Commvault®

ОТ СИСТЕМ РЕЗЕРВНОГО КОПИРОВАНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

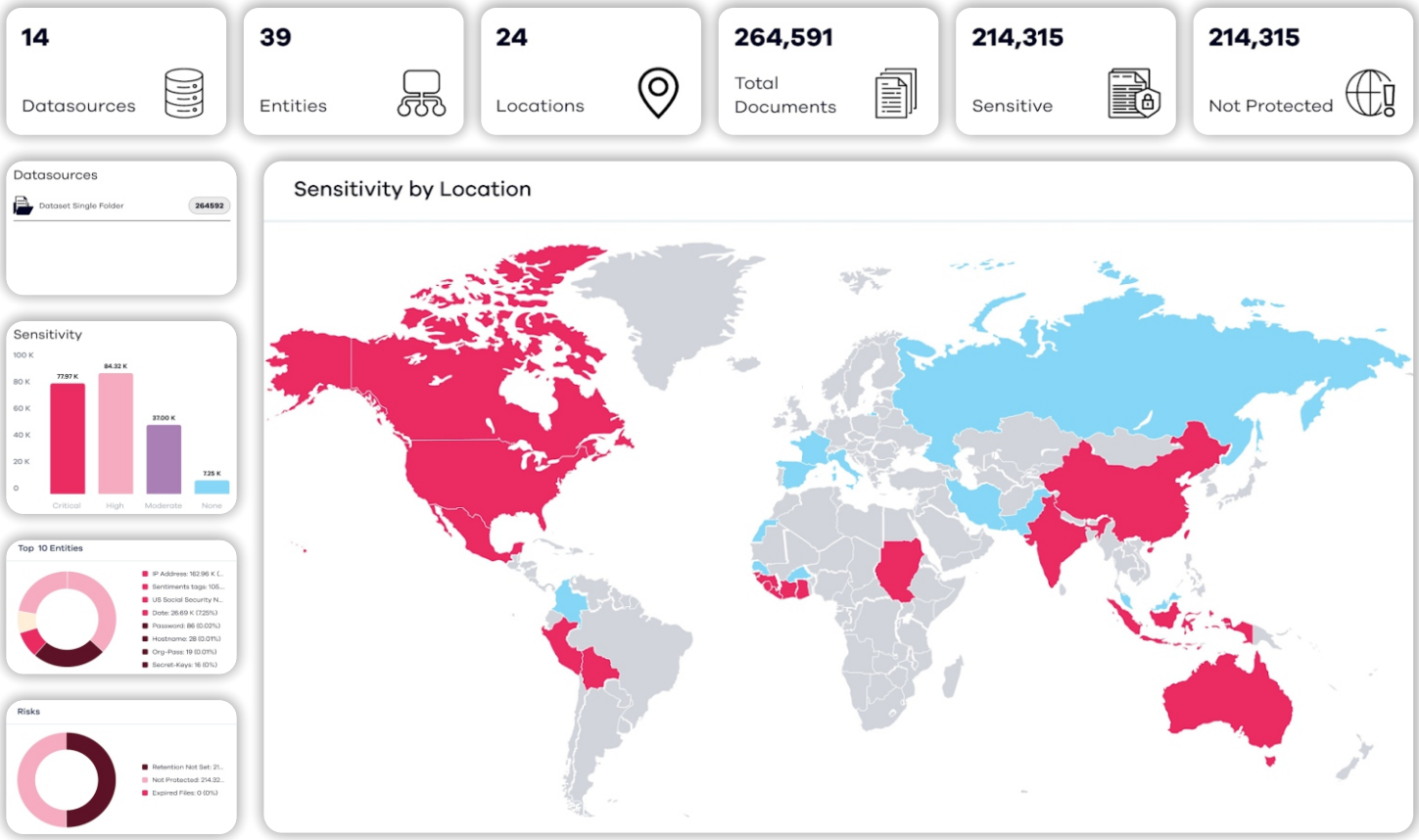
Платформа **Commvault** обеспечивает защиту и управление данными во всех типах ИТ-сред — локальных (on-premise), облачных и гибридных инфраструктурах.

Классическая защита данных

- Резервное копирование, восстановление, репликация и архивирование
- Поддержка физических серверов, виртуальных машин, баз данных и корпоративных приложений
- Точечное и гранулярное восстановление данных
- Защита ПК сотрудников с порталом самообслуживания
- Надежное хранение копий с встроенным функционалом дедупликации, компрессии, шифрования без необходимости использования внешних СХД

Защита облаков и гибридных сред

- Резервное копирование и восстановление облачных сервисов и гибридных сред (AWS, Azure, Google Cloud и других). Облако → Облако, Облако → on-premise и наоборот
- Поддержка контейнеров и Kubernetes
- Защита SaaS-сервисов, включая Microsoft 365



Платформа защиты СУБД Satori

- Data Security Posture Management — обнаружение, инвентаризация и оценка рисков для структурированных данных
- Data Access Governance — управление доступом к данным и контроль прав на основе принципа наименьших привилегий. Контроль прав на уровне таблиц и отдельных записей в БД.
- Database Activity Monitoring — мониторинг активности пользователей и сервисов при работе с базами данных
- Data Classification — классификация чувствительных данных (PII, финансовые, коммерческая тайна)
- Data Masking — динамическое маскирование данных без изменения источников выявление аномального поведения и попыток несанкционированного доступа

Киберзащита и киберустойчивость

- Deception - технологии для проактивного выявления векторов атак и определения точек уязвимости до момента их эксплуатации.
- Threat Scan - обнаружение атак и любых ransomware/malware в наборах данных с помощью Threat Intelligence от партнеров, включая обнаружение Zero day уязвимостей.
- Технологии Air Gap – возможность изолировать часть инфраструктуры от потенциального вредоносного воздействия.
- Изолированное восстановление в чистой среде (Cleanroom), позволяющее безопасно восстановить бизнес-процессы даже при полном уничтожении инфраструктуры, а также провести расследование киберинцидентов

Программно-определяемая система хранения данных Hyperscale X

- Горизонтально масштабируемая архитектура хранения с добавлением узлов без остановки системы
- Встроенная дедупликация, компрессия и оптимизация хранения
- Отказоустойчивость и распределённое хранение данных
- Оптимизация производительности backup и recovery для больших объёмов данных
- Возможность построения изолированных (в том числе air-gapped) хранилищ для критичных данных
- Концепция неизменяемого хранения (Immutable storage) при необходимости

Интеграции с системами ИБ и дополнительные функции безопасности

- Защита Identity (Active Directory, ENTRA ID). Мониторинг изменений, выявление подозрительной активности и возможность восстановления AD как критического компонента инфраструктуры
- Интеграции с SIEM/SOAR и XDR-решениями для передачи, корреляции и обогащения инцидентов
- Взаимодействие с EDR/XDR-платформами (например, CrowdStrike) для использования внешних индикаторов компрометации и контекста атак
- Экспорт событий и телеметрии в системы мониторинга безопасности (например, Splunk)

Индексирование, классификация и управление данными

- Поиск, индексирование и классификация данных - от предоставления сотрудникам поискового движка по содержимому до фильтрации персональных данных для соответствия требованиям регуляторов.
- Контроль доступа и управление правами по принципу наименьших привилегий (Zero Trust)

FORTIS DISTRIBUTION

commvault@fortis-distribution.com

www.fortis-distribution.com