DATA SHEET

Data Security for Microsoft 365

Protect, detect, understand, and recover Microsoft 365 data with layered cyber resilience and data security posture management

MICROSOFT 365 IS BUSINESS-CRITICAL DATA THAT NEEDS MORE THAN BACKUP.

Commvault extends Microsoft 365 backup with Threat Scan and Data Posture 360, available as additional capabilities that can be adopted independently or together. Threat Scan analyzes protected data for indicators of compromise, while Data Posture 360 helps discover sensitive data, understand exposure, and reduce risk.


Exchange Online


Teams


Sharepoint


OneDrive

THREAT SCAN

Layer multiple detection mechanisms across protected Microsoft 365 data to identify threats and add security context to cyber recovery.

- **Google Threat Intelligence** — Apply global threat intelligence to help identify malicious and suspicious content.
- **Malware detection** — Detect known and previously unseen malware using heuristics, machine learning, and malware analysis.
- **Encryption detection** — Identify suspicious encryption activity that may indicate ransomware.
- **Anomaly detection** — Surface significant or unusual changes in protected data.
- **Security signals & IOCs** — Correlate partner EDR/XDR signals and customer-defined indicators of compromise with backup data.

Cyber recovery context

- See threat findings associated with recovery points.
- Reduce the risk of reintroducing malicious content.
- Make informed recovery decisions with security context.

DATA POSTURE 360

Data Posture 360—brings DSPM to Microsoft 365 so organizations can understand what sensitive data they have, where it is exposed, and where to act.

- **Discover sensitive data** — Identify and inventory sensitive information across protected Microsoft 365 data.
- **Classify and understand data** — Add context to determine which data is most sensitive or important.
- **Reduce data blind spots** — Surface sensitive information that may otherwise remain unknown or overlooked.
- **Understand access** — Gain visibility into permissions and excessive access to sensitive content.
- **Accelerate risk assessments** — Provide a clear, classified view of sensitive data to help teams evaluate risk faster.
- **Strengthen compliance readiness** — Maintain a consistent inventory of sensitive data to support governance, audits, and compliance decisions.

Proactive data-risk reduction

- Give security, privacy, and compliance teams data-centric posture visibility.
- Reduce unnecessary exposure before it becomes an incident.

Detect active threats with Threat Scan. Reduce data exposure with Data Posture 360.

LAYERED SECURITY ACROSS THE MICROSOFT 365 DATA LIFECYCLE

Commvault safeguards Microsoft 365 data with isolated backup and recovery, then adds security capabilities that help teams understand risk, detect malicious activity, and recover with greater confidence.

SECURITY LAYER	COMMVAULT THREAT SCAN	COMMVAULT DATA POSTURE 360
Understand	Detect malware, encryption, anomalies, and IOCs in attachments and files.	Discover and classify sensitive data; understand access and exposure.
Prioritize	Identify suspicious data and recovery points that are better candidates for restore.	Prioritize sensitive and overexposed data based on posture and business risk.
Act & recover	Use threat findings to inform cyber recovery and reduce reinfection risk.	Drive remediation to reduce unnecessary exposure and strengthen data posture.

MICROSOFT 365 SERVICES SUPPORTED

Commvault Microsoft 365 protection supports:

- ✓ Microsoft 365 Exchange Online
- ✓ Microsoft 365 OneDrive
- ✓ Microsoft 365 Teams
- ✓ Microsoft 365 SharePoint

RESILIENCE IS THE FOUNDATION

- Add-on security services to comprehensive backup and recovery for Microsoft 365 data
- Active threat monitoring and automatic quarantine to identify and isolate malicious files, reducing the risk of reintroducing threats during recovery
- Threat hunting with file hashes and YARA rules to proactively search protected data for known indicators of compromise and uncover threats that may have evaded detection.
- Discover and classify sensitive data across Microsoft 365 to understand where critical and confidential data resides
- Identify overexposure and access risk by understanding who has access to sensitive data, how it is shared, and where permissions create unnecessary exposure
- Prioritize and remediate data risk with actionable insights that help security and compliance teams focus on the highest-risk data and reduce exposure

Protect data, understand risk, and detect threats – so you can recover with confidence.

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

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