



# Commvault Cloud

## В эпоху киберустойчивости

НОВАЯ СТРАТЕГИЯ И ВОЗМОЖНОСТИ

Дмитрий Иванюк

Март 2025

# Agenda

- Commvault Overview
- Cyber Recovery
- Active Directory
- Arlie AI
- Threat Scan



# Мир изменился



Ransomware везде — включая резервные копии

**99% of ransomware** tampers with security and backup infrastructure



Взломы становятся нормой

66% of organizations surveyed were breached in 2024<sup>1</sup>



Среднее время восстановления является катастрофическим

24 days is the average reported time to recover from a cyberattack

# Наши основные принципы.

**Одно решение.**

**Полная  
устойчивость**

Гибридные  
инфраструктуры  
нуждаются в едином,  
универсальном решении.  
Абсолютная устойчивость.

Во всем.

**Из коробки.**

**Никаких костылей**

Безопасность данных и  
кибервосстановление  
должны быть  
интегрированы. Единый  
механизм политики.  
Последовательный  
контроль.

**Искусственный  
интеллект**

Интеграция  
искусственного  
интеллекта должна  
быть привязанной ко  
всему, чтобы  
обеспечить  
автоматизацию,  
скорость, масштаб и  
надежность.

**Гибридная  
инфраструктура**

Гибридный мир требует  
настоящей облачной  
операционной модели с  
масштабом, гибкостью и  
эффективностью, подобными  
облаку.

# Фундаментальная защита

FP

Защищайте и восстанавливайте любые данные, где бы они ни находились

## Unified Management

Software – SaaS - Appliance

**Risk Analysis**  
Discover sensitive files &  
prevent exfiltration



**Auto Recovery**  
Analyze, validate, &  
orchestrate recoveries



**Security IQ**  
Alerting & security  
posture improvements



Commvault  
Cloud

Powered by Metallic AI

### Zero-Trust Architecture

Immutability – Air-Gapping – Credential Vault



### ThreatWise

Gain early warning of threats  
with cyber deception



### Threat Scan

Isolate malware, remediate  
risks, & prevent reinfection



### Backup & Recovery

Fast, flexible, &  
reliable response

## Security Integrations

Visibility, coordination, & countermeasures

# АВТОНОМНОЕ ВОССТАНОВЛЕНИЕ

AR

Защищайте и восстанавливайте любые данные, где бы они ни находились

## Unified Management

Software – SaaS - Appliance

**Risk Analysis**  
Discover sensitive files &  
prevent exfiltration



**Auto Recovery**  
Analyze, validate, &  
orchestrate recoveries



**Security IQ**  
Alerting & security  
posture improvements



### Zero-Trust Architecture

Immutability – Air-Gapping – Credential Vault



### ThreatWise

Gain early warning of threats  
with cyber deception



### Threat Scan

Isolate malware, remediate  
risks, & prevent reinfection



### Backup & Recovery

Fast, flexible, &  
reliable response

## Security Integrations

Visibility, coordination, & countermeasures

Обеспечение безопасности, защита и восстановление данных в любом месте при минимальной совокупной стоимости владения.

## Unified Management

Software – SaaS - Appliance



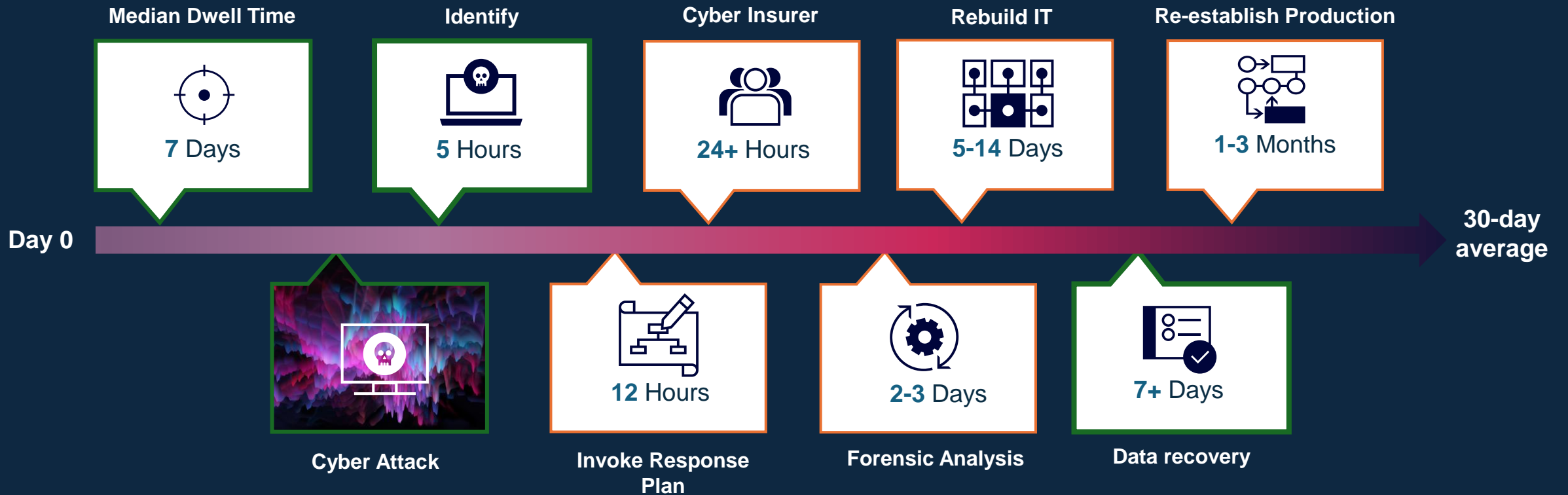
## Security Integrations

Visibility, coordination, & countermeasures

# Cyber Recovery



# Сроки восстановления после кибератак





# Zero Trust Access

MFA | Multi Person Auth | SAML | PAM | RBAC | KMIP | YubiKey | MS Auth | Google Auth

Palo Alto | MS Sentinel | Dark Trace | Netskope | CyberArk | Entrust | ServiceNow



## Risk Analysis



## Early Warning



## Indicators of Compromise



## Immutable Storage



## ThreatScan AI

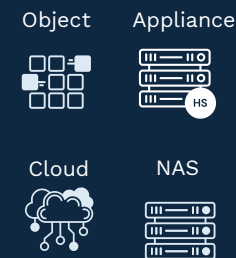


## Clean Recovery

- ✓ Identify Data Owners | Access | Permissions
- ✓ PII or other critical GDPR contents for leakage or exposure risks

- ✓ Canary Files
- ✓ Threat Sensors (SaaS)

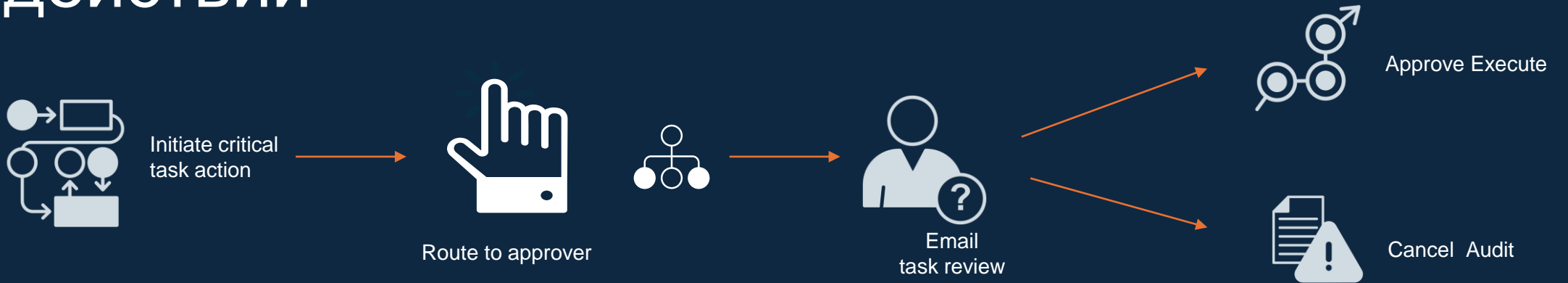
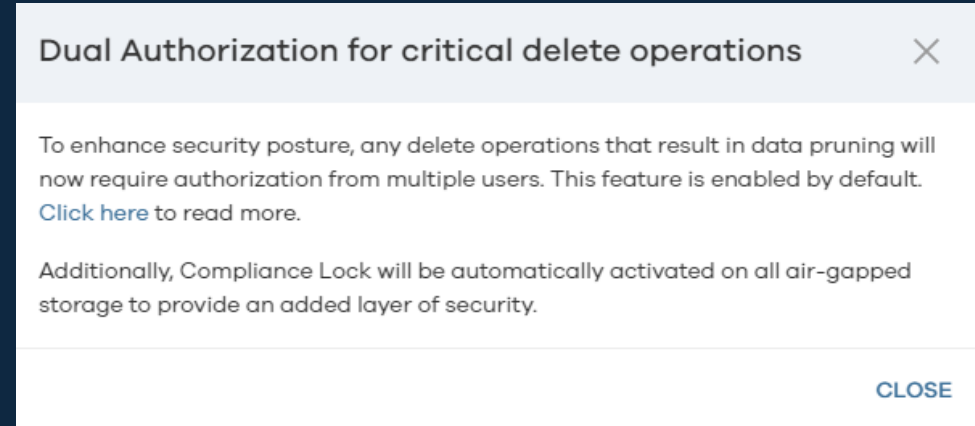
- ✓ File hashing
- ✓ Agentless VM CMDR
- ✓ Extension changes
- ✓ MIME Type Mismatch



- ✓ File Entropy | Corruption | Encryption Detection
- ✓ Quarantine suspicious files
- ✓ Pre-view Corrupt file versions SIM Hash
- ✓ Signature Based scan
- ✓ AI Zero Day Scan

- ✓ On-premise IRE
- ✓ Cloud IRE
- ✓ Forensics
- ✓ Validate Recovery Points

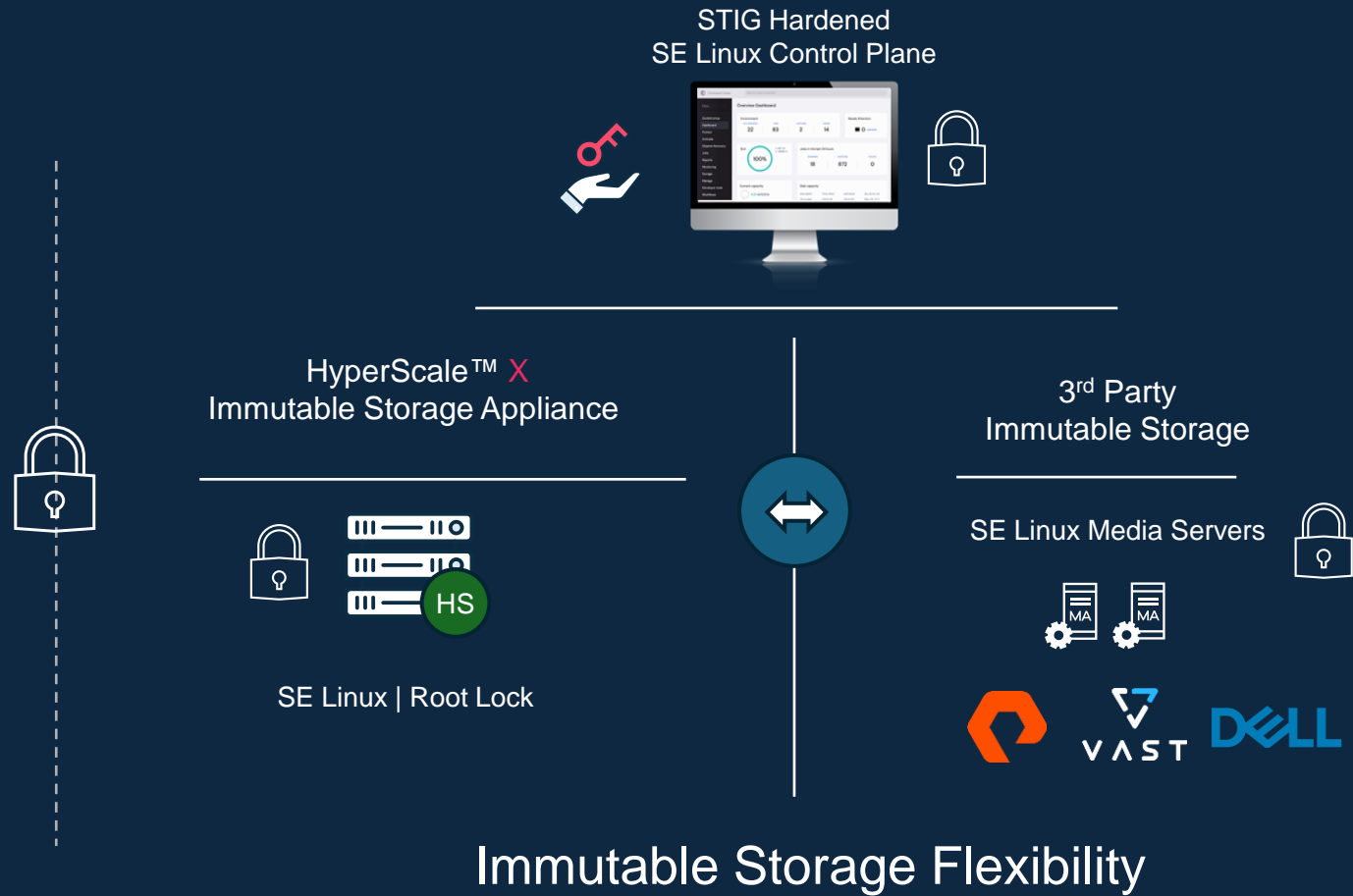
# Контроль нескольких авторизаций для предотвращения несанкционированных действий



“4 Eyes” - Authorized tasks with “Restricted” Control workflows

# Неизменяемое хранилище в любом месте

- ✓ STIG Hardened Control Plane
- ✓ Immutable File System
- ✓ MPA - Multi-person Authorization
- ✓ Compliance Lock WORM
- ✓ Ransomware Lock & Airgap
- ✓ 3<sup>rd</sup> Party Hardware WORM Locks



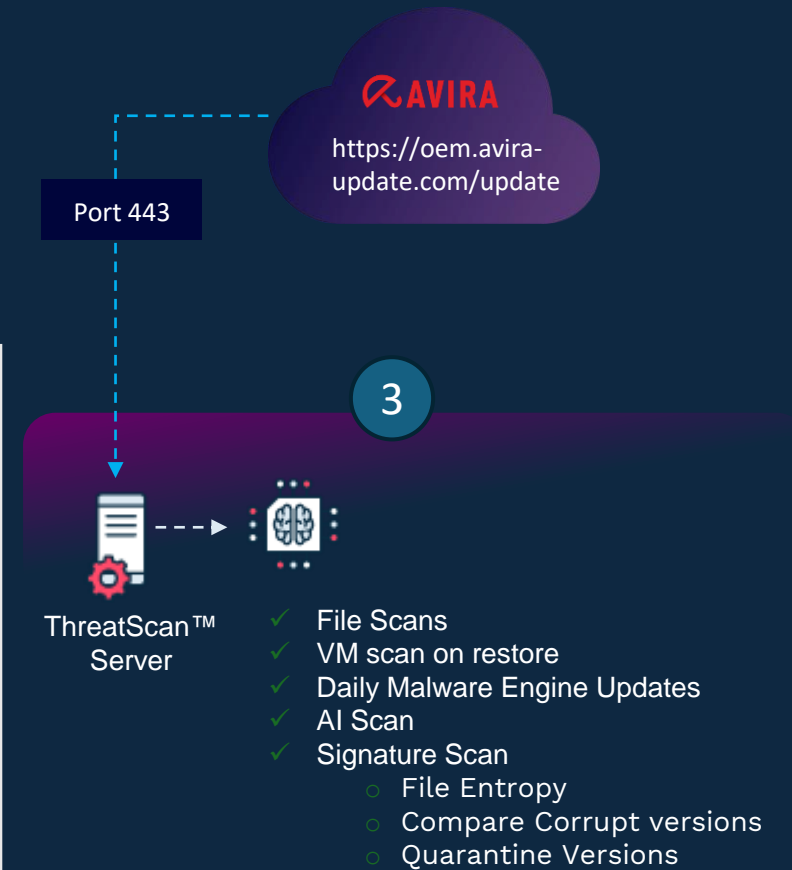
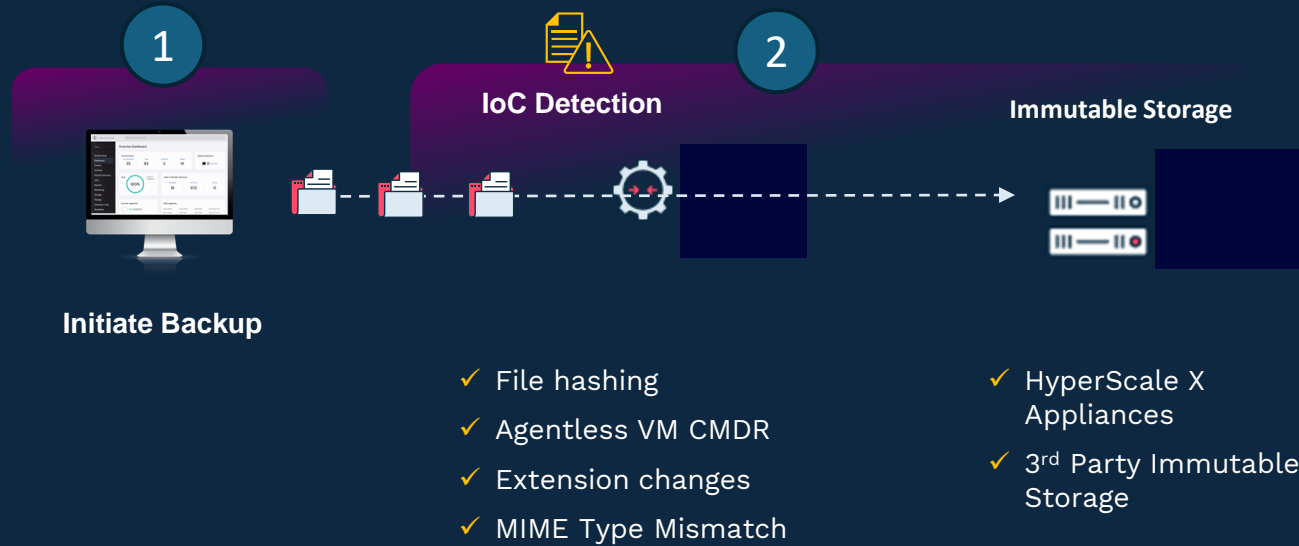
Immutable Storage Flexibility

- THREAT DETECTION

# Threat Detection

- ✓ Ai & Signature Malware Scanning

# ThreatScan™ for Files High-level Flow



# Suspicious File Activity Dashboard

**Threat Analysis**

File & VM AI Threat Scan

- ✓ File Entropy
- ✓ View Corrupt versions
- ✓ Quarantine Versions
- ✓ Signature Based Scan
- ✓ AI Zero Day Scan



# Automatic Threat Quarantine

Commvault SEARCH Search server, plans, jobs, storage... Select a company admin


Threat indicators / Threat analysis

hwtestta-r Clear anomaly Manage tags

Threat analysis

Threats

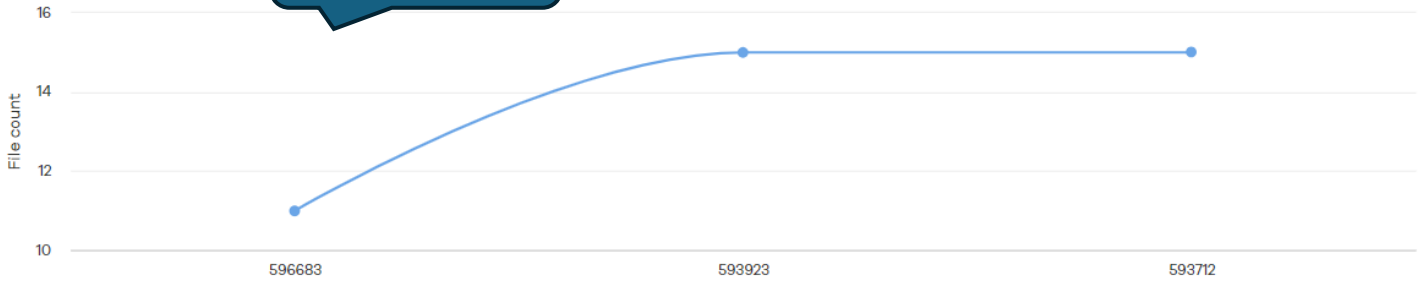
Threats Detected



- TR/AD.TestFile.Y ...
- BDS/Rustock.J.6...
- TR/ATRAPS.Gen ...
- TR/Offend.5478...
- TR/Rootkit.Gen ...
- TR/Rootkit.Gen2...
- TR/Spy.Gen : 1 (5...

Threats detected

Infected File Count



| Restore job id | File count |
|----------------|------------|
| 596683         | 11         |
| 593923         | 15         |
| 593712         | 15         |

File information

+ Add filter

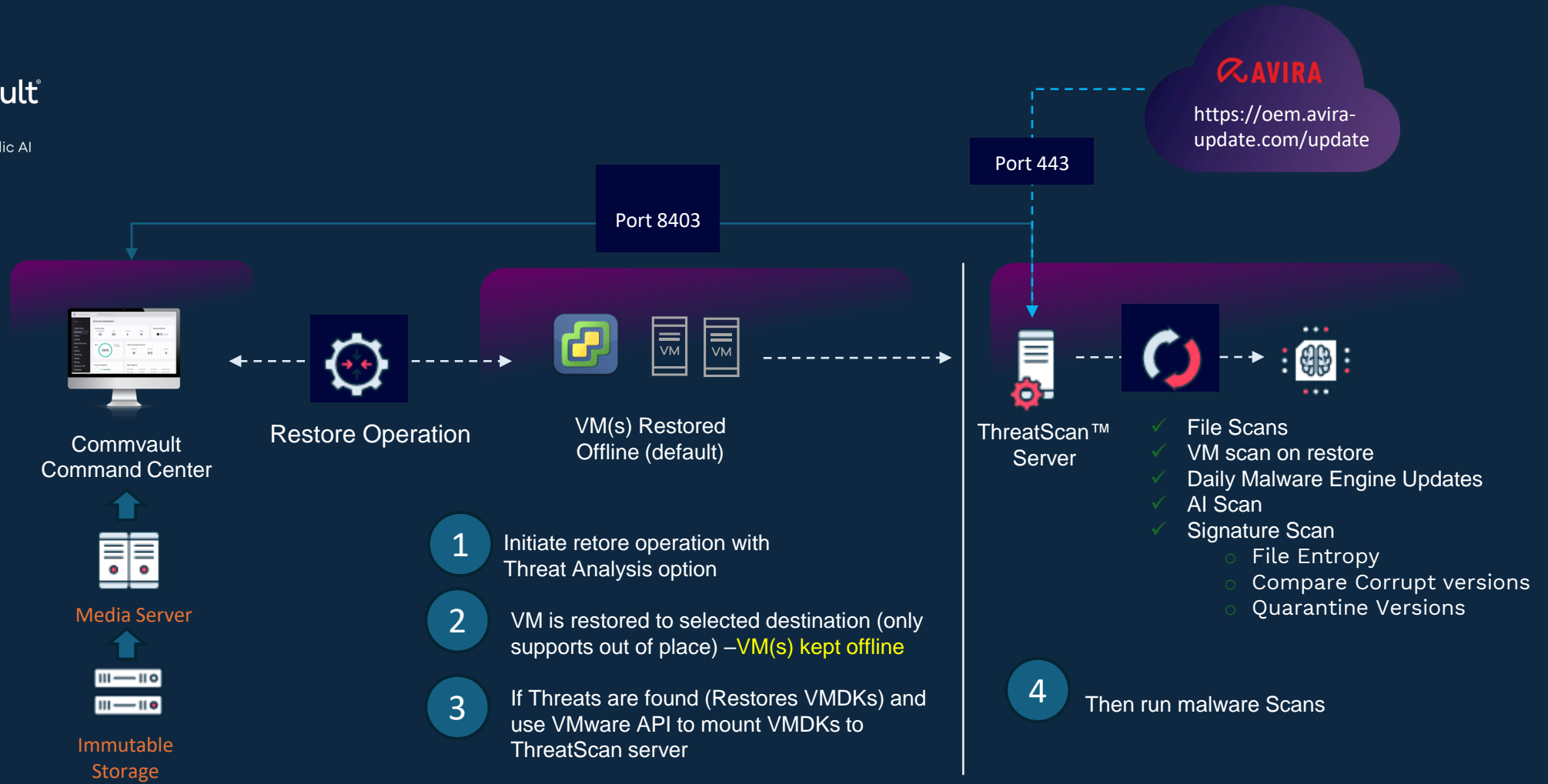
Drag a column header and drop it here to group by that column

| Path  | Threat name      | Restore job id |
|---|------------------|----------------|
| C:\TA\mvtest.risklevels (2)\test-risk-level-4.exx | TR/AD.TestFile.Y | 593712         |
| C:\TA\mvtest.risklevels (2)\test-risk-level-5.exx | TR/AD.TestFile.Y | 593712         |
| C:\TA\mvtest.risklevels (2)\test-risk-level-6.exx | TR/AD.TestFile.Y | 593712         |
| C:\TA\mvtest.risklevels (2)\test-risk-level-7.exx | TR/AD.TestFile.Y | 593712         |

Malware Signature



# ThreatScan™ for VMs High-level Flow



# Active Directory

# Active Directory под прицелом

НОВЫЙ ВЕКТОР ДЛЯ ОРГАНИЗАЦИИ АТАК



## Gain Control

Использование неверных конфигураций и «слепых зон» для компрометации привилегированной учетной записи



## Move Laterally

Бесшумное перемещение по инфраструктуре, рабочим станциям и приложениям



## Execute Attack

Распространение кибератак и контролировать доступ к сети клиентов

Establishing a foothold for cyberthreats

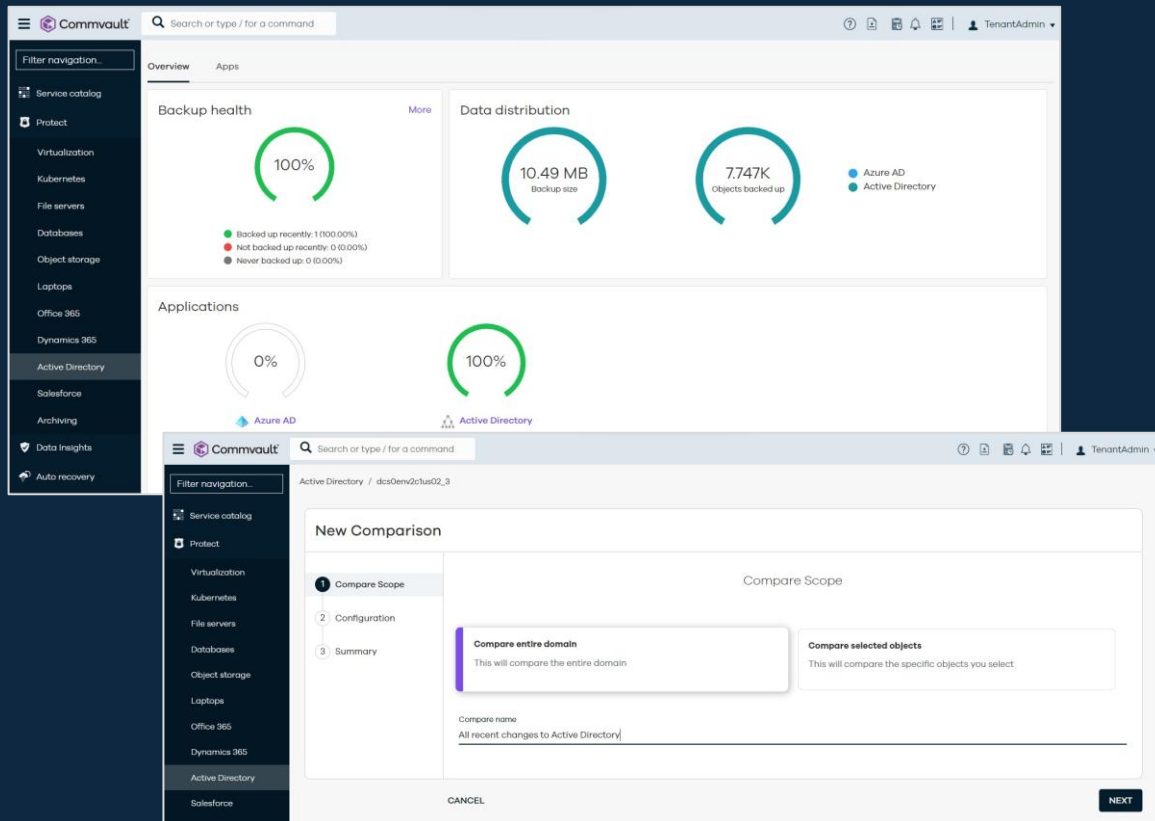
# Backup & Recovery for Active Directory

For Entra ID and Microsoft AD

MS Active Directory



MS Entra ID



Automated backups for single-solution protection of Microsoft AD and Entra ID



Comprehensive coverage of objects, attributes, users, groups, app registrations, and more



Granular recovery to roll back damaging, unwanted, or accidental changes



Layered security with data encryption and air-gapped ransomware protection

# Сравнение

|                  |   | Legacy Offering | New Offering |
|------------------|---|-----------------|--------------|
| ACTIVE DIRECTORY | Restore users, groups, contacts, computer objects                   | ●               | ●            |
|                  | Protect Group Policies  |                 | ●            |
|                  | Backup GPO settings from SYSVOL                                     |                 | ●            |
|                  | Compare before and after state for a single object                  | ●               | ●            |
|                  | Interactive, domain-wide comparisons of all objects and attributes  |                 | ●            |
|                  | Rollback overwritten attributes across thousands of objects at once |                 | ●            |
| Entra ID         | Restore users, groups, app registrations, enterprise applications   | ●               | ●            |
|                  | Recover roles   |                 | ●            |
|                  | Protect Conditional Access Policies                                 |                 | ●            |
| GENERAL          | One scheduled backup a day  | ●               |              |
|                  | On demand user-initiated backup                                     | ●               | ●            |
|                  | Frequently scheduled backups for a lower RPO                        |                 | ●            |

The background features a dark blue gradient with abstract, flowing lines in shades of purple and blue. There are also numerous small, out-of-focus light spots (bokeh) scattered across the scene, creating a sense of depth and movement.

Arlie

# “Arlie” AI Assistant

Для генерации ответов использует следующие данные :

1. **Active Insights:** Customer tickets, knowledge base articles, selected job status, and error description
2. **API Code Assist:** User question or query, Commvault API documentation in [api.commvault.com](https://api.commvault.com)
3. **Arlie Chatbot:** User question or query, Commvault product documentation, Commvault store description text

## Note

Arlie does not use your data to train the generative AI models. Furthermore, Arlie does not utilize your backed-up data for any purpose.

# Arlie – AI Assistant

- Side by side view of AI assistant and Command Center

The screenshot displays the Arlie AI Assistant interface. On the left is a navigation sidebar with icons and labels for: Guided setup, Dashboard, Protect, Data Insights, Auto recovery, Jobs, Reports, Monitoring, Storage, Manage, and Developer tools. The main area is split into two panes. The left pane shows the 'Active jobs' section with a summary: 'Active jobs 127 Running | 62 Pending | 211 Waiting | 7 Queued | 0 Suspended | 432 Total'. Below this is a table of jobs with columns for Job ID, Operation, Status, Destination, Agent, Subclass, Size, Start time, Elapsed time, Progress, Error, and Error code. The right pane is titled 'Arlie Backup a VM' and contains text explaining backup functionality and options.

**Active jobs** 127 Running | 62 Pending | 211 Waiting | 7 Queued | 0 Suspended | 432 Total

| All                      | Focused jobs | Laptop jobs | Pending Jobs |           |           |          |          |          |          |          |           |           |
|--------------------------|--------------|-------------|--------------|-----------|-----------|----------|----------|----------|----------|----------|-----------|-----------|
| + Add filter             |              |             |              |           |           |          |          |          |          |          |           |           |
| <input type="checkbox"/> | Job ID       | Oper...     | Status       | Desti...  | Agen...   | Subcl... | Size     | St... ↑  | Elaps... | Progr... | Error ... | Error ... |
| <input type="checkbox"/> | 32041...     | Back...     | Queu...      | degg...   | Wind...   | com...   | 0.00 B   | May 1... | 2 min... | 0%       | Edge ...  | 19:2126   |
| <input type="checkbox"/> | 3367...      | Archi...    | Runni...     | Exch...   | Exch...   | User...  | 769.3... | Oct 1... | 18 da... | 68%      | Infras... | 19:2599   |
| <input type="checkbox"/> | 33762...     | Back...     | Pendi...     | airfor... | Wind...   | defa...  | 0.00 B   | Oct 2... | 0 sec... | 0%       | Unab...   | 19:1131   |
| <input type="checkbox"/> | 3376...      | Back...     | Pendi...     | up10...   | Linux...  | defa...  | 0.00 B   | Oct 2... | 0 sec... | 0%       | Unab...   | 19:1131   |
| <input type="checkbox"/> | 3376...      | Back...     | Pendi...     | ibmai...  | AIX Fi... | defa...  | 0.00 B   | Oct 2... | 0 sec... | 0%       | Unab...   | 19:1131   |
| <input type="checkbox"/> | 3376...      | Back...     | Pendi...     | CVIT-...  | Wind...   | defa...  | 0.00 B   | Oct 2... | 0 sec... | 5%       | Unab...   | 19:1131   |
| <input type="checkbox"/> | 33770        | Back        | Pendi        | TranX     | Wind      | defa     | 0.00 B   | Oct 2    | 0 sec    | 0%       | File      | 19:1313   |

### Arlie

#### Backup a VM

You can perform backups automatically based on the configuration for a hypervisor or VM group, or manually for a VM group or a specific VM. The first backup of a VM is always a full backup. By default, all subsequent backups are incremental, capturing any changes to VM data since the last backup.

You can recover virtual machine data, even when the most recent backup was incremental.

Backups run based on the following options:

- **Initial full backup:** When you use Guided setup to set up the Virtualization solution, use the Back up now option to perform a backup for the default VM group.
- **Scheduled incremental**



# Thank You