



| SCALITYDAY26



RATP

How RATP leverages ARTESCA for its Cyber Recovery with CommVault on a unique Tier



Jérémy Barrault
Product Owner
Infra DC
RATP



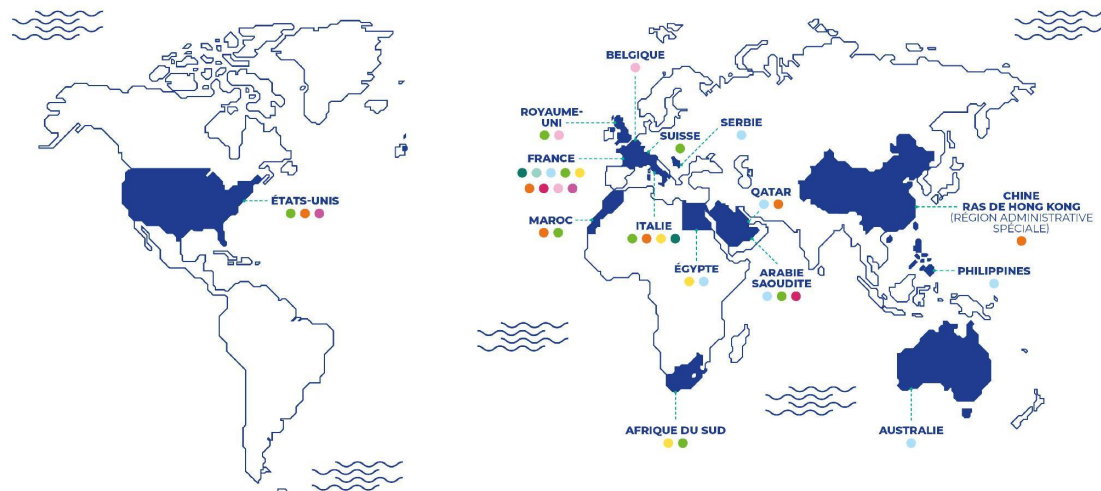
Alexandre Patti
System
Engineer
Commvault



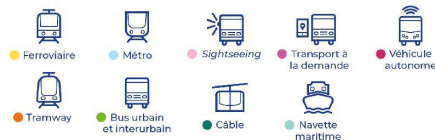
Jean-Marie Nana
Senior Sales
Engineer
Scality



La RATP en chiffres



9 MODES DE TRANSPORT



4 MODES OPÉRÉS EN PARTENARIAT



- 73500 collaborateurs
dont $\frac{1}{4}$ à
l'international (16
pays)

- Près de 4,5 milliards
de voyages opérés
dans le monde dont $\frac{1}{4}$
à l'international

- Plus de 270 métiers

- Leader mondial du
métré automatique

Un Groupe structuré autour d'entités expertes



LA FABRIQUE
DIGITALE



LA RATP



RATP
SERVICES
FERRÉS

RATP
SÛRETÉ

RATP
RÉSEAUX
DE SURFACE

RATP
INFRASTRUCTURES

SES FILIALES

MOBILITÉS

RATP dev

RATP cap
ÎLE-DE-FRANCE

SERVICES URBAINS

RATP
SOLUTIONS VILLE

RATP
CAPITAL
INNOVATION

RATP
CONNECT

RATP
REAL ESTATE

RATP
HABITAT

AUTRES EXPERTISES

RATP
SMART SYSTEMS

RATP
TRAVEL RETAIL

RATP
MAINTENANCE
IS

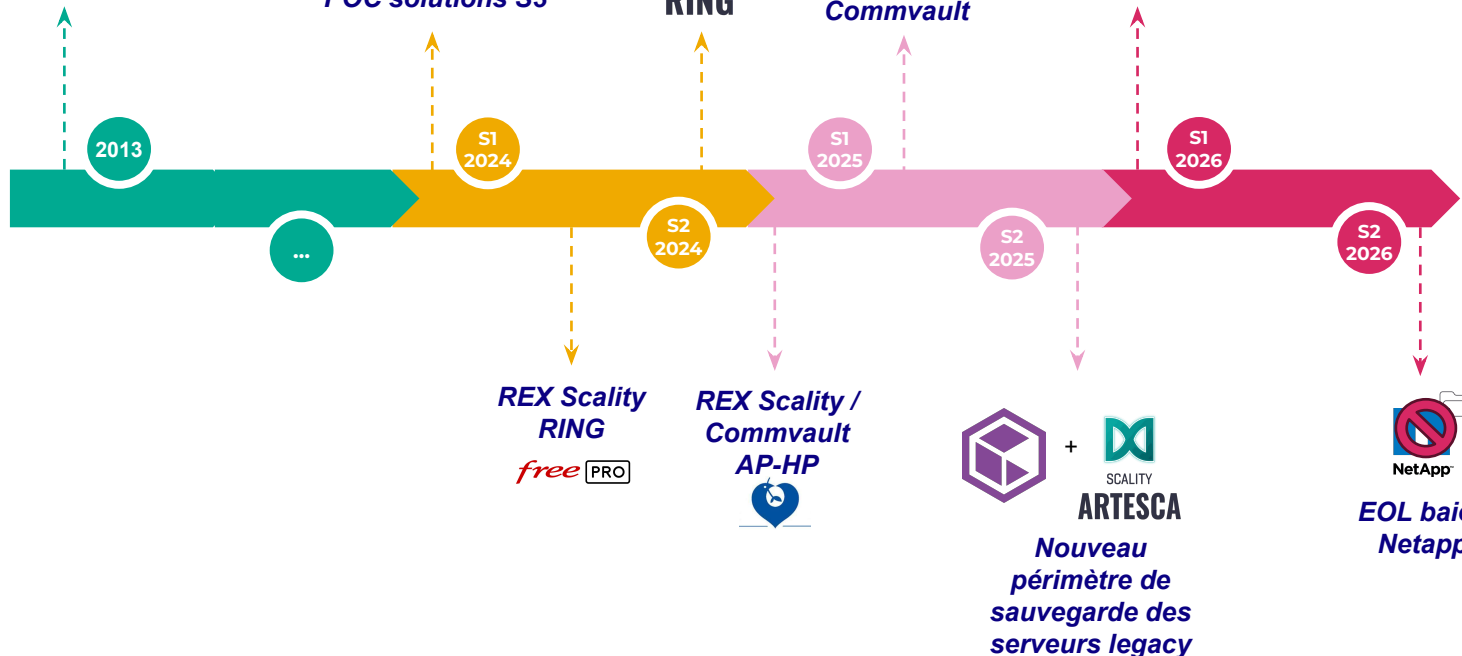
RATP
SÉCURITÉ
EXPERTISES

SA FONDATION

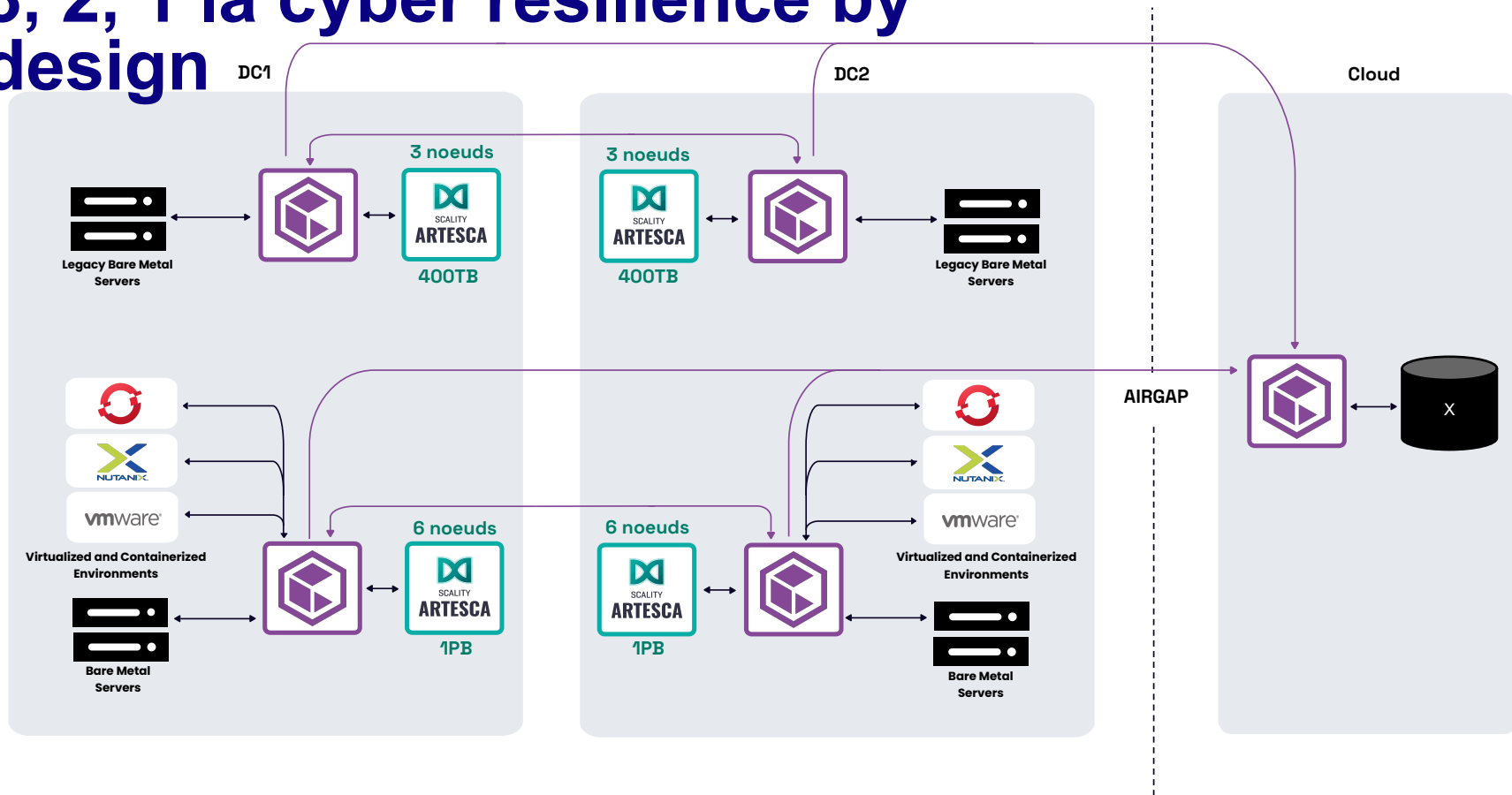
FONDATION
GROUPE
RATP

Toute une histoire ...

Nouveau socle de sauvegarde



3, 2, 1 la cyber résilience by design



Les apports de ARTESCA et la roadmap

Les gains

**Réduction des coûts
du prix au TB de 50%**

**Simplification de
l'exploitabilité** (micro
prunning/upgrade/distance au
mur)

**Cyber : Passage de
NFSv3 à Https**

La roadmap

**Upgrade
capacitaire**

**Etude de la mise en
place de Maestro**

**Etude de la
fonctionnalité de
sanctuarisation**



MERCI

!





SCALITY DAY · PARIS · OCTOBER 8, 2026

Detect. Validate. Recover clean.

Commvault cyber resilience
combined with Scality object storage

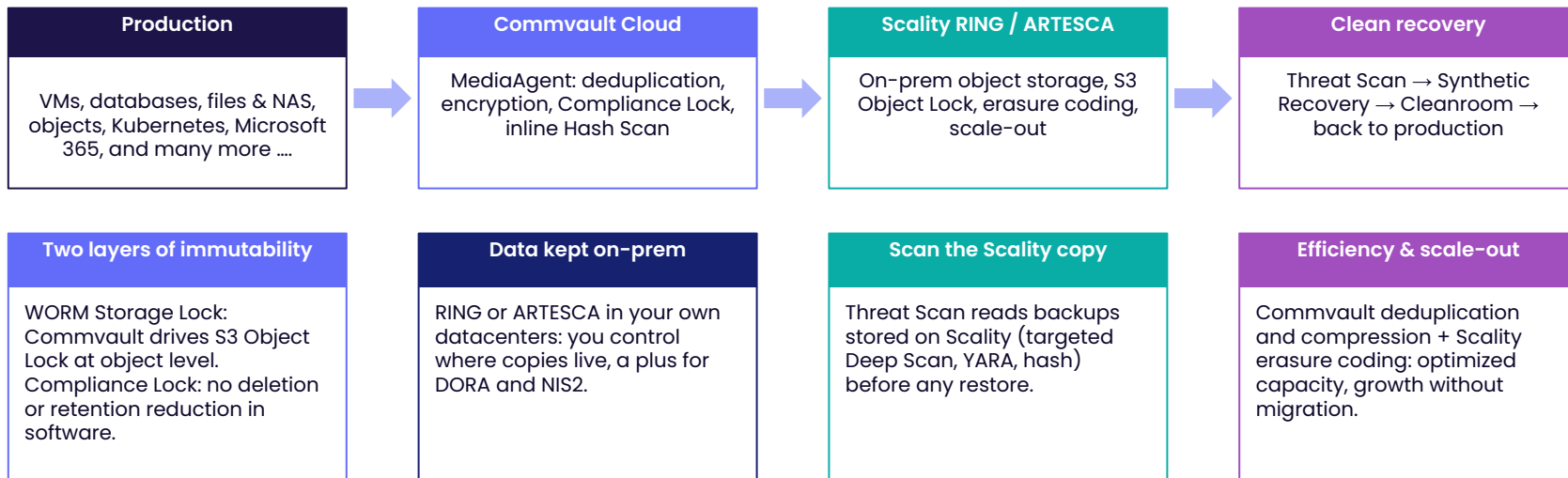
ALEXANDRE PATTI
Channel Sales Engineer
COMMVAULT



Commvault®

Scality: the immutable foundation for cyber recovery

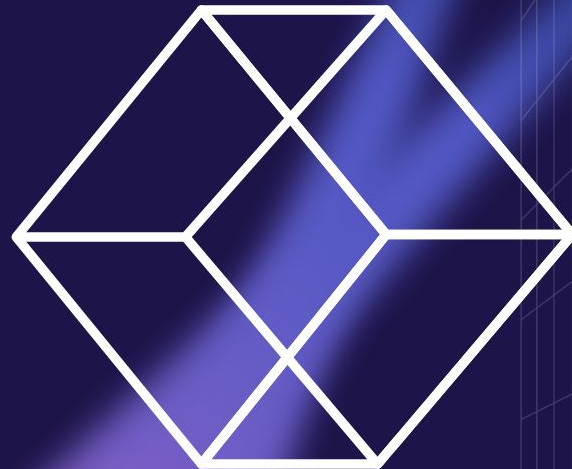
Commvault writes backups over S3 to Scality RING or ARTESCA: Scality makes the copy immutable, Commvault proves it is clean.



COMMVAULT × SCALITY

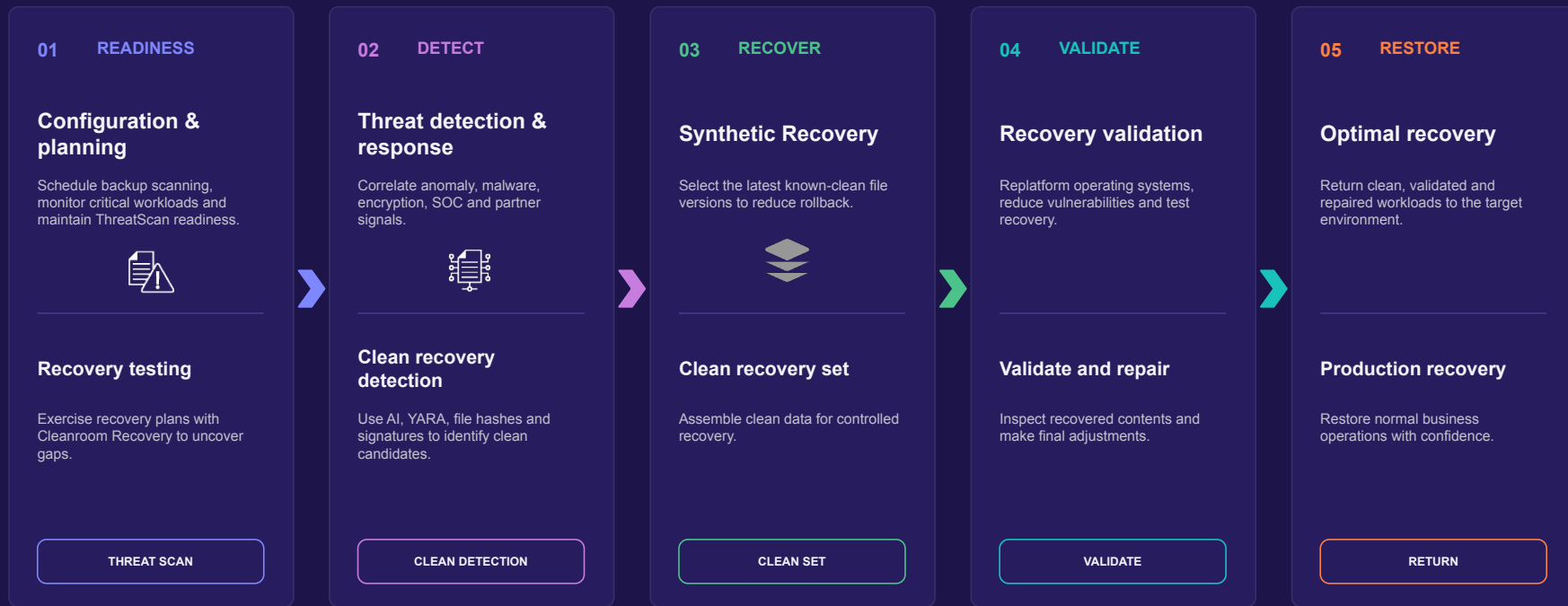
Threat Detection to Clean Recovery

From operational anomalies and AI-powered Threat Scan to targeted IOC hunting — Commvault helps you find risk fast and recover with confidence.



A Closed-Loop Cyber Recovery Process

Move from ongoing readiness through rapid clean-data detection, recovery validation and production restoration.



Prove the backup is actually clean

Layered scanning, forensic analysis, clean-point assembly, and isolated validation establish confidence before production recovery.

VALIDATION JOURNEY

Scan → Inspect → Assemble → Validate

Each recovery point moves through progressively stronger checks before data is promoted back into production.

1

SCAN

Find suspicious content

2

INSPECT

Flag abnormal behavior

3

ASSEMBLE

Build a clean point

4

VALIDATE

Prove recoverability

01



Threat Scan

ON EVERY RESTORE

Combines signature-based malware detection with AI/ML prediction, YARA, and hash-based threat hunting to identify known and emerging indicators of compromise in backup data.

02



Deep Inspection

FORENSIC FLAGGING

Uses machine learning, heuristics, encryption detection, entropy, and hash-change analysis to identify ransomware-like behavior and isolate suspect recovery data.

03



Synthetic Recovery

AI-ASSEMBLED CLEAN POINT

Builds a point-in-time recovery image from the latest known-good file versions across recovery points, minimizing rollback while excluding flagged items.

04



Cleanroom Validation

BEFORE PRODUCTION

Validates the assembled recovery point in an isolated cleanroom, boots the workload, confirms recoverability, exercises runbooks, and documents evidence before production promotion.



Finding Risk Before It Reaches Production

Four complementary Commvault 11.44 capabilities work together to flag, confirm, and hunt for threats hiding in backup data

THREAT VALIDATION JOURNEY

Detect → Confirm → Hunt → Validate

Signals progress from behavioral anomalies to malware findings, data-integrity analysis, and targeted indicator searches before a recovery point is trusted.

1

DETECT

Flag abnormal activity

2

CONFIRM

Identify malicious content

3

HUNT

Search IOCs and patterns

4

VALIDATE

Prove backup integrity

01



Anomaly Detection

BEHAVIORAL EARLY WARNING

- ✓ **File activity** Spikes in create, modify or delete.
- ✓ **Extension & MIME** Rare extensions, MIME mismatches.
- ✓ **Backup size** Unexpected jumps or drops in volume.
- ✓ **Canary files** Decoys flag ransomware activity.

02



Threat Detection

MULTI-SOURCE SIGNALS



- ✓ **Avira & MicroVision** Signature, fileless, mutable, and local ML scanning.
- ✓ **Google Threat Intelligence** Enriches findings with GTI and VirusTotal context.

03



ML Encryption & Corruption

DATA-INTEGRITY ANALYSIS

- ✓ **Encryption** Entropy analysis flags ransomware-encrypted files.
- ✓ **Corruption** Identifies damaged backup data before restore.
- ✓ **Faster** Analyzes one snapshot without historical comparisons.

04



YARA & Hash Search

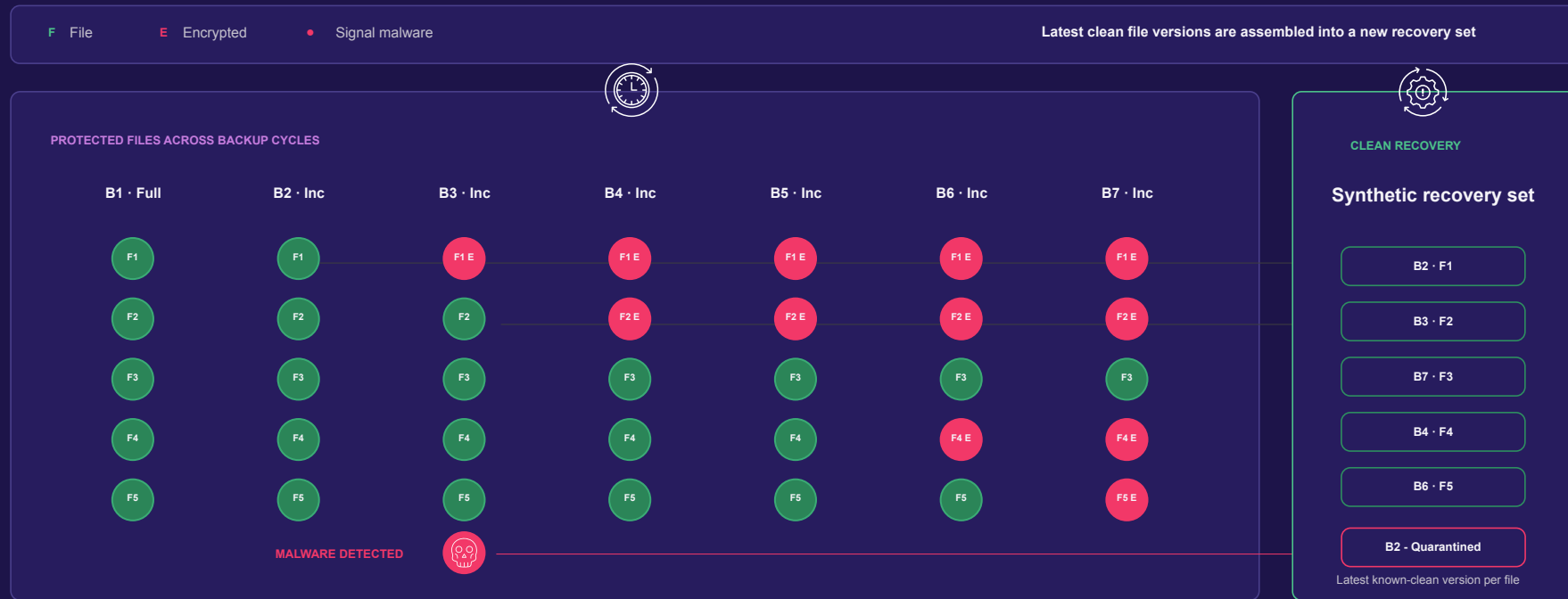
TARGETED THREAT HUNTING

- ✓ **Threat hunting** Searches for known indicators of compromise.
- ✓ **Hash & YARA rules** Combines fast hash lookup with custom patterns.
- ✓ **On-demand or scheduled** Runs after incidents or on a recurring cadence.



Patent-Pending “Synthetic Recovery”

Select the latest known-clean version of each file across backup cycles to minimize rollback during recovery.



QUICKLY AND EASILY FIND THREATS IN YOUR DATA

New Threat Hunting capabilities help you find threats within your data—and prevent them from being restored.

- Google Threat Intelligence Feeds – *Early Adopter*
- Custom YARA rules and threat hunting via hashes
- New workflows and scheduling to automate Threat Scan, including intelligent, automatic scanning of anomalies, and scheduled scans of specific workloads.
- New, simple recovery option directly into a Cleanroom



Risk-Based Threat Scanning

Speed where possible. Depth where needed



SCAN FAST

Hash Scan (Inline)

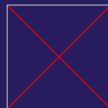
Compares backup file hashes with Google Threat Intelligence without restoring or analyzing file content (inline to backup).

BEST FOR

- Broad, frequent scanning across large backup datasets
- Rapid identification of known malicious files
- Trusted detection using continuously updated threat intelligence

LIMITATION

Known-hash coverage only; unknown or modified threats may require deeper analysis.



THOROUGH ANALYSIS

Deep Scan (Deep Inspection)

Rehydrates targeted backup files and analyzes content using signatures, YARA rules, and machine learning.

BEST FOR

- Higher-fidelity investigation of elevated-risk files
- Detection beyond known hashes and static indicators
- Analysis of polymorphic malware and encryption indicators

TRADE-OFF

More time and infrastructure are required to access, rehydrate, and analyze file content.

1

SCAN BROADLY

Use trusted hash intelligence for rapid coverage



2

PRIORITIZE RISK

Escalate when a threat or elevated risk is identified



3

ANALYZE DEEPLY

Apply content inspection only where warranted



ThreatScan – detection & remediation

The screenshot displays the Commvault ThreatScan interface. The left sidebar contains navigation options: Try new navigation, Filter navigation..., Service catalog, Dashboard, Companies, Protect, Discover, Data Insights, Security services, Cleanroom, Threat scan (selected), Auto recovery, Jobs, Reports, Metrics, Monitoring, Storage, Manage, Developer tools, Workflows, Download center, Store, and My apps.

The main content area is titled "FileServerSite1" and shows a list of threats. The "Threats (18)" table lists various files and their threat types. The "Threat intel" column provides additional details for each threat.

File name	Threat type	Backup time	Threat intel
amd64_duel_sobus.inf 31b0856ed364e35_13.0.143...	Encryption	May 06, 2026 05:27:16 PM	Encryption detection
amd64_duel_usb.inf 31b0856ed364e35_10.0.1433...	Encryption	May 06, 2026 05:27:16 PM	Encryption detection
amd64_microsoft-windows-mu-cd\hermanage-dll...	Encryption	May 06, 2026 05:27:16 PM	Encryption detection
amd64_microsoft-windows-profsvc_31b0856ed364...	Encryption	May 06, 2026 05:27:16 PM	Encryption detection
CvLT_DUMMY_FIL.F10.pdf	Malware	May 06, 2026 05:27:16 PM	Scanning engine
CvLT_DUMMY_FIL.F15.pptx	Malware	May 06, 2026 05:27:16 PM	Scanning engine
CvLT_DUMMY_FIL.F16.pptx	Malware	May 06, 2026 05:27:16 PM	Scanning engine
CvLT_DUMMY_FIL.F17.xlsx	Malware	May 06, 2026 05:27:16 PM	Scanning engine
CvLT_DUMMY_FIL.F2.pdf	Malware	May 06, 2026 05:27:16 PM	Scanning engine
CvLT_DUMMY_FIL.F22.pptx	Malware	May 06, 2026 05:27:16 PM	Scanning engine
CvLT_DUMMY_FIL.F25.pdf	Malware	May 06, 2026 05:27:16 PM	Scanning engine
CvLT_DUMMY_FIL.F26.pdf	Malware	May 06, 2026 05:27:16 PM	Scanning engine
CvLT_DUMMY_FIL.F5.pdf	Malware	May 06, 2026 05:27:16 PM	Scanning engine
CvLT_DUMMY_FIL.F7.pptx	Malware	May 06, 2026 05:27:16 PM	Scanning engine
data.dat	Encryption	May 06, 2026 05:27:16 PM	Encryption detection
elcarscripts.zip	Malware	May 06, 2026 05:27:16 PM	Yara Rule
elcar2.ps1	Malware	May 06, 2026 05:27:16 PM	Yara Rule
elcar2_elcar2.ps1	Malware	May 06, 2026 05:27:16 PM	Yara Rule

The "elcarscripts.zip" threat is highlighted, and its details are shown in the right sidebar. The details include the threat name, type, intel, path, and time. A summary section provides additional context about the threat.

elcarscripts.zip

Arise Insights

Threat Name: TRELLIX_ARC_Malw_Eicar
SHA256: 0d10f8e365c2e51ba633d031d8eac0b5f7f19c5cf2f1b6d0db6c0671a

Summary:
TRELLIX_ARC_Malw_Eicar is identified as malware using Yara Rule detection during a scan on May 6, 2026. The file detected was located at the path \\FileServerSite1\c:\ncascripts\elcarscripts.zip. This threat is associated with the well-known ELIUM test file, which is commonly used as a standardized test file for antivirus solutions and malware detection.

Details

Threat name: TRELLIX_ARC_Malw_Eicar
Threat type: Malware
Threat intel: Yara Rule
Threat path: \\FileServerSite1\ncascripts\elcarscripts.zip
Detected time: May 06, 2026 05:27:16 PM

SHA256: 0d10f8e365c2e51ba633d031d8eac0b5f7f19c5cf2f1b6d0db6c0671a

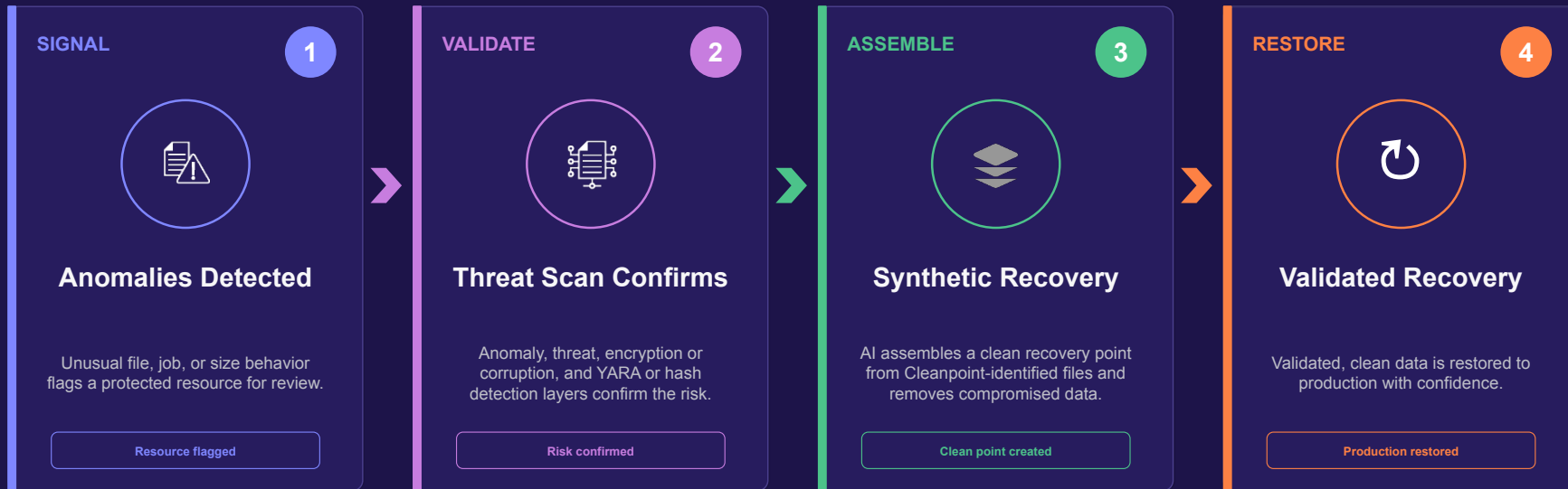
Impact
(Impacted jobs): 158/54

Cancel



In Summary ... from Protection to Detection to Clean Recovery

Commvault unifies threat detection and recovery into one automated, left-to-right workflow.



CONTINUOUS ASSURANCE

Each stage builds on the last, moving from anomaly identification to a validated production recovery.





THANK YOU

Questions & discussion

APATTI@COMMVault.COM

SCALITY
DAY26