Journey to Cyber Resilience

Recovering Your Business from a Sophisticated Attack

Ionut Rosca
Data Protection Solutions Specialist
Dell Technologies

April 2024

DELL Technologies

Agenda

1. Cyber attacks and Risks
2. Cyber Attack Evolves
3. Cyber Recovery Solution
4. Follow up

DELL Technologies

Cyber attacks and Risks

What is the 3RD world economy ?

Cybercrime

State of Cybercrime

The Damage & Costs Continue to Rise

Cybercrime To Cost The World $10.5 Trillion Annually By 2025

Cybercrime Magizine, Nov. 13, 2020

DELL Technologies

The Evolving Cyber Threat Landscape

A Cyber Attack Occurs

every

11 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

Ask: What's your plan to recover from a Cyber Attack?

DELL Technologies

Evolution of Cyber Threat Actors

Different Motivations, Techniques, & 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)

DELL Technologies

Cyber Security Evolve

DELL Technologies

Organizations are desperate to stay out of the news

Colonial Pipeline, May 2021

JBS S.A. May 2021

CNA, March 2021

69%

increase in reported cyber attacks in 2020

(ISC)²

34%

of attacks in 2020 involved an insider

verizon

67%

of respondents not confident in ability to recover

DELL Technologies

82%

of employers report a shortage in cybersecurity skills

CSIS

Of those surveyed, the average estimated cost of unplanned systems downtime throughout the past 12 months is over **$500,000 (USD)***

DELL Technologies

Recent Guidance

Gartner

Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware

Published 6 January 2021 - ID G00733304 - 20 min read

By Nik Simpson, Ron Blair

Infrastructure and operations leaders responsible for
protection features as critical p
features that aid in detecting ra

Overview

Key Findings

- Increasingly sophisticated ransomw
- No single solution can completely protect an organization from
- The threat from increasingly sophisticated ransomware is grov organizations worldwide.
- Ransomware is frequently deployed as a component of a broa administrative functions.

Recommendations

Infrastructure and operations leaders responsible for data center

- Eliminate network sharing protocols — Avoid the use of simple implementing storage for backup data.

https://www.gartner.com/doc/reprints?id=1-25T

Backup your data, system images, and configurations, regularly test them, and keep the backups offline: Ensure that backups are regularly tested and that they are not connected to the business network, as many ransomware variants try to find and encrypt or delete accessible backups. Maintaining current backups offline is critical because if your network data is encrypted with ransomware, your organization can restore systems.

FROM: Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology

SUBJECT: What We Urge You To Do To Protect Against The Threat of Ransomware

DATE: June 2, 2021

The number and size of ransomware incidents have increased significantly, and strengthening our nation's resilience from cyberattacks – both private and public sector – is a top priority of the President's.

Under President Biden's leadership, the Federal Government is stepping up to do its' part, working with like-minded partners around the world to disrupt and deter ransomware actors. These efforts include disrupting ransomware networks, working with international partners to hold countries that harbor ransomware actors accountable, developing cohesive and consistent policies towards ransom payments and enabling rapid tracing and interdiction of virtual currency proceeds.

HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B1/15C
B9/29C

18 May 2021

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

kup

ritically assess the
counter the risk of

ng concern as they
thorised alteration
. In light of recent
arbor initiative to
d the Hong Kong
n STDB that are

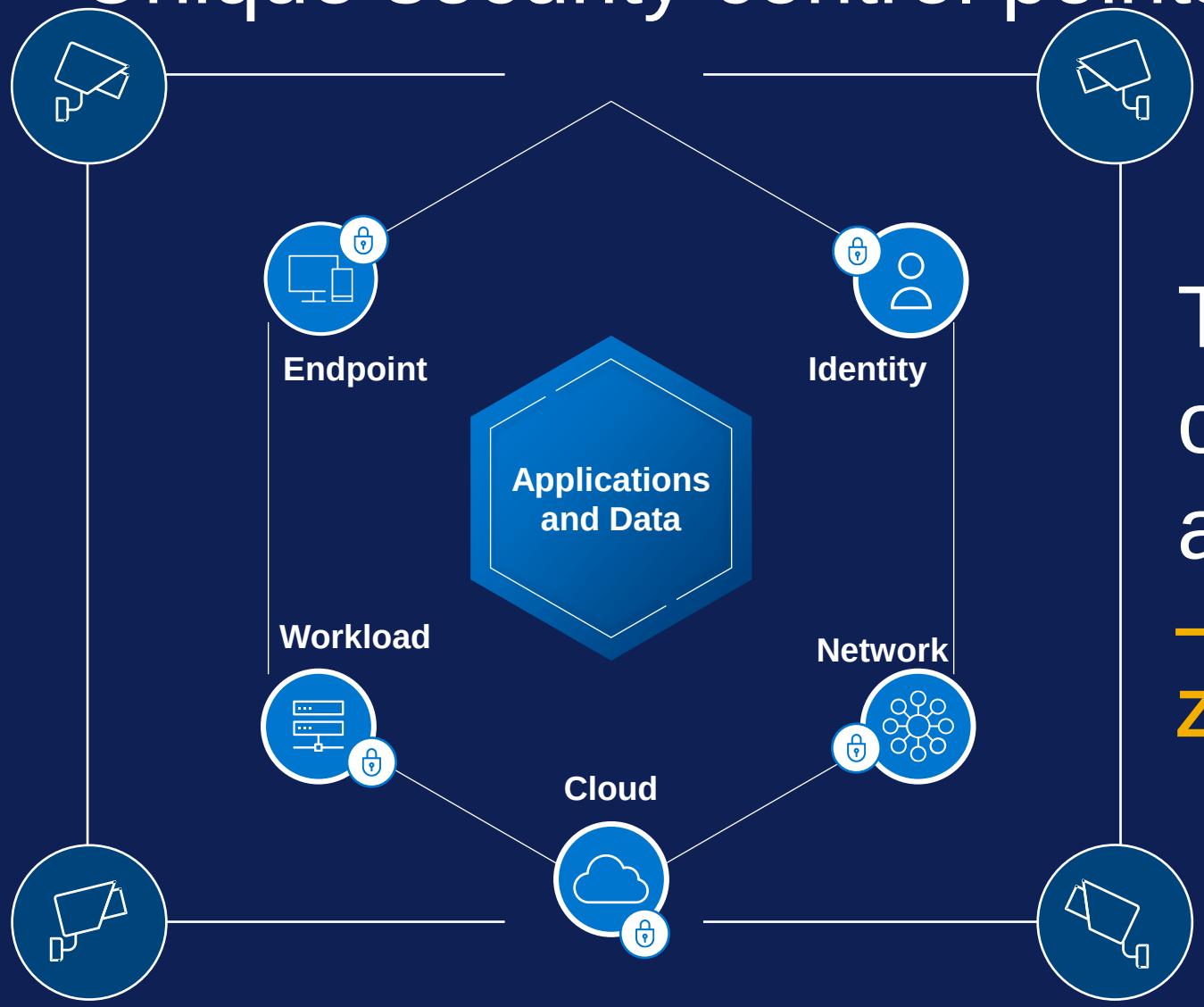
's call, the HKAB formed a STDB Taskforce to
f the guidelines. After extensive consultation with
HKAB issued the "Secure Tertiary Data Backup
021. The STDB Guideline provides guidance to
eed to take into account in deciding whether to set
nplementation issues they need to overcome in
of the STDB. The Guideline covers 8 high-level
the headings of Governance, Design and Data

B an effective measure to enhance cyber resilience
Hong Kong. It expects all AIs to critically assess
an STDB having regard to their risk exposure and
iciples stipulated in the HKAB's STDB Guideline.

entre, 香港中環金融街8號國際金融中心2期55樓
網址：www.hkma.gov.hk

DELL Technologies

Unique security control points



The shifting nature of security requires a new approach.

Zero Trust

DELL Technologies

Zero Trust Journey

Brings **explicit control** to the IT environment.

User & device management

Risk management

Threat management

Dell Technologies – your trusted partner

Supply Chain

Starts with the foundation – PC

Enable zero trust features on Servers, Network and Storage

Unlock resources/skill shortage

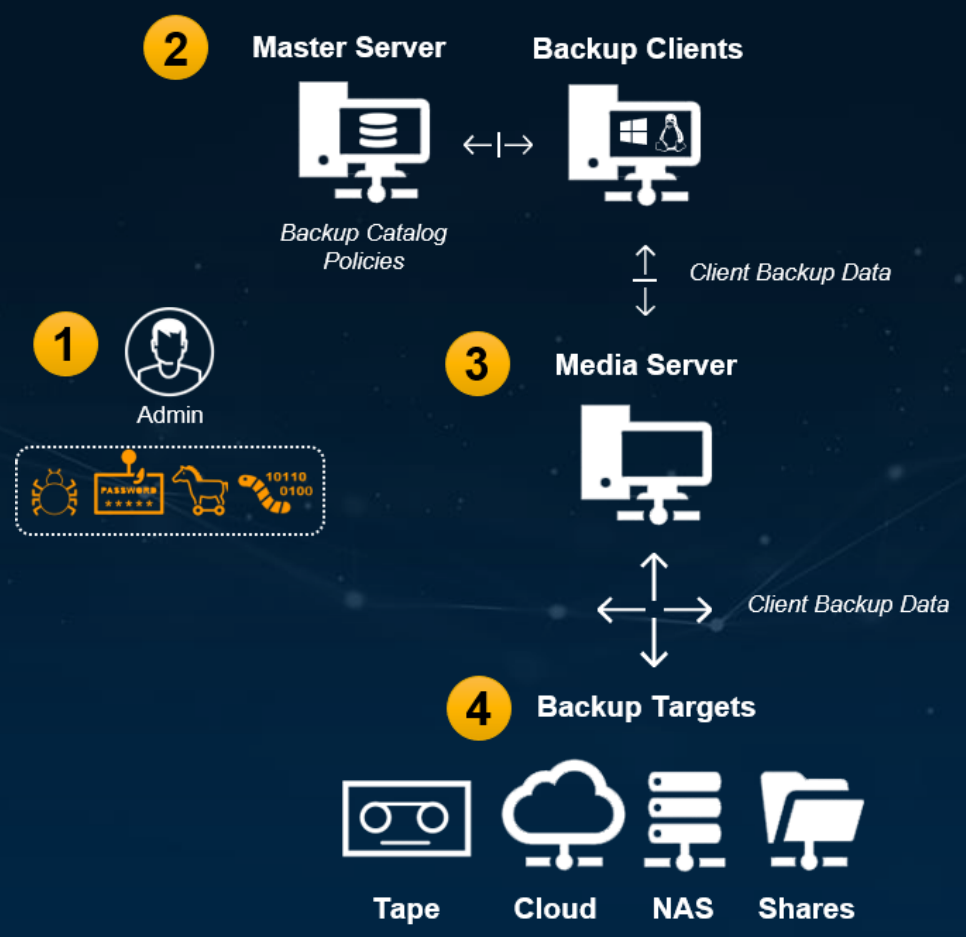
Knowing what is good in your environment

Trusted Peripherals

Do you have an un-compromised policy engine?

Engage our Services

Ransomware Increasingly Targeting Primary Backups



1. **IT and Backup admins are main targets for compromise**

2. **Master Server (Backup Catalog):** Backup master server is targeted and infected resulting in encrypted/wiped backup catalog, or pre-mature policy expiration

3. **Media Server:** All mounted filesystems on the media server are targeted and encrypted/wiped

4. **Backup Targets:**

   Disk / NAS: Filesystems on the media server are targeted and encrypted/wiped. Backup repositories can become encrypted/wiped from ransomware crawling network file shares

   Tape: Provides a better chance to recover from the destructive event if threat was removed from the environment prior to attack. However, if backup catalog is held hostage or destroyed, recovering from the tape will be increasingly difficult

   Cloud: General-purpose or Public Cloud offer the advantage of remote protection but are inherently less secure due to reliance on internet (always on) or unsecure networks, leaving data, backups and catalogs exposed

DELL Technologies

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

In addition, tape backup is not a resilient solution due to the performance and the difficulty to rebuild a complex environment.

DELL Technologies

NIST Cybersecurity Framework

Identify **Protect** **Detect** **Respond** **Recover**

https://www.nist.gov/cyberframework

DELL Technologies

Anatomy of a Cyber Event

Planning, Execution, Results

Initial Access

Attack Launched

Reconnaissance:
The adversary is trying to gather information they can use to plan future operations.

Resource Development:
The adversary is trying to establish resources they can use to support operations.

Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command & Control
Exfiltration

- Active Directory **DESTROYED**
- Data Centers **ISOLATED**
- Email access **BLOCKED**
- **DOWN**
  - Network Management
  - IP Phone system
  - Bridge access
- **DISABLED**
  - All Windows logins
  - Internet Access
- **ERASED**
  - DNS
  - vCenter
  - Customer Care

Dwell Time
212 days

Recovery & Containment
75 days

MITRE ATT&CK

DELL Technologies
Data Protection Solutions
Global Technology Office

Mitre Att&ck Impact Analysis

Attack Type	Attack Description	Mitre Att&ck Impacts	Backup	Immutability	Isolation	Intelligence
Ransomware	• Infects endpoints and servers • Encrypts all CIFS and NFS shares it can access	• **Data Encrypted for Impact**	!	✓	✓	✓
Ransomware + Backup Deletion	• Infects endpoints and servers • Backups are manually deleted (admin credentials)	• **Data Encrypted For Impact** • **Data Destruction** • **Inhibit System Recovery**	✗	✓	✓	✓
Ransomware + Platform Wipe	• Infects endpoints and servers • Backup infrastructure is wiped at platform level	• **Data Encrypted For Impact** • **Data Destruction** • **Disk Wipe**	✗	✗	✓	✓
Ransomware + Firmware Attack	• Infects endpoints and servers • Backup and other platforms are crashed at firmware level	• **Data Encrypted For Impact** • **Data Destruction** • **Firmware Corruption**	✗	✗	✓	✓
Ransomware + VM Level Attack	• Infects endpoints and servers • VMs are deleted (includes SW-defined backup infra)	• **Data Encrypted For Impact** • **Data Destruction**	✗	✗	✓	✓
Dormant Ransomware	• Infects endpoints and servers • VMs are deleted (includes SW-defined backup infra)	• **Data Encrypted For Impact** • **Data Destruction** • **Data Manipulation**	✗	✗	✓	✓
Hidden Encryption	• Infects endpoints and servers	• **Data Manipulation**	✗	✗	✗	✓

Worst case scenario

Imagine a severe but plausible scenario where:

All Production and DR systems have been impacted by a cyber event including the backup systems.

The business needs to be recovered from the ground up.

Network Security

Network Firewall

Infoblox, Cisco, Barracuda, Dell SonicWALL, Juniper, Hewlett Packard Enterprise, untangle, StormShield, McAfee, Fortinet, Sangfor, Hillstone, CATO, Huawei, BlueCat, paloalto, WatchGuard, Check Point, Sophos

Network Monitoring/Forensics

F5, Blue Coat, Sec, Cisco, ixia, DeepNines, NetScout, Gigamon, ProtectWise, Lumeta, solarwinds, SpiceWorks, packetsled, Corvil, Juniper, utimaco, ForeScout, Bradford Networks, RSA, riverbed

Intrusion Prevention Systems

IBM, Cisco, corero, Sophos, Check Point, Hewlett Packard Enterprise, paloalto, Fortinet, DeepNines, Extreme, McAfee, Huawei, FireEye, Juniper, NSFocus, radware, AirTight

Unified Threat Management

Fortinet, Juniper, paloalto, FireEye, Dell, Hillstone, Cisco, Check Point, endian, gateprotect, StormShield, Sophos, Huawei, clavister, Barracuda, WatchGuard

Endpoint Security

Endpoint Prevention

McAfee, Cylance, deepinstinct, avast, Kaspersky, F-Secure, PSafe, Microsoft, sparkcognition, ThreatTrack, AhnLab, CrowdStrike, Minerva, Webroot, Fortinet, Barkly, ivanti, eset, invincea, StormShield, paloalto, SaferVPN, SentinelOne, Malwarebytes, FixMeStick, Bitdefender, AVG, Carbon Black, Sophos, Trend Micro, Ensilo, Morphisec, panda, Bromium, Symantec

Endpoint Detection & Response

OPSWAT, ziften, SentinelOne, cybereason, Cyphort, ZoneFox, morphick, CounterTack, Fluency, Tanium, red canary, Hexis, Bromium, certego, TopSpin Security, Hexadite, QinetiQ, Guidance, Outlier, Carbon Black, CyberBit, FireEye, AUCONET, Cynet, Core Security, invincea, Nehemiah Security, tex, RSA, LightCyber, Fidelis, CrowdStrike, SECDO, Digital Guardian, nexthink, ENDGAME.

Application Security

WAF & Application Security

A10 Networks, Penta security, Qualys, namogoo, F5, Alert Logic, StealthSecurity, Trustwave, waratek, Prevoty, Sucuri, NSFocus, Zenedge, onapsis, SHAPE, Akamai, denyall, ARXAN, Fireblade, netsparker, Certes Networks, SOHA, ergon, Citrix, DBappSecurity, Fortinet, Real Geeks SEWORKS, Barracuda, radware, Positive Technologies, Imperva

Vulnerability Assessment

bugcrowd, WhiteHat Security, RapidD, Trustwave, Checkmarx, McAfee, FLEXERA, BlackDuck, nccgroup, onapsis, Hewlett Packard Enterprise, RandomStorm, CORE Security, VERACODE, hackerone, snyk, SRC:CLR, IBM, BeyondTrust, Synack, Cigital, Outpost24, Qualys

Managed Security Service Provider

at&t, Solutionary, verizon, Trustwave, OPTIV, Alert Logic, Symantec, CSC, rackspace, Clone Systems, Netswitch, nuspire, MegaPath, CenturyLink, IBM, SecureWorks, Hewlett Packard Enterprise, DATASHIELD, BT, orange, WIPRO, esentire, BAE SYSTEMS

Web Security

Blue Coat, distil networks, Cisco, Sophos, StealthSecurity, Trustwave, Cloudflare, SHAPE, zscaler, ZenMate, F5, Akamai, appriver, ContentKeeper, WHEEL, EASYSOLUTIONS, FireEye, CYBERFEND, perimeterx, CYREN, namogoo, Check Point, arrest, smoothwall, Barracuda, iboss, SHIELDSQUARE, EdgeWave, golden frog, Forcepoint, Webroot, NEXUSGUARD, Symantec, Trend Micro, GWAVA, Fortinet, OpenDNS, SPAMINA

Messaging Security

proofpoint, Forcepoint, Microsoft, PHISHME, EdgeWave, FireEye, Cisco, Trustwave, AstraID, MEDIAPRO, GreatHorn, ValiMail, BAE SYSTEMS, SPAMINA, Dell, Fortinet, CLOUDMARK, WatchGuard, VOTIRO, GWAVA, PHISHLABS, CYREN, Symantec, McAfee, appriver, Barracuda, clearswift, SOLEBIT, AGARISOPHOS, Trend Micro, mimecast

Risk & Compliance

PICUS Security, cytegic, GRX, R-sam, RiskVision, RiskSense, REDSEAL, MetricStream, PREVALENT, BITSIGHT, ATTACKIQ, FICO, bringa, tufin, kenna, UpGuard, PALADION, SecurityScorecard, FIREMON, VERODIN, netwrix, TEMPLAR, corax, algosec, CRONUS, SafeBreach, RSA Archer, CYENCE, riskrecon, MEDIAPRO, NOPSEC, NormShield, Cobalt

Security Operations and Incident Response

SIEM

IBM, LogRhythm, sumologic, RSA, TIBCO, tenable network security, EventTracker, RedLock, splunk>, logentries, SAWMILL, CorreLog, SKYBOX Security, Logscape, EIQ, panaseer, Huntsman, NetIQ, Hewlett Packard Enterprise, Trustwave, solarwinds, BLACKSTRATUS, logz.io, Fortinet, NETMONASTERY, Alert Logic, Fluency, logpoint

Security Incident Response

Phantom, radar, DFLABS, DEMISTO, UPLEVEL, ayehu, servicenow, HEXADITE, resilient, cybereason, encode, packetsled, GUIDANCE, Enclase Cyber Security, Hexis Cyber Solutions, csg INVOTAS, PALADION, SKYBOX Security, CYBER TRIAGE, SIEMPLIFY, RAPIDD, CYBERBIT, swimlane, Raytheon Foreground Security, CYBERSPONSE, SYNCURITY, THREAT CONNECT, SECDO, DARKLIGHT, nuix

Threat Intelligence

iSIGHT PARTNERS, ThreatMetrix, RISKIQ, INTEL471, DOMAINTOOLS, THREATQUOTIENT, SensaCy, ANOMALI, Recorded Future, digital shadows_, brandprotect, THREAT CONNECT, OpenDNS, FLASHPOINT, SIXGILL, CENTRIPETAL NETWORKS, RiskBased Security, SURFWATCH, eclectic iq, CROWDSTRIKE, FORSIGHT SECURITY, servicenow, Malware Patrol, Cyberint, Infoblox, LOOKINGGLASS, Intsights, WEBROOT, Blueliv, 4iQ, VERISIGN

Specialized Threat Analysis

IronNet Cybersecurity, FORTSCALE, niara, Bay Dynamics, invincea, sparkcognition, TRAPX SECURITY, exabeam, ZEROFOX, IMVISION, INTERSET, GuardiCore, SEC, observable networks, BehavioSec, Attivo Networks, JASK, SS8, Mobile System 7, TEMPERED Networks, NYOTRON, AREA 1, VECTRA, VENAFI, LIGHTCYBER, Palantir, sqrrl, ACALVIO, dataphy, DB NETWORKS, PROTECTWISE, fireglass, Cymmetria, SKYPORT SYSTEMS, lastline, Avecto, deepinstinct, SECURONIX, REDOWL, VOTIRO, Seculert, prelert, DARKTRACE, NOVETTA, VMRAY, MINERVA, ENDGAME., CYLANCE, VIDDER, pocketsled, SOLEBIT, Bromium, DATAVISOR, 8 SECURITY, CYPHORT, GURUCUL, namogoo, IONIC SECURITY, esentire, patternex, illusive, Menlo Security

Data Security

OPSWAT, SPIRION, VERA, nuro, THINAIR, StorageCraft, DB NETWORKS, Actifile, ENSILO, wickr, IONIC SECURITY, MENTIS, WINMAGIC DATA SECURITY, globalvelocity, virtru, CYPHRE, PKWARE, COVERTIX, SECURITYFIRST, druva, PRIVITAR, BLACK FOREST, CODE42, SOMANSA, Vormetric, CipherCloud, REVERSING LABS, BlueTalon, CENTRI, SECLORE, DIGITAL GUARDIAN

Mobile Security

Lookout, MobileIron, Skycure, AppDome, wandera, nuro, bitglass, silent circle, airwatch, tigertext, PSafe, BLUE CEDAR NETWORKS, MOCANA, TRUSTLOOK, ATESKALABS, appthority, SnoopWall, InAuth, iovation, BETTER, OPTIOLABS, CyberadAPT, V-Key, AirTight Networks, wickr, NowSecure, COMMUNITAKE, KOOLSPAN, pradeo, saltDNA, pindrop, OPENPEAK, ZIMPERIUM, TeleSign

Identity &Access Management

covisint, WHEEL, Nok Nok LABS, ORACLE, UNIKEN, CLOUDWAY, okta, WISEkey, GIGYA, UnboundID, CORE Security, Trulioo, SAASPASS, VIRGIL SECURITY, CLEF, SailPoint, PingIdentity, IBM, SECURE KEY, FORGEROCK, INTRINSIC ID, BeyondTrust, EXOSTAR, id experts, onelogin, RSA, SAVIYNT, BALABIT, foxtechnologies, BITIUM, welcome, DEVICE AUTHORITY, Auth0, AVERON, simeio, PIREAN, tascent, verato, DUO, ShoCard, imprivata, Centrify, Deep Identity, SaferPass, SECUREAUTH, AXIOMATICS, janrain, Avecto, ID.me, ilantus, CYBERARK, gemalto, iovation, ca, thycotic

Cloud Security

SAVIYNT, CloudPassage, StrataKey, illumio, Qualys, threat stack, CloudLock, Managed Methods, EnCrypted Cloud, zscaler, bitglass, evident.io, AVANAN, panda, SOHA, BRACKET COMPUTING, Vaultive, VERA, RedLock, CODE42, CLOUDWAY, CLOUD RAMP, covata, Microsoft, HYTRUST, ORACLE, palerra, ARMOR, guardtime, FIRELAYERS, Dome9, CATO NETWORKS, FORTYCLOUD, ClearDATA, WhiteHat Security, skyhigh, netskope, VMware, boxcryptor, Actifile, vARMOUR, BLUE COAT, BetterCloud, Twistlock, CipherCloud

IoT Security

MOCANA, cryptosoft, Bastille, utimaco, Rubicon, ICON LABS, IMUBIT, riscure, ZingBox, endian, IOActive, Cloudwear, Infineon, DEVICE AUTHORITY, Arilou, CYPHRE, PFP, CYBERBIT, TEMPERED Networks, CLAROTY, WEBROOT, ARGUS Cyber Security, Indegy, Karamba Security, SECURITHINGS, ARM, BAYSHORE

Fraud Prevention

FICO, UNIKEN, feedzai, iovation, ethoca, BIOCATCH, IdenTrust, NU DataSecurity, EARLY WARNING, FORTER, SIGNIFYD, ThreatMetrix, Guardian Analytics, AU10TIX, CARDINAL COMMERCE, siftscience, NU DataSecurity, SOCURE, riskified, Brighterion, IdentityMind GLOBAL, MAXMIND, Acculynk, Kount

Cyber Resilience is not a Secure Backup

Secure/Immutable backups

Objective:
Make sure NO Ransomware can destroy your Backups.

USE CASE: RESTORE DATA

Key Takes:
- Better Together
- Superior Competitor Value
- Disaster Recovery
- Multi Deployment (On Prem and Cloud)
- Flexible Consumptions Models (Apex / TLA)

Dell Key Advantages:
- Immutability and Retention Lock
- **Data Domain Invulnerable Architecture**
- Scale up VS Scale Out (network ports to monitor and administrate)
- Cyber Anomaly Threat detection
- Ecosystem with other SW vendors

Cyber Resilience

Objective:
Warranty Return to Business After An Attack

USE CASE: REBUILT BUSINESS

Key Takes:
- Map Organization's Survival Time Objective
- Map Organization Business Survival Priorities
- Map Organization Governance Policies
- Compliance with New Cyber Regulations (NIS2, DORA, etc…)

Dell Key Advantages:
- True Isolated Protection Storage and Clean Rooms
- Offline Deep Analytics Impact Oriented
- Immediate Readiness and Response, blue teams, run books
- One Vendor with Unmatched Supply Chain and Flexibility

Cyber Resilience = Survival Kit when everything else has failed

DELL Technologies

Cyber recovery

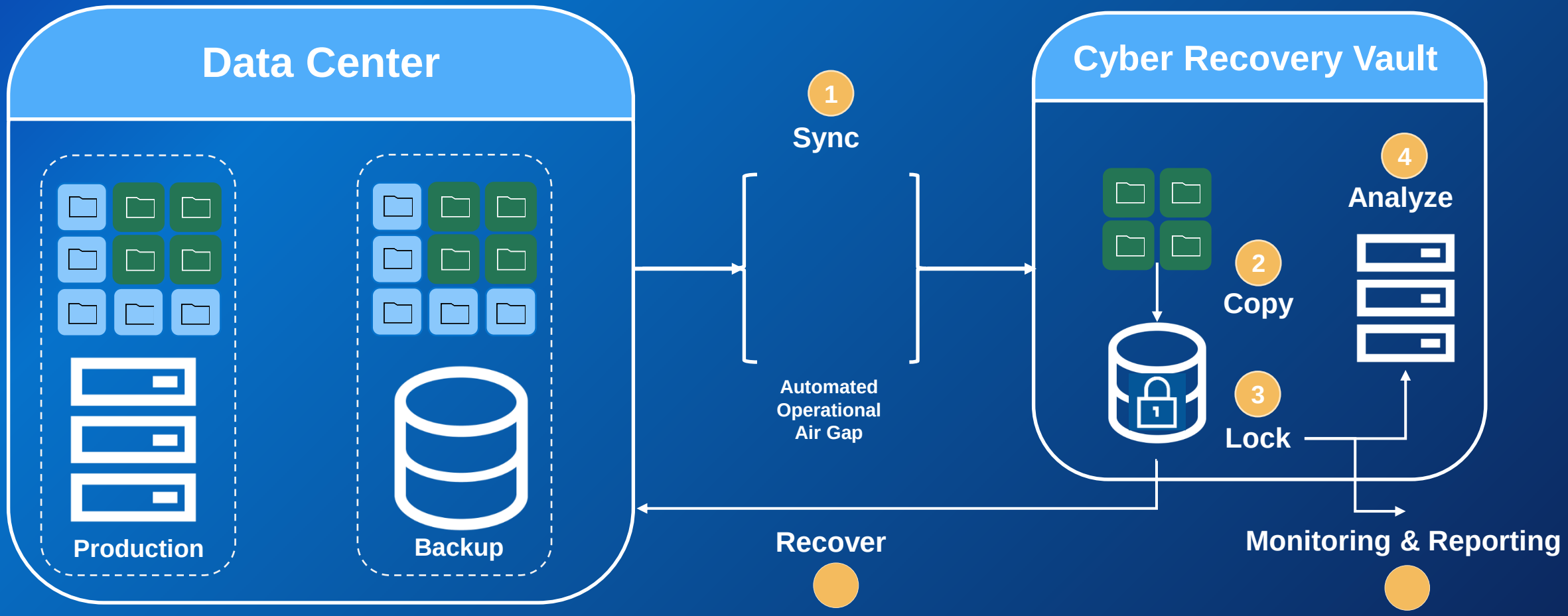
Isolation
Physical & logical separation of data

Immutability
Preserve original integrity of data

Intelligence
ML & analytics identify threats

PowerProtect Cyber Recovery

Data Vaulting and Recovery Processes



Proactive Analytics

Anomaly Detection, Threat Isolation

Index

CyberSense scans critical data sources, including unstructured files and databases to create an observation. Data can be located on network file systems or in backup images.

Analytics

More than 180 statistics generated from each observation. Statistics include analysis of file entropy, similarity, corruption, mass deletion/creations, and much more.

Analysis

Machine learning algorithms are used to analyze the statistics to indicate if an attack on the data has occurred.

Repeat

The process repeats and a new observation is created by scanning network or backup data. New observations are compared to previous observations to see how data changes.

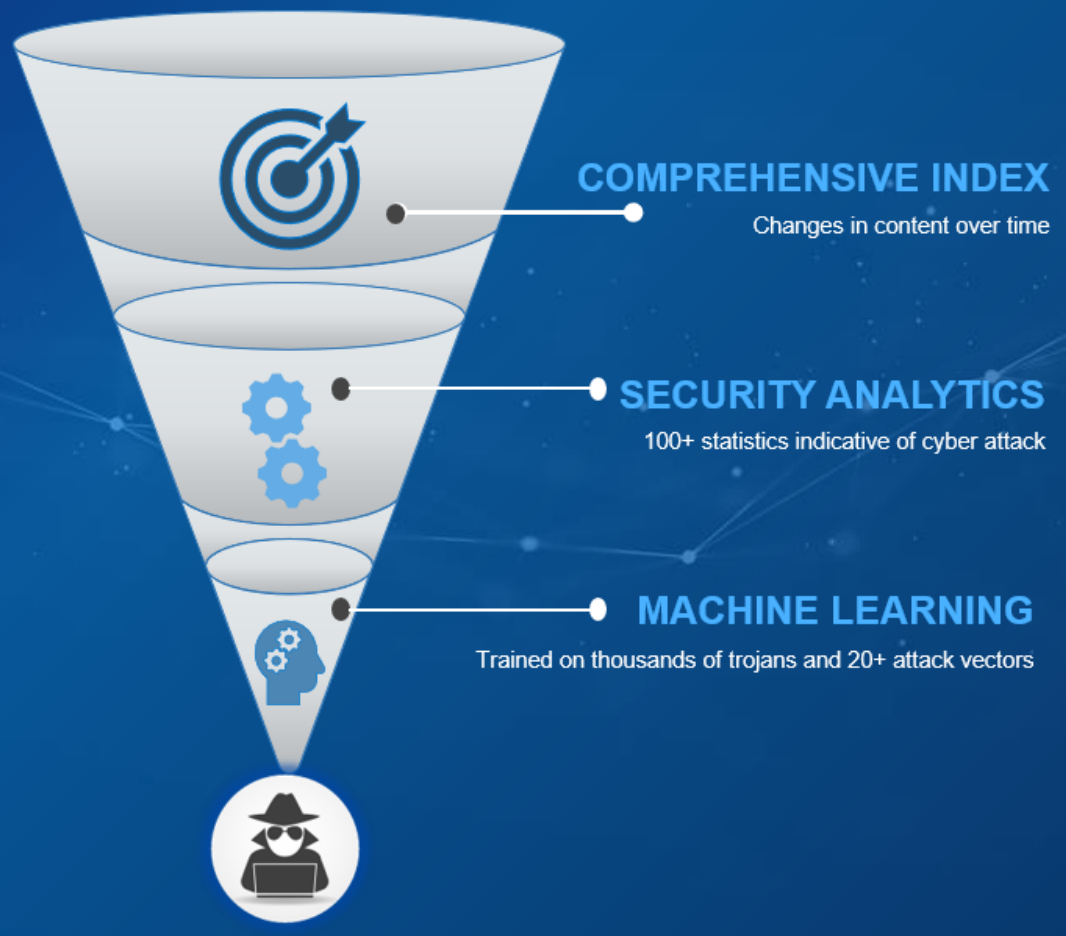
Investigate

Forensic reporting and analysis tools are available after an attack to find corrupted files and diagnose the type of ransomware.

© Copyright 2021 Dell Inc.

Dell EMC CyberSense Analytics:

Machine Learning Enables Early Detection & Rapid Recovery from a Cyber Attack



Dell EMC Cyber Recovery with CyberSense

- Attack Vector Notification
- Ransomware
- Corrupted File Details
- Data Changes / Deletions
- Breached User Accounts
- Breached Executables
- Recovery of Last Good Copy

Comparison of Metadata vs Content Analytics

AlphaLocker – Strong Encryption Maintaining Original File Name

Users | Security | **Metadata** | Text

File:	StackOverflow2010.mdf
Result ID:	52240570843-1-6466.0
Path:	mssqldem2/C/Program Files/Microsoft SQL Server/MSSQL.1/MSSQL/DATA/
Size:	1.728 GB
File Type:	Microsoft SQL Database File
Signature:	945E4A05B5A46A7DB3C001B7F5551735
User:	s-1-6-1-500@mssqldem2/File
Modified:	Apr-12-2019 at 02:18:10 PM
Backup Host:	mssqldem2
Backup Time:	Apr-01-2019 at 12:01:01 PM
Deactivation Time:	Apr-02-2019 at 12:01:01 PM
Software:	NetBackup
Policy:	CyberSenseData_20190401
Backupset ID:	mssqldem2_1554134461
Ingestion Method:	CRAWL
Volume Label:	192.168.16.210-06.04.2021 at 07:27 PM-633
Durable ID:	f493b6ae-a93d-404b-9ed5-29a7d80fc373-6466
Indexed Owner:	S-1-6-1-500
File Entropy:	48

Metadata Intact
File Name/Ext
File Size

Content Changed
File Header
Entropy/Encryption

01 Pre-Attack Version
Last good version

02 Post-Attack Version
Corrupted file

Users | Security | **Metadata** | Text

File:	StackOverflow2010.mdf
Result ID:	52240570843-1-6469.0
Path:	mssqldem2/C/Program Files/Microsoft SQL Server/MSSQL.1/MSSQL/DATA/
Size:	1.728 GB
File Type:	Unknown
Signature:	B01B38EEF3C803404379DCAF32127AC3
User:	s-1-6-1-500@mssqldem2/File
Modified:	Apr-15-2019 at 04:24:36 PM
Backup Host:	mssqldem2
Backup Time:	Apr-02-2019 at 12:01:01 PM
Software:	NetBackup
Policy:	CyberSenseData_20190401
Backupset ID:	mssqldem2_1554220861
Ingestion Method:	CRAWL
Volume Label:	192.168.16.210-06.04.2021 at 07:27 PM-633
Durable ID:	f493b6ae-a93d-404b-9ed5-29a7d80fc373-6469
Indexed Owner:	S-1-6-1-500
File Entropy:	99
File Entropy Delta:	51

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

Cyber Recovery Vault Recommendations

Applications

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 Runbooks & checklists
- Management extracts
- HR resources & contacts lists

Supporting infrastructure

Authentication, Identity & Security

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

Networking

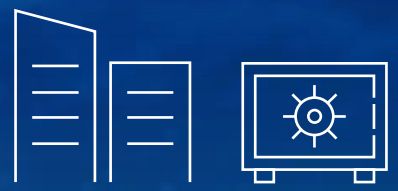
- Switch / router configuration
- Firewall / load-balancer settings
- IP Services design
- Access Control configuration
- Firmware / microcode / patches

Storage

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

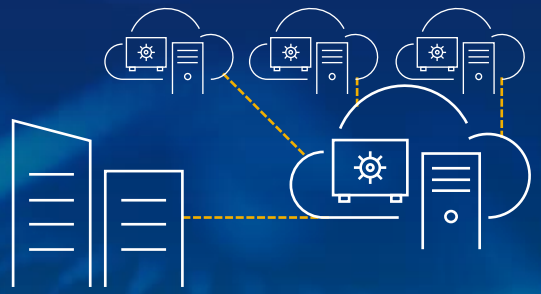
DELL Technologies

Flexible deployment options



On-premises

Maximum control of data and infrastructure with a more secure on-premises vault solution.



Multi-cloud

A Multi-cloud managed service providing a secure dedicated vault with predictable performance.

Managed Services

Quick and easy deployment with a more secure on-premises vault solution and enhanced security.

Follow up

ARE YOU RESILIENT?

Dell Technologies can help you via our Cyber workshop to evaluate and assist in that journey

LOGIC COMPUTER

They will follow up with you to define the action plan

DELL Technologies