Recovering Your Business from a Cyber Attack

PowerProtect Cyber Recovery

Matteo Ghielmi – Regional Channel Sales

DELL Technologies

“79% of global executives rank cyber attacks and threats as one of their organization's highest risk management priorities in 2020 “ -
Marsh & McLennan

"69% of global IT decision-makers lack confidence their organizations could reliably recover all business-critical data in the event of a cyber attack. "

Global Data Protection Index Survey 2020 Snapshot

Dell EMC commissioned Vanson Bourne for the Global Data Protection Index, which was conducted between September and November 2019.

©Copyright 2020 Dell Inc.

DELL Technologies

Cyber threats: the facts

A cyber attack occurs

every **39** sec

Source: Security Magazine

verizon

71%

of breaches are financially motivated

verizon

43%

of breaches involved small business

accenture

$13M

Avg cost of Cybercrime for an organization

accenture

$5.2T

of global risk over the next 5 years

Avg. cost of cyber attack

by Industry

Industry	Avg Cost
Banking	$18.4M
Utilities	$17.8M
Software	$16M
Automotive	$15.8M
Insurance	$15.8M
High Tech	$14.7M
Capital Markets	$13.9M
Energy	$13.8M
US Federal	$13.7M
Consumer Goods	$11.9M
Health	$11.9M
Retail	$11.4M
Life Sciences	$10.9M
Media	$9.2M
Travel	$8.2M
Public Sector	$7.9M

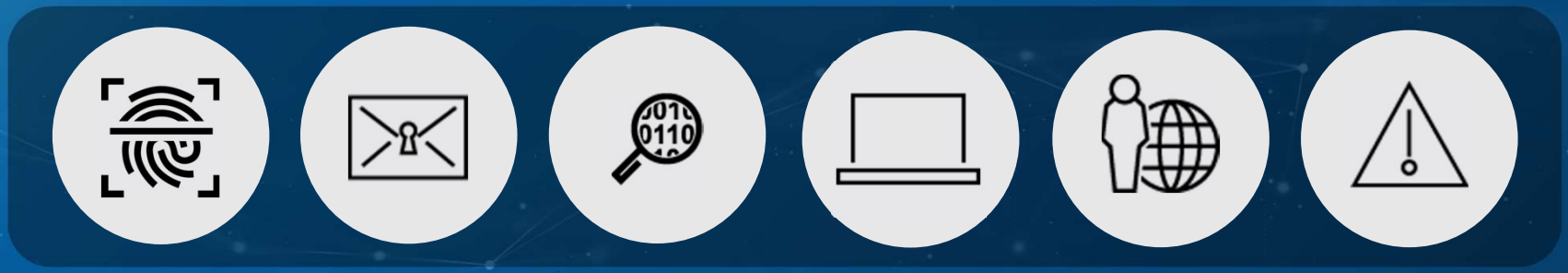
accenture

DELL Technologies

© Copyright 2020 Dell Inc.

Bad actors

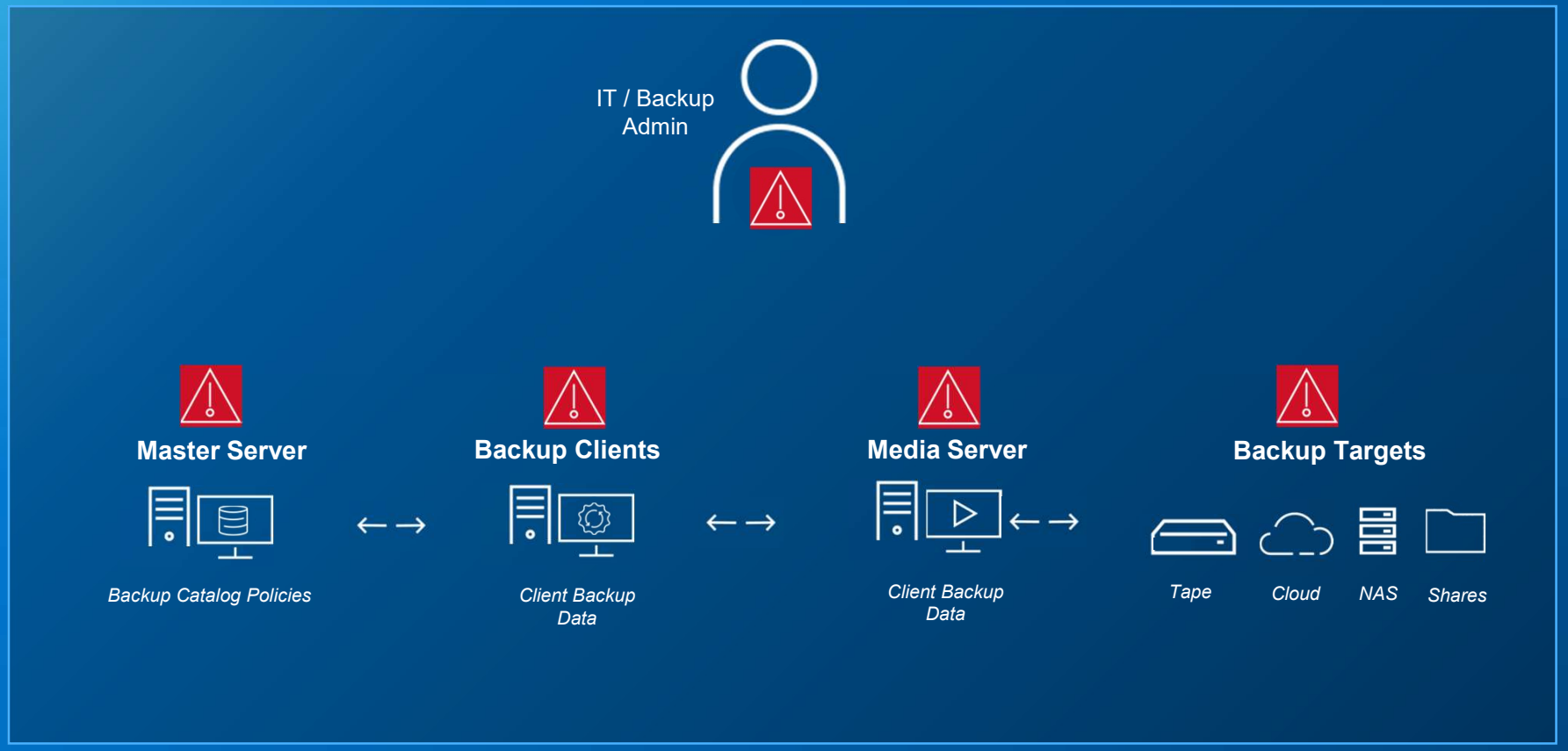
Motivations, Techniques and Goals



CRIME	INSIDER	ESPIONAGE	HACKTIVISM	TERRORISM	WARFARE
Theft & extortion for financial gain	Trusted insiders steal or extort for personal, financial, & ideological reasons. Increasingly targeted because of privileged access to systems	Corporate or Nation-state actors steal valuable data	Advance political or social causes	Sabotage & destruction to instill fear	Nation-state actors with destructive cyber weapons (Not Petya)

© Copyright 2020 Dell Inc.

Cyber attack target: your backups



© Copyright 2020 Dell Inc.

Disaster recovery is not cyber recovery

Disaster Recovery / Business Continuity is not enough to address modern cyber threats

Category	Disaster Recovery	Cyber Resilience
Recovery Time	Close to instant	Reliable & fast
Recovery Point	Ideally continuous	1 day average
Nature of Disaster	Flood, power outage, weather	Cyber attack, targeted
Impact of Disaster	Regional; typically contained	Global; spreads quickly
Topology	Connected, multiple targets	Isolated, in addition to DR
Data Volume	Comprehensive, all data	Selective, includes foundational services
Recovery	Standard DR (e.g., failback)	Iterative, selective recovery; part of CR

© Copyright 2020 Dell Inc.

Cyber resilience: legal and regulatory trends

"An air-gapped data backup architecture…"

"Confidentiality, integrity, availability and resilience"

"It is critical to maintain offline, encrypted backups of data"

"Ransomware payments may risk violating OFAC regulations"

"Ensure backups are not connected to the networks they back up."

© Copyright 2020 Dell Inc.

PowerProtect Cyber Recovery

DELL Technologies
Cyber resilience leadership

2015 – First “Isolated” recovery solution with custom deployment

2018 – Introduced PowerProtect Cyber Recovery solution

2019 – First technology vendor in Sheltered Harbor Alliance Partner Program

2020 – First Endorsed Sheltered Harbor Solution – PowerProtect Cyber Recovery

350+ Cyber Recovery Customers

#1

Data Protection Appliances & Software*

SHELTERED® HARBOR ALLIANCE PARTNER

SHELTERED HARBOR ENDORSED SOLUTION

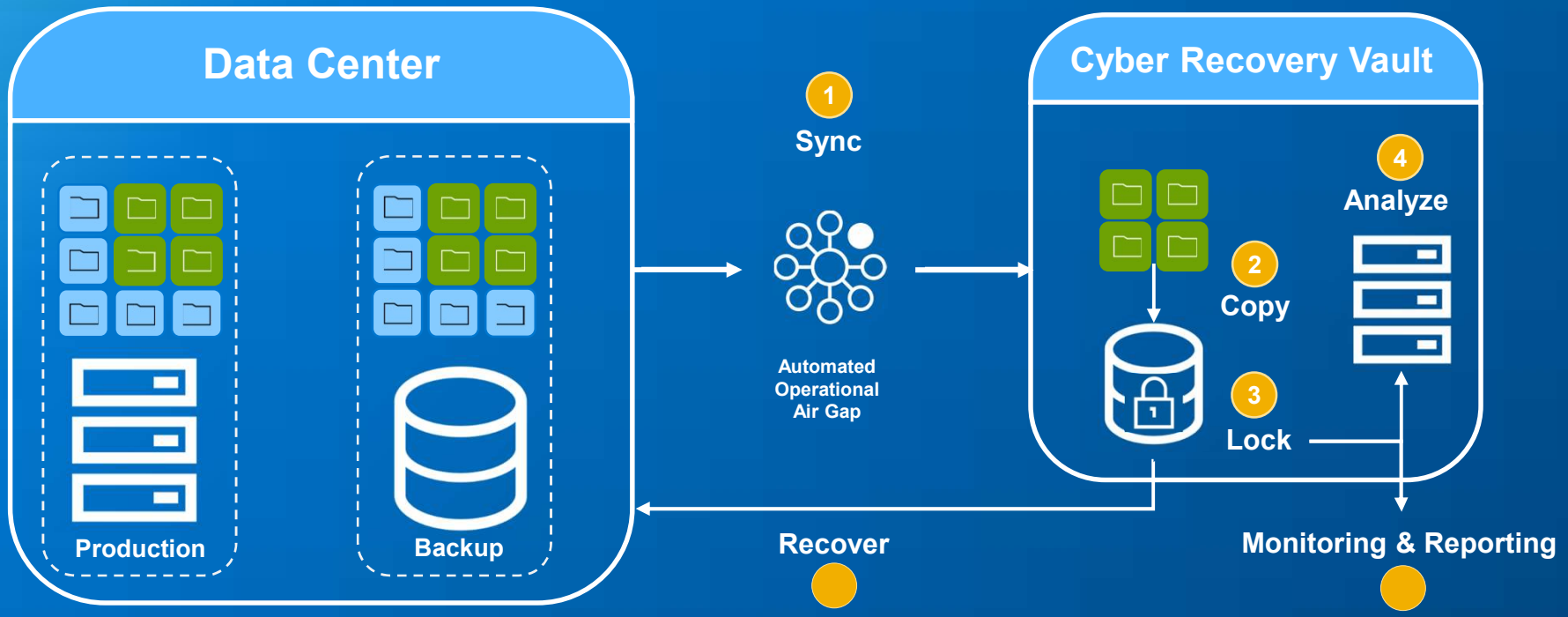
*Based on combined revenue from the IDC 3Q19 Purpose-Built Backup Appliance (PBBA) Tracker, with select Storage Software segments from the 3Q19 Storage Software and Cloud Services Overview

DELL Technologies

© Copyright 2020 Dell Inc.

PowerProtect Cyber Recovery

Data Vaulting and Recovery Processes



© Copyright 2020 Dell Inc.

Why Cyber Recovery is best

Best

- Automated, Vaulted Air Gap
- Full Context Indexing with AI / ML Analytics
- Endorsed by Sheltered Harbor (Endorsement expected mid-2020)
- Enhanced Recovery Tools

Better…

- Protection From Insiders
- Multi Backup SW-Vendor Support

Good…

- Integrated Lock SEC 17a-4(f) Compliant | WORM Immutable
- Elevated Security Credentials

DELL Technologies

© Copyright 2020 Dell Inc.

Cyber Recovery analytics with CyberSense

Recover and restore critical data with confidence

© Copyright 2020 Dell Inc.

Compare: Cyber Recovery with CyberSense vs. Competitor ‘A’

Ours:

On-Premises Analytics Engine

Scans:

1. File metadata
2. Document metadata
3. Document content

VS.

Theirs:

On-Premises Analytics Engine

1. Scans only file metadata

Cloud Analytics Engine

2 3

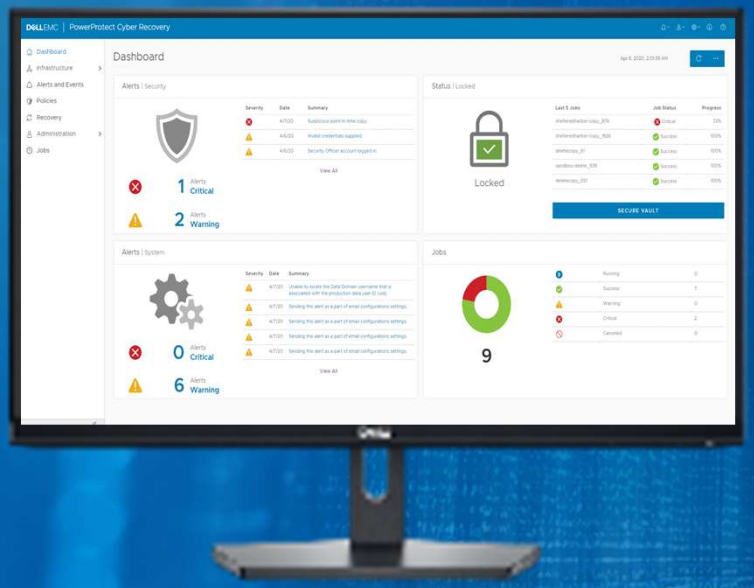
Suspicious files sent to cloud for 2nd pass or full content analysis

*Based on Dell analysis using publicly available data for competitive cyber recovery solutions on March 2020.

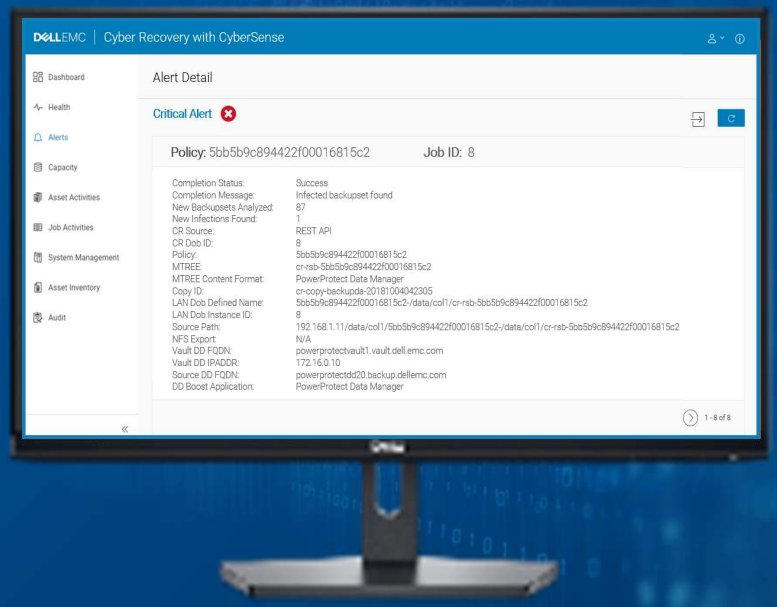
© Copyright 2020 Dell Inc.

DELL Technologies

Cyber Recovery Dashboard



CyberSense Alert



© Copyright 2020 Dell Inc.

Key Data to Protect by Industry

Healthcare
Electronic Medical Records, scheduling, payment and billing systems

Financial Services
Payments, Core Banking, Trading, Treasury, Sheltered Harbor data

Life Sciences
Research and development, drug discovery & Clinical trial data

Retail
Point of sale, inventory, shipping

Legal
Document management, conflicts checking, billing, email

Oil & Gas
Seismic & geographical exploration data

Government
Property records and taxes, justice systems, payment collection, licenses

Manufacturing
Plant manufacturing and scheduling, ordering systems, inventory

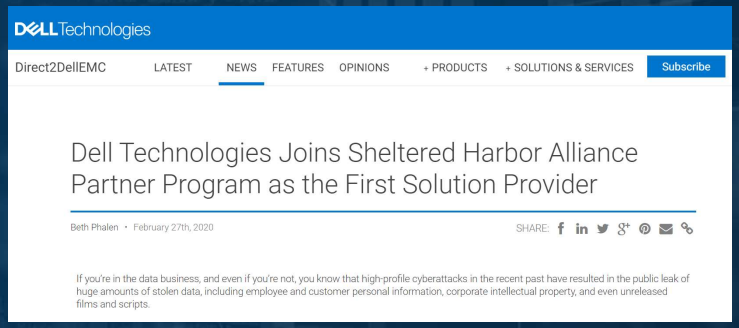
DELL Technologies

© Copyright 2020 Dell Inc.

Overview: Sheltered Harbor

- ✓ Unchangeable
- ✓ Separated
- ✓ Survivable
- ✓ Accessible
- ✓ Decentralized
- ✓ Owned and managed by institution or service provider

Protects confidence in the U.S. financial system


DELL Technologies

Direct2DellEMC LATEST NEWS FEATURES OPINIONS + PRODUCTS + SOLUTIONS & SERVICES Subscribe

Dell Technologies Joins Sheltered Harbor Alliance Partner Program as the First Solution Provider

Beth Phalen • February 27th, 2020 SHARE:

If you're in the data business, and even if you're not, you know that high-profile cyberattacks in the recent past have resulted in the public leak of huge amounts of stolen data, including employee and customer personal information, corporate intellectual property, and even unreleased films and scripts.

PowerProtect Cyber Recovery is first turnkey data vaulting solution to be endorsed by Sheltered Harbor

DELL Technologies

© Copyright 2020 Dell Inc.

Start Now!

Cyber Recovery Vault recommendations

Authentication, Identity & Security

- Active Directory / LDAP
- DNS dumps
- Certificates
- Event logs (including SIEM data)

Networking

- Switch / router configuration
- Firewall / load-balancer settings
- IP Services design
- Access Control configuration
- Firmware / microcode / patches

Storage

- Backup hardware configuration
- SAN / array configurations
- Storage abstraction settings
- Firmware / microcode / patches

Intellectual Property

- Source code
- Proprietary algorithms
- Developer libraries

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 D/R and Cyber Recovery Run-books &checklists
- Management extracts
- HR resources & contacts lists

DELL Technologies

© Copyright 2020 Dell Inc.

Why Dell EMC for Cyber Recovery

- Isolated, operational air gap for data vaulting
- Multi-layered security design protects against a full array of threats - including insiders
- Automated, orchestrated operation with a modern UI
- Secure, vault-based analytics with full content analysis
- First Sheltered Harbor endorsed turnkey data vaulting solution
- Mature solution with 5 years in the market, hundreds of customers

© Copyright 2020 Dell Inc.