Commvault Metallic

Overview

Commvault's data protection capabilities are offered as standalone SaaS offerings through its Metallic division, launched in 2019. Services are available through Commvault managed service partners. Additionally, Commvault has a strategic, multi-year partnership with Microsoft that includes joint engineering for Metallic and Azure, as well as joint go-to-market initiatives selling the services through channel, the Azure Marketplace and from Commvault directly.

Cohesity brought its first solution to market, a hyperconverged data protection appliance that integrated its DataProtect backup and recovery software with partners' hardware, in 2015. While these systems remain in deployment in customer environments and available for purchase through Cohesity partners, Cohesity has since evolved to a software-led model. This includes adding the ability for deployment in the public cloud and through Cohesity's data management-as-a-service (DMaaS) portfolio.

The currently available services include:

- Metallic VM & Kubernetes Backup
- Active Directory Backup
- Database Backup
- Endpoint Backup
- File and Object Backup
- SaaS app protection
    - Microsoft 365
    - Microsoft Dynamics 365

Highlights

- Protection for a variety of on- and off-premises infrastructure, apps, and databases
- Flexibility for storage target
- Commvault IntelliSnap snapshots
- Metadata cataloging and search
- Granular recoveries
- Complementary services (Commvault cloud storage, ThreatWise)
- SecurityIQ dashboard
- Ability to support Hyperscale X

    - Salesforce
- ThreatWise ransomware detection (based on the 2022 acquisition of TrapX)
- Metallic Government Cloud (FedRAMP High)
- Metallic Recovery Reserve cloud storage

Usage and Deployment

Metallic is Commvault's SaaS delivery model for data protection services.

- Characteristics
    - SaaS control plane is hosted in Azure
        - On-premises gateway required to back up on-premises sources
        - Commvault IntelliSnap snapshots
    - Access control
        - Multi-factor authentication (MFA)
        - Role-based access control (RBAC)
    - Encryption
        - Data at rest and in flight
        - Embedded key management service with tenant-specific key
    - Immutability
    - Isolation of data in tenant-specific containers
    - Hyperscale X in Metallic edge mode, which allows Commvault's Hyperscale X hyperconverged appliances to serve as the on-premises footprint for Metallic
    - ThreatWise threat detection
        - Add-on service based on 2022 acquisition of TrapX
- Applications/Use Cases
    - Backup and operational recovery
        - On-premises-to-cloud data mobility requires on-premises SaaS connector
    - Global search and granular recovery
- Protected Environments
    - Metallic VM & Kubernetes Backup protects:
        - Any CNCF-Certified Kubernetes sources, including:
            - Azure Kubernetes Service (AKS)

        - Amazon Elastic Kubernetes Service (EKS)
        - Commvault Distributed Storage
        - Red Hat OpenShift Kubernetes
        - VMware Tanzu
    - Hypervisors:
        - Microsoft Hyper-V
        - VMware vSphere
    - Cloud infrastructure-as-a-service (IaaS):
        - Amazon EC2 (native VMs)
        - Azure (native VMs)
        - Azure VMware Solution (AVS)
        - Oracle Cloud Infrastructure (OCI)
        - VMware Cloud on AWS
- Database Backup protects:
    - Amazon Cloud Native Databases
        - RDS
        - DynamoDB
        - DocumentDB
        - Redshift
    - Azure Cloud Native Databases
        - CosmosDB
        - Managed SQL
        - MariaDB
        - MySQL
        - PostgreSQL
        - SQL Server
    - Microsoft SQL Server
    - Oracle
    - Oracle RAC
    - SAP HANA
- File and Object Backup protects:
    - Amazon S3 storage
    - Microsoft Azure Blob and Files
    - Microsoft and Linux/UNIX file systems

- SaaS app protection
  - Microsoft 365 Backup and Recovery includes protection for:
    - Exchange Online
    - Groups
    - OneDrive
    - Project Online
    - SharePoint Online
    - Teams
    - Active Directory and Azure Active Directory included for free
  - Microsoft Dynamics 365
  - Salesforce Backup includes protection for the Salesforce Sales, Service, Financial and Health Clouds (both sandbox and production).
- Supported Storage Targets:
  - Varies depending on the source being protected. Options include:
    - Metallic Recovery Reserve cloud storage on Microsoft Azure or Oracle Cloud Infrastructure (OCI)
    - Customer-provided ("bring-your-own") target:
      - On-premises:
        - Commvault Distributed Storage
        - Dell PowerProtect DD, PowerScale
        - Hitachi HCP, HNAS, VSP
        - HPE 3PAR, Nimble, Primera, StoreOnce Catalyst
        - NetApp E-Series
        - Pure Storage FlashArray, FlashBlade
      - Public cloud-based:
        - Amazon S3
        - AWS
        - HPE Cloud Volumes Backup
        - Microsoft Azure
        - Oracle Cloud Infrastructure
- Deployment and Administration
  - Cloud deployment, as-a-service through Metallic or Metallic partners
    - Metallic control plane hosted in Azure
  - Metallic SaaS-based control plane can be configured in Command Console.
    - Dashboarding, monitoring, and reporting

- SecurityIQ dashboard

Key Capabilities

Architecture and Deployment

Commvault handles data protection infrastructure management and maintenance for the Metallic service, while the customer or Metallic partner manages the daily backup and recovery operations. The Metallic control plane itself runs in Azure. It is typically deployed in a region close to the customer's data center, and it can be configured stand-alone or as a part of a customer's Commvault Command Console implementation.

An on-premises gateway is required to back up on-premises sources. Customers can configure any number of gateways. A gateway can either have captive storage (directly attached) or connection to a NAS system. A gateway with captive storage is limited to 50TB of capacity. For a gateway using NAS for storage, capacity is the same as the network share size configured on the NAS storage.

Administration and Management

The Metallic Hub user interface provides dashboarding, monitoring, and reporting for protection jobs. It also provides the ability to configure storage targets, and to manage roles and users. Usage reports are available.

Additionally, Metallic includes the Security IQ Dashboard, which provides visibility into the security posture, anomalous user behavior and file activity, as well as audit trails and alerts all for the Metallic environment. This dashboard makes it easier for administrators to oversee and apply new security controls, and to monitor for potential nefarious activity.

Effective June 2023, Metallic services can be centrally managed with Complete instances via the Cloud Command interface.

Data Cataloging, Search and Analytics

Metadata is cataloged and searchable. SecurityIQ dashboard identifies anomalous events and file activity. In August 2020, eDiscovery capabilities were added for Microsoft 365 and endpoint data, and compliance with the European Union's (EU's) General Data Protection Regulation (GDPR) was achieved.

Backup Processes

Metallic can meet a range of RPOs and RTOs, and compliance and security requirements. Backups can occur to the customer's own AWS, Azure, or Oracle Cloud Infrastructure (OCI) cloud storage account, or to a Metallic-provided Azure or OCI target (with the customer being able to

choose their region). For public sector customers, Metallic offers its FedRAMP High-certified Government Cloud storage service. Unlimited Metallic cloud storage and retention are included in licenses for Microsoft 365, Dynamics 365, and Salesforce protection (the latter of which also has the option for customers to bring their own cloud storage target). For the VM & Kubernetes, Database and File & Object protection services, customers also have the option to own on-premises storage, or a Commvault HyperScale X scale-out backup target – allowing for the option to keep an active local copy for faster recovery times. A Commvault Complete instance is required for the on-premises deployment.

Automated resource discover requires a Commvault Complete instance. The backup process and granularity varies based on the source being protected. For example, Microsoft Dynamics tables and entire environments can be protected, and Commvault IntelliSnap snapshots can be used to protect VMs.

Recovery and Replication

Metallic includes granular and self-service recovery capabilities. Cross-cloud recoveries are possible, where the source metadata is supported by the target cloud provider (e.g., Amazon system metadata that is not supported by Azure, cannot be restored into Azure). As mentioned in the Backup Processes section of this report, customers have the option to keep a local, on-premises copy for faster recovery times for the VM& Kubernetes and the Database and File & Object protection services. Like backup jobs and retention policies, VM conversions and migrations are automated. There are no egress fees for recovery or other utilization costs.

Data Efficiency

Deduplication, compression, and network bandwidth optimization are applied for data efficiency and to control costs.

Encryption and Immutability

256 bit-AES encryption is applied to data at rest & in flight. The key management system (KMS) is embedded and tenant-specific keys are used, but third-party key management systems are not supported. Immutable storage targets are supported.

Access Control

Metallic is a multi-tenant, cloud-hosted solution. Tenants' data paths are segregated, and a number of security layers are built in, including encryption keys that are localized to the customer's environment, and access control via granular RBAC and MFA (even SRE teams internal to Metallic/Commvault cannot access customer data). Role-based access is controlled via an API gateway. Cohesity SecurityIQ allows customers to create sub-organizations, and to require more than one administrator to approve actions such as delete jobs.

Data Archive and Vaulting

Commvault positions Metallic Recovery Reserve as a tool for operational air-gapping. While the solution meets compliance requirements such as GDPR, ISO27001, and SOC 2 Type 2, and there is the FedRAMP High Ready offering, Evaluator Group has not vetted the back-end storage target from the stand point of its ability to provide data isolation (e.g., looking for isolated networking and the ability to control the data transfer window).

Significant Announcements

- 2023
  - June:
    - New Product Launch: Threat Scan
      - Looks for corrupted, encrypted files to identify the last known good recovery point.
    - New Product Launch: Risk Analysis
      - Assessment of the risk profile of data, to guide protection policies.
        - Utilizes metadata-based classification (e.g., social security number is identified and then assigned certain permissions).
        - Commvault-defined and customized permissions are supported.
      - Assesses both live and backup data for data versioning and modifications, based on file entropy.
      - Remedial actions can be automated, to support AI Ops.
    - Cloud Command (new interface; NOT sold as a stand-alone product)
      - Integrating the Metallic and Complete management interfaces, in order to build upon the success of Metallic.
        - Now making a cohesive and single UI.
        - Centrally supports multiple services from Metallic, instantiations of Complete.
    - Partner Integrations
      - Cortex XSOAR and Microsoft Sentinel
        - Alerting and runbook-based automation.
        - Bi-directional support that builds on the previously announced, extensible and API-based framework for integrating.
      - CyberArk Identity and Access Management
        - Dynamic, just in time credentials that are created as needed and not stored by Commvault. Addresses large volume of attacks that are based on compromised credentials.
  - July 2023
    - General Availability in the Microsoft Azure Marketplace

- Automatic discovery of Azure Kubernetes Service (AKS) clusters
- Centralized backup policy management across regions and accounts
- Guided recovery operations
- Migration to AKS from:
  - Amazon Elastic Kubernetes Service
  - Google Kubernetes
  - On-premises Kubernetes clusters

- Launch of Metallic: Salesforce Backup, Recovery & Sandbox Seeding – Unlimited Storage on Salesforce AppExchange.

- November
  - Launch of Commvault Cloud, Powered by Metallic AI

Futurum Group EvaluScale – Backup-as-a-Service

The Futurum Group product review methodology "EvaluScale" assesses each product within a specific technology area. The evaluation of each product is based on its capabilities, with capabilities for each technology segment grouped into distinct categories. For the Backup-as-a-service EvaluScale, products are evaluated based on the following 4 criteria categories:

- Protection Environment
- Advanced Capabilities
- Cyber Resiliency
- Ability to Execute

The full Backup-as-a-Service EvaluScale can be found here.

The Futurum Group Opinion and Outlook for Commvault Metallic

Competitively speaking, Metallic offers support for a broad range of sources, including the ability to protect both Microsoft 365 and Salesforce alongside VMs. It also offers a high degree of flexibility in the underlying storage target, including a Metallic-operated target. The inclusion of egress fees in its licenses increases predictability, and possibly cost-effectiveness, for customers. Customers should be aware that an on-premises gateway us required to protect on-premises sources, and that a Commvault Complete instance is required for some capabilities including automated recovery.

Among its differentiators are the fact that unlimited storage and retention are included in licenses for Microsoft 365, Dynamics 365, and Salesforce protection (the latter of which also has the option for customers to bring their own storage target), and that there are no egress fees for recovery or other utilization costs. For the VM & Kubernetes, Database and File & Object protection services, users have the option to purchase Metallic storage or to use their own cloud-based or on-premises storage – allowing for the option to keep an active local copy for faster recovery times.