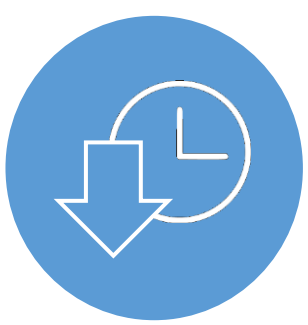
The Challenge: Cyber Attacks are the enemy of data-driven businesses

Cybercrime has been called the greatest transfer of wealth in history. Accenture estimates that $5.2 trillion of global value is at risk by cybercrime in the next 5 years.[1]

Regardless of the industry or size of the organization, cyber attacks continually expose business and governments to compromised data, lost revenue due to downtime, reputational damage and costly regulatory fines. The average annual cost of cybercrime per company increased to US$13M in 2018, a surge of 72% in just the last 5 years.[1]

Having a cyber recovery strategy has become a mandate for business and government leaders. 79% of global executives rank cyber attacks as one of their organization's highest risk management priorities according to a 2019 Marsh & Microsoft study.[2]

Ransomware costs forecast to reach $20 Billion by 2021[3]



Downtime increased by 200% YOY, with costs 23x greater than the average ransom[4]

34% of businesses took a week or more to recover full access to their data [5]

Ransomware Attacks Forecast to Occur Every 11 Seconds, a 21% YOY increase[3]

Trends – Air Gapped/Offline Protection

FBI: Cyber Defense Best Practices - Regularly back up data and verify its integrity. Ensure backups are not connected to the computers and networks they are backing up. For example, physically store them offline. Backups are critical in ransomware; if you are infected, backups may be the best way to recover your critical data.

FDIC: Joint Statement on Heightened Cybersecurity Risk – Securely store system and data backups off site at separate geographic locations and maintain offline or in a manner that provides for physical or logical segregation from production systems

Federal Financial Institutions Examination Council - An air-gaped data backup architecture limits exposure to cyber attack … and restoration of data to a point in time before the attack

Federal Reserve – financial institutions should consider … logical network segmentation, hard backups, air gapping [and] physical segmentation of critical systems

The Dell Technologies Value

DELL TECHNOLOGIES CYBER RECOVERY

- Providing the *only* automated, vaulted air gap solution in the market
- All vaulted data is immutable and untraceable
- Full context indexing coupled with intelligence and machine learning analytics
- Deep multi-layer data analysis capability
- Robust enhanced recovery tools
- First technology solution provider in the Sheltered Harbor solution provider program [*http:// www.shelteredharbor.org]*

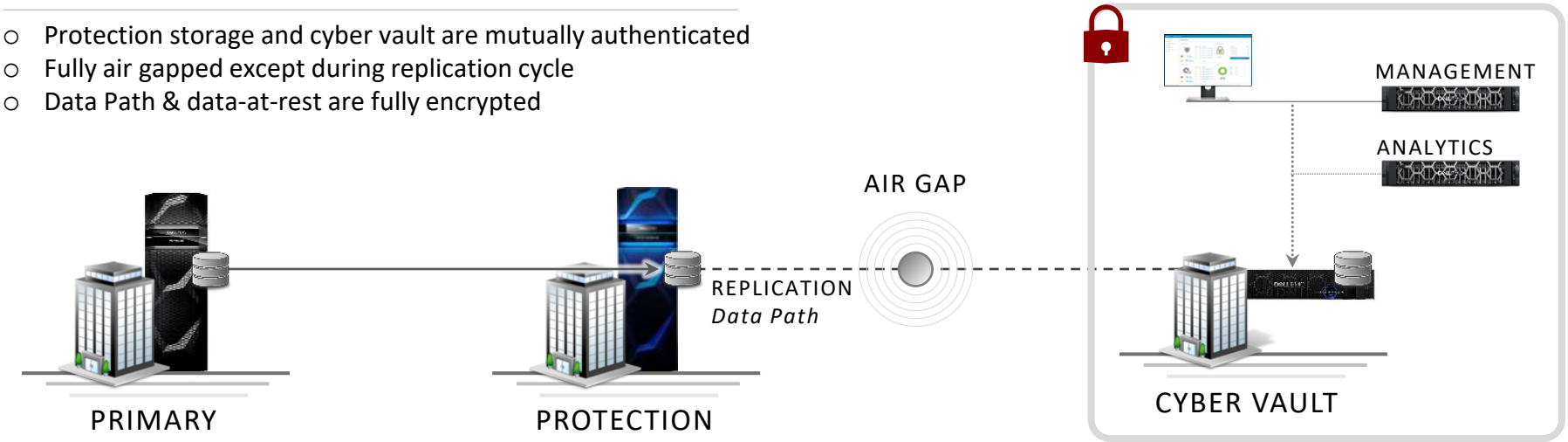
CYBER RECOVERY DIFFERENTIATION

GOOD	Retention Lock, Immutable Copy	✓
	Elevated Security Credentials	✓
BETTER	Insider Protection	✓
	Multi-Backup Software Vendor Support	✓
BEST	Automated, Vaulted Air Gap	✓
	Full Context Indexing with Machine Learning Analytics	✓
	Robust Recovery Tools	✓
	Sheltered Harbor Program	✓

Solution Overview

CYBER RECOVERY ARCHITECTURE & WORKFLOW

- Protection storage and cyber vault are mutually authenticated
- Fully air gapped except during replication cycle
- Data Path & data-at-rest are fully encrypted



Business Differentiation

DISASTER RECOVERY vs CYBER RECOVERY

BUSINESS VARIABLE	DISASTER RECOVERY	CYBER RECOVERY
Nature of Disaster	Flood, Power Outage, Weather	Cyber Attack; Targeted Approach
Impact of Disaster	Regional; Typically Contained	Global; Widespread Across Organization
Topology	Connected; Multiple Targets	Isolated; Additional to Disaster Recovery
Data Volume	Randomized; All Data	Targeted Specific Data
Recovery	Standard DR; Failback	Iterative; Selective Recovery

How do I start? IT Infrastructure - Critical Rebuild Material

Authentication, Identity & Security
- Certificates
- Active Directory / LDAP
- DNS dumps
- Event logs (including SIEM data)

Intellectual Property
- Source code
- Proprietary algorithms
- Developer libraries

Networking
- Switch / router configuration
- Firewall / load-balancer settings
- IP Services design
- Access Control configuration
- Firmware / Microcode / Patches

Storage
- SAN / Array configurations
- Storage Abstraction settings
- Backup Hardware configuration
- Firmware / Microcode / Patches

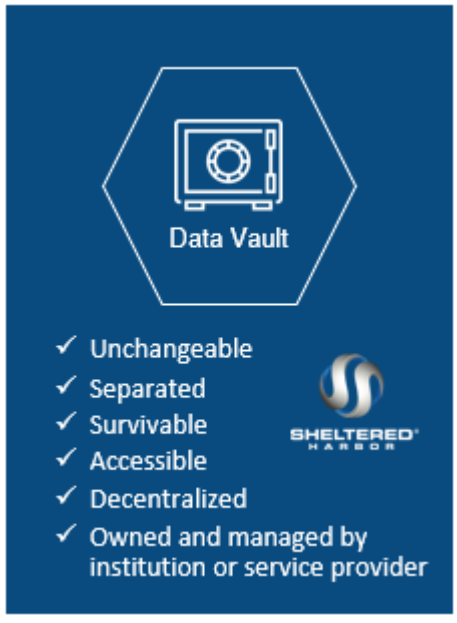
Host and Build Tools
- Physical/Virtual Platform Builds
- Dev Ops tools & automation scripts
- Firmware / Microcode / Patches
- Vendor software
  - Binaries (golden images)
  - Configurations & settings

Documentation
- CMDB / asset management extracts
- D/R and Cyber Recovery Run-books & Checklists
- HR Resources & Contacts Lists
- Incident Response Plan

Sheltered Harbor – First Solution Partner

Created in 2015 by the financial industry the Sheltered Harbor standard incorporates a set of cyber resilience and data protection best practices and safeguards for protecting U.S financial data. Cyber threats, including ransomware, data destruction, or theft targeting production and backup systems, put consumer and corporate financial data at risk

Dell Technologies is the first technology solution provider to join the Sheltered Harbor Alliance Partner Program. To comply with the Sheltered Harbor Specification, the Cyber Recovery vault architecture is being extended to perform the Archive Generation and Secure Repository processes. Extracted Sheltered Harbor data is saved in production, then securely replicated via a logical, air-gapped, dedicated connection to the vaulted environment where the remaining steps, such as retention locking, are performed.



Common Misconceptions – Limited protection/recovery from ransomware attacks

Data Encryption
- No protection for destructive or ransomware attacks
- For Data Protection, not for Recovery

More Security
- Can't succeed every time
- Consider insider threats, human error, and system complexity

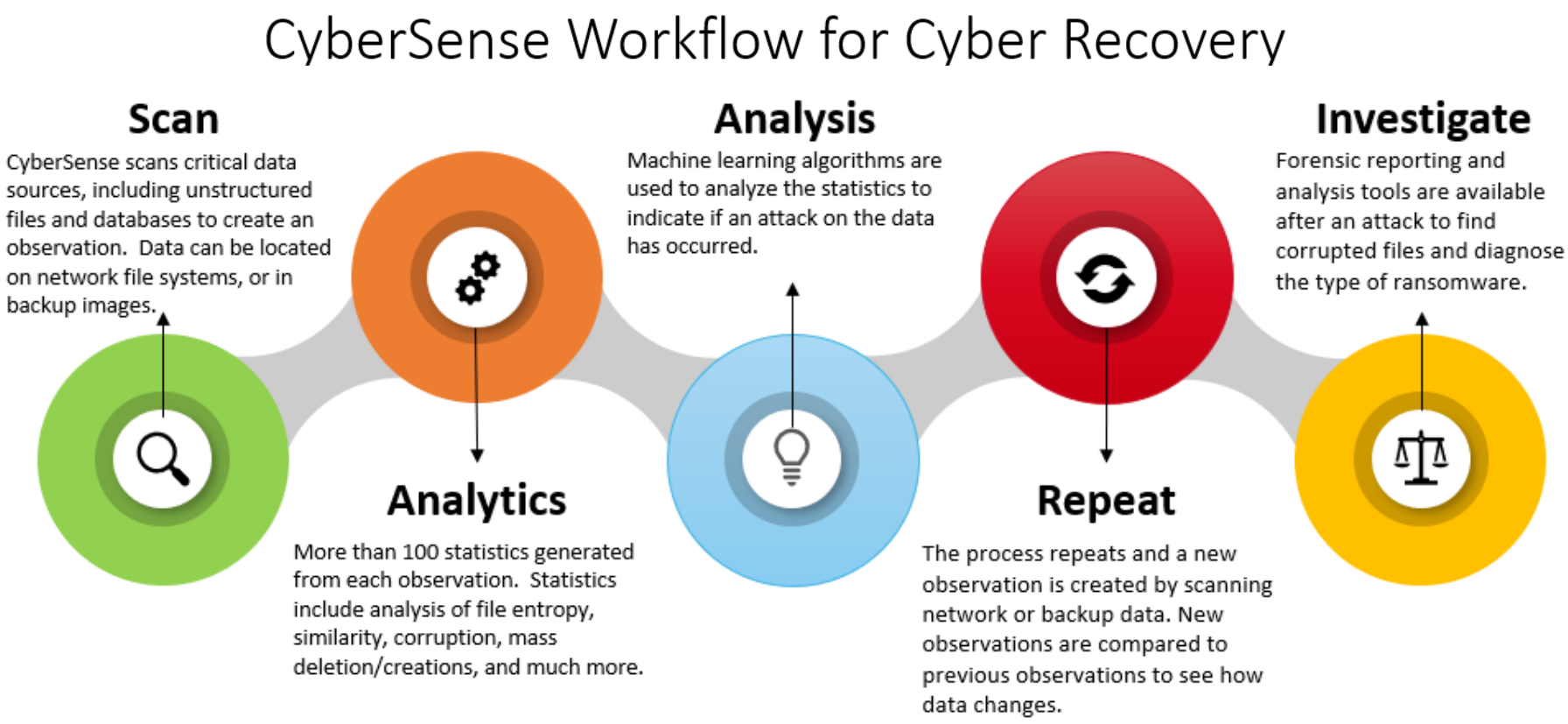
Tape Backups
- Weeks to recover as losses mount each day
- Requires backup infrastructure

Traditional DR
- Backups are attacked
- Replication spreads the problem

Retention Lock (Prod)
- Locking production backups still leaves them as a target
- Disaster copies easily accessed

Cyber Recovery Analytics

CyberSense works with data protection software and analyzes data in backups to identify files and databases that have been unknowingly corrupted by ransomware. CyberSense utilizes a combination of full-content-based analytics and machine learning to detect if an attack has occurred. CyberSense analytics are indicative of all common attack vectors including entropy changes, known ransomware extensions, data corruption and deletion, and over 100 other statistics. Machine learning analyzes CyberSense's statistics to determine if data corruption has already occurred.



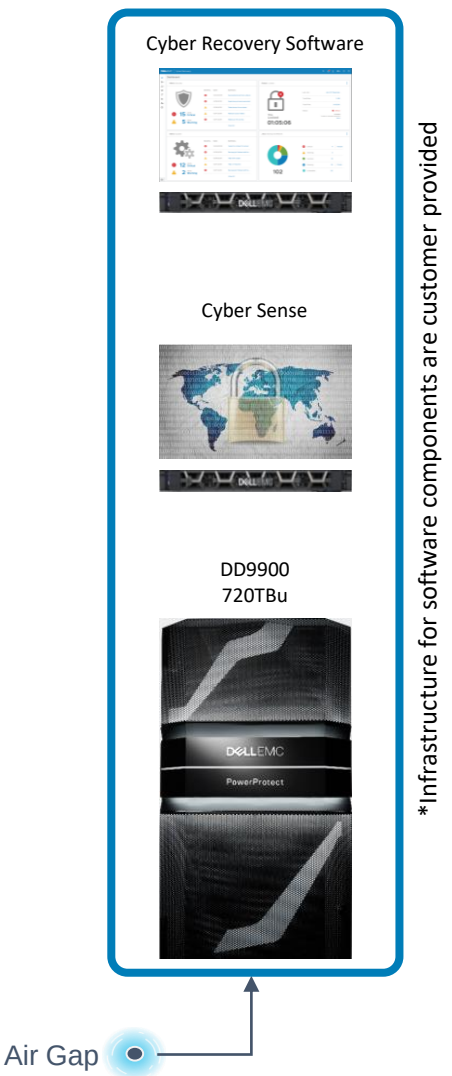
CyberSense: Post Attack Workflow

Post attack, CyberSense provides forensic tools to diagnose and recover. This includes reports on files that were impacted so they can be replaced with the last know good version, the type of attack vector, and with analysis of event logs the specific users accounts and executables or malware that performed the attack. CyberSense analytics, machine learning and forensic tools deliver the knowledge you need to quickly detect and recover from cyberattacks.

Investment Summary

CYBER RECOVERY T-SHIRT SIZE	Starter	S	M	L	XL
Front End TB	**3**	**32**	**128**	**256**	**384**
PowerProtect Data Domain	$11,375.00	$107,800.00	$290,500.00	$599,200.00	$912,100.00
CyberSense Software	$3,325.00	$15,050.00	$56,175.00	$110,250.00	$164,500.00
Estimated Price to Customer	**$14,700.00**	**$122,850.00**	**$346,675.00**	**$709,450.00**	**$1,076,600.00**
All Vault Infrastructure Elements	$61,950.00	$102,900.00	$156,100.00	$203,000.00	$243,600.00
ENHANCED & BASE PRICE	**$76,650.00**	**$225,750.00**	**$502,775.00**	**$912,450.00**	**$1,320,200.00**
Elements Included: Infrastructure Server, Management Workstation, KMM Switch, Firewall, Switches, Rack, CyberSense Server(s)					

Base Vault



Enhanced Vault

Where do we start?

Critical Rebuild examples:

- Network Configs
- DNS
- AD
- Firmware/Patches
- CMDB, DR Run Books
- Source Code
- Proprietary Algorithms
- Access Control

Size the vault for this ⬆ *then,*

✓ **Pick 5 mission critical applications**

❑ **Now you can size your vault!**

For More Information Contact:

- Abby Henstein| Dell Technologies Account Executive | Abby.Henstein@dell.com
- Lonnie Aanden| Dell Technologies DPS Field CTO| Lonnie.Aanden@dell.com

Source Information:

1. Source: Accenture “The Cost of Cybercrime Study” 2019
2. Source: Marsh & Microsoft “Global Cyber Risk Perception Study” 2019
3. Source: Cybersecurity Ventures “Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021” 2019
4. Source: Datto’s “Global State of the Channel Ransomware Report” 2019
5. Source: Kaspersky Lab survey

*Provided pricing is guidance ONLY. Actual solution size and price may vary based on assessment by account team.

Dell Customer Communication - Confidential

T-Shirts – Choose your Size & Color

	Cyber Recovery	Starter	S	M	L	XL
	Front End TB	**3.0**	**32**	**128**	**256**	**384**
BASE	**Data Domain**					
	Data Domain Model	DD 3300	DD6900	DD 6900	DD 9400	DD9900
	Capacity Configured RAW TB	16	60	240	480	720
	Capacity Configured Useable TB	4	48	192	384	576
	Capacity System Usable TB	4TB - 32TB	48TB - 288TB	48TB - 288TB	192TB - 768TB	576TB - 1,248TB
	Cyber Recovery SW	Yes	Yes	Yes	Yes	Yes
	DD Licensing	Included	Boost-RL-Replication	Boost-RL-Replication	Boost-RL-Replication	Boost-RL-Replication
+	**CyberSense Software**					
	Cyber Sense Subscription	**3**	**32**	**128**	**256**	**384**
ENHANCED	**Vault Servers (Infrastructure)**					
	Server Model	PowerEdge R440				PowerEdge R640
	No. of Servers	**1**				**1**
	ESX VMware Licensing	Standard				Standard
	Cyber Recovery Server (OVA)	1				1
	Backup Server VM	1				1
	AD / DNS	Hosts File				1
	Server Storage (TB)	Internal 14.4 TB				24 TB
	Vault Management Workstation					
	Workstation Model			Powe	Edge R240	
	KMM Switch			DKM	MLED185	
	Vault Network					
	Vault Firewall	Sonicwall NSa 3650			Sonicwall NSa 6650	
	Vault Switch	S4112T		4112T		S4128T
	No. of Switches	**1**		**2**		2
	No. of Ports	12		24		56
	Cabling	incl.		incl.		incl.
	Vault Racking					
	Vault Rack			Netshelter Deep Rack		
+	**CyberSense Server**					
	Server Model	R440	R440	R640	R640	R640
	No. of Servers	**1**	**1**	**1**	**2**	**3**
	CPU Cores	20	30	30	60	90
	Memory (GB)	128	256	256	512	768
	Storage (TB)	7.68	11.52	19.2	38.4	53.76

SIMPLIFY

CHOOSE YOUR

T-SHIRT

SIZE & COLOR

DELL Technologies