DATA SHEET

Threat Scan – Essentials

Understand sensitive data. Reveal exposure. Act with confidence.

HIGHLIGHTS

- **Requirements Review:** Validate objectives, selected workloads, infrastructure readiness, licensing, connectivity, access requirements, and deployment prerequisites before implementation.
- **Threat Scan Installation & Configuration:** Install and configure the applicable Threat Scan components for supported file and virtual machine backup data.
- **Guided Validation Testing:** Execute an agreed test plan to validate the initial configuration and demonstrate Threat Scan functionality using selected backup data.
- **Knowledge Transfer:** Provide operational guidance and review the implemented configuration, test results, and recommended next steps with Customer administrators.

OFFERING SUMMARY

Accelerate the onboarding of Commvault Threat Scan with guided implementation and knowledge transfer from Commvault specialists. This focused service helps establish a validated starter configuration aligned with your selected use case, environment, and operational objectives.

- **Expert-assisted implementation:** Work with Commvault specialists to review prerequisites and configure Threat Scan for file system and virtual machine backup use cases.
- **Structured validation:** Test the starter configuration against agreed scenarios and review the observed results with your team.
- **Practical knowledge transfer:** Build familiarity with the implemented configuration, operating considerations, and customer-owned next steps.

CUSTOMER OUTCOMES

The service provides a defined and supportable starting point for adopting Threat Scan while helping your team develop the knowledge needed to operate and extend the implementation.

- **Improved implementation readiness:** Confirm key prerequisites, dependencies, responsibilities, access, connectivity, and licensing requirements before configuration begins.
- **Validated starter use case:** Establish and test an agreed Threat Scan configuration for selected file or virtual machine backup content.
- **Stronger operational ownership:** Equip your team with an understanding of what was configured, how it was tested, and which follow-up activities remain customer-owned.

KEY COMPONENTS AND BENEFITS

The engagement combines planning, guided configuration, validation, and knowledge transfer within a focused onboarding scope.

- **Discovery and readiness review:** Align on objectives, selected workloads, prerequisites, roles, access requirements, and acceptance criteria.
- **Guided configuration and testing:** Configure the applicable Threat Scan components for the agreed starter use case, execute defined test scenarios, and review observed results.
- **Knowledge transfer and handover:** Walk through the implemented configuration, key operating considerations, documented outcomes, and recommended next steps with the customer team.

WHAT IS ACTIVE RESILIENCE?

Active Resilience is the ability to confidently answer two critical questions at any moment of disruption:

- Are you protected?
- Can you recover?

Commvault Services helps you answer **YES** to both - not just at go live, but continuously over time. This confidence is built through delivery that transfers capability, not dependency.

Through structured knowledge transfer, clear and reusable document deliverables, and witness testing that proves recovery outcomes, your teams gain the skills, evidence, and operational readiness required to recover with confidence. Protection enables resilience, but **recovery is the outcome** - and Active Resilience enables you to achieve it when it matters most.

Learn more, visit **commvault.com/services**

© 2026 Commvault. See here for information about our trademarks and patents. 11_26