

Software Product Description

Advanced User Data and Security Management
for any Data-Driven Organisation

“

*Una singola soluzione, per i responsabili
dell'infrastruttura e della sicurezza, per
gestire senza problemi due mondi.*

”

Consente a chiunque di lavorare con le informazioni in modo efficiente, aiutando a gestire e proteggere i dati in modo efficace, soddisfacendo così le due principali esigenze relative all'uso dei dati.

Data Rover viene utilizzato negli ambiti aziendali in cui la gestione e la protezione delle informazioni e dell'infrastruttura IT sono cruciali per il successo del business. Si rivela estremamente potente in quei contesti in cui l'infrastruttura di storage è complessa o in presenza di numerosi utenti con diversi livelli di autorizzazione per accedere ai dati. Il software fornisce un'analisi dettagliata delle autorizzazioni di accesso ai dati ed è progettato per aziende che devono garantire la conformità alle normative sulla protezione dei dati del personale.

Data Rover rende chiare quelle informazioni vitali che consentono di prendere decisioni strategiche e consapevoli per proteggere, sfruttare e condividere in modo sicuro le proprie informazioni, offrendo inoltre una maggiore conoscenza sull'efficienza dell'uso delle risorse.

Qual è l'obiettivo tecnico di Data Rover?

Data Rover svolge un ruolo chiave nella protezione delle informazioni e nella definizione delle politiche di gestione dei dati aziendali.

Tra le sue caratteristiche chiave, l'applicazione fornisce informazioni preziose per l'analisi dei privilegi di accesso ai file e alle cartelle sui dispositivi di storage aziendali. Consente di analizzare le autorizzazioni effettive (effective permissions) degli utenti, ovvero quelle reali. Il software aiuta a identificare e distinguere gli asset preziosi dalle informazioni inutili che diventano un peso superfluo ed un costo ingiustificato per l'azienda.

Data Rover fa da ponte tra le attività legate alla sicurezza informatica e la gestione dei dati, offrendo informazioni che sarebbero difficili e troppo dispendiose da ottenere manualmente o attraverso l'uso di numerosi strumenti di sistema contemporaneamente. Data Rover migliora le operazioni di gestione dell'infrastruttura di storage e consente di identificare con precisione falle di sicurezza e gli sprechi di risorse. Inoltre, come conseguenza, Data Rover riduce in modo significativo il "carbon footprint" dell'azienda, portando a un significativo risparmio complessivo.

Fornisce anche un ambiente sicuro per trasferire e scambiare dati internamente all'azienda e con il mondo esterno.

A chi si rivolge?

L'utilizzo di Data Rover porta benefici al personale IT, in particolare a coloro che sono responsabili della gestione delle infrastrutture IT e della loro sicurezza, identificando e risolvendo i problemi di sicurezza e gli sprechi di risorse sui dispositivi storage aziendali.

Data Rover è principalmente rivolto ai Chief Technical Officers (CTO), ai Chief Information Officers (CIO), ai Chief Information Security Officers (CISO) e ai Data Protection Officers (DPO), ma anche ai responsabili IT, agli ingegneri di sistema, sistemisti e ai responsabili aziendali.

Data Rover porta vantaggi anche ai dipendenti dell'azienda che generano e lavorano continuamente sui dati, poiché fornisce informazioni preziose che identificano situazioni che richiedono attenzione. Questo aspetto di Data Rover è cruciale per rendere l'utente consapevole e coinvolto nella gestione dei dati.

È una soluzione applicabile praticamente in tutti i settori aziendali: sanitario, finanziario, industriale, legale, pubblico, e può essere utilizzata in aziende di qualsiasi dimensione, dalle PMI in su.

Data Rover è stato pensato per rispondere alle esigenze di aziende con storage locale o in migrazione al Cloud.

Funzioni di Data Rover

Data Analytics

Data Rover offre *on-demand* una vista completa e dettagliata sui privilegi di accesso ai file e alle cartelle presenti su tutti i dispositivi di archiviazione aziendali, presentandoli come se fossero un unico dispositivo. Grazie alla funzione di visualizzazione delle *effective permissions*, è possibile selezionare un utente o un gruppo e vedere precisamente a quali file e cartelle ha accesso e con quale livello di privilegio. Viceversa, è possibile selezionare un file o una cartella e visualizzare l'elenco completo di tutti gli utenti e i gruppi che hanno la possibilità di lavorare sulla risorsa specificata, presentando i privilegi effettivi disponibili alle varie persone. In questo modo è possibile determinare chi può, ad esempio, accedere, modificare o eliminare quelle informazioni e identificare eventuali problemi di sicurezza e privilegi di accesso non autorizzati.

I permessi sono rappresentati graficamente e sono facilmente riconoscibili grazie a uno schema di colori ricorrente. Inoltre, al di là della consueta visualizzazione tabellare, è possibile navigare all'interno dei file e delle cartelle utilizzando il "Security Tree" dinamico: i rami dell'albero assumono colori diversi per rappresentare i livelli di privilegio dell'utente, seguendo lo stesso schema di colori dei permessi standardizzati da Data Rover.

La funzionalità "Point in Time" permette agli utilizzatori di controllare e analizzare lo stato dei permessi muovendosi indietro nel tempo per risalire a cambiamenti e discrepanze che possono aver creato (o creare) problemi di sicurezza. "Point in Time" è uno strumento potente per assicurare che la sicurezza dei dati e la loro conformità siano garantite lungo tutto il ciclo di vita dell'informazione aziendale.

Explore Storage Tree

Nelle aziende moderne, è comune l'utilizzo di numerosi dispositivi di storage per memorizzare i dati: Data Rover consente di sfogliare ogni dispositivo sfruttando un'interfaccia di navigazione standardizzata.

Lo "Storage Tree" consente di visualizzare l'intera struttura del file system di ogni dispositivo di storage. Gli amministratori IT possono navigare facilmente attraverso tutte le cartelle presenti nei dispositivi e possono avviare analisi specifiche attivando le funzionalità di data analytics con un semplice click sull'elemento desiderato. È così possibile ottenere una panoramica sui dati senza dover trascorrere ore alla ricerca e all'analisi manuale dei file e delle cartelle uno per uno.

Dark Data e Data Screening

I "Dark Data" sono dati inutili e totalmente superflui che si accumulano naturalmente nel tempo e costituiscono un costo ingiustificato per l'azienda. Il 100% delle aziende soffre di questo problema.

Questi dati si possono presentare in varie forme: file inutilizzati o obsoleti, documenti duplicati, dati appartenenti a ex dipendenti o file vietati o non pertinenti all'attività dell'azienda. L'accumulo di questi dati nel tempo comporta non solo un aumento dello spazio di storage occupato, ma anche un dispendio ulteriore di tempo di gestione, energia e persino costi legali che non portano alcun valore aggiunto all'azienda.

Identificare e rimuovere i Dark Data migliora l'efficienza e la sicurezza dell'infrastruttura di storage, liberando spazio e risorse per i dati più importanti, e riducendo il rischio di perdite o violazioni.

Data Rover offre informazioni precise per l'identificazione di ogni specifico tipo di Dark Data e fornisce informazioni statistiche che consentono di valutare l'impatto di questi dati sulle infrastrutture e quindi di comprendere la gravità della situazione e agire sui responsabili.

Attraverso la funzione Data Screening, è possibile configurare procedure di analisi periodiche basate sui report Dark Data, che raggruppano i dati inutili di ogni proprietario, manager o stakeholder e li notificano via email. L'utente viene così regolarmente aggiornato sull'utilizzo del proprio spazio storage, in modo da poter autogestirsi e contribuire a mantenere i sistemi di storage aziendali puliti ed efficienti. Coinvolgere gli utenti e gli stakeholder permette all'azienda di acquisire una maggiore consapevolezza dei dati.

Security Reports

Data Rover genera report di sicurezza specifici che forniscono analisi estremamente precise e dettagliate sulle effective permissions applicate ai file e alle cartelle, privilegi che possono rivelarsi potenzialmente errati e/o pericolosi per la sicurezza delle informazioni. I report offerti si concentrano sui seguenti privilegi:

"Full Control"

Fornisce all'utente la possibilità di eseguire qualsiasi tipo di operazione sul file o sulla cartella. Ad esempio, un utente che acquisisca illecitamente tale permesso su una cartella critica per le attività aziendali potrebbe modificare o eliminare file e compromettere il lavoro o la sicurezza dell'intera azienda. O ancora, un malintenzionato, sfruttando tale privilegio, potrebbe eliminare/modificare i file, o addirittura spostarli in un'altra posizione, impedendo così agli altri utenti di accedere a quelle informazioni. Una forma di ricatto.

"Change Permissions"

Consente all'utente di modificare i privilegi assegnati agli utenti su un file o una cartella. Ad esempio, se un utente non autorizzato acquisisce i diritti per modificare le autorizzazioni di accesso su una cartella, potrebbe concedere l'accesso a dati riservati a sé stesso o ad altri utenti. O, al contrario, potrebbe impedire ad altri utenti di accedere a determinati file o cartelle.

"Change Ownership"

Permette agli utenti di acquisire la proprietà di un file o di una cartella e acquisire così tutti i relativi privilegi. Ad esempio, se un aggressore acquisisce la proprietà di una cartella contenente dati sensibili, potrebbe ottenere il controllo totale sulla cartella e sui suoi contenuti e quindi disporre di quelle informazioni a sua completa volontà.

"Delete"

È il privilegio che permette all'utente di eliminare un file o una cartella. Ad esempio, se un aggressore acquisisse i diritti per eliminare una cartella critica per l'attività, potrebbe eliminare i file e influire sulla continuità del lavoro dell'azienda.

Questi sono solo alcuni semplici esempi di come configurazioni errate possano permettere a utenti non autorizzati di compromettere la sicurezza dell'azienda e del lavoro. I report di Data Rover identificano rapidamente queste aree di rischio in modo da poter adottare le misure di sicurezza appropriate per proteggere sia il personale sia le attività aziendali.

File Auditing

Il “File Auditor” di Data Rover essenzialmente mostra chi ha eseguito quale operazione, da dove (indirizzo di rete) e quando.

Il sistema di auditing è uno strumento importante per monitorare l'attività degli utenti e degli amministratori sulle cartelle e sui file condivisi in rete da file server basati su Windows. Consente di tenere accuratamente traccia di tutte le operazioni eseguite – creazione, modifica o eliminazione di un file o di una cartella – da chi e quando. Inoltre, grazie al sistema di tracciamento degli indirizzi di rete, Data Rover identifica anche la posizione da cui è stata eseguita l'azione.

Il sistema di file auditing fornisce informazioni essenziali per la sicurezza dei dati dell'azienda: si può verificare se un utente o più utenti abbiano operato su uno o più file, o può essere utilizzato per rilevare altri comportamenti anomali, come modifiche ripetute a file o cartelle di dati sensibili. Le informazioni ottenute possono anche essere utilizzate per identificare violazioni delle policy aziendali e di adottare quindi le misure necessarie per prevenirle.

L'accesso e l'utilizzo del File Auditing di Data Rover, è riservato, nel rispetto delle normative sulla privacy, a soggetti speciali, incaricati dall'Azienda e autorizzati dalla normativa vigente.

Data Gate - Advanced Data Exchange and Tracking

Data Gate offre alle aziende un sistema avanzato di scambio e tracciamento dei dati appositamente progettato per le esigenze di business. La soluzione garantisce funzionalità e sicurezza senza precedenti. Include funzioni automatizzate di pulizia che eliminano i file più vecchi dalle condivisioni, prevenendo così lo spreco di spazio di archiviazione e potenziali perdite di dati. È possibile anche limitare il periodo di condivisione delle informazioni, assicurandosi che siano disponibili solo per un determinato intervallo di tempo, garantendo che nulla resti accessibile in modo incontrollato.

Data Gate integra uno strumento di gestione delle quote di archiviazione per utente, in modo che il personale possa occupare solo una quantità predefinita di spazio su disco per un periodo determinato, senza così impattare sulle risorse degli altri. Offre inoltre un efficace sistema di definizione di "data policy", per stabilire quali tipi di file possono essere condivisi e di impostare dei limiti sulla dimensione dei file.

L'integrazione con l'infrastruttura Active Directory aziendale permette di definire i privilegi di utilizzo attraverso i gruppi AD, consentendo di scegliere chi può utilizzare Data Gate e con quale livello di autorizzazione configurando direttamente Active Directory.

Uno dei casi d'uso più comuni riguarda lo scambio di file tra un mittente all'interno di un ambiente "affidabile", come la rete aziendale (Intranet), e un destinatario esterno in un ambiente pubblico non affidabile (Internet). Grazie a Data Gate, questi due soggetti possono scambiarsi file in totale sicurezza, ma comunque con facilità.

La soluzione vanta un potente strumento di audit interno che traccia tutte le azioni effettuate all'interno di Data Gate, garantendo la sicurezza e il controllo pieno sull'intero ciclo di vita delle informazioni scambiate.

Effective Permissions: cosa sono?

Il modulo "Effective Permissions" di Data Rover identifica i privilegi attribuiti volontariamente e indirettamente agli utenti così da evidenziare le loro reali capacità di operare accessi e modifiche ai file e cartelle nello storage aziendale.

Le "autorizzazioni effettive" (effective permissions) sono i reali privilegi che un utente o un gruppo di utenti ha su un determinato file o cartella in un sistema di storage informatico. Questi privilegi sono determinati da numerosi fattori che evolvono nel tempo e sono l'unione delle autorizzazioni assegnate all'utente o al gruppo nel file system e possono differire da quelle inizialmente assegnate a causa dell'ereditarietà, sovrapposizioni o autorizzazioni nidificate, o altri fattori ancora. Ad esempio, un utente potrebbe avere l'autorizzazione di "lettura" su una cartella perché appartenente al gruppo, ma non avere l'autorizzazione di "scrittura" a causa di sovrapposizioni di autorizzazioni assegnate direttamente all'utente. La funzione "effective permissions" in Data Rover consente di identificare esattamente lo stato dei veri privilegi di accesso per ogni utente o gruppo e semplifica la gestione delle autorizzazioni e la protezione dei dati sensibili. Con Data Rover è possibile individuare potenziali falle di sicurezza o identificare quali utenti e gruppi hanno accesso a informazioni a cui non dovrebbero accedere.

L'estrazione e l'analisi di informazioni dettagliate e accurate sulle effective permissions è straordinariamente complessa perché dipende da numerosi fattori, come la struttura gerarchica degli utenti e dei gruppi, le autorizzazioni dirette di utenti e gruppi, le autorizzazioni ereditate dalla cartella genitore e altri fattori che possono influire sul risultato finale. Inoltre, può succedere che le autorizzazioni di accesso ai file e alle cartelle vengano assegnate e modificate nel tempo, rendendo l'analisi ancora più intricata. La complessità aumenta ulteriormente in un ambiente aziendale, dove ci sono moltissimi file e cartelle e dove l'accesso alle risorse potrebbe essere consentito a un gran numero di utenti e gruppi. Per questi motivi, gli amministratori IT troveranno molto difficile mantenere il controllo e garantire la sicurezza dei dati aziendali senza l'aiuto di strumenti software specializzati. In questo caso Data Rover eccelle nella sua capacità di fornire report ad alta definizione sull'ambiente storage.

Tramite l'utilizzo di Data Rover si può ottenere il controllo totale su chi può accedere a cosa.

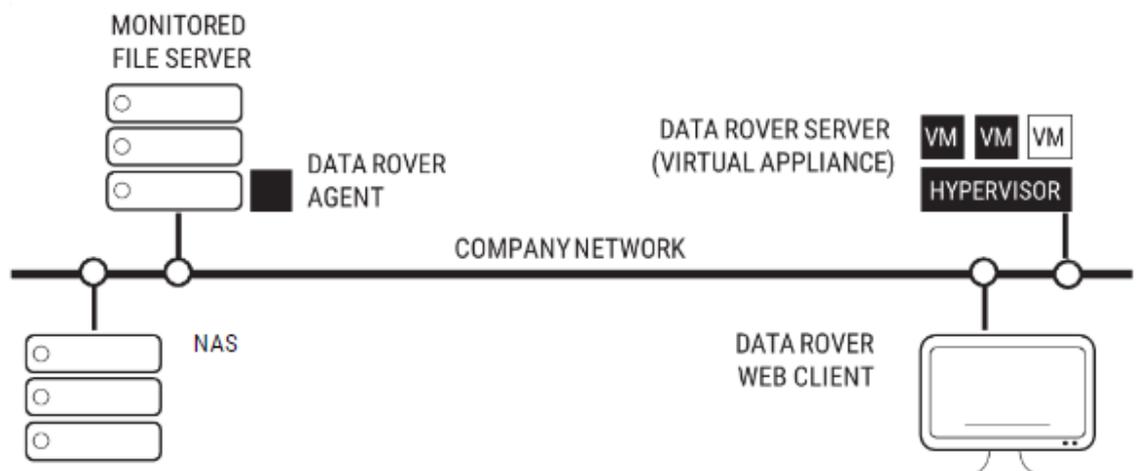
Infrastruttura e componenti di Data Rover

La soluzione Data Rover, in versione minima, richiede due componenti: l'Appliance e l'Agent, collocati in una infrastruttura on-premise del Cliente.

Descrizione

L'Appliance è una macchina virtuale ospitata su infrastruttura VMWare vSphere o Microsoft Hyper-V. L'Agent è un software installato su macchina Microsoft Windows Server 2016 o superiore che, attraverso un utente con credenziali autorizzate, acquisisce informazioni e dati dallo storage da monitorare (storage Windows del tipo NTFS nativamente, tuttavia è anche capace di raccogliere informazioni da cartelle condivise di rete tramite protocollo Windows SMB/CIFS). L'Agent si occupa di reperire e inviare i dati all'Appliance, dove vengono processati e resi consultabili dagli utenti applicativi.

Data Rover interagisce con l'infrastruttura Active Directory del Cliente (Microsoft Active Directory schema version 69 o superiore), da cui preleva le informazioni sugli utenti, gruppi, domini, ecc. per poterle incrociare con i dati raccolti dall'Agent e produrre i vari report. La scansione degli elementi Active Directory avviene tramite l'Agent oppure direttamente dalla Virtual Appliance tramite protocollo LDAP.



Nello schema vediamo rappresentata una classica installazione Data Rover. Il server Data Rover trova collocamento all'interno dell'infrastruttura virtuale del cliente. Il monitoraggio delle risorse storage (File Server o NAS) avviene tramite Agent. L'Agent può essere installato nativamente sui file server Windows-based oppure tramite una macchina di servizio di appoggio per la scansione dei dispositivi NAS.

Requisiti Minimi di Installazione

DATA ROVER APPLIANCE 6.0.1:

Compatibile con ESXi 6.5 e superiori

Processori: 2x2 vCPU (Core)

Memoria: 8 GB RAM

Storage: 4 Dischi Virtuali (formato "Thin"):

Disco OS: 80 GB

Disco MemoriaSwap: 16 GB

Disco Dati 1: 500 GB

Disco Dati 2: 600 GB

DATA ROVER AGENT:

OS Microsoft Windows Server 2016 o superiore

Microsoft .NET Framework 4.8

Supporto WMI (Windows Management Instrumentation) abilitato

Processore Quad-Core di ultima generazione almeno 2,5 GHz

Memoria: 4 GB Ram

Spazio disco: 150 MB (installazione)

Spazio disco: 20 GB (dati di cache)

Esecuzione del servizio "Data Rover Agent" con un account utente:

1. che sia un utente di dominio abilitato alle interrogazioni Active Directory (LDAP)
2. che sia un utente appartenente al gruppo amministratori sulla macchina locale
3. che sia un utente al quale siano stati concessi i permessi almeno di lettura e accesso ai rami file system che si intende monitorare

I requisiti qui indicati sono quelli minimi: il dimensionamento dell'appliance Data Rover e la configurazione finale degli agent dipende dalle caratteristiche e dalla dimensione dell'infrastruttura da analizzare. Si rimanda al manuale del prodotto per informazioni dettagliate.

Licenza

Il software di Data Rover richiede una licenza d'uso valida, inserita durante l'installazione e verificata periodicamente con la connessione di rete al Cloud Data Rover. Il License Server effettua un controllo dei parametri di funzionamento dell'installazione (parametri oggetto della licenza).

Attenzione: una assenza di collegamento prolungata al License Server impedirà l'utilizzo delle informazioni dal software.

Questo documento descrive le potenzialità e le funzionalità previste del software a scopo informativo e illustrativo. I clienti e i lettori sono responsabili di effettuare una propria valutazione indipendente delle informazioni contenute nel documento, le quali sono fornite "così come sono" senza alcuna garanzia, sia espressa che implicita. Le informazioni contenute nel documento sono valide al momento della pubblicazione e potrebbero essere soggette a modifiche senza preavviso.

Il presente documento non crea alcuna garanzia, rappresentazione, impegno contrattuale, condizione o assicurazione da parte di Data Rover Ltd, dei fornitori o dei licenziatari.

Nessuna parte di questo documento può essere riprodotta o utilizzata senza il consenso scritto di Data Rover Ltd.

Copyright © Data Rover 2023

DocID: T-SWPRDE-IT | Version: 00010



+4402080089.0006



info@data-rover.com



Bexhill o/s, E. Sussex, UK