Financial Industry Is a Prime Target for Cyberattacks

Cyberattacks are on the rise, causing greater lost revenue, negative publicity and customer distrust. In several recent cases, public companies suffered losses that exceeded $250M from a single breach.

The financial industry needs a comprehensive approach to cyber-risk mitigation. One that goes beyond threat detection and remediation to significantly strengthen incident response and associated data security and recovery strategies.

Cyber Recovery Capabilities Protect Your Customer’s Critical Data

Attackers are increasingly targeting backup data, and most backup systems are not designed to recover from cyberattacks. But Unisys Stealth® with Dell EMC Cyber Recovery is different. It adds an additional level of protection and lowers 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).

---

**STAY ONE STEP AHEAD**

- **Be proactive.** It’s not enough for banks to evaluate your security technology in the aftermath of a security breach. Financial service institutions need to behave like they are already under attack.

- **Understand the MO.** Get an outside perspective as to why the organization is a target, how vulnerable it is and the most common methods used to attack it. Understanding the MO of the criminals targeting the organization puts financial services institutions in a better position to prevent it from happening.

- **Build a cybercrime division.** Don’t let criminals exploit gaps in the organization. Break down silos within the bank (particularly security, fraud and legal) and integrate the knowledge, processes and technology under a single banner to manage risk. A collaborative approach will prevent fraud and fight crime in a proactive and united environment.
Stealth is a “defense-grade” solution that uses identity-based segmentation. Network segments 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 PowerProtect Recovery vault so it’s virtually invisible to hackers and malware and only allows access to authorized devices.

**Why Do Financial Services Need Unisys Stealth with Dell EMC PowerProtect Cyber Recovery?**

Trust is a precious commodity in today’s world of financial services. As threats continue to evolve, banks who want to secure their position as a trusted partner and bank of choice must ensure they have the most effective tools and solutions in place to mitigate risk. Stealth provides an extra level of protection to the Dell EMC Cyber Recovery solutions to increase deployment flexibility and lower your risk profile.

---

**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

---


---

**Unisys Stealth with Dell EMC PowerProtect Cyber Recovery**

The Unisys Stealth with Dell EMC PowerProtect Cyber Recovery solution protects systems-of-record data in their original form and secures all traffic with (and within) the vault with trusted encrypted access.

---

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