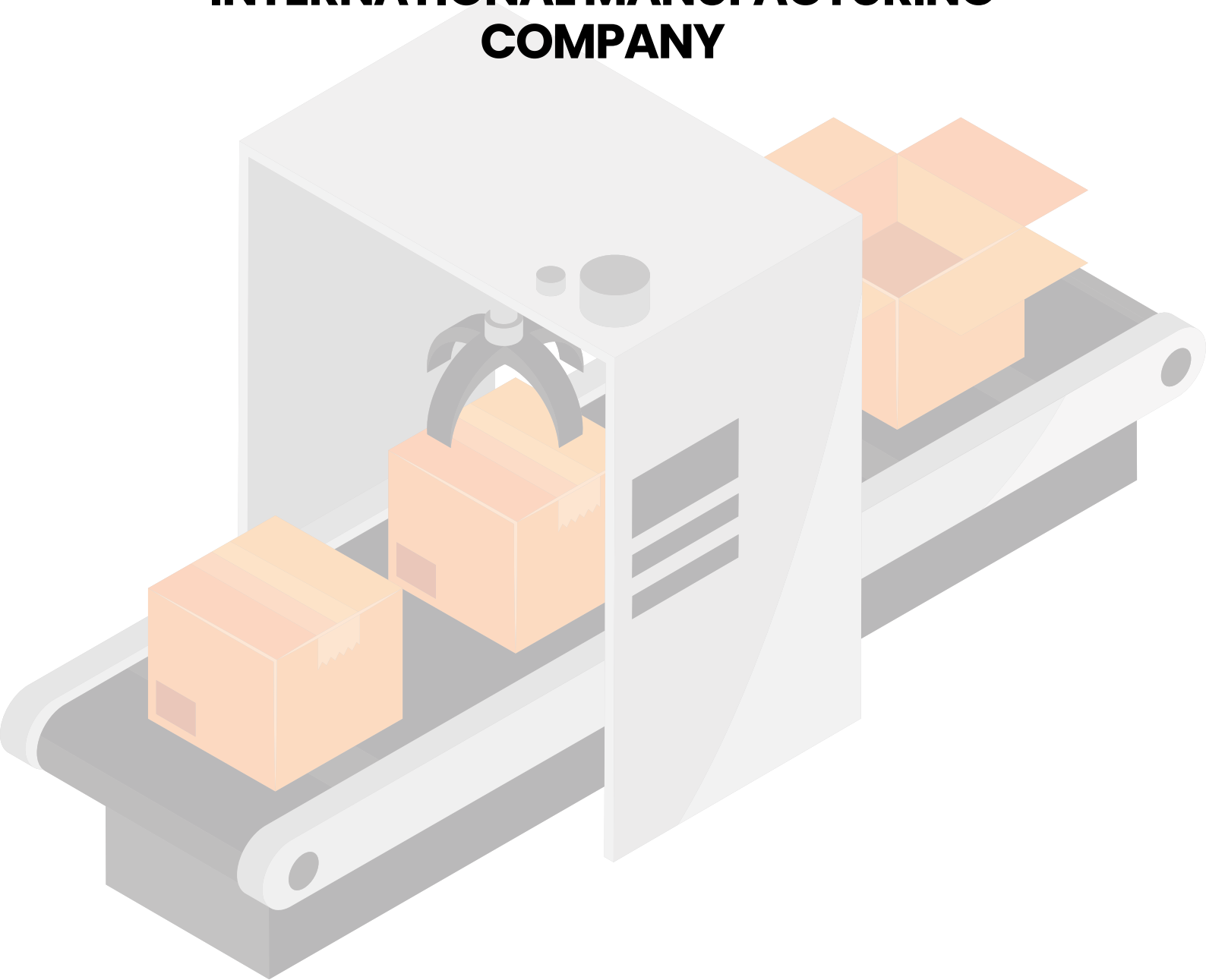
INTRATEL

veeam

PROTECTION OF SERVER INFRASTRUCTURE AGAINST RANSOMWARE ATTACKS

HOW TO PROTECT DATA IN AN INTERNATIONAL MANUFACTURING COMPANY



INTRODUCTION

The modern business world is increasingly dependent on information technologies. Digitalization of processes, cloud computing, and Big Data are just a few of the trends revolutionizing how businesses operate. At the same time, as the number of digital assets grows, so does the risk of cyberattacks. Manufacturing companies, due to the nature of their operations, are particularly vulnerable to such threats.

This case study presents a real-world example in which an international manufacturing company faced severe consequences following a ransomware attack. Cybercriminals exploited a security vulnerability to encrypt all backup files of virtual machines, preventing data restoration and paralyzing critical business processes.

WHAT WAS ATTACKED?

As a result of an advanced cyberattack, the physical VMware ESXi server, a central component of the client's IT infrastructure, was compromised by ransomware. Cybercriminals exploited vulnerabilities in the server's security, gaining unauthorized access to a wide range of storage resources connected to the VMware environment.

Among these resources was a critical volume used for storing backups of virtual machines, which contained valuable business data. After gaining control of this volume, the attackers carried out a coordinated encryption of all files stored on it. Furthermore, their actions extended beyond this specific volume. As the attack escalated, all volumes accessible within the VMware environment, including those containing production data, were encrypted, rendering them inaccessible to authorized users.

EFFECTS OF THE ATTACK

The consequences of the ransomware attack proved catastrophic for our client. The entire production infrastructure, based on virtual machines, was paralyzed. By encrypting both the production machines and their backups, the cybercriminals deprived the company of access to critical business data.

The loss of backup data stored on dedicated arrays was particularly severe. Although the implementation of snapshot mechanisms on production arrays allowed for partial recovery of data from the virtual machines, the company permanently lost historical backups, including previous versions of files, system configurations, and archived data. This resulted in the need to restart many processes from scratch and the risk of losing valuable information that could be crucial in the future.
ci.

SOLUTION

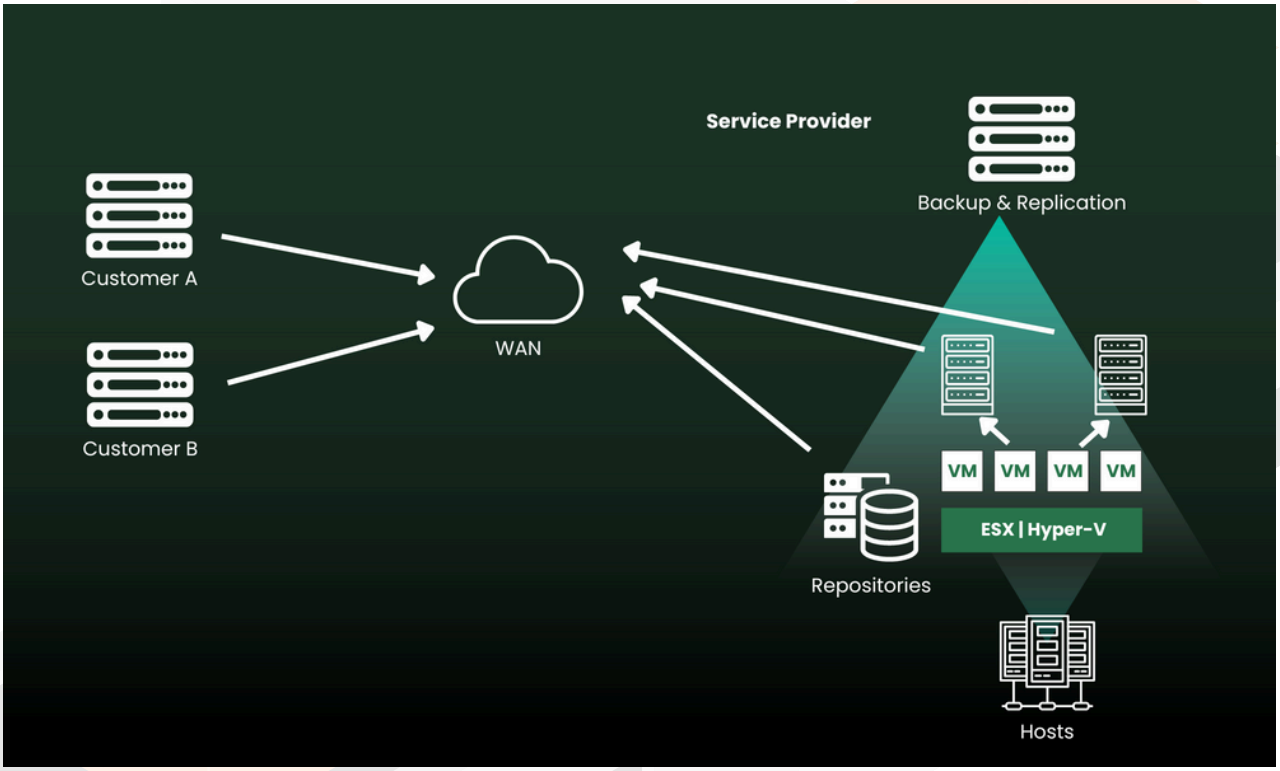
In the face of the serious consequences of the ransomware attack, Intratel proposed a comprehensive solution based on extending the functionality of the Veeam Backup & Replication platform. The goal was not only to restore operational continuity but, most importantly, to ensure maximum data protection against future threats.

VEEAM CLOUD CONNECT:

To enhance resilience against attacks and provide an additional layer of security, the Veeam Cloud Connect solution was implemented. With this feature, backups are replicated in real-time to the secure Intratel Data Center, located outside the client's infrastructure. The replication process is highly efficient, as only the changes made since the last backup are copied, minimizing network bandwidth and disk space usage. This solution ensures that even in the event of major incidents, such as the complete destruction of local infrastructure, the client has access to up-to-date backups, enabling rapid restoration of operations.

VEEAM HARDENED REPOSITORY:

Simultaneously, the Veeam Hardened Repository feature was implemented to ensure the highest level of security for stored backups. This solution effectively prevents accidental or intentional deletion, overwriting, or modification of backup data. An additional benefit is its resilience to infections affecting the Veeam server's operating system, meaning that even in the event of an attack on the internal infrastructure, the backups remain intact and protected.



Veeam Cloud Connect

IMPLEMENTATION OF A BACKUP SOLUTION

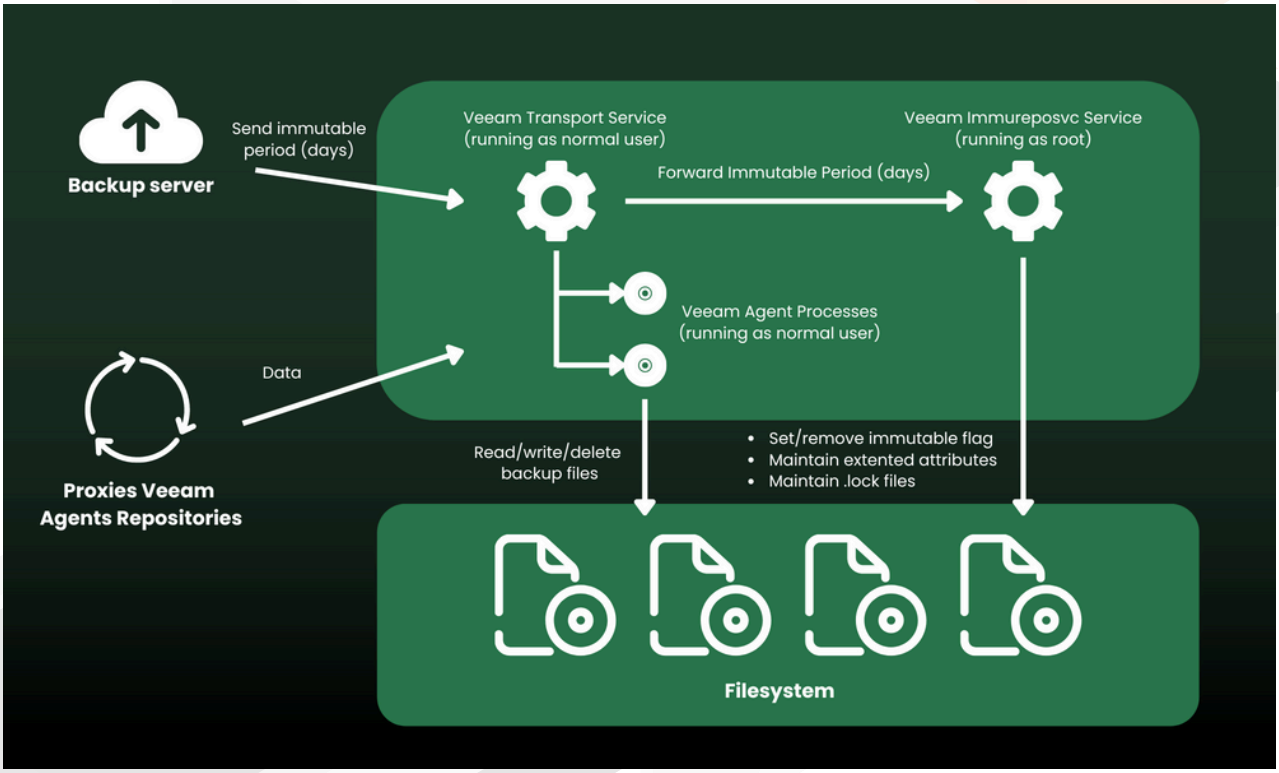
As part of the advanced backup system implementation project, key functionalities of Veeam were deployed, including Veeam Cloud Connect and Veeam Hardened Repository.

VEEAM CLOUD CONNECT:

The Veeam Cloud Connect functionality was implemented by replicating the client's daily backups to the secure Intratel Data Center. For this purpose, dedicated Intratel infrastructure was utilized, serving as a trusted Veeam Cloud Connect partner. This process ensures not only the automatic creation of backups but also their storage in an external data center, significantly enhancing the security and availability of the data. The replication to the Intratel Data Center is entirely automated, with guarantees of the integrity and confidentiality of the stored data.

VEEAM HARDENED REPOSITORY:

The Veeam Hardened Repository functionality was installed on a dedicated physical server equipped with local disks. To maximize data protection, the operating system of this server was further secured in accordance with DISA STIG (Defense Information Systems Agency Security Technical Implementation Guides) guidelines. The application of these stringent guidelines ensures protection of data and configurations from unauthorized access, which is crucial for maintaining a high level of security. Additionally, the server was configured so that all write operations are irreversible, meaning that once data is written, it cannot be modified or deleted.



Veeam Hardened Repository

IMPLEMENTATION RESULT

The implementation of the advanced functionalities of Veeam Cloud Connect and Veeam Hardened Repository brought the client a number of significant benefits that greatly impacted data security and management efficiency.

1

Increased Data Security

Thanks to the implementation of Veeam Cloud Connect, backups are now stored outside the client's organization in the secure Intratel Data Center. This storage architecture provides a high level of protection against various threats, including ransomware attacks. The data is replicated automatically, minimizing the risk of human errors and ensuring the integrity of the backups. The Veeam Hardened Repository further secures this data, making it resistant to modifications and deletions, which is crucial in the fight against cyberattacks.

2

Faster Data Recovery

One of the key outcomes of the implementation is a significant reduction in the time required for data recovery. In the event of a virtual machine failure, its backup can be quickly and efficiently restored from the secure Intratel Data Center. This means minimal downtime in the client's operational activities, which is particularly important in environments where continuity of operations is crucial.

3

Greater Peace of Mind

The implementation of modern Veeam backup solutions also contributes to greater peace of mind for the client. The client can be confident that their data is protected at the highest level and can be quickly restored if needed. Knowing that their data is securely stored and safeguarded against all threats allows the client to focus on the core aspects of their business without worrying about potential data loss.

In summary, the implementation of Veeam Cloud Connect and Veeam Hardened Repository significantly enhanced data security, accelerated the data recovery process, and provided the client with confidence that their resources are adequately protected and accessible in any emergency situation.

CONCLUSIONS

The ransomware attack on the manufacturing company highlighted the critical role that robust server infrastructure security plays in protecting key data. This experience underscored that traditional protection methods are insufficient in the face of modern cyber threats, especially in industries where data loss can lead to severe downtimes and financial losses.

The implementation of solutions such as Veeam Cloud Connect and Veeam Hardened Repository proved crucial in significantly enhancing the security level of the client's IT infrastructure. With Veeam Cloud Connect, data was effectively replicated to an external, secure Data Center, which not only protects against data loss but also enables rapid recovery in the event of a failure. Meanwhile, Veeam Hardened Repository, with its advanced protection mechanisms, ensures that data is safeguarded against unauthorized access and cannot be modified or deleted, which is essential in the context of ransomware protection.

These advanced solutions not only increased the level of data security but also provided the company with long-term protection against future attacks. The firm that experienced the repercussions of the ransomware attack now has greater confidence that its resources are adequately protected. As a result, the implementation of these technologies represented a strategic step toward building a resilient IT infrastructure that not only defends against current threats but is also prepared for future challenges.

ADDITIONAL BENEFITS OF IMPLEMENTATION

1

Ease of Use

One of the key advantages of the implemented solution is its intuitiveness. Veeam Backup & Replication has been designed with user-friendliness in mind, significantly simplifying both the initial configuration and the subsequent management of the system. The user-friendly interface and clear documentation ensure that the solution can be used not only by IT specialists but also by less experienced users, reducing the time and costs associated with implementation and ongoing maintenance.

2

Scalability

As the client's company grows, the demand for storage space and data management resources also increases. Veeam Backup & Replication offers high scalability, allowing the system to be flexibly adapted to the growing business needs. The ability to easily add new resources and expand the backup infrastructure ensures that the solution will support the company at every stage of its development, regardless of the scale of operations.

3

Profitability

Veeam Backup & Replication is a solution that offers an excellent value-to-price ratio. With advanced functionalities such as Cloud Connect and Hardened Repository, the client receives a comprehensive tool for data management and protection that minimizes the risk of downtime and data loss while optimizing operational costs. Its ability to effectively protect data, ensure rapid recovery, and facilitate ease of management means that the investment in this solution quickly pays off, yielding long-term savings.

SUMMARY

In addition to enhanced data security, the implementation of Veeam Backup & Replication with Cloud Connect and Hardened Repository functionalities has provided the client with a range of additional benefits, such as ease of use, scalability in line with the company's growth, and a high return on investment. These features ensure that the solution not only meets but often exceeds client expectations, providing stable and flexible support for data management.

WHY CHOOSE INTRATEL?

A key factor in the success of this implementation was the collaboration with Intratel, specialists in IT and data protection. With years of experience and in-depth knowledge of Veeam technologies, Intratel provided a professional implementation tailored to the client's individual needs. This company offers comprehensive support at every stage of the project—from needs analysis and planning to implementation and ongoing management and optimization of the backup system. Choosing Intratel guarantees that the implementation will be carried out smoothly, and the solutions applied will effectively protect the client's data while ensuring the system's flexibility and scalability in the future.

CONTACT

Let's discuss solutions tailored for your company.

Mariusz Bakun
IT Solution Architect
m.bakun@intratel.pl
tel. +605 237 228

Intratel Sp. z o.o.
Aleja Tysiąclecia
Państwa Polskiego 39A
15-111 Białystok