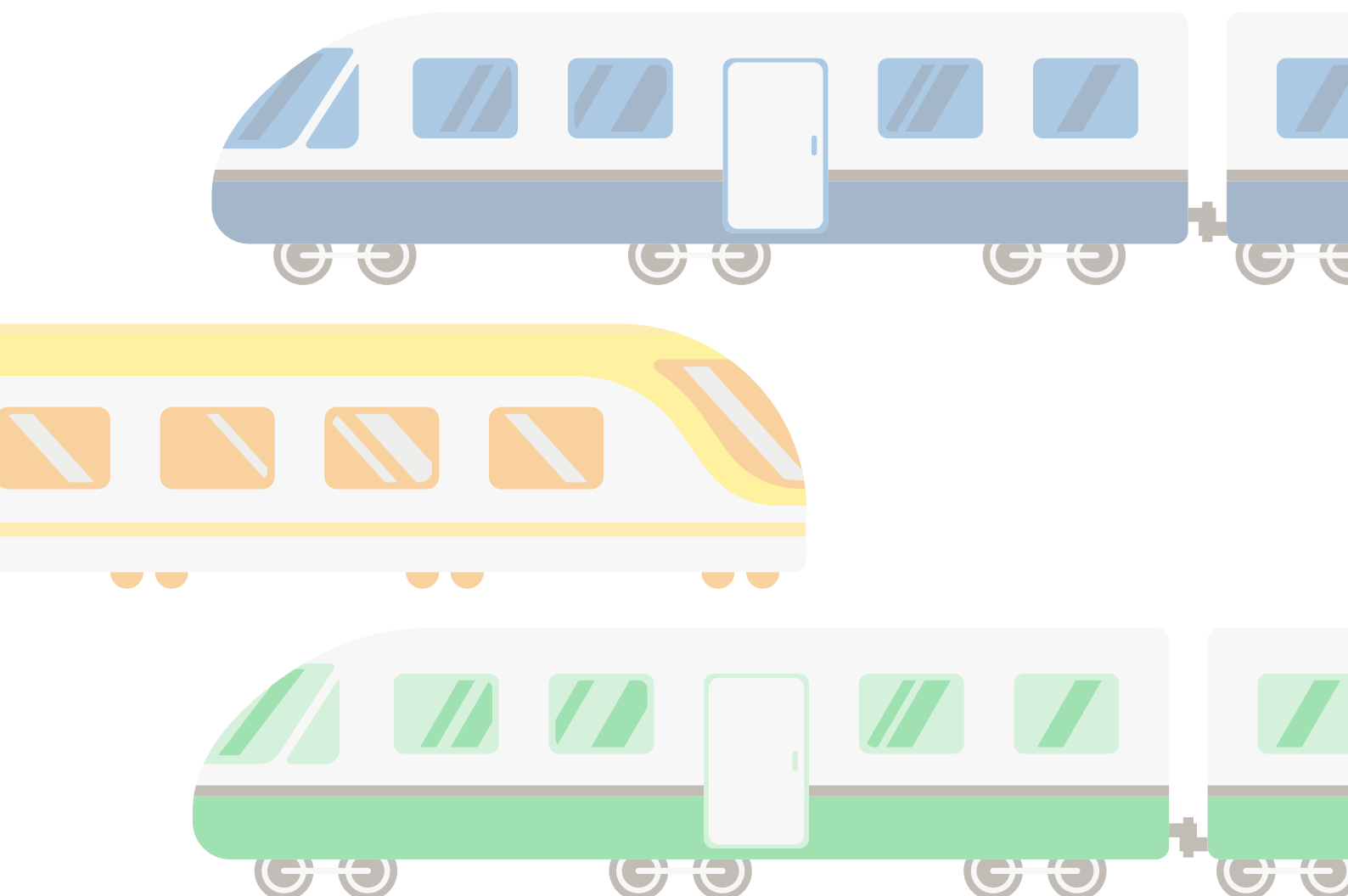


INTRATEL



DIGITAL THREATS IN THE TRANSPORTATION INDUSTRY

HOW FREIGHTLINER PROTECTS DATA



INTRODUCTION

In today's digital world, data security is critical for every company. Modern enterprises handle vast amounts of information that are essential for their daily operations and long-term success. This data includes sensitive customer information, internal financial reports, strategic plans, and operational data. Losing access to this data or experiencing a breach can have devastating consequences, making protection against cyber threats, including ransomware attacks, a top priority.

RANSOMWARE ATTACKS: WHAT THEY ARE AND THEIR IMPACT ✓

Ransomware attacks are a form of cybercrime where malicious software encrypts a victim's data, and cybercriminals demand a ransom to unlock it. Typically, the attack begins with the infection of a computer system or network through phishing (fraudulent emails) or malware downloaded from the internet. Once the ransomware gains access to the data, it starts encrypting it, making it impossible for users to access their files. The cybercriminals then display a ransom note, threatening to permanently delete or publicly release the data if the ransom is not paid.

THE IMPACT OF RANSOMWARE ATTACKS ✓

"In our industry, where every delay and data loss can result in significant losses, data security is an absolute priority. That's why we chose Veeam and Intratel solutions. We believe they offer the best protection for our backups, providing us not only with security against ransomware attacks but also ensuring business continuity."

*Rafał Śladowski, IT
Manager, Freightliner*

1

Data Loss

Without the ability to decrypt files, companies can lose access to critical data, leading to operational disruptions and a loss of customer trust.

2

Operational Downtime

Companies may be forced to temporarily shut down or significantly scale back operations, resulting in substantial financial losses.

3

Financial Costs

In addition to the potential ransom, companies incur costs related to system restoration, incident investigation, and implementing new security measures.

4

Reputation

Loss of customer data or inability to provide services can negatively impact a company's reputation, leading to long-term business consequences.

5

Legal Risk

Companies may face legal actions related to breaches of personal data protection, especially in the context of regulations such as GDPR.

FREIGHTLINER CASE: PURSUING SECURITY

Freightliner, a company specializing in rail freight transportation in Poland and neighboring countries, is acutely aware of the seriousness of these threats. Operating in a critical transport sector, the company handles and processes vast amounts of data related to logistics, transportation schedules, contracts, and customers. Understanding the importance of protecting this data from ransomware and other threats led Freightliner to seek robust backup protection solutions.

Backup security is a fundamental element of a defense strategy against ransomware. With properly secured and isolated backups, companies can quickly regain access to their data. Solutions such as regular backups, integrity testing, and storage in secure, encrypted locations are becoming essential components of IT strategies for businesses aware of the risks posed by ransomware attacks.

By investing in advanced data protection technologies, Freightliner safeguards against ransomware and enhances its resilience to various other cyber threats. Implementing effective defense mechanisms ensures operational continuity and protects the company's reputation in the market.

CHALLENGE



Freightliner's existing backup solutions required modernization to effectively counter emerging threats such as ransomware attacks. The previous system did not provide adequate protection against the encryption or deletion of data by cybercriminals. A successful attack could paralyze Freightliner's operations for an extended period, leading to catastrophic consequences for both their logistics and their clients.

In response to these threats, the client sought an advanced solution that would not only secure backups but also ensure their integrity and immutability. They required a system that would protect backups from unauthorized modifications while ensuring that the data remained continuously available and ready for restoration in the event of a failure. The new solution needed to offer features such as write immutability, real-time monitoring, and mechanisms for detecting and responding to suspicious activities, enabling immediate action against potential threats.

This approach aimed to not only enhance data protection but also elevate information security standards across the organization, providing Freightliner with confidence that their data would remain secure and accessible at all times, regardless of the scale of any potential attack.

SOLUTION

VEEAM HARDENED REPOSITORY: RELIABLE BACKUP PROTECTION FOR FREIGHTLINER

In response to the escalating threats posed by ransomware attacks, Freightliner opted to implement Veeam Backup & Replication with Hardened Repository functionality, as recommended by Intratel, a specialist in data security and availability. This innovative tool offers advanced backup protection features, ensuring the immutability of backups and resistance to unauthorized modifications.

DATA IMMUTABILITY

1

Defining the Immutability Period

Set the duration for which backups remain immutable, preventing any edits or deletions.

2

Leveraging the Linux System

Immutability features in the Linux operating system secure backup files

3

Immutability Attribute

Each backup file is protected by the immutability attribute, preventing any modifications.

4

Metadata Protection

Metadata associated with backups is protected from being written to or deleted until the immutability period expires.

"Veeam Hardened Repository is one of our preferred solutions for clients seeking the highest level of backup protection. Its advanced security features, such as data immutability and one-time credentials, not only effectively protect against ransomware attacks but also ensure data integrity and availability in any situation. This tool provides us with confidence that client data is secure, reliable, and compliant with regulatory requirements."

Paweł Mikulicz, IT Solutions Expert at Intratel

ONE-TIME CREDENTIALS

1

Maximizing Security

One-time credentials are used when adding a Linux server to the backup infrastructure.

2

Secure Storage

Credentials are not stored on the Veeam Backup & Replication server, minimizing the risk of leakage in the event of a breach.

3

Protection in the Event of a Breach

Even if the Veeam server is attacked, the attackers will not gain access to the secured backup copies.

ADDITIONAL BENEFITS OF VEEAM HARDENED REPOSITORY



1

Ransomware Protection

Effectively protects backups from encryption by ransomware and other malicious software.

2

Failure Resilience

Ensures the integrity of backups, protecting them from accidental deletion or modification.

3

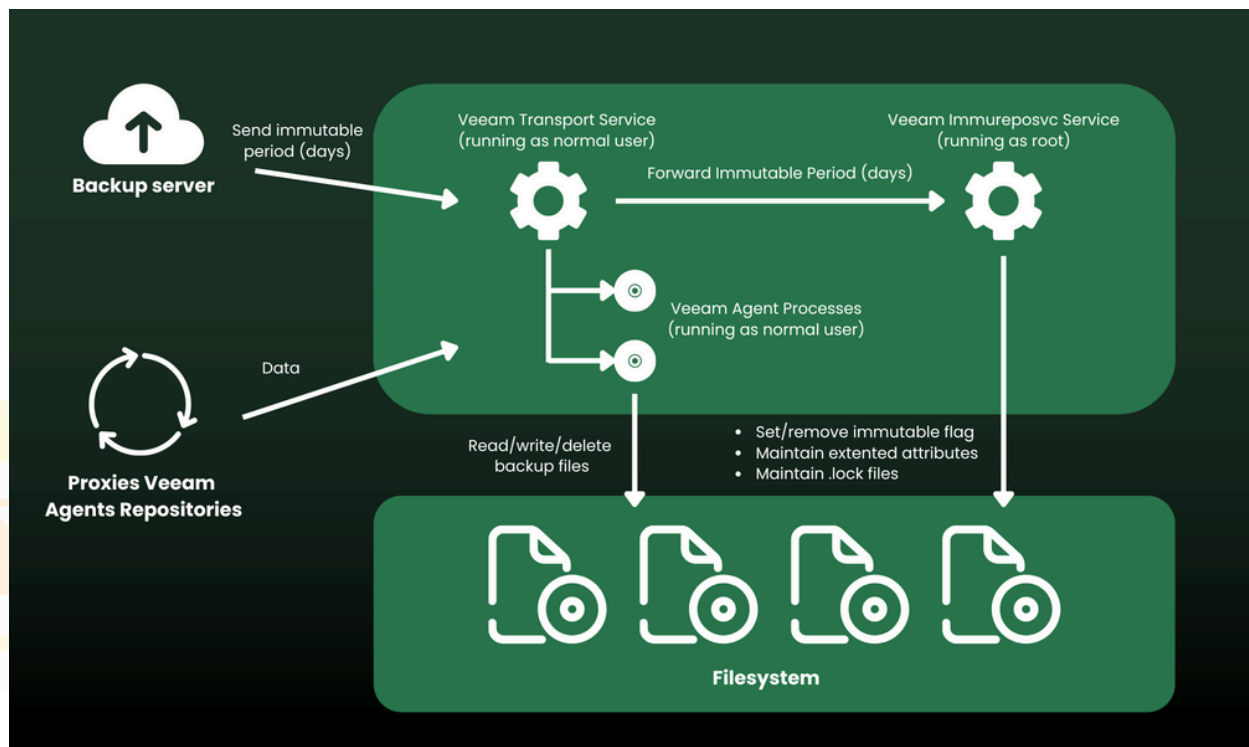
Streamlined Data Recovery

Enables quick and efficient data recovery in the event of a failure or cyberattack.

4

Regulatory Compliance

Helps meet stringent data protection requirements.



CONCLUSIONS

The implementation of Veeam Hardened Repository has proven to be a tremendous success for Freightliner, delivering benefits beyond initial expectations. This solution not only effectively enhanced backup protection against ransomware attacks and other threats but also significantly improved overall efficiency and streamlined the monitoring of backup processes.

Enhanced Data Security and Protection

With Veeam Hardened Repository, Freightliner has gained confidence that their backups are protected from encryption, deletion, or modification by malicious software. Features such as data immutability ensure that backup files remain intact for a specified period, preventing unauthorized modifications. This means that even in the event of a successful ransomware attack, the backup data is resistant to tampering, allowing for swift data recovery without the risk of information loss.

Improved Performance and Monitoring

The implementation of Veeam Hardened Repository has also enhanced operational efficiency in backup management. The system has been optimized for faster backup creation and restoration, reducing downtime in the event of a failure. Advanced monitoring tools have enabled more precise tracking of backup status and immediate detection of potential issues, allowing for quicker response and resolution of any threats.



Increased Data Security



Enhanced Performance



Immutability and Integrity of Backups



Streamlined Monitoring



Compliance with Regulatory Requirements

INTRATEL SUPPORT – THE KEY TO SUCCESS



The success of this implementation is attributed not only to the technological solution itself but also to the support from Intratel, a trusted IT security advisor. Intratel's experts thoroughly analyzed Freightliner's needs, considering the company's operational specifics and data protection requirements. As a result, Intratel facilitated the selection and effective deployment of Veeam Hardened Repository, which perfectly integrates into Freightliner's operational framework, ensuring compliance with regulatory requirements and security standards.