Commvault®

SOLUTION BRIEF

Know your data to better protect it from ransomware.

Stay cyber resilient: Understand your data
to minimize risk

When it comes to data security and management, what you don't know can hurt you and your business. Most likely, some of your critical and sensitive data still lives in the data center – the rest is spread across hybrid, multi-cloud, endpoint, SaaS, remote, and distributed environments. And with many employees working at home and in the office, your critical and sensitive data is further dispersed. This high-risk game of data hide-and-seek expands your attack surface, elevating your risk of ransomware attacks, data breaches, and data exfiltration.

$4.5M the average cost of a data breach[1]

To properly secure, defend, and recover your dispersed data from these threats, you need to answer this not-so-simple question: Do you know where all your critical data resides?

IDENTIFY, SECURE, AND PROTECT YOUR SENSITIVE AND CRITICAL DATA

A unified management platform that provides complete visibility and control across your diverse data locations is essential to any data protection or cybersecurity strategy. You need to know what data is where, who has access to it, and if it resides in a location you can protect. Commvault® Cloud, powered by Metallic® AI, provides a cyber-resilient platform with a single way to see AND govern your cyber resilience – even for sophisticated hybrid enterprises with data sprawling across clouds, regions, applications, and data centers. We scan your data (both backups and live data) to locate sensitive data, take action, and remediate. Is personally identifiable information (PII) in the wrong place?

Furthermore, AI-driven analytical insights are critical for incident assessment and response. For example, knowing which data sets have been affected by a ransomware incident helps you prioritize recovery and determine the potential scope of exfiltration by allowing you to audit impacted assets quickly. Do the criminals have anything of value, or are they bluffing to extort payment? With the right analytics in place, you'll know.
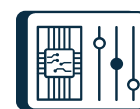
Define what is sensitive data.

Identify and remediate sensitive data from live and backup data sources.

Formalize access and deletion request processes (right to access/right to be forgotten).

Collaborate, review, and approve remediation actions and requests.

RISK ANALYSIS – LOWER RANSOMWARE RISKS

Commvault® Cloud Risk Analysis helps ensure that sensitive data is secure, constantly monitored, and thoroughly understood – helping to limit data exposure, reduce exfiltration risks, and ensure backups are safe and usable when facing cyber incidents. Plus, because it streamlines backups by identifying redundant, obsolete, and trivial (ROT) data for removal from production systems, Commvault Risk Analysis enables faster recoveries.

Adding Risk Analysis to Autonomous Recovery gives you simple, scalable, comprehensive backup, replication, and disaster recovery orchestration for all modern workloads.

- Safeguard and manage sensitive data (and its permissions) to help ensure compliance.

- Respond to security events faster – before data encryption, leakage, or exfiltration.

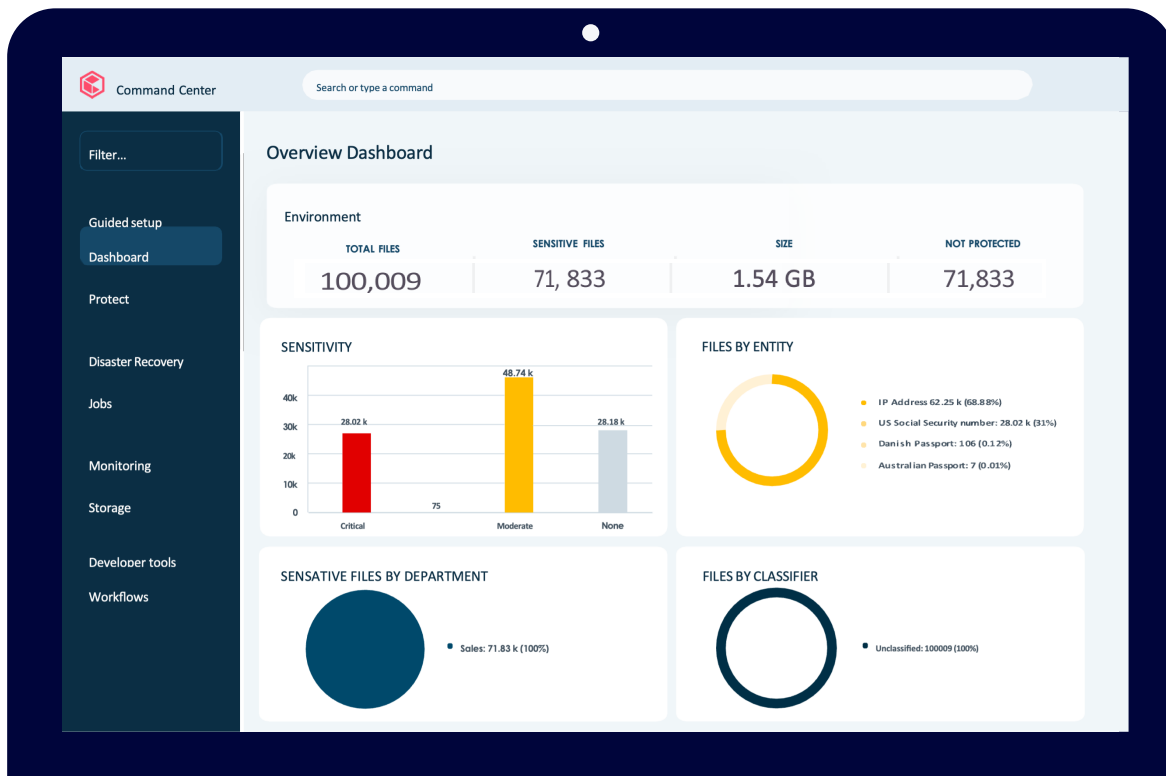- Identify and remove ROT data to reduce costs and accelerate recovery time.

Figure 1 (Image for illustrative purposes) – Commvault Command Center™ is a single dashboard to protect and manage all your data – regardless of where it resides.

THREAT SCAN – KEEP BACKUP DATA CLEAN

Malware and other threats could lurk in backup copies without proper visibility. Identifying infected backup content can be manual and time-consuming, introducing user oversight and increasing recovery times and reinfection risks. Know that your backup data is clean and recoverable with Commvault® Cloud Threat Scan.

Defend your backup data by proactively identifying malware threats to help avoid reinfection during recovery. Threat Scan analyzes backup data to find and remove encrypted and corrupted files, ensuring that you quickly recover trusted versions of your data.

- Scan backup content for malware and nefarious changes

- Automatically quarantine and isolate infected datasets

- Rapidly restore data to clean states without reinfection risk

Enhance your backup data protection platform by adding Autonomous recovery with Commvault Cloud Threat Scan to ensure easy, scalable, and comprehensive backup, replication, and disaster recovery orchestration for all your data, no matter where it is located.

THREATWISE™ – DETECT THREATS BEFORE DATA IS COMPROMISED

Strengthen your security posture with sophisticated early-warning capabilities and cyber threat detection. With Threatwise, you can surface and minimize advanced attacks sooner - before your data is compromised.

Using patented cyber deception technology, Threatwise uncovers silent threats and bad actors who bypass conventional security tools so that you can respond before data encryption, exfiltration, or damage.

- Deploy fake assets to hide legitimate resources and backup environments.

- Identify zero-day and unknown threats in your production environment before they reach your data.

- Seamlessly alert IT and security teams without false positives.

Your Data

On-Prem
Cloud SaaS
Apps Edge

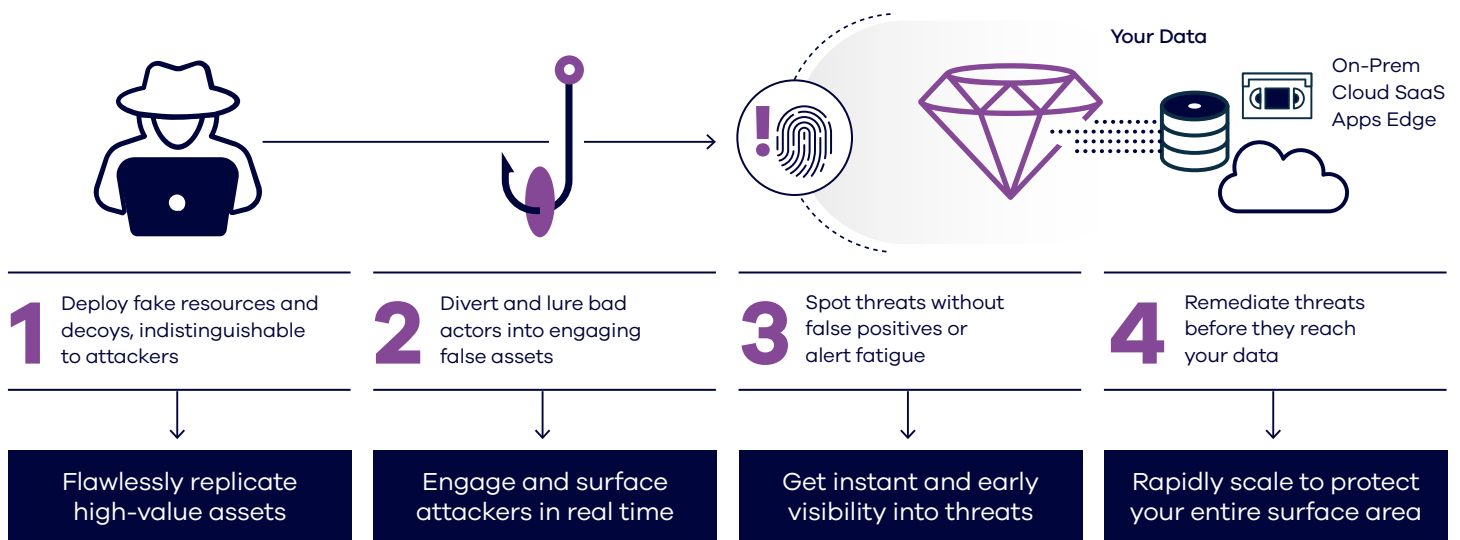| 1 Deploy fake resources and decoys, indistinguishable to attackers	2 Divert and lure bad actors into engaging false assets	3 Spot threats without false positives or alert fatigue	4 Remediate threats before they reach your data
Flawlessly replicate high-value assets	Engage and surface attackers in real time	Get instant and early visibility into threats	Rapidly scale to protect your entire surface area

Figure 2 – Threatwise™ tricks bad actors into engaging with fake assets, alerting you to network infiltration and distracting cybercriminals while you contain and remediate threats.

CLEANROOMS – GUARANTEED MALWARE-FREE CLOUD ENVIRONMENTS

To ensure your data is always safe, clean, and recoverable, benefit from a guaranteed malware-free cloud environment. Simplify and cost-effectively manage cleanrooms with Cleanroom Recovery, providing continuous testing and secure data recovery. Continually test recovery so that when it matters most to your business, you are ready to go and can ensure rapid, frictionless, and reliable recovery.

- Secure recovery with isolated cloud instances with virtually air-gapped storage, insulated and safeguarded from malware and threats.

- Instant cloud readiness without costly dedicated infrastructure.

- AI-powered recovery scaling for industry-leading, rapid, and reliable massive data restoration capabilities

Data security and protection are essential to protect critical and sensitive data from ransomware attacks, data breaches, and data exfiltration. Commvault® Cloud Risk Analysis, Commvault® Cloud Threat Scan, Threatwise™, and Cleanrooms provide the insight and cyber-resilient protection needed to keep data secure and safe while also helping to reduce costs and accelerate recovery time. You can ensure your data is secure and protected with the right tools and solutions.

To learn more, visit **commvault.com**