VEEAMON 2023

The Veeam Journey of Rabobank

Colin Chatelier

Rabobank
Manager, Storage Services, Europe

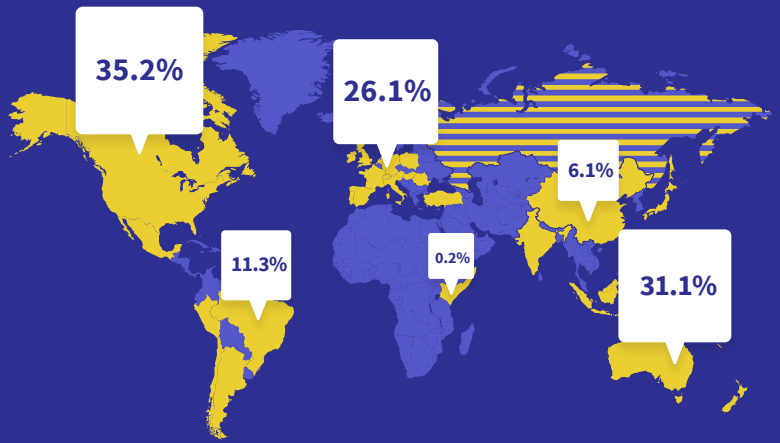
Bram de Laat

Veeam
Solutions Architect

Rabobank at a glance

Situation on June 30, 2022

International



€ 74.2 billion
Private sector lending to food & agriculture

€ 39.1 billion
Private sector lending to trade, industry and services

€ 35 billion
Leasing

38 countries
Including the Netherlands

VEEAMON 2023

How it all started

How it all started

Bought as a DR solution, later replacing TSM on VMs

Virtual only Hyper-V to VMware migration

Retail & wholesale IT merged, and best of breed solutions chosen

New requirements along the journey

Compelling financial business case to move to Veeam®

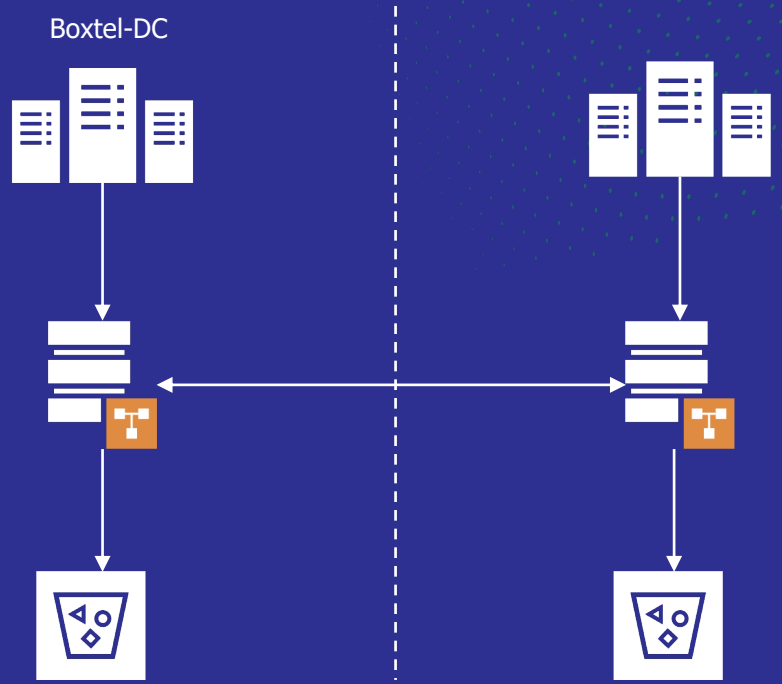
New workloads

Immutable copy

The immutable copy requirement

What are we protecting against?

- Sophisticated attackers will encrypt primary and corrupt backup data.
- Your backups likely already contain the infection.
- We want a copy of our data which can not mutate.



Sifting through the immutable options

Capacity Tier to a new S3-compatible storage platform!

1. Redesign of the topology

2. A new storage vendor introducing cloudian hyperscale:
   - PoC for scale out workloads
   - Designing for the peak workloads
   - Peak turns out to be CPU spiking as older backups age and are removed

3. OK. This works — now the rest of the world!

VEEAMON 2023

The next chapter

VEEAMON 2023

How do you recover a bank?

The recovery steps

Planning for the “unknown”

We have an immutable copy, but then:

What do we trust in the immutable copy?

Recreate servers from scratch if practical

Where not possible recreate from backup & clean

What solutions for a very tight RPO?

Preparing for the worst

In some cases, it's not only the servers which are attacked, but the key infrastructure

- Clean room as a boot-strap DC
- Rebuilding infrastructure
- Store updated configuration files on immutable storage
- Design your config "DROPBOX"

The cleanroom

Air-gap/restricted access:

- Limit access, patch, patch, pen test, patch

KISS:

- With limited staff managing a clean room, automate and use standard components

Hired help:

- You may need to accommodate an external forensics teams
- The forensics team will bring specific tools for the actual issue, what can we facilitate?

Infrastructure layers:

- Storage/compute/isolation

Command and control layer:

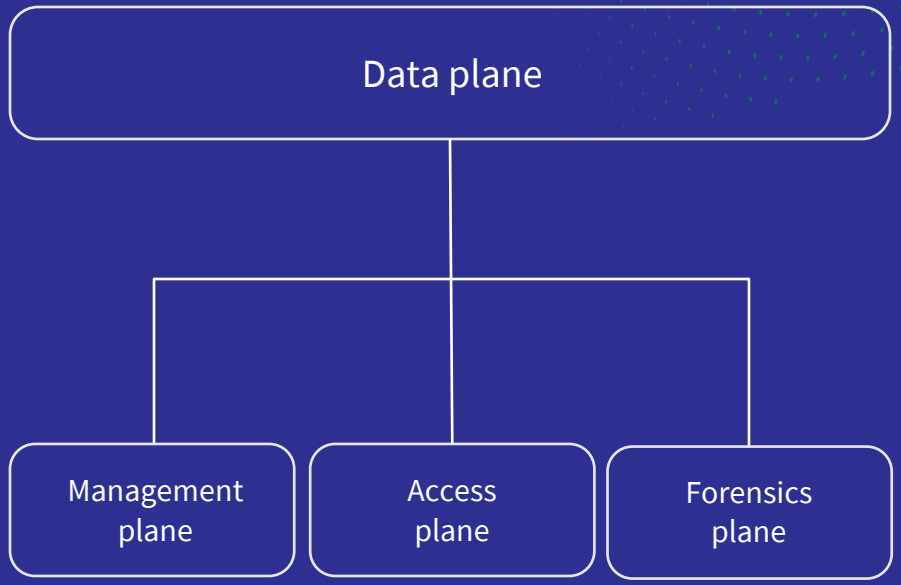
- Which tools do we trust? Which can we populate? Isolated restore environment

Preventing the re-infection spiral

If recovering a backup infected, but not yet affected by malware how do we prevent it reinfecting our estate?

We recover into an isolated environment

- A cleanroom
- Restore cluster
- Forensics
- How to recover back to production



Stakeholders and communication

Outage vs. catastrophe — set expectations

Define the minimal viable business

Classify your application chains by RTO and RPO and design solutions accordingly:

- 24-hour backup is not helpful for a payments system
- Databases may need to be treated differently to static data

In an application chain, are you able to recreate data from upstream and downstream?

Internal and external communication

Avoid every kingdom building a castle

Recap

- **Build protection**, but plan for the worst
- **You are preparing for the unknown**, so its ok for your solution to start basic and evolve
- **Immutable backups** are fundamental for recovery
- **Business must classify your applications** for solution and priority
- **App support** prepare to resynchronize data recovery upstream and downstream
- **Where backups** are infected, you will need a clean room
- **A clean room should minimize** #staff and use standard tooling
- **Consider an infra immutable “DROPBOX”** for infected hardware rebuild
- Penetration test, patch, recovery test


Thank you!
VEEAMON 2023