



Modernize your Cyber Resilience approach

Ravi Baldev

CTO – Cyber Resilience

Dell Technologies EMEA

Cyber Resilience

The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.



Can your business withstand a cyber attack?

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

Complexity – The Fundamental Security Challenge

Fragmented Market and Disjointed Threat Centric approach to Security in the Enterprise

Digital Risk Management

crisp CYBERSPRINT digital shadows_ DigitalStakeout
EXPANSE LOOKINGGLASS NAMO-GOO PHISHLABS
RISKIQ SafeGuard Cyber ZEROFIX

Mobile Security

appdome BETTER BlackBerry blue cedar Fyde
Check Point centrox COMMUNITATE Cyber@APT
INPEDIA KODLABIN Lookout mobiliron
prodoo Psa SaltDNA silent circle SOTI
Symantec TeleSign tigerixt TRUSTLOOK
WULTO wander wickr ZIMPERIUM

Endpoint Security

AhnLab avast Avecto Avira Barkly BitDefender
BISBY DEFENSE BLUEBRIDGE BUFFERZONE Carbon Black
Check Point COMODO CROWDSTRIKE CYBERARK
cybereason CYCLANCE depinstinct ENDGAME
ERICOM es31 F-Secure Fortanix FORTINET
HYSOLATE intego ivanti KAJPERKY McAfee
Microsoft MORPHSEC NYSTRON OPSWAT panda
SENTINELONE SOPHOS sparkcognition STONEXHELLO
Symantec TETRIS WEBROOT ZCO

Data Security

anuna baffle bescrypt CipherCloud CLOUDM365
CryptoMove DATALOCKER Fortanix NCCorp virtuo
clearswift CODE42 Fidelis McAfee
Symantec BlueTalon druux opentext SECLONE

Block Chain

Chain guardtime IDEE NuID remme
eChain ShoCard Xage

Security Operations & Incident Response

BlackStratus CORRELOG CYBILANT DEVO
exabeam FORTINET HanSight Huntsman IBM RSA
IGLOO JASK logentrics logpoint LogRhythm
logz.io McAfee HUBOTS Palantir SUMMIL SECURIX
solarwinds splunk sumologic TIBCO Trustwave arc42
ataris ayehu CYBERST Bay Dynamics DARKTRACE AWAKE
CYBERRANGE BARKLIGHT Cymru DTEX
DEMISTO DLABS FIREYE mistnet observe IPONSET
Microsoft paloalto radar RAPID
Raytheon resilient SEC RSA FORTINET Reservoir Labs
servicenow SECURITY SIFT ALL THREATCYBER THE TARAY
SWIMLANE THREATINTELLIGENCE pattemx haystack Veriato
ThreatConnect UPLEVEL VERINT VECTRA SECURIX

Threat Intelligence

4i@ Blueliv. ANOMALI LOOKINGGLASS Nucleon
Bluevantage Centripetal CISCO Recorded Future RISKIQ
digital shadows DOMAINTOOLS SensorCy Sixgill SURFWATCH
O'Electrico FORTISIGHT GROUPe SpyCloud ThreatConnect
FLASHPOINT HanSight HYAS ThreatMetrix THREATQUOTIENT
INTEL471 INTSIGHTS KELA ThreatSTOP TRUSTAR WEBROOT

Cloud Security

anchore aqua deepfence CODEWISE Guardicore ITRUST
NewVector POLYVERSE portashift threat stack WAMACOR AVANAN
Qualys StackRox Sysdig Managed Methods Microsoft netskope
Twistlock cloud betacloud illumio lacework SH-HELIX
PRACTET cavinr Check Point bitglass CipherCloud CISCO CORONET
cloud.confirmy CLOUDWAVE CYBRANE

Risk and Compliance

AXONIOS Balbix cavinr ODR RESERVER
cyber GRX DELVE KENNA
FRESHMASH NOPSEC OPAG Outpost24
panaseer PERVALENT RESERVAL riskrecon
SEKYBOX tenable UpGuard VENAFI
zeguro BITSIGHT CORAX FICO RiskLens
SecurityScorecard ATACRACK Cobalt CRONUS
CYBERRAT CYCIGNTO CVMULATE BETH tuftin
MAZEBOLT PCYSYS PICUS
RAPID SafeBreach VERODIN
algosec SECURE Lockpath MetricStream
neturix Onspring RESOLVER RSA
Barracuda COME CyberVista S4I GLOBAL
BONSCALES proofpoint BRANDEFORCE

WAF and Application Security

AXONIOS Akamai ALERT LOGIC ANOMALI
Barracuda CHECKPOINT citrix ergon THREATX
CykickLabs FORTINET SHIP
imperva NETSPI Tonopsis TEMPLARBIT
netsparker CONTRAST ZENITH Synack STACKPATH
Qualys ORACLE CloudSploit warim Vicidius IBM
portshift PURESEC hackerone SEVENSIX
RAPID Rebase riverbed riverbed SUCURI
PentaSecurity radware Signal Sciences saeen
waratek Trustwave VERACODE
sentry AWAKE BRICTRA CGS
DARKTRACE Extrahop GigaBlast
PERCH Pliker SEC7 SSS

Identity & Access Management

Accepto Auth0 AVERON BehaviorSec BiOCATCH Calsign
CLEF CORE EXOSTAR FORGELOCK FUDU Google
IDEA Imprivata INTRANSICO nok nok pindrop plonID SASPASS
transmit SECUREPUSH SILVERFORT tascant ThreatMetr.
TransUnion TRUSONA UNBJOND UNIKEN V-KEY VIRGIS Certify
Centrify IBM idaptive Microsoft okta RSA HPR
onelogin ORACLE THALES BeyondTrust PLENITUDE
CYBERARK HITACHI ManageEngine ONE IDENTITY
Remediant SECURELINK thycotic AXIOMATICS Duxberry
helpsystems ScalPoint simelo Akamai IDExperts
logradius Truico vchain verato VERIFF ID.me

Network & Infrastructure Security

Barracuda BLUEHEXAGON BLUVECTOR CISCO CORSA
FIREYE FORTINET HUAWEI HYSOLATE JOESecurity Juniper
mimecast OPSVAAT paloalto RESEC GATESCANNER SONICWALL SOPHOS
Symantec VOTRO VOTRO VOTRO
Check Point EXTERNA FORGEGOUT NANOSEC SKYPORT NETWORLD pornox nextgen
Trustwave zeniter Genians TEMPERO VERSA ZENON
imperva neustar NEUSGUARD NINFOCUS ORACLE Corelight
SECUREM STACKPATH BLUECAT neustar ThreatSTOP 8888 Quod MixMode
efficientIP Infoblox GUNSHIELD Hiltner OPAG SANGFOR McAfee
seccloud SONICWALL STORMSHIELD tuftin fidels WAVE ACALISE SPINR PAS
ANIR Invasive Counter Craft VIPER CyberTrap SMOKEGREEN
Cymmetria TRAPX APERIO BAYSHORE BELDEN CERIFENCE
CYBERBIT FIRMITAS Indegy dimension SCAMMER corvit NETSCOUT
CyberX DRAGOS PFP radiflow Rhebo CORE Trustnet
CloudShark ultimaco GREYCORTEX

The Time for Resilience is Now!

The Gartner logo is displayed in a white rectangular box on the left side of the slide. The word "Gartner" is written in a bold, dark blue, sans-serif font, with a registered trademark symbol (®) to the right of the letter "r".

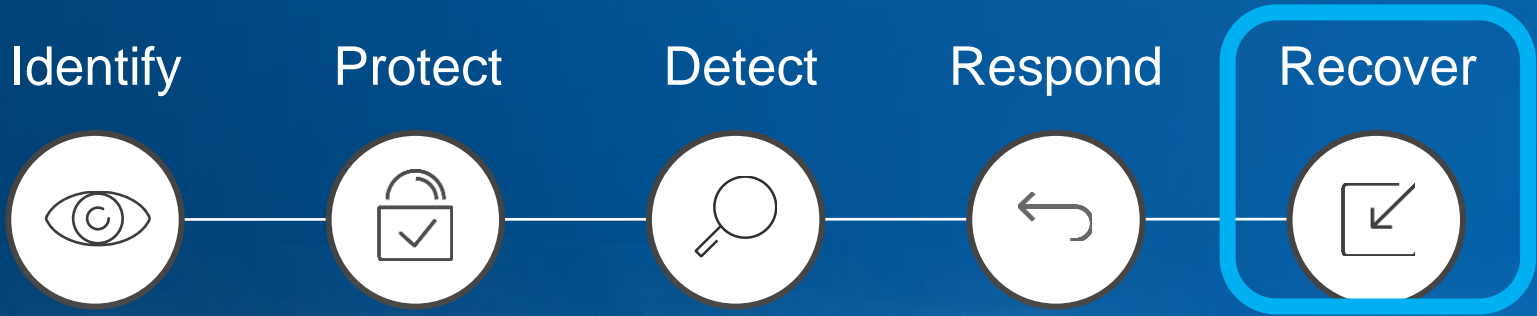
“Transforming cybersecurity into cyber-resilience involves prioritizing resilience over defense, and elevating the native disciplines and skills used by the business continuity management office above cybersecurity teams’ traditionally defensive strategies.”

Gartner, *You Will Be Hacked, So Embrace the Breach!*

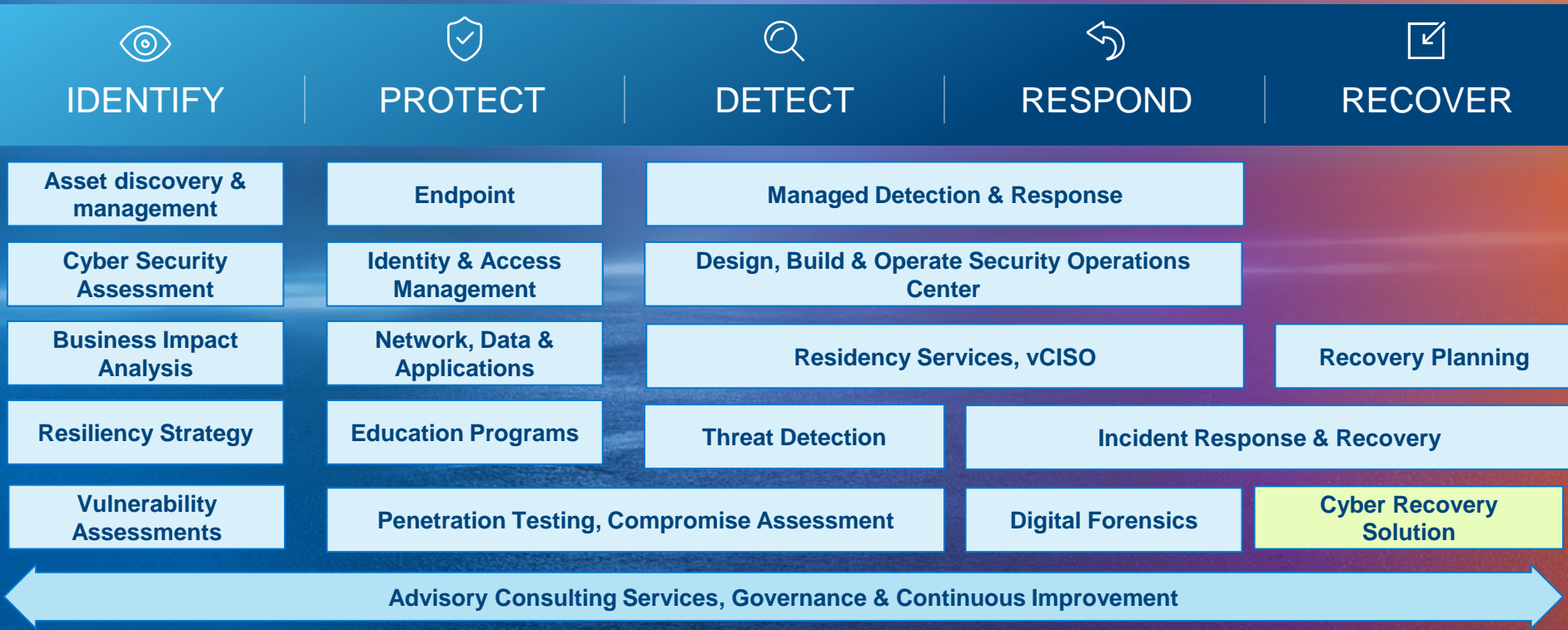
"Implement at least an immutable backup copy by selecting write lock or WORM media before starting any other initiative, as having an immutable copy of the backup is the most important item to start protecting backup data."

Gartner, *Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults*

NIST Cyber Security Framework



Our approach: NIST Cybersecurity Framework



Progress Markers in a Cyber Resilience Journey



App Stack Resilience

- How Apps are built
- How Apps are updated
- How Apps are allowed to fail and recover
- Stateless vs. Stateful
- How much control do you have



Infrastructure Resilience

- Operating environment resilience
- Infrastructure Trust – from the Hardware Root to the OS/Platform
- 'Ring of Fire' and Defense in Depth & Breadth



Data Resilience

- Data classified based on Value
- Data assets mapped to Organization's *Survival Time Objective*
- Having a non-suspicious Golden Copy of business data assets
- Having an isolated Air-Gap

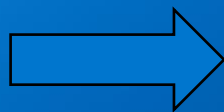
Zero Trust is the foundation

Data Resilience made Practical

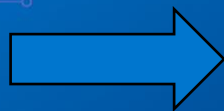


Data Resilience

- Data classified based on Value
- Data assets mapped to Organization's *Survival Time Objective*
- Having a non-suspicious Golden Copy of business data assets
- Having an isolated Air-Gap



Business “STO” & “MVO”



Blue Teams + LoB



Trusted Infrastructure +
Clear Run Books

Incident Response

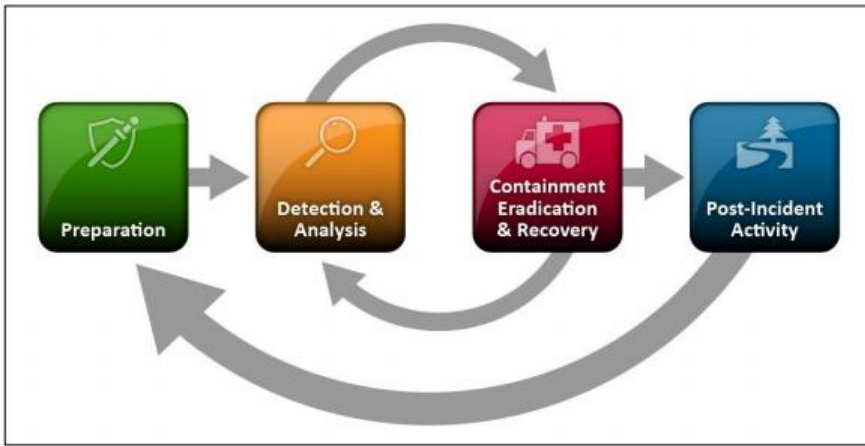


Figure 3-1. Incident Response Life Cycle

3.3.4 Eradication and Recovery

Eradication and recovery should be done in a phased approach so that remediation steps are prioritized.

For large-scale incidents, recovery may take months; the intent of the early phases should be to increase the overall security with relatively quick (days to weeks) high value changes to prevent future incidents.

ACPO Principle 1:

No action is taken that should change data held on a digital device including a computer or mobile phone that may subsequently be relied upon as evidence in court.

- NIST SP800-61 Computer Security Incident Handling Guide
- NIST SP800-86 Guide to Integrating Forensic Techniques into Incident Response
- ***NIST SP800-184 Guide for Cyber Security Event Recovery***
- ACPO Good Practice Guide for Digital Evidence

Cyber Resilience – What is the difference?

Immutability

'Unchanging over time or unable to be changed'

- Efficient Data Consumption & shortest time to recover certified clean data
- Anomaly Alerting and Reporting for audit and regulatory compliance
- Zero Trust with Dual role and Multi Factor Authentication
- Proven Data Integrity since 2001 (DIA)
- Immutability with Retention Lock (2012)



Multiple reports following real world events have indicated that *immutability is only one consideration...*

Cyber Resilience

'The ability to continue operations following a cyber incident'



Isolation

Immutability

Intelligence

A proven offline copy

Secure Global Supply Chain

Incident Response Plan & Testing

Fastest Time to Recovery of Good Data

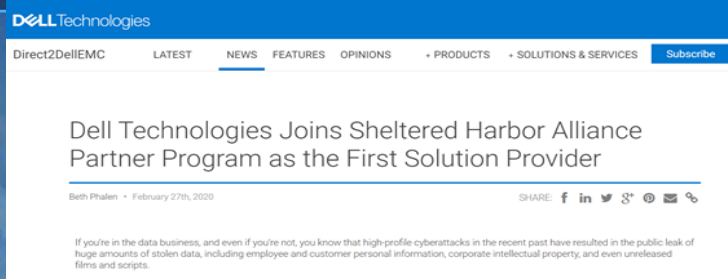
Regulatory Compliance Through Accurate Analysis and Reporting



Dell Technologies Cyber recovery contributions



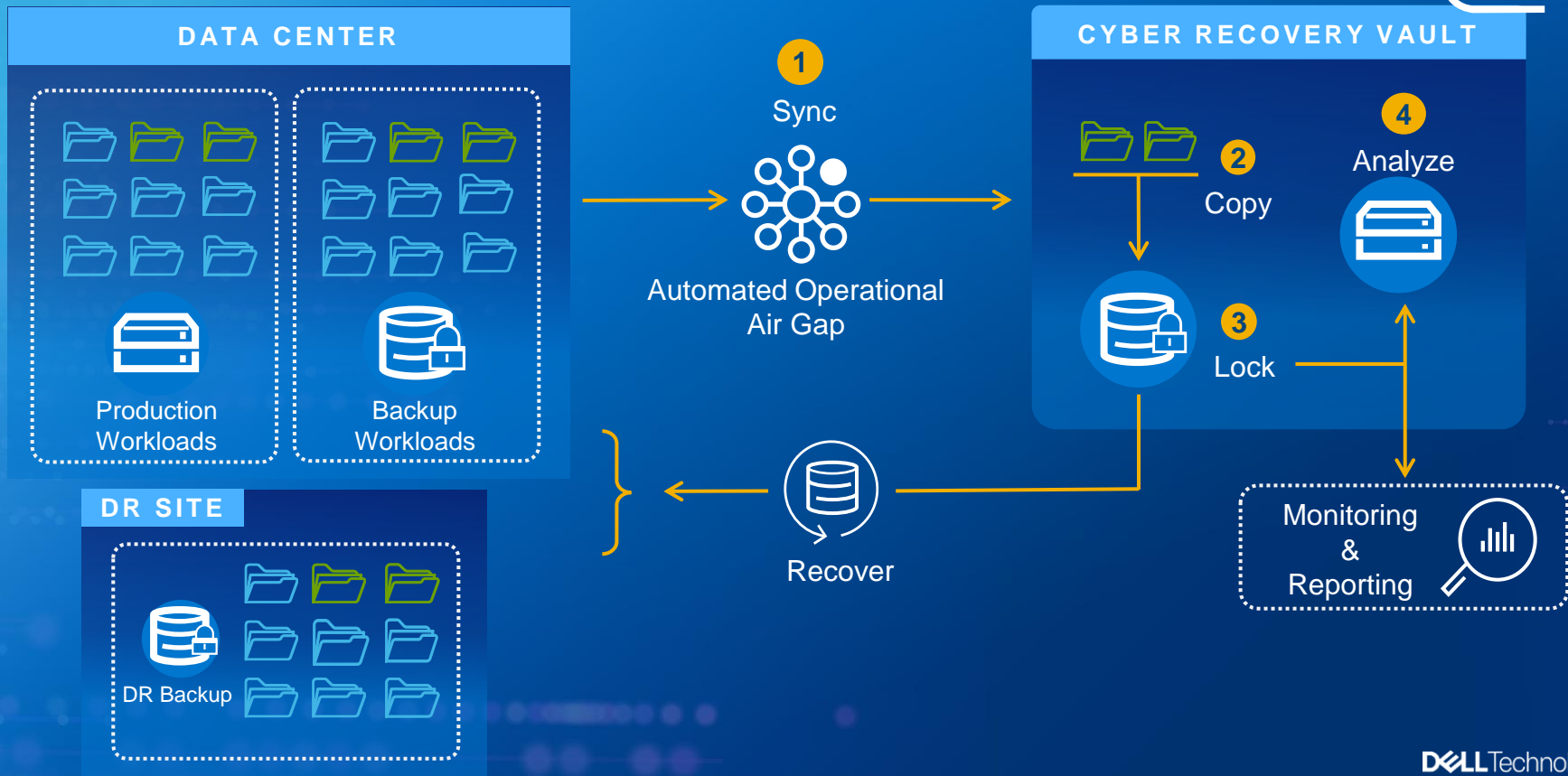
2015	First "Isolated" recovery solution with custom deployment
2018	Introduced PowerProtect Cyber Recovery solution
2019	First technology vendor in Sheltered Harbor Alliance Partner Program
2020	First Endorsed Sheltered Harbor Solution – PowerProtect Cyber Recovery
2021	Introduced PowerProtect Cyber Recovery for Multi-Cloud
2021	Introduced PowerProtect Cyber Recovery for AWS
2022	Introduced PowerProtect Cyber Recovery for MS Azure



1300+ Cyber Recovery Customers

Dell PowerProtect Cyber Recovery

Ensuring Recovery After A Cyber Disruption



New Alerts

- ! 2 Critical
- ! 1 High
- ! 5 Medium

New Alerts (8)

Cleared Alerts (24)

Alert Type	Time	Alert Name	Files	Size	Hosts	Job Name
!	Dec 14, 2021 01:30	Watchlist Changed	1,872 files	300GB	2 hosts	jobname91bd86a2fead20c79b6ce389ad50c70810...
!	Dec 14, 2021 01:30	Suspected Ransomware	36,332 files	400GB	4 hosts	jobname91bd86a2fead20c79b6ce389ad50c70810...
!	Dec 14, 2021 01:30	Watchlist Changed	1,872 files	300GB	2 hosts	jobname91bd86a2fead20c79b6ce389ad50c70810...
!	Dec 14, 2021 01:30	Suspected Ransomware	12,345 files	240GB	1 hosts	jobname91bd86a2fead20c79b6ce389ad50c70810...



Dec 14, 2021 12:30pm: Suspected Ransomware

In this case, there were a small number of new files where the average entropy of new files had a high average entropy. The Machine Learning Model recognized this as a type of ransomware attack that takes place on certain application servers, such as a database server.

Clear

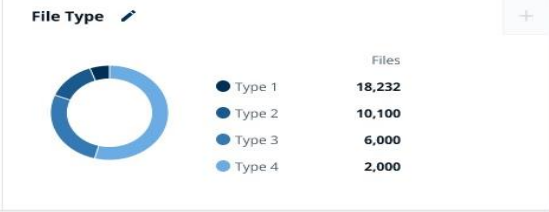
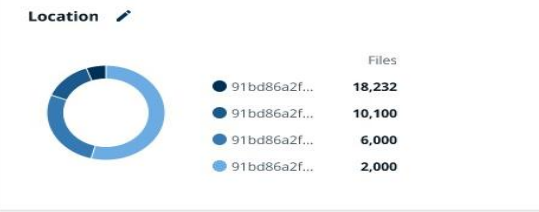
Default View

36,332 Suspect Files

400 GB Affected

4 Suspect Hosts





























Job Name: jobname91bd86a2fead20c79b6ce389ad50c70810102



No grouping applied. Drag and drop a column header here to group.

<input type="checkbox"/>	NAME	HOST	OWNER	LAST MODIFIED ↓	ACCESSED	SIZE	DIRECTORY	LAST KNOWN BACKUP ID	<input type="checkbox"/>
<input type="checkbox"/>	Another File Name that is too...ng.exe	91bd86a2fe...	Jonathan Anderson	Dec 14, 2021 01:30	Dec 14, 2021 01:30	1TB	Directory Name	12345	
<input type="checkbox"/>	Another File Name that is too...ng.exe	91bd86a2fe...	Jonathan Anderson	Dec 14, 2021 01:30	Dec 14, 2021 01:30	1TB	Directory Name	12345	
<input type="checkbox"/>	Another File Name that is too...ng.exe	91bd86a2fe...	Jonathan Anderson	Dec 14, 2021 01:30	Dec 14, 2021 01:30	1TB	Directory Name	12345	
<input type="checkbox"/>	Another File Name that is too...ng.exe	91bd86a2fe...	Jonathan Anderson	Dec 14, 2021 01:30	Dec 14, 2021 01:30	1TB	Directory Name	12345	

MITRE Att&ck Impact Analysis

Attack Type	Attack Description	Mitre Att&ck Impacts	Backup	Immutability	Isolation	Intelligence
Ransomware	<ul style="list-style-type: none"> • Infects endpoints and servers • Encrypts all CIFS and NFS shares it can access 	<ul style="list-style-type: none"> • Data Encrypted for Impact 				
Ransomware + Backup Deletion	<ul style="list-style-type: none"> • Infects endpoints and servers • Backups are manually deleted (admin credentials) 	<ul style="list-style-type: none"> • Data Encrypted For Impact • Data Destruction • Inhibit System Recovery 				
Ransomware + Platform Wipe	<ul style="list-style-type: none"> • Infects endpoints and servers • Backup infrastructure is wiped at platform level 	<ul style="list-style-type: none"> • Data Encrypted For Impact • Data Destruction • Disk Wipe 				
Ransomware + Firmware Attack	<ul style="list-style-type: none"> • Infects endpoints and servers • Backup and other platforms are crashed at firmware level 	<ul style="list-style-type: none"> • Data Encrypted For Impact • Data Destruction • Firmware Corruption 				
Ransomware + VM Level Attack	<ul style="list-style-type: none"> • Infects endpoints and servers • VMs are deleted (includes SW-defined backup infra) 	<ul style="list-style-type: none"> • Data Encrypted For Impact • Data Destruction 				
Dormant Ransomware	<ul style="list-style-type: none"> • Infects endpoints and servers • VMs are deleted (includes SW-defined backup infra) 	<ul style="list-style-type: none"> • Data Encrypted For Impact • Data Destruction • Data Manipulation 				
Hidden Encryption	<ul style="list-style-type: none"> • Infects endpoints and servers 	<ul style="list-style-type: none"> • Data Manipulation 				

In Summary...

Their destruction



Penetrate



Enumerate & Exfiltrate data



Obfuscate



Compromise Production Backups



Encrypt, Disrupt & Destroy

Your Protection



Single Incident Management Partner
Turnkey Cyber Incident Command



Isolate backups from production
Make backups Tamper proof



Zero Trust, isolated deep scan



Reduce the attack surface and neutralise
elevated privileges



Strategize recoveries and relaunch plans