Security

ADVANCED UNIBYTE

Webinar
Commvault Cloud - The Platform of Cyber Resilience

Andreas Kugel
Solution Architect (Backup)

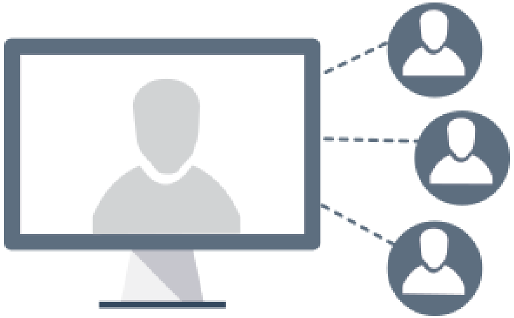
andreas.kugel@au.de
+497123 9542 - 270

Michael Spengel
Commvault
Senior Sales Engineer

mspengel@commvault.com
+49 162 248 1193

Organisatorisches

Über dieses Webinar



Dieses Webinar wird aufgezeichnet

- Ihr Mikrofon ist automatisch stummgeschaltet
- Fragen bitte über die Q&A Funktion in Webex stellen
- Im Anschluss an das Webinar senden wir Ihnen die Präsentation gerne zu

What is a Cyber Attack?

Personally motivated attackers seek financial gain through money theft, data theft or business disruption. Likewise, the personally motivated, such as disgruntled current or former employees, will take money, data or a mere chance to disrupt a company's system. Mainly, they seek retribution.

Your last line of defense.

> “The most important defense for any organization against ransomware is a robust system of backups. Having a recent backup to restore from could prevent a ransomware attack from crippling your organization. The time to invest in backups and other cyber defenses is before an attacker strikes, not afterward when it may be too late.

According to the FBI

https://www.ic3.gov/Media/Y2019/PSA191002

Cyber Attacks At A Glance

Proper cybersecurity hygiene demanded by cyber insurance underwriters

Average dwell time

Assume Breach

[illegible]

days

68%

of businesses that paid, were compromised again within a month

62%

of all attackers do not use malware to gain access

96%

of businesses that pay the ransom don’t get all their data back

Days lost to downtime increased to

21

on average

Attacks are faster than ever.

What once took months, now takes minutes.

Access

Breach and gain foothold

Damage

Execute attacks below the radar, exfiltrating and encrypting data

Disable

Break operational continuity to prevent recovery

ACROSS HYBRID MULTI-CLOUD ENVIRONMENTS

Azure aws ORACLE salesforce

Average breakout times have accelerated to › **84 MINUTES**

Incident responders have a short window of time to contain breaches after an initial compromise.

Source: CrowdStrike 2023 Global Threat Report

Attacks are broader than ever.

Increasing risk to backup & recovery environments.

Access

Breach and gain foothold

Damage

Execute attacks below the radar, exfiltrating and encrypting data

Disable

Break operational continuity to prevent recovery

Attackers don't just attack the crown jewels ›

83% INCREASE IN RANSOMWARE

Featuring double or triple extortion

Backup & recovery are exposed to more risk

Source: Venafi 2022 Ransomware Survey

Recovery as last-line-of-defense is necessary but insufficient.

Access

Breach and gain foothold

Damage

Execute attacks below the radar, exfiltrating and encrypting data

Disable

Break operational continuity to prevent recovery

Key aspects of the NIST security framework are not covered.

This is where you need data protection in today’s modern environment; without it, you’re left defenseless to attacks.

Recover

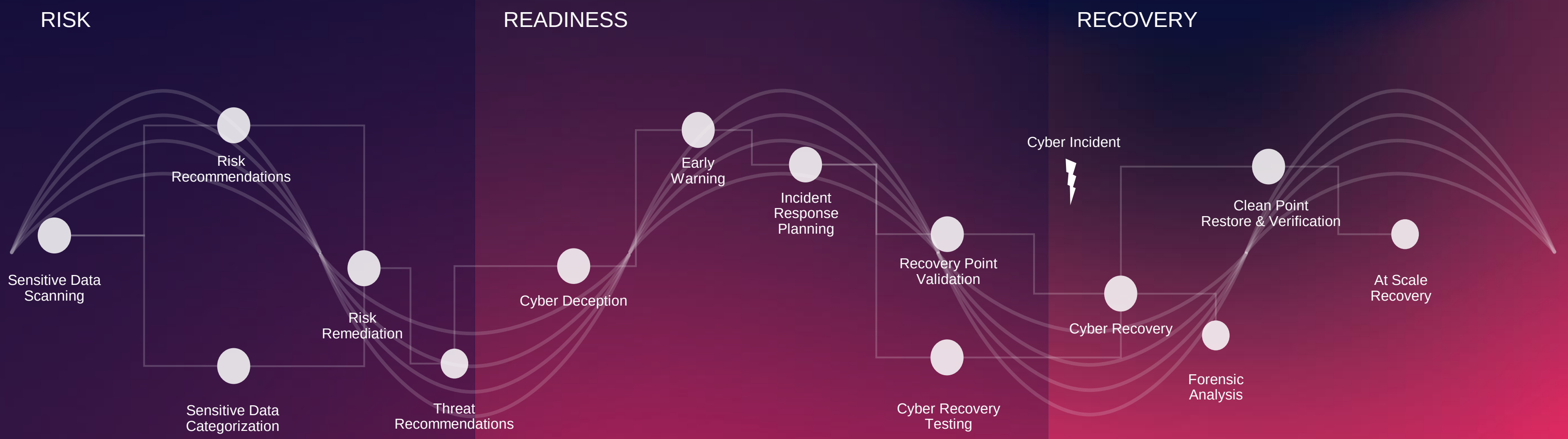
Recover faster

This is your last line of defense, but by the time you’re here, it’s too late.

WHAT'S REQUIRED

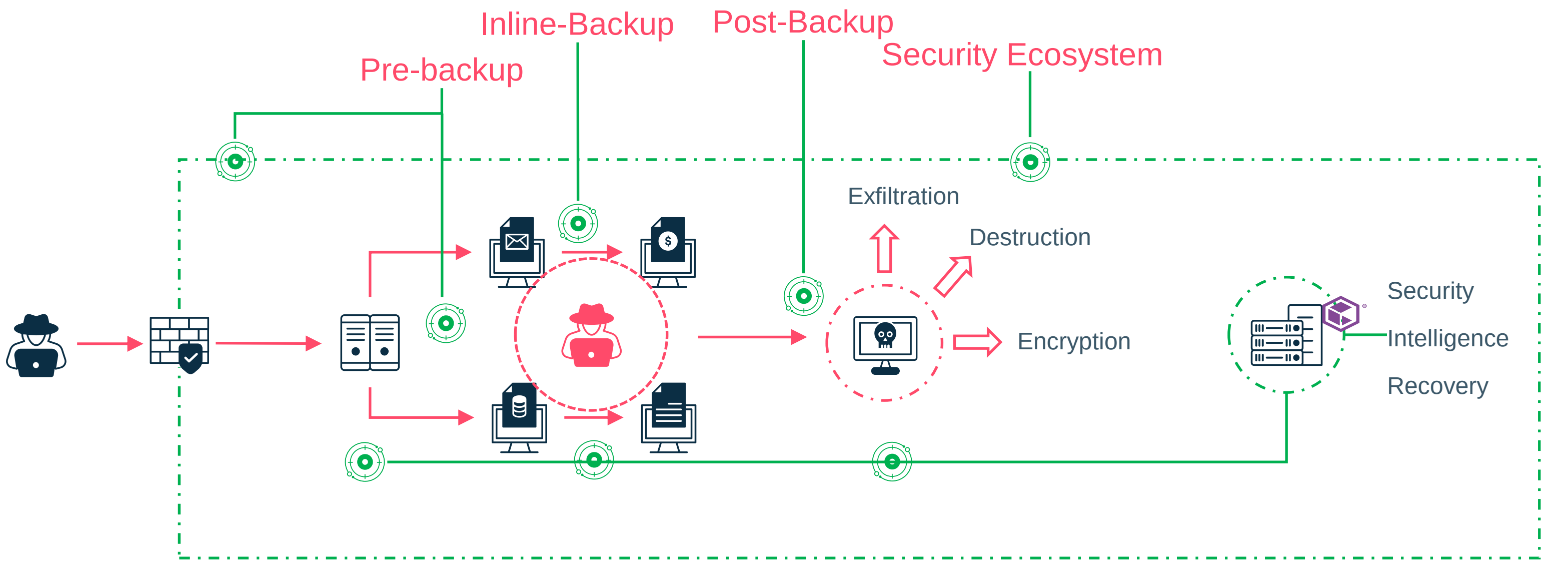
True cyber resilience starts before the attack — and never ends.

Based on MITRE CREF and NIST frameworks



Commvault

Cyber Resilience | Counter Measures | Data Enrichment | Incident Response



Pre-backup

- Threatwise
- Risk Analysis
- Canary Files*
- Live Anomaly

Inline-Backup

- File Activity
- File Type
- Backup Size*
- Extensions*
- Operational

Post-Backup

- Threat Scan
- Risk Analysis
- Data Verification
- Auto/Clean Recovery

Security Ecosystem

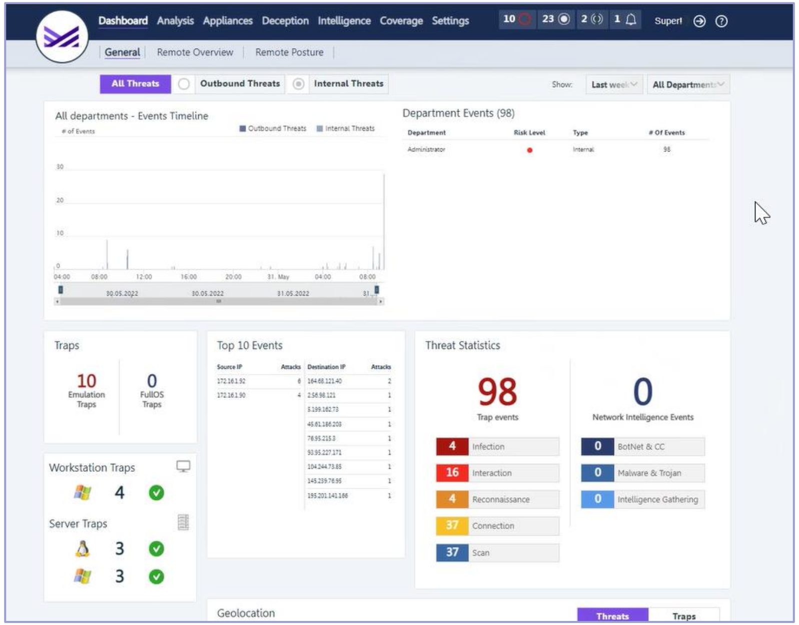
- SIEM/SOAR
- Threat intelligence
- EDR/XDR/NDR
- Vulnerability

*New feature

Threat Wise Early Cyber Deception

Threatwise™

EARLY WARNING CYBER DETECTION



Department Events (98)

Department	Risk Level	Type	# Of Events
Administrator	●	Internal	98

Top 10 Events

Source IP	Attacks	Destination IP	Attacks
172.16.1.92	6	164.68.121.40	2
172.16.1.90	4	2.56.98.121	1
		5.199.162.73	1
		45.61.186.203	1
		76.95.215.3	1
		93.95.227.171	1
		104.244.73.85	1
		145.239.76.95	1
		195.201.141.166	1

Trap events		Network Intelligence Events	
4	Infection	0	BotNet & CC
16	Interaction	0	Malware & Trojan
4	Reconnaissance	0	Intelligence Gathering
37	Connection		
37	Scan		

Intelligent decoys that mimic and behave like legitimate assets

Precise alerts to pinpoint threats early, without false-positives or alert fatigue

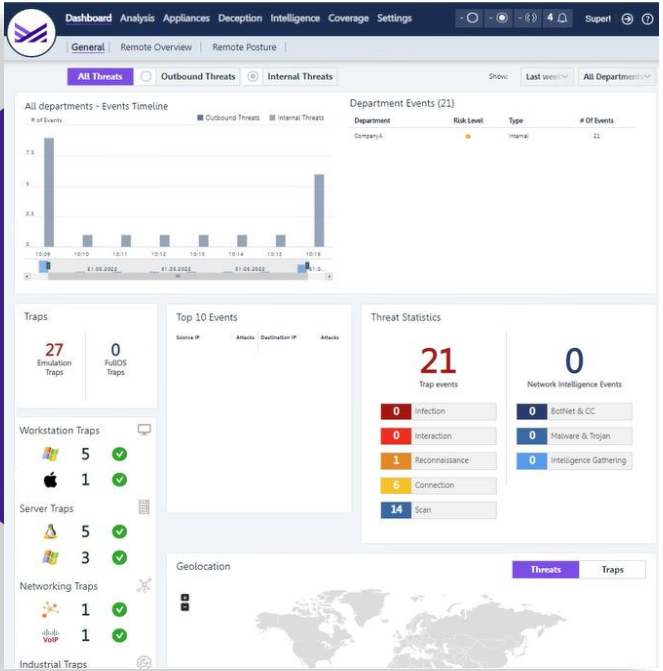
Robust integrations across critical security tooling and backup environments

Simple SaaS delivery with flexible, lightweight architecture and rapid scalability

TSOC

ThreatWise™ Security Operations Console

Metallic®
Control Plane



Department Events (21)

Department	Risk Level	Type	# Of Events
CompanyA	●	Internal	21

Traps

27 Emulation Traps

0 FullOS Traps

Workstation Traps

Windows	5	✓
Apple	1	✓

Server Traps

Linux	5	✓
Windows	3	✓

Networking Traps

Network	1	✓
VoIP	1	✓

Industrial Traps

Top 10 Events

Source IP	Attacks	Destination IP	Attacks

Threat Statistics

21 Trap events

0	Infection
0	Interaction
1	Reconnaissance
6	Connection
14	Scan

0 Network Intelligence Events

0	BotNet & CC
0	Malware & Trojan
0	Intelligence Gathering

Manage ThreatWise™ appliances, deploy threat sensors and view events

Point of Integration to Security Eco-System such as SIEM, Firewall, NAC and Sandboxes

Accessed via **Metallic Hub/Control Plane**

Appliance

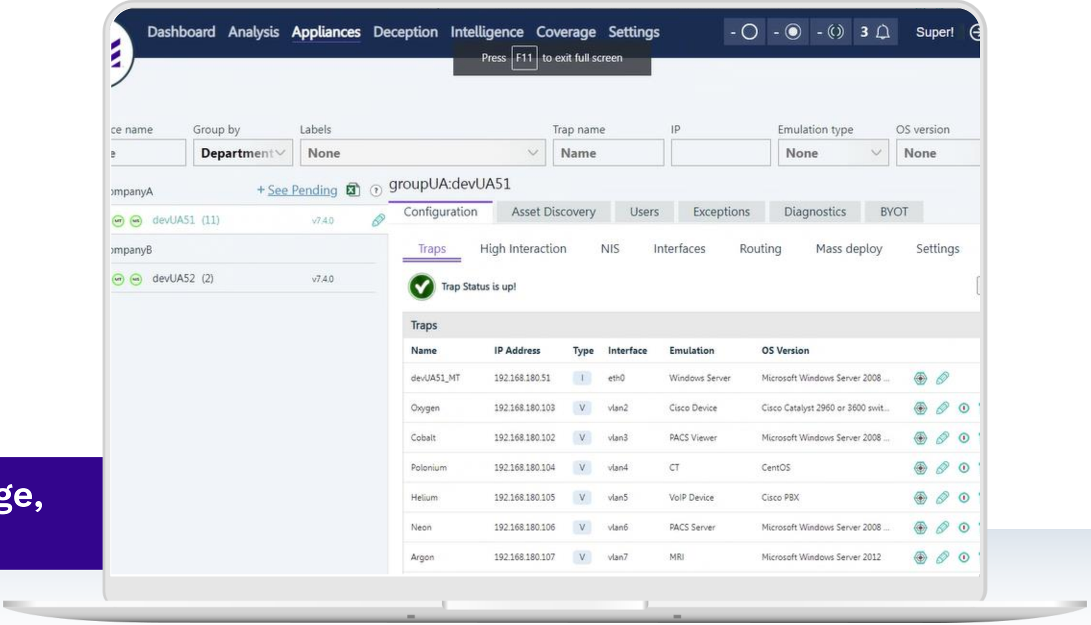
Infrastructure Components

A virtual machine deployed to a hypervisor provided by the customer

(VMware ESXi, Hyper-V, KVM, AWS AMI, Azure)

- Each Appliance supports 512 individual Threat Sensors
- Seamless deployment with Metallic® ThreatWise™ templates
- **Security is enhanced** by using outbound communication to the TSOC

To increase surface area coverage, deploy more appliances



ce name: e
Group by: Department
Labels: None
Trap name: Name
IP:
Emulation type: None
OS version: None

ompanyA + See Pending

devUA51 (11) v7.4.0

ompanyB

devUA52 (2) v7.4.0

groupUA:devUA51

Trap Status is up!

Traps

Name	IP Address	Type	Interface	Emulation	OS Version
devUA51_MT	192.168.180.51	I	eth0	Windows Server	Microsoft Windows Server 2008 ...
Oxygen	192.168.180.103	V	vlan2	Cisco Device	Cisco Catalyst 2960 or 3600 swit...
Cobalt	192.168.180.102	V	vlan3	PACS Viewer	Microsoft Windows Server 2008 ...
Polonium	192.168.180.104	V	vlan4	CT	CentOS
Helium	192.168.180.105	V	vlan5	VoIP Device	Cisco PBX
Neon	192.168.180.106	V	vlan6	PACS Server	Microsoft Windows Server 2008 ...
Argon	192.168.180.107	V	vlan7	MRI	Microsoft Windows Server 2012

metallic®
A Commvault Venture

Lures

Infrastructure Components

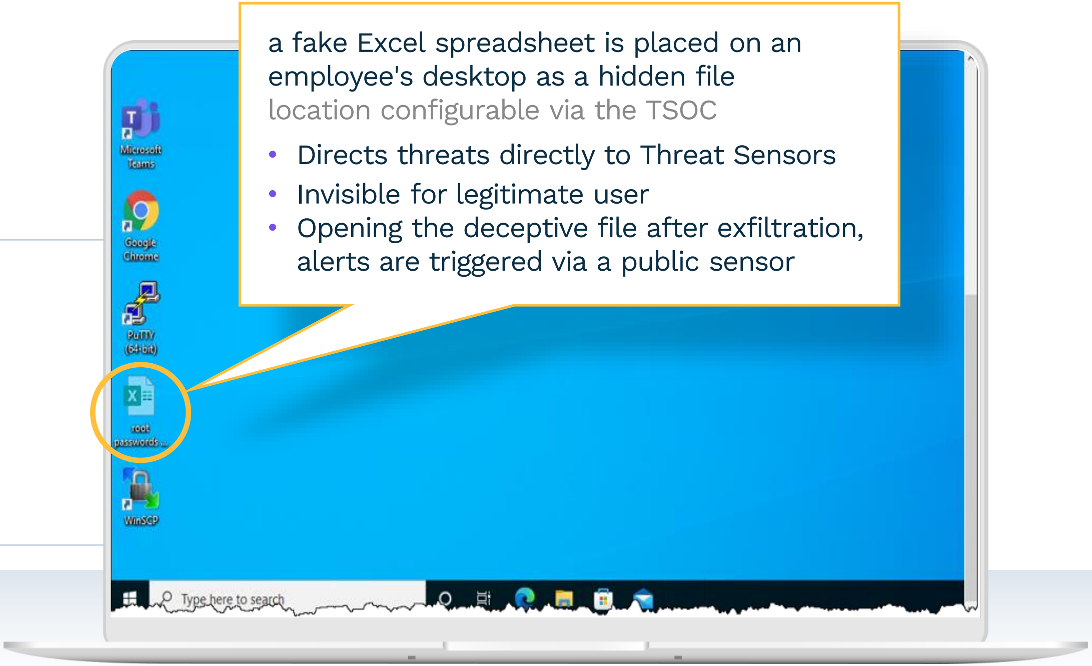
Lures are agentless pieces of data

They lure attackers in and direct them to the Threat Sensors

- Deployed on endpoints or strategic points

Lures include

- Cached credentials
- Deceptive files (Word or Excel files)
- Fake SMB drives
- Browsing history
- Entries to HOSTS file
- Stored sessions (e.g., RDP Shortcut, SSH, Putty and WinSCP)
- Active Directory



a fake Excel spreadsheet is placed on an employee's desktop as a hidden file
location configurable via the TSOC

- Directs threats directly to Threat Sensors
- Invisible for legitimate user
- Opening the deceptive file after exfiltration, alerts are triggered via a public sensor

Threat Sensor Deployment

Out of the box

Threat Sensor

Replicated Network Assets

- ✓ Highly scalable due to mass and bulk deployment
- ✓ Seamless blend in due to configurable services
- ✓ Deployed in Seconds

Category	Used Cases	
Workstation	• Windows, Linux or Mac Endpoints	
Servers	• Databases • Backup Servers	• Virtual Machines
IoT Devices	• Printer • Security Cameras	• Point of Sale • Smart Lights
Networking	• Switches (incl. PBX)	• VPN
Medical	• MRI • CT	• PACS Systems
Industrial	• SAP • PLC	• SCADA
Financial	• SWIFT	• ATM

Indistinguishable Threat Sensor

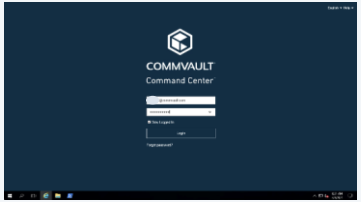
To blend-in each Sensor type has various ways to enhance the configuration

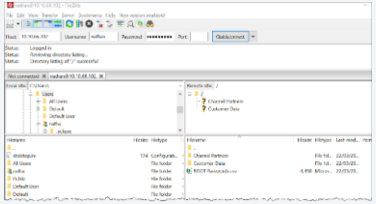
Replicate a Backup Server

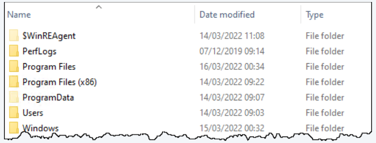
Threat Sensor Type: Windows Server 2019

Deploy

Enhance the interface upload html/css files




Status: Logged in
Status: Retrieving directory listing...
Status: Directory listing of "/" successful



Name	Date modified	Type
$WinREAgent	14/03/2022 11:08	File folder
PerfLogs	07/12/2019 09:14	File folder
Program Files	16/03/2022 00:34	File folder
Program Files (x86)	14/03/2022 09:22	File folder
ProgramData	14/03/2022 09:07	File folder
Users	14/03/2022 09:03	File folder
Windows	15/03/2022 00:32	File folder

Fake SMB & FTP enabled content are uploaded to a (default) “Data” folder

Individualize Sensor Template

Deceive

re-use templates in multiple deployments

metallic®
A Commvault Venture

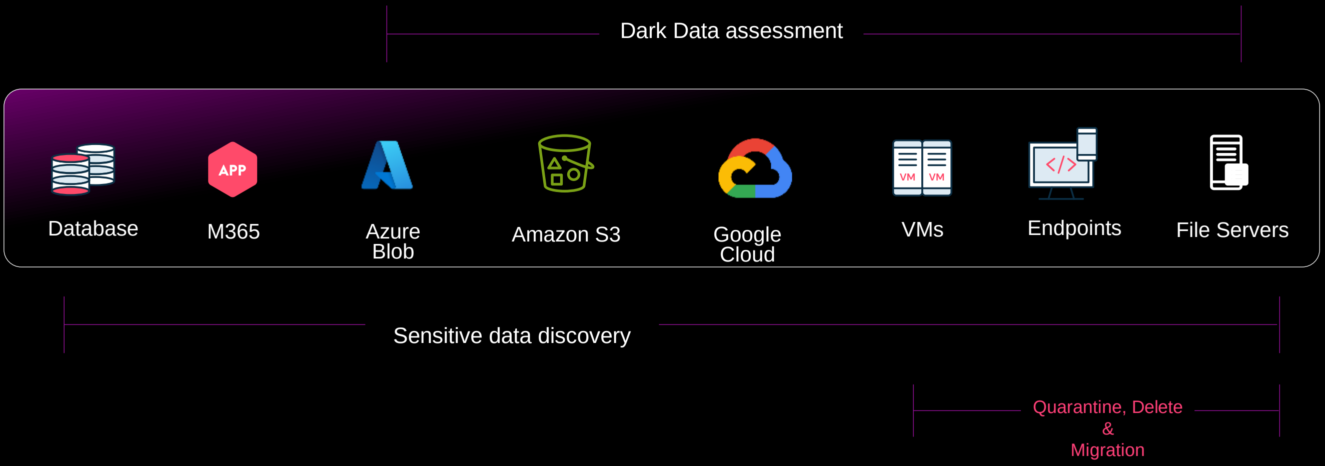
Risk Analysis

A quick recap on Risk Analysis

Secure
NIST 1800-25
Asset Identification and protection

Defend
NIST 800-53
Security monitoring

Commvault Cloud
Powered by Metallic AI



Dark Data assessment

Database

M365

Azure Blob

Amazon S3

Google Cloud

VMs

Endpoints

File Servers

Sensitive data discovery

Quarantine, Delete
&
Migration

- A unified solution, boosting efficiency and reducing the complexity of managing dark and sensitive data
- Continuously analyze live and backup data for proactive decision-making and risk management insights
- Minimize sensitive data exposure to enable faster recoveries with streamlined backups
- Achieve flexible data migration across diverse storage, optimizing resources and adapting to evolving business needs
- Enhance security by isolating sensitive data, minimizing risks and safeguarding network against malicious activities

Requirements

Risk Analysis Server requirements:

- RHEL and Windows based server

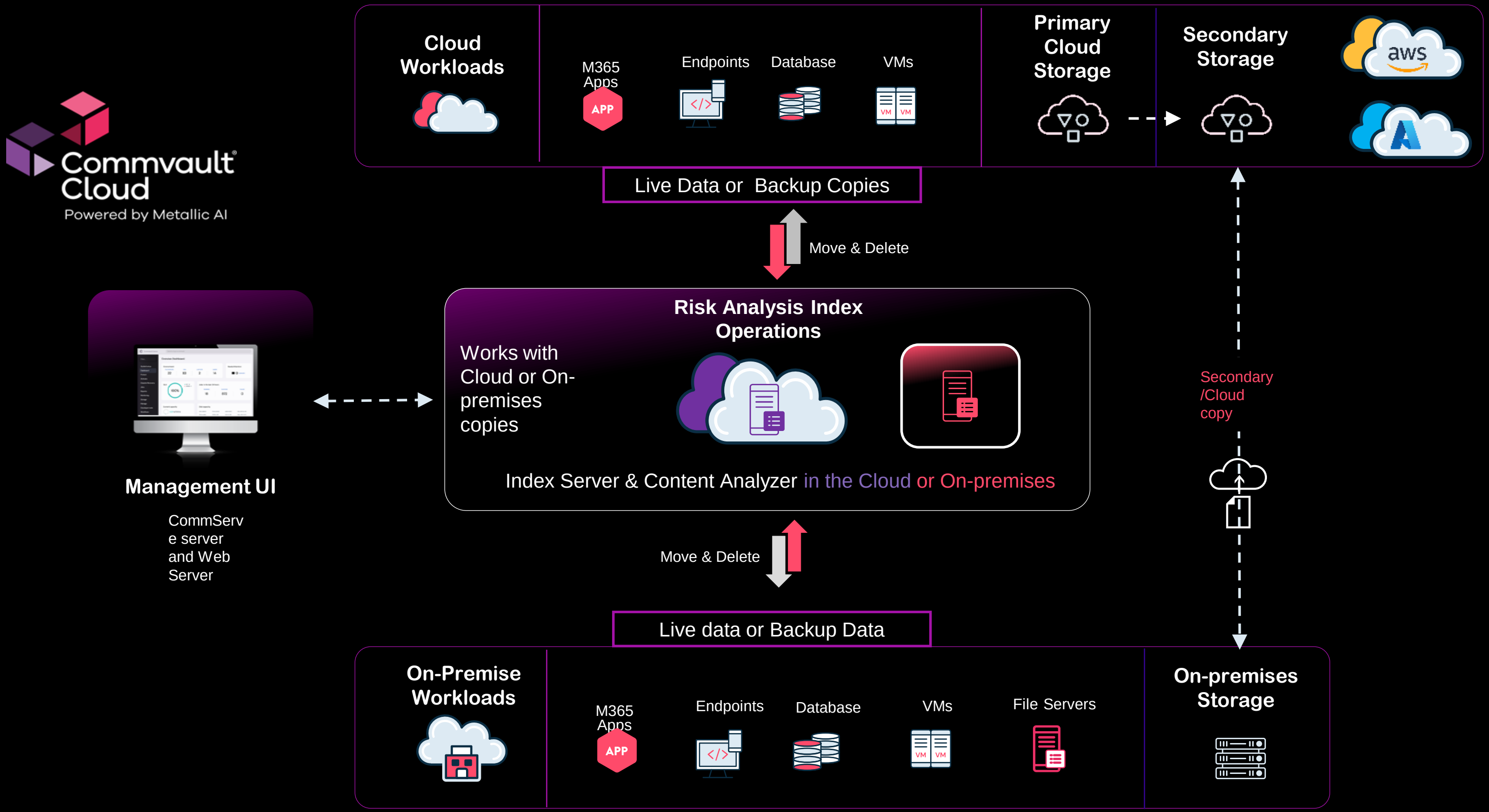
Required install packages:

- Index Store
- Index Gateway
- Content Analyzer

Risk Analysis Index Server Requirement		
Component	Large (320TB data size)	Medium (160 TB data size)
CPU	32 cores	16 cores
RAM	64 GB	32 GB
Disk Cache	12 TB	6 TB

See Index sizing guidance https://documentation.commvault.com/11.34/essential/160754_risk_analysis.html

Risk Analysis Architecture



Canary files

A canary file is **a fake computer document that's placed among real documents to help detect unauthorized data access, copying, or modification**. The name comes from canaries, which were used in coal mines as an early warning to miners.

Canary file enhancements

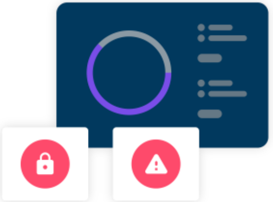
BUSINESS CHALLENGE

Organizations are challenged with identifying malicious behavior such as file encryption, corruption, or file tampering as soon as possible to fortify protection of data to maintain Cyber Resilience.

- Tampering with Commvault's software can prevent backups
- Early detection of file corruption, changes or encryption
- Respond as quickly as possible

OUR SOLUTION

Commvault’s canary file technology helps organizations enrich their existing threat intelligence by providing simple, robust, customizable, in-built monitoring for file tampering that can indicate malicious activity so that organizations can fortify defenses faster, to keep data safe, and backups ready for recovery.



CUSTOMER BENEFITS

Who

IT/Backup Admins, Sec Ops

Why

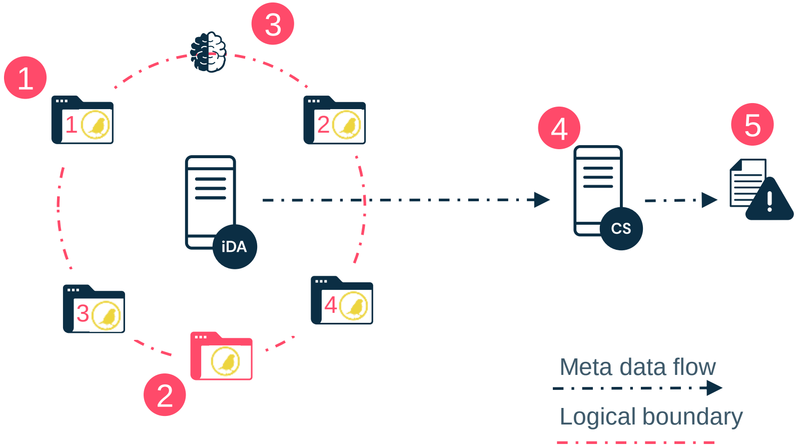
- Detect potential Commvault software tampering, which could impact ability to backup and restore data
- Broader honeypot support provides file tampering detection capabilities for other locations to provide early warning of threat activity
- Helps enrich existing threat intelligence used by security teams

Canary file enhancements

Architecture

High Level Architecture

1. Four default Canary file system locations
2. Add Canary files to custom locations
3. Client-side monitoring of canary change conditions included with File System app
4. If the canary file is modified, extension is changed, or deleted – then an alert it triggered
   - Windows systems provide real-time alert
   - Linux systems alert every 4 hours (configurable)
5. Email/Webhook/Syslog Alerts (SIEM/SOAR)



Early Adopter

Backup size anomaly

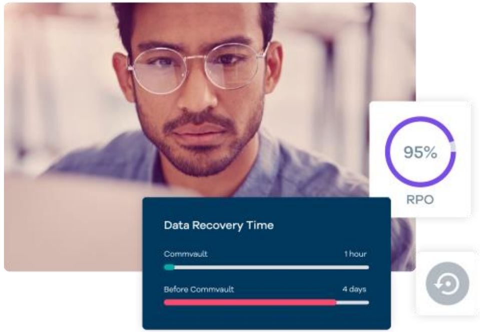
Early adopter

Backup size anomaly

BUSINESS CHALLENGE

Malware threats can impact files prior to backup. Organizations are challenged with monitoring and identifying backup changes, since unusual changes may indicate the files that are being backed up are not good.

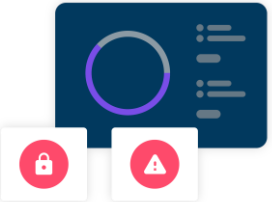
This problem exists across most workloads.



OUR SOLUTION

Backup size anomaly detection, is a framework for identifying unusual backup size changes based on data written and dedupe block change rates. This helps organizations identify potentially infected backup content so they can respond and recover clean data quickly.

CUSTOMER BENEFITS



Who

IT/Backup Admins, Sec Ops

Why

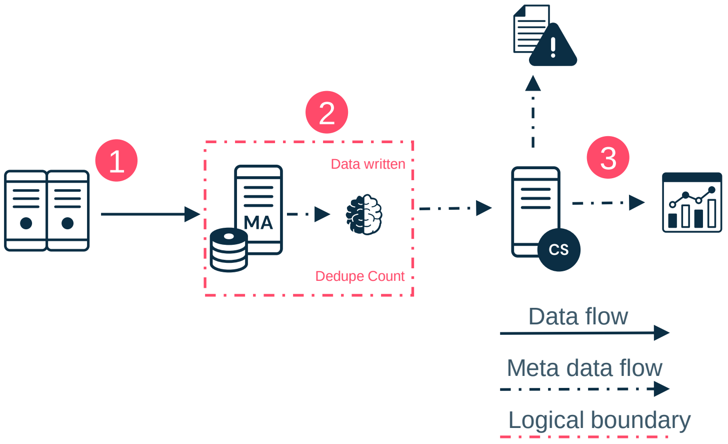
- Provides a workload agnostic anomaly framework that can easily support future workloads providing a competitive advantage
- Leans into core-value prop around backup and recovery - helping organization's accelerate recovery time objectives with clean recovery.
- Helps identify backups with large change rates, which can indicate malicious file changes prior to backups

Backup size anomaly

Architecture

High Level Architecture

1. Backup with deduplication enabled
2. Dedupe primary count, and data written analytics are sent and processed by the AI/ML engine on the Media Agent
3. Detected anomaly is sent through the CommServe as an Email/Webhook/Syslog alert and Security IQ dashboard is updated



How does it work…

USES EXISTING BACKUP INDEX ANOMALY FRAMEWORK

1. Need at least 10 backups
2. After backup, job stats are fed to the anomaly engine using backup size and dedupe block count as data inputs for the algorithms
    - Part of MA CvStatAnalysis service
3. If backup size has increased above the machine learning threshold, then an anomaly is generated
4. Anomaly available on the Unusual file activity dashboard
    - Run Threat Scan analysis
    - Perform pre-anomalous recovery

Early Adopter

Suspicious file extensions

COMMVAULT

Early Adopter

AI/ML Suspicious file extensions

What:

- Suspicious extension detection is a backup anomaly feature that alerts the user when a suspicious extension is detected on a file system
- Originally Introduced in CPR 2022E

New Change:

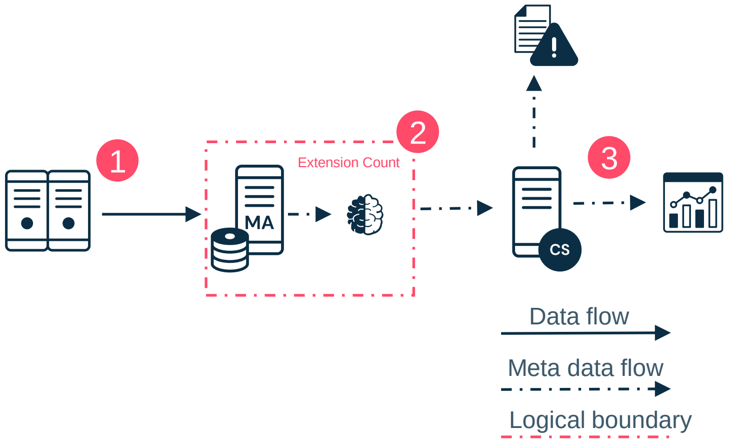
- **Early Adopter available for opt-in Feb 15th**
- Previous version used a **hardcoded list of extensions**. This caused a large number of false positives.
- New framework removes the hardcoded extension list and instead monitors for anomalous extension change rates.
- Monitors top 30 extensions – if top 5 extensions decrease In count send an alert. If any extension increases send an alert
- This requires at least 10 backup jobs for history to use with the machine learning algorithm
- Provides greater accuracy to when data changes are occurring and eliminates the false positives
- Uses Backup Index anomaly framework

AI/ML Suspicious file extensions

Architecture

High Level Architecture

1. After backup the index is analyzed. Extension count for top 30 extensions are collected
2. Extension count is processed by the AI/ML engine
3. Top 30 extensions are monitored
    1. If one of the top 5 extensions decrease In count send an alert.
    2. If any extension increases in count send an alert



Agentless file activity monitoring for Virtual Machines

COMMVAULT

Agentless file activity monitoring for Virtual Machines

BUSINESS CHALLENGE

Organizations are challenged with ensuring that their data is properly backed up and is recoverable.

Cyber threats and bad actors pose a risk to recovery, as they attempt to infect, and corrupt data before it is backed up.

Organizations need insights when their backups may be at risk, so they can respond, and recover clean data quickly.

OUR SOLUTION

Agentless file activity monitoring for Virtual Machines uses a Commvault® machine learning engine, to identify when there have been anomalous file activity changes occurring within VM backups, so organizations can easily respond, investigate, and recover clean versions of data.

CUSTOMER BENEFITS

Who

IT/Backup Admins

Why

- Provides data insight that Security teams can use to enrich threat intelligence
- Helps identify backups that may contain maliciously changed content
- Easily locate clean versions of virtual machine backups for recovery
- Providing agentless monitoring for Virtual Machines simplifies our solution and improves competitive aspects.

Agentless file activity monitoring for Virtual Machines

BEHAVIOR KEY BENEFITS

- Monitoring File Activity Anomalies within VM Guests is now supported without an in-guest agent
- Supports Windows and Linux VM’s
- Uses existing VM file level indexing framework
- Supports all Hyper-Visors that support File level indexing
- Provides pre-anomalous recovery of VM’s
  - Recovery of anomalous VM data is possible for Security Forensic purposes as well

How it works

BUILT ON TOP OF EXISTING VM FILE INDEXING

1. Enable File Indexing for VM or VM Group
2. Perform normal backups of VM’s or VM Group
3. Requires 10 Full and Incremental backups before anomalies can be detected
   - Synth fulls are excluded
4. File Indexing happens automatically after backup
5. File change activity information is collected as part of indexing operation
6. File activity information provided to the Anomaly engine on the indexing MA
7. Anomalous file change rates will send an alert, and the anomaly will show in the Unusual File Activity Dashboard
8. Recoveries will revert to a recovery point prior to the anomaly unless overridden

File anomalies are based on unusual:

- Files created
- Files modified
- Files renamed
- Files deleted

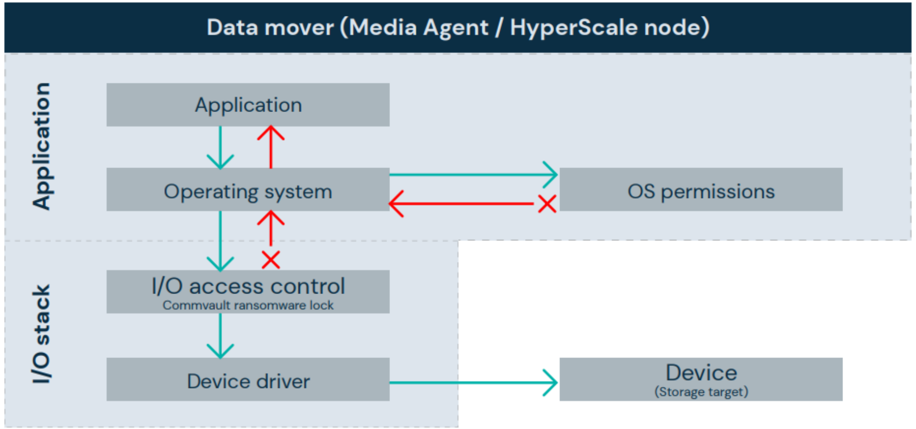
Protecting the Backupstorage

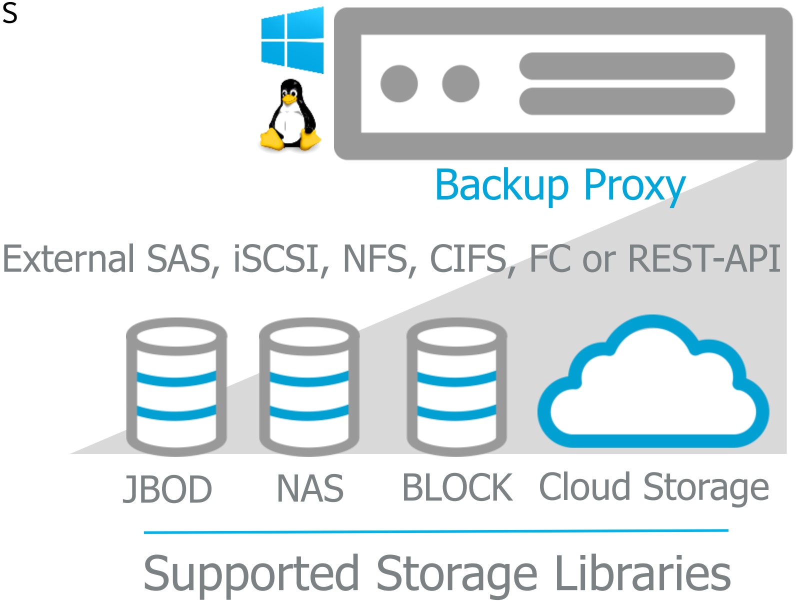
Backupspeicher schützen

Ransomware Protection auf Backup Proxy

Storage I/O Control

- Backupspeicher kann nur durch CommVault Prozess verändert werden!



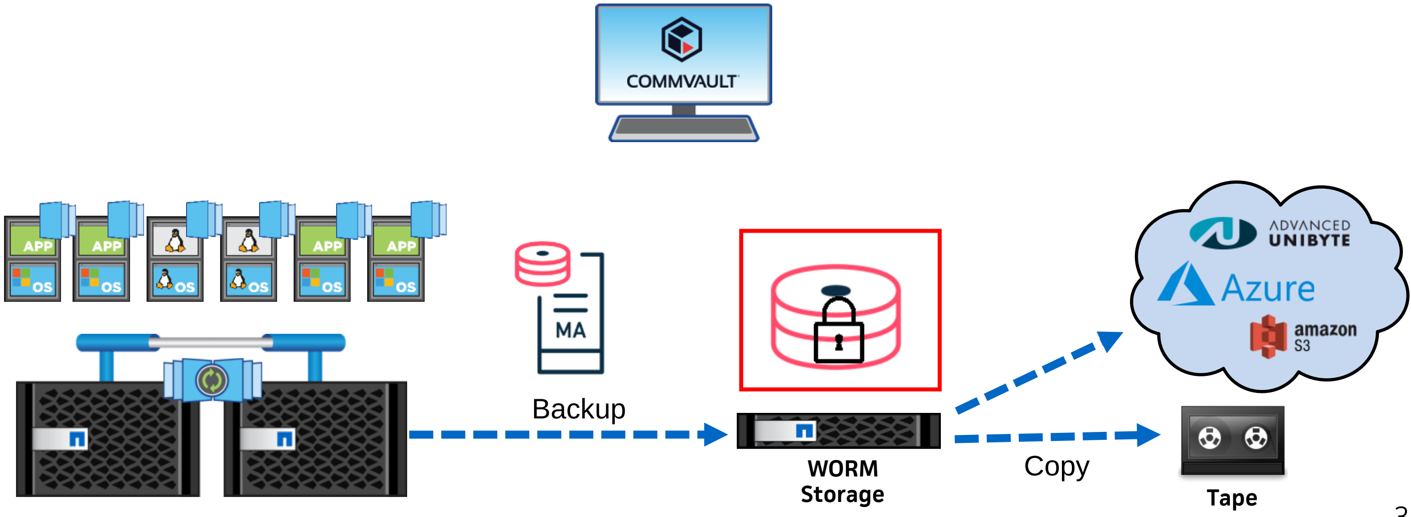

Backup Proxy
External SAS, iSCSI, NFS, CIFS, FC or REST-API
JBOD
NAS
BLOCK
Cloud Storage
Supported Storage Libraries

Backupspeicher schützen

Immutable Storage

WORM Storage Support

- WORM Storage wird als Backupspeicher supported
- Mehrere Hersteller werden unterstützt (zum Beispiel **NetApp Snaplock**)



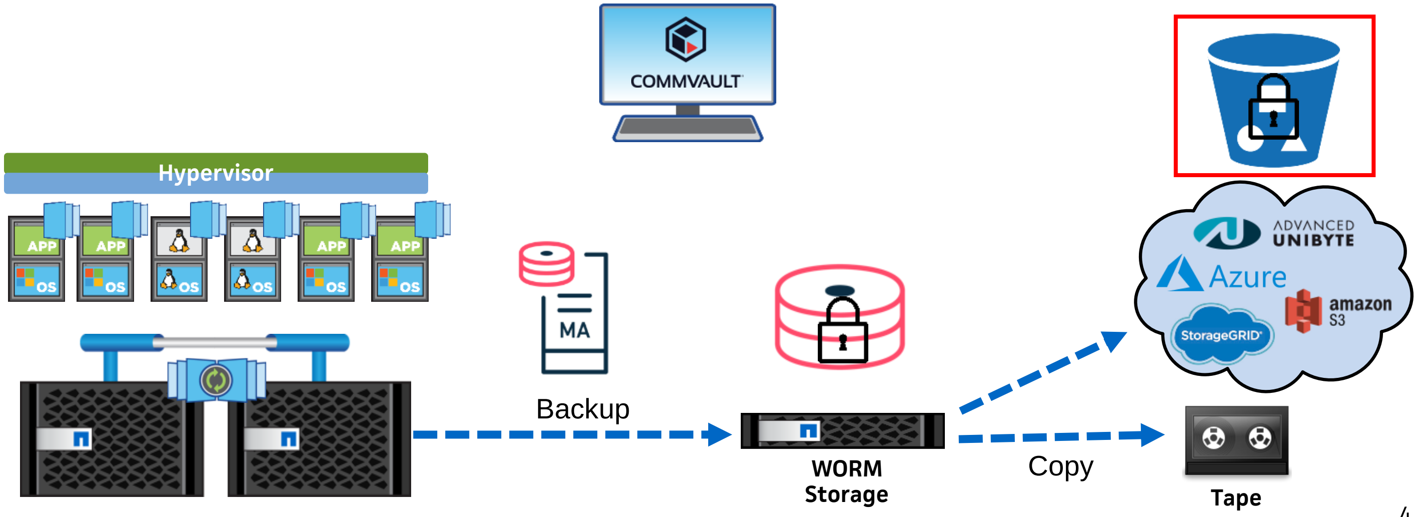
https://documentation.commvault.com/v11/expert/configuring_worm_storage_mode_on_disk_libraries.html

Backupspeicher schützen

Immutable Storage

Object Lock Support

- S3 Object Lock bietet einen WORM-Mode für Daten in S3
- Mehrere Hersteller werden unterstützt (zum Beispiel **NetApp StorageGRID**)



https://documentation.commvault.com/v11/expert/configuring_worm_storage_mode_on_cloud_storage.html

ThreatScan
Clean Recovery

Commvault Threat Scan

Business challenge

As threats remain dormant for days at a time, backups are continuous. Files may contain infection prior to backup, causing a false sense of safety and impact to recoveries.

- *Customers often recover older data sets to avoid malware reinfection using best guess insights*
- *Customers perform manual scanning operations to find malware threats on recovered data*
- *There are no analytic tools to help customers inspect their backups to instill trust that the content is safe*
- *There is no easy way to recover clean data up front without post processes*

Our solution

Commvault® threat scan addon package allows organizations to scan backup content for malware and encryption, so they can recover clean data and avoid reinfection.

How this helps

Who?

- IT/Backup Admins, SecOPS

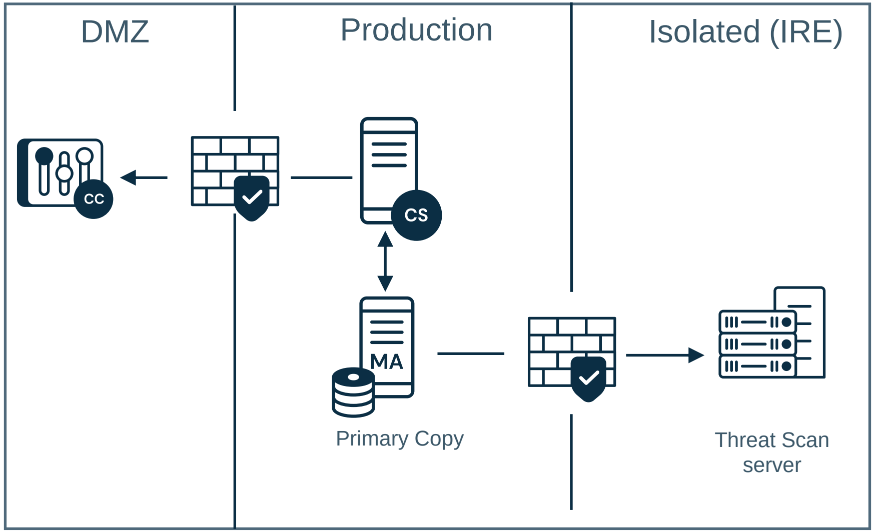
Why?

- Helps organizations **Identify** threats within their backups so they can make informed **Response** and **Recovery** actions
- Improves recovery scenarios by reducing post recovery processes and guess work
- Instills trust and confidence
- Provides insights that can help drive informative actions

Architecture

- Secure scanning operation
  - Files are removed as soon as they are processed by the Threat Scan engine

- Threat Scan isolation
  - Threat scan server and operations can be integrated within an Isolated Recovery Environment (IRE)
  - Use Commvault® network topologies to tunnel and isolate connectivity



Threat scan – How does it work

MALWARE SCANNING

1. Malware scanning occurs on predefined plan schedule for assigned servers/server subclients
2. Latest backup cycle is selected for scanning – **Threat Analysis** administrative job
3. Subsequent scans only scan incremental changes to backup cycle
   - Commvault® uses a built-in signature based antivirus engine
   - Antivirus Definitions are updated prior to scanning operations within 24-hour window
4. Files are restored out of place to cache on the Threat Scan server
5. Files are indexed, and scanned using the built-in AV engine
6. After files are scanned, they are removed from cache
7. If malware is detected, the file is flagged in the backup index
8. An alert is sent that threats were detected, and the infected files are visible on the Unusual file activity dashboard
9. Infected files are automatically quarantined from the backup content, and will be skipped during recovery

Threat Scan – How does it work

SCANNING FOR ENCRYPTED CONTENT

1. Select Analyze file data on triggered anomaly (unusual file activity dashboard)
2. Select timeframe to analyze
3. Browse operation is executed for the time frame selected
4. Data is recovered and staged to the Threat scan server
5. Files are indexed and processed, then removed from cache
6. When multiple versions of files are found, they are analyzed and compared using built-in entropy and hash algorithms
7. Single version of files found are checked for high entropy only
8. Analysis results become viewable on the Unusual File Activity dashboard
9. When marking files corrupted, the backup index is updated so that those files are skipped for recovery

Threat scan techniques

Avoid traps … FOCUS ON THE RECOVERY OUTCOME

File extraction

- Extract contents of files – **compare content or binary** information of the file

How its used:

- Extract contents of files to **analyze the file as a binary or application** type file

Value:

- Where **application files are now binary** type, they will be labeled **suspicious** so the user can mark corrupt

File Entropy

- Algorithm that **measures increased level of randomness** within a file. Increases in entropy indicates **corruption, encryption** or a file containing **hidden data.**

How its used:

- Entropy score **increases by 2** between multiple versions of backup files
- Entropy **score is 6 or higher** for single version of a file

Value:

- **Helps find encrypted, corrupted or files with hidden data**, so user can mark corrupt

SIM Hash

Hashing algorithm (Google) designed to find **similarities between versions of backup files**. Files are flagged **suspicious** for **significant change** if there are large amounts of variance.

How its used:

- Multiple versions of files are analyzed and if there is a **bit difference of more than 10 between v1 and v2 file** its flagged as **suspicious** for significant change

Value:

- Find files with **significant change** that could indicate **ransomware** infection, so the user can mark corrupt

Signature based

- Built-in **signature-based** malware engine to find and **quarantine malware** within the backup.

How its used:

- Recover and scan on schedule using built-in scanning engine to **find malware**
- Signatures **updated every 24 hours** automatically

Value:

- **Auto-quarentines** threats within backups

Recover **last known good versions** of data and **avoid re-infection** from dormant malware threats

COMMVAULT

Cleanroom Recovery

What is a cleanroom?

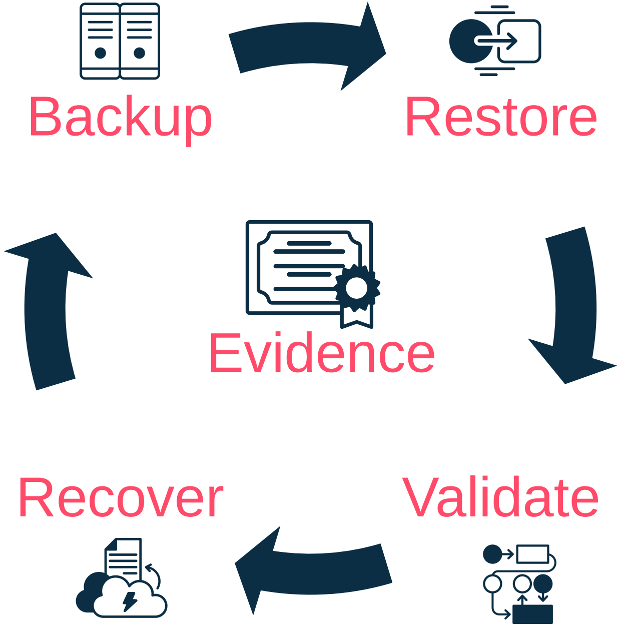
A clean room is a **Cyber Security term** used to describe an **isolated data center** (virtual or physical) utilized for **data recovery testing, validation, and security forensic operations**. Cleanrooms typically have **no network connectivity to other networks** including the internet to eliminate “contamination” leaving or entering the data center, to reduce any outside influence on the testing, as well as eliminate risk of infecting production.

Commvault Cloud’s Clean Room Solution Includes:

- Cleanroom control plane recovery (CommServe Infrastructure)
- Cleanroom Application Recovery (Auto Recovery)

CommServe Recovery Validation Service

Demonstrate and show evidence of Cyber Recovery



Backup

Restore

Evidence

Validate

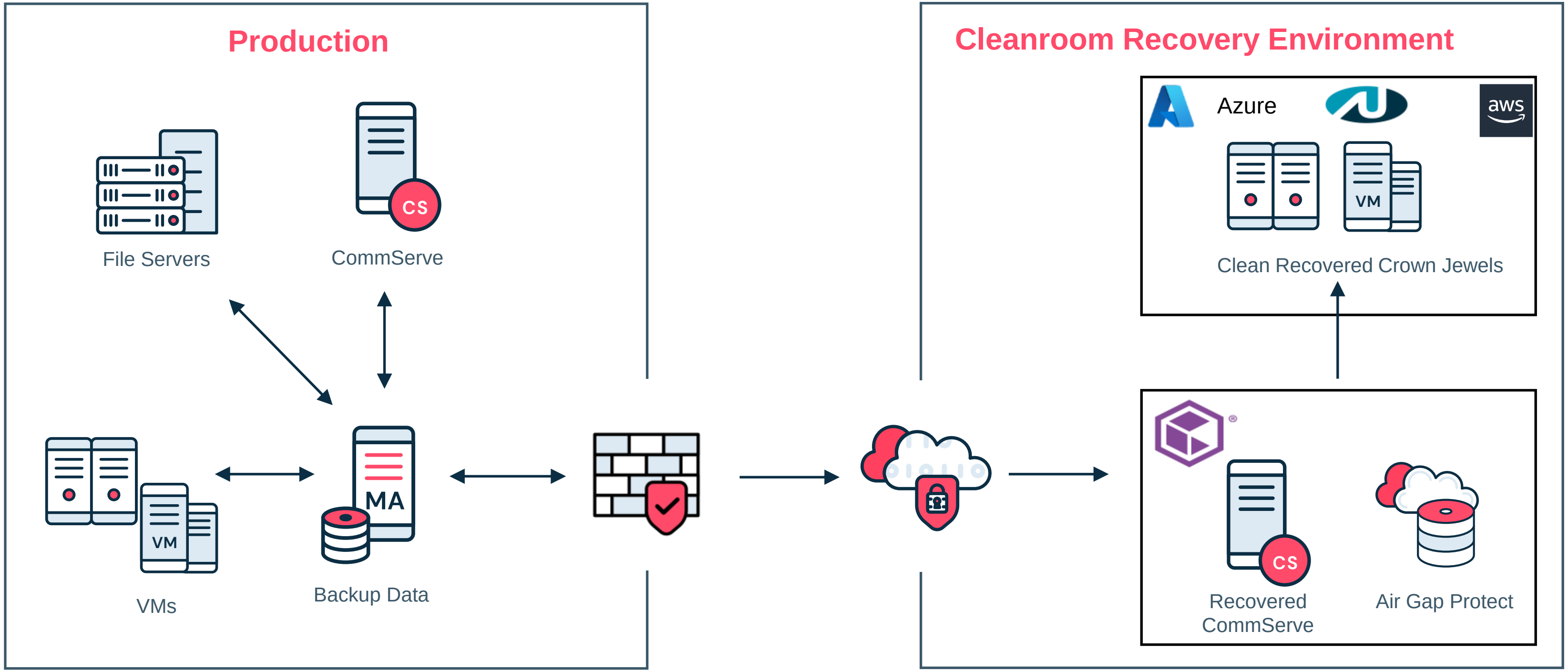
Recover

Recover NIST 800-184

NIST 800-184 publication emphasizes the importance of having a well-defined and tested cybersecurity event recovery plan in place to ensure that organizations can quickly and effectively recover from a cybersecurity incident.

1. Build and Execute a Backup plan
2. Build and Execute a Restore Plan
3. Validate data recovery
4. Prove you can recover in the event of a disaster
5. Provide evidence

Cleanroom Recovery Addresses Customer Concerns About Data Validation and Recovery Readiness



COMMVAULT

DR-Rollbox

Disaster Recovery – testen Sie den K-Fall

Einsatzszenarien

- Simulation des Katastrophenfalls in Ihrer IT
- Simulation eines Ransomware Angriffs
- Notfalleinsatz – bspw. nach einem Angriff

https://www.au.de/loesungen/backup/disaster-recovery-rollbox

DR-Rollbox

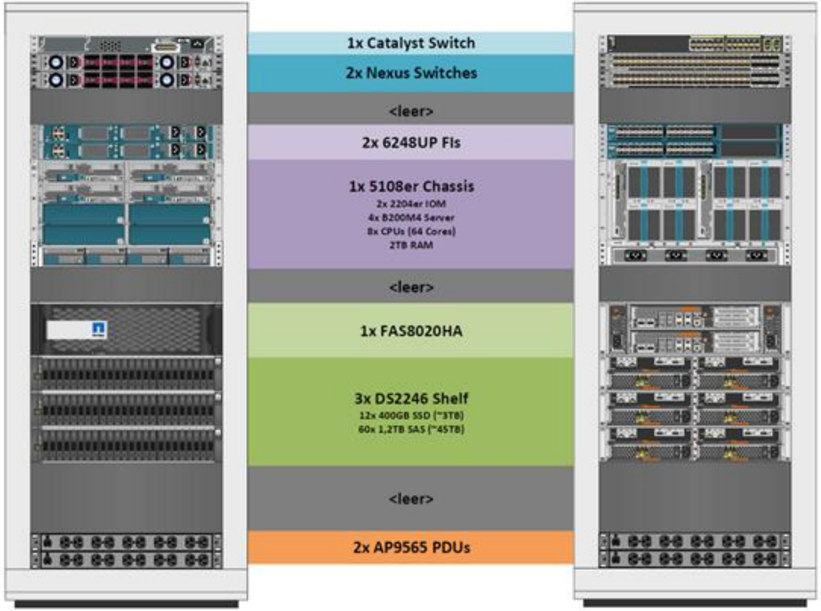
Disaster Recovery – testen Sie den K-Fall

Ihre Vorteile

- Mit der DR-Rollbox testen Sie live, wie gut ihr RZ auf den DR-Fall vorbereitet ist.

- Mit der **DR-Rollbox** testen Sie völlig stressfrei, ohne dabei ihre Produktivumgebung zu gefährden.

- Im Rahmen eines **Proof-of-Concept (POC)** stellen wir Ihnen unsere DR-Rollbox zur Verfügung.
  - Dauer POC = 6 Wochen
  - Preis POC = 1.800€



https://www.au.de/loesungen/backup/disaster-recovery-rollbox

CommVault Hardening Workshop

ADVANCED UNIBYTE

Der CommVault Hardening-Workshop enthält unter anderem:

Teil 1 – Vorstellung der Infrastruktur

- Aktuelle CommVault Umgebung und Version
- Aktuelles Backup-Konzept

Teil 2 – Präsentation

- Allgemeines – unabhängige Security Best Practices
- CommVault Hardening Optionen

Teil 3 – Kunde berichtet

- Aktuelle Probleme
- Verbessungswünsche

Teil 4 – Check und Besprechung der Umgebung

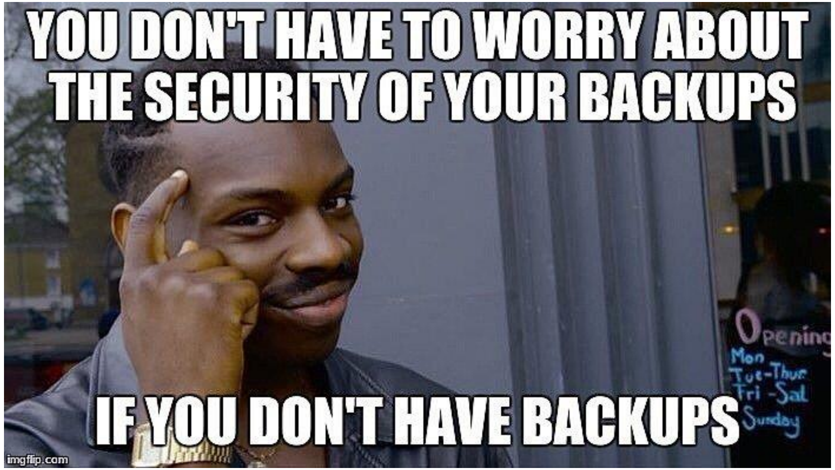
- Blick auf die Umgebung
- IST-Situation gegen die AU-Checkliste

Teil 5 – Outro

- Definition was wird umgesetzt/was nicht

Teil 6 – Dokumentation/Report der Findings

- Übergabe der Findings mit Handlungsempfehlungen an den Kunden


YOU DON'T HAVE TO WORRY ABOUT THE SECURITY OF YOUR BACKUPS
IF YOU DON'T HAVE BACKUPS
Opening
Mon
Tue-Thur
Fri-Sat
Sunday
imgflip.com

CommVault Hardening Workshop

Der CommVault Hardening-Workshop enthält unter anderem:

Teil 1 – Vorstellung der Infrastruktur

- Aktuelle CommVault Umgebung und Version
- Aktuelles Backup-Konzept

Teil 2 – Präsentation

- Allgem s – un gi urity B st Practices
- CommVa

Teil 3 – K

- Aktuell
- Verbessungs

Teil 4 – Check und Bes chun er Umge ung

- Blick auf die Umge ung
- IST-Situation gegen die AU-Checkliste

Teil 5 – Outro

- Definition was wird umgesetzt/was nicht

Teil 6 – Dokumentation/Report der Findings

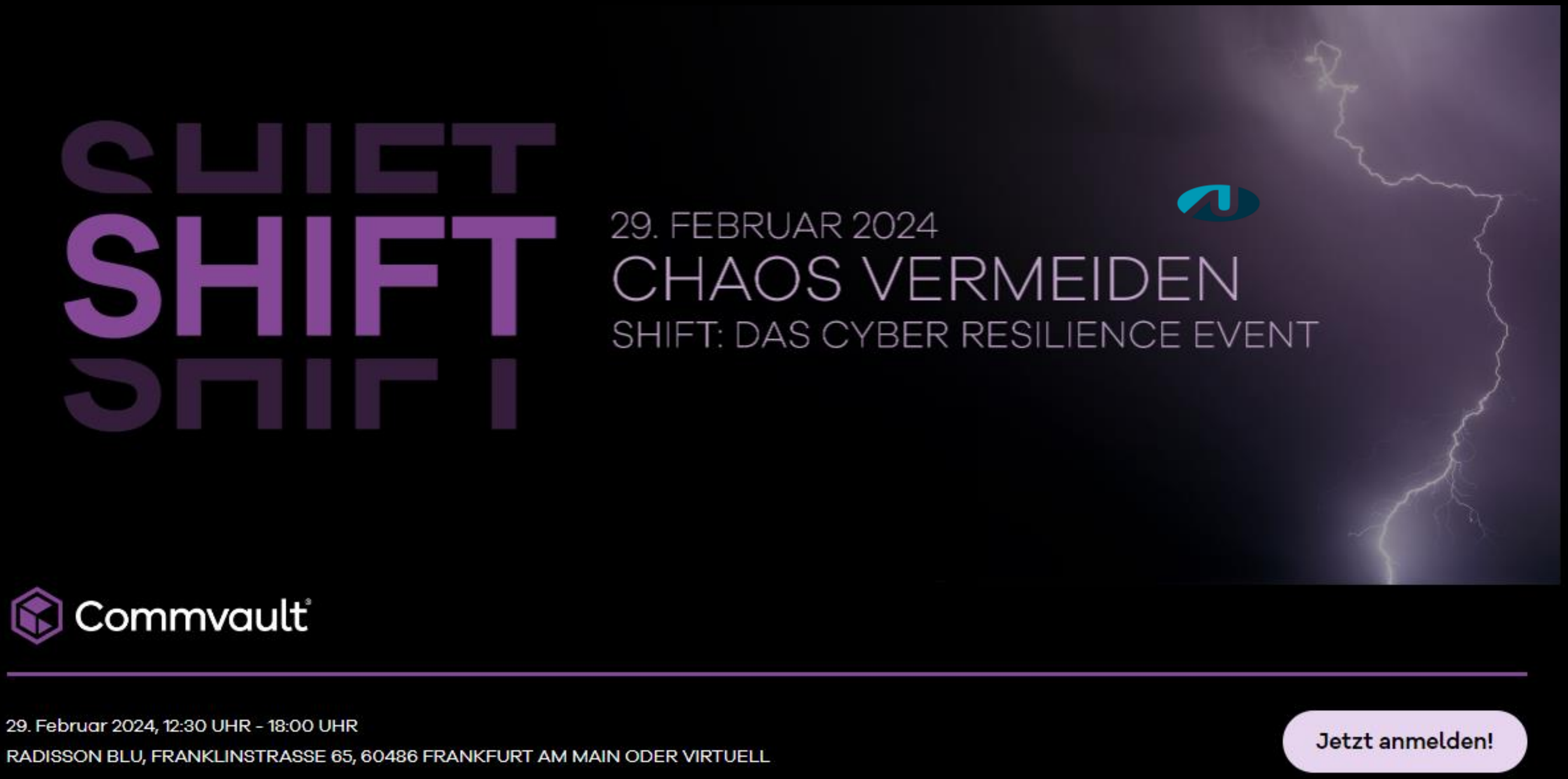
- Übergabe der Findings mit Handlungsempfehlungen an den Kunden

3.000 €/netto pro Workshop

https://discover.commvault.com/event-shift-roadshow-frankfurt_registration.html

Commvault Cloud

Powered by Metallic AI



SHIFT

29. FEBRUAR 2024

CHAOS VERMEIDEN

SHIFT: DAS CYBER RESILIENCE EVENT

Commvault

29. Februar 2024, 12:30 UHR - 18:00 UHR

RADISSON BLU, FRANKLINSTRASSE 65, 60486 FRANKFURT AM MAIN ODER VIRTUELL

Fragen