Cyberattacks Can Cripple Your Company

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.

A 2018 ISACA global survey of cybersecurity professionals revealed that 50 percent are seeing a higher volume of attacks than in the previous year.

The magnitude of today’s cybersecurity risks has made IT security an essential part of digital enterprise strategy.

• By 2020, 100% of large enterprises will be asked to make annual reports on cybersecurity to their board of directors, according to Gartner.

• Preventing cyberattacks has been a priority. However, the likelihood of discovering all IOCs (indicators of compromise) before harm is done are slim.

• Early detection of IOCs is extremely difficult, which gives hackers enough time to orchestrate attacks ranging from extortion to outright destruction.

• According to Gartner’s Top Seven Security and Risk Management Trends for 2019, Data Security Governance Frameworks will drive the prioritization of data security investments.¹

Enterprises need 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 Most Critical Data

Attackers are increasingly targeting backup data and most backup systems are not designed to recover from cyberattacks.

But Dell EMC Cyber Recovery with Unisys Stealth® is different. It adds an additional level of protection and lowers the risk.
Dell EMC Cyber Recovery

To help counter ransomware and other cyberattacks, Dell EMC recently created a powerful cyber recovery solution. It uses innovative Dell EMC automation, workflow, and security analytics tools to ensure that gold copies of critical data are isolated yet available, which allows business processes to resume as quickly as possible.

Security is improving in most areas, but companies still need a way to quickly recover lost data to avoid costly downtime. The Dell EMC Cyber Recovery solution combines data isolation with business continuity capabilities to minimize the impact of an attack and help quickly recover critical data and systems.

The 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 disaster recovery. Because of its native data deduplication and seamless integration with backup workflows, automated processes can move and retain protected copies of critical data to the Dell EMC Cyber Recovery Vault. This cloud-enabled backup storage removes the vital data from the attack surface. Once the data is in the vault, it can be tested and analyzed without performing a restore, eliminating the risk of activating malware.

Systems that share a COI (community of interest) key can communicate subject to the policies of their COI. No user or device that is not a member can communicate or detect other systems unless permitted by their CIO policy.

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. Access is sold to the highest bidder on underground networks.

Users are a significant source of incidents. Either from malicious employees inside the organization or accidental user actions.

Budgets can be difficult for security professionals to acquire, but are essential for an effective program. Ironically, money becomes no object after a large-scale data breach that negatively impacts the company.
Adding Unisys Stealth to Dell EMC Cyber Recovery

What Is Unisys Stealth?

Unisys Stealth is a software suite that transforms an existing network—both on-premises and in the cloud—into a Zero Trust Network. Stealth™ overlay technology requires no 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 (always based upon reliable identification).
- Stealth is a ‘defense-grade’ solution that uses identity-based segmentation. Network segments can be defined and managed using an identity management system that has high business alignment, such as Active Directory or LDAP.

Stealth’s Zero Trust Solution Stops Data Breaches

Stealth creates dynamic, identity-based microsegments called communities of interest (COI) to reduce risk.

- Stealth treats all network traffic as untrusted, only permitting communication when COI membership is confirmed.
- By establishing a secure COI, Stealth separates trusted systems, users, and data from the untrusted.
- All communications between COI members are encrypted; end points are concealed and undetectable from unauthorized users.
- Product architecture consists of host agents and network components, making the architecture very flexible.

Why Layer Unisys Stealth with Dell EMC Cyber Recovery?

The Dell EMC Cyber Recovery solution protects your organization from sophisticated attacks focused on destroying data or holding it hostage. Stealth adds an additional level of protection, increases deployment flexibility, and lowers your risk profile.

Stealth creates a cryptographic “air gap,” ensuring that systems in the Dell EMC Cyber Recovery vault network are undetectable and inaccessible from other systems in your production network.

Stealth also gives you the flexibility to place the vault boundary anywhere in the network, with granularity as small as a single system or user. Stealth restricts traffic to specific authorized users—even between members of a COI.
The potential cost of failing to secure data²

5 most cyberattacked industries over the past five years
Healthcare, Manufacturing, Financial Services, Government, and Transportation³

70% of organizations
Report at least one security incident that negatively impacted operations⁴

72% of enterprises
Are still immature (or worse) in capabilities involving incident response and recovery⁵

The Complete Trust Resilience Solution
Every business is different, with unique goals, applications, and threats. Our services professionals will help you develop processes and procedures for protecting and recovering your critical data in the event of a breach.

The Dell EMC Cyber Recovery solution with Unisys Stealth secures all traffic within the vault and enables swift cyber recovery:

1. Creates a safe, isolated recovery environment
2. Streamlines security and regulatory compliance by safeguarding against data destruction and ransom attacks
3. Provides secure COIs that reduce attack surfaces and prevent threats from propagating
4. Drops unauthorized incoming packets and deters the reconnaissance phase of attacks
5. Uses security policies based on identity (not IP addresses), allowing flexibility without security compromise
6. Requires no application changes or disruptions to existing environments
7. Encrypts data in motion during replication and recovery for additional protection
8. Has NIAP security certification

Learn More About
Dell EMC Cyber Recovery with Unisys Stealth
www.unisys.com/cyber-recovery

Unisys
www.unisys.com
Dell EMC
www.dellemc.com

Engage
Andrew Peters
Unisys
Stealth Business Development Director
andrew.peters@unisys.com
+1.650.245.7683

Cara Thomas
Dell EMC
Dell Technologies Global Alliance Account Manager
cara.thomas@dell.com
+1.415.227.3800

© 2019 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

4. RSA Cybersecurity Poverty Index.