lock up computers and charge a ransom
- Steal confidential information
- Destroy data to get attention

Some malware—such as a remote access Trojan (RAT)—just sits in the network, waiting to be triggered and often ends-up in “secure” back-up systems, just waiting to be restored for active duty. Access is sold to the highest bidder on underground networks.

Users are a significant source of incidents, from malicious employees to accidental user actions.

Budgets can be difficult for security professionals to acquire, but are essential to preventing a large-scale data breach that negatively impacts the company.
Unisys Stealth with Dell EMC PowerProtect Cyber Recovery

Why Do Public Sectors Organizations Need Unisys Stealth with Dell EMC PowerProtect Cyber Recovery?

Municipalities are generally less prepared to battle cyberattacks than companies, security professionals say. They increasingly rely on technology to deliver city services, but have aging computer systems, according to Standard & Poor’s.

Unisys Stealth securely microsegments data centers and protects data and systems by cloaking strategic assets, making them undetectable and inaccessible from other systems inside and out of the production network.

Why Does It Matter?

$2.2M to $6.9M is the potential cost of failing to secure data.

70% of organizations report at least one security incident that negatively impacted operations.

72% of enterprises are still immature (or worse) in capabilities involving incident response and recovery.

Learn More about Unisys Stealth with Dell EMC PowerProtect Cyber Recovery at