Disaster recovery naar Azure in de praktijk

WHOAMI

Bart Verboven

Azure Technical consultant

bart.verboven@realdolmen.com

bverboven

What I'm going to talk about

- Settings some definitions
- Key challenges
- Azure Site Recovery capabilities
- Design principals
- Reference design
- Q&A

HIGH AVAILABILITY

- Component failure
- Automated failover
- Automated failback
- No data loss

DISASTER RECOVERY

- Big smoking hole
- Manual failover
- Complex failback
- Data loss possible

KEY CHALLENGES: ORGANIZATIONAL

- Have a clear scope against what you're trying to recover from
  - ▶ "big smoking hole"
  - ▶ ransomware?
  - ▶ doesn't replace backup as a business requirement
- Design to keep it as simple as possible: limit panic mode
  - ▶ operational at production runtime
  - ▶ during a disaster scenario
- Documentation & passwords
- RTO & RPO
- Never assume
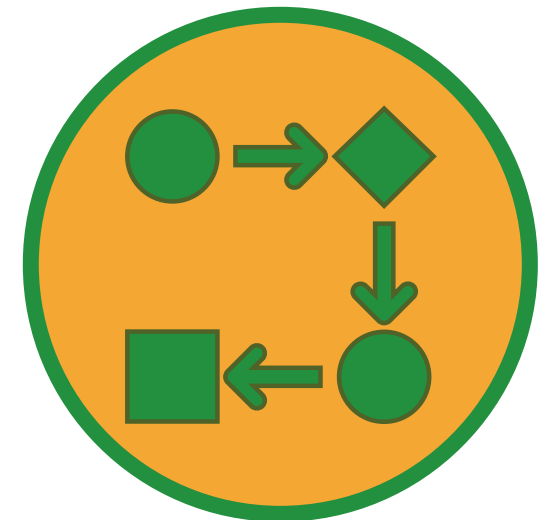
KEY CHALLENGES: TECHNICAL

- Connectivity
  - who needs to connect to what and how
  - how will users connect?
  - how will external partners and applications connect?
  - Size for your requirements
- Identity: Don't lose your keys
- Performance is not our concern.
- Keep your failover scripts accessible (e.g. Azure DevOps)

a successful technical disaster recovery doesn't mean your business is back up & running

AZURE SITE RECOVERY CONCEPTS

- Replication (async)
  - ▶ Support for Hyper-V , VMware & physical servers
  - ▶ Windows & Linux
  - ▶ On-premises to Azure
  - ▶ Azure to Azure
  - ▶ VSS Capable: Application consistent

- Pricing
  - ▶ ASR agent: €21,08 / server / month
  - ▶ Storage: €20 / TB / month
  - ▶ No compute costs for ASR compute in production scenario
    - Additional running VMs might be required

DESIGN PRINCIPALS

- Try to keep the IP plan where possible
  - ▸ Azure networking starts at Layer 3
- Design to keep it manageable
- Have identity ready to go
- ASR isn't always one-size-fit-all
  - ▸ check the compatibility matrix
  - ▸ The application might do it better
- Have a minimal hot standby setup as beachhead
  - ▸ management server
  - ▸ firewall nodes
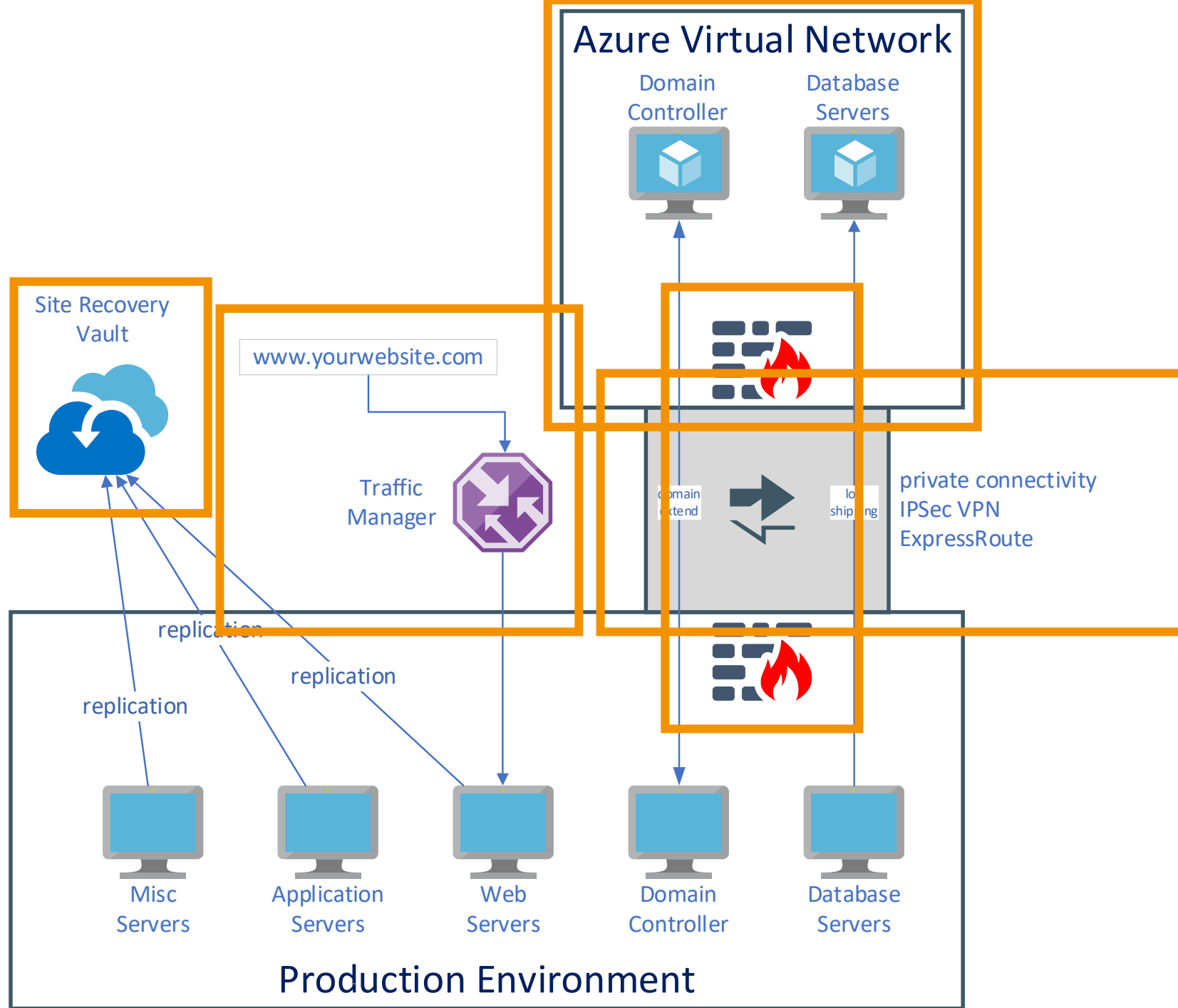 - ▸ vpn endpoints
- Execute tests

SOLVING THE NETWORK QUESTION

- External DNS: Traffic manager

- Reroute BGP or VPN connectivity

- Publish external services

- How to provide connectivity for end users?
  - ▶ Point to Site VPN (e.g. Azure VPN gateway or NGFW)
  - ▶ Application / Desktop delivery (e.g. Windows Virtual Desktop)
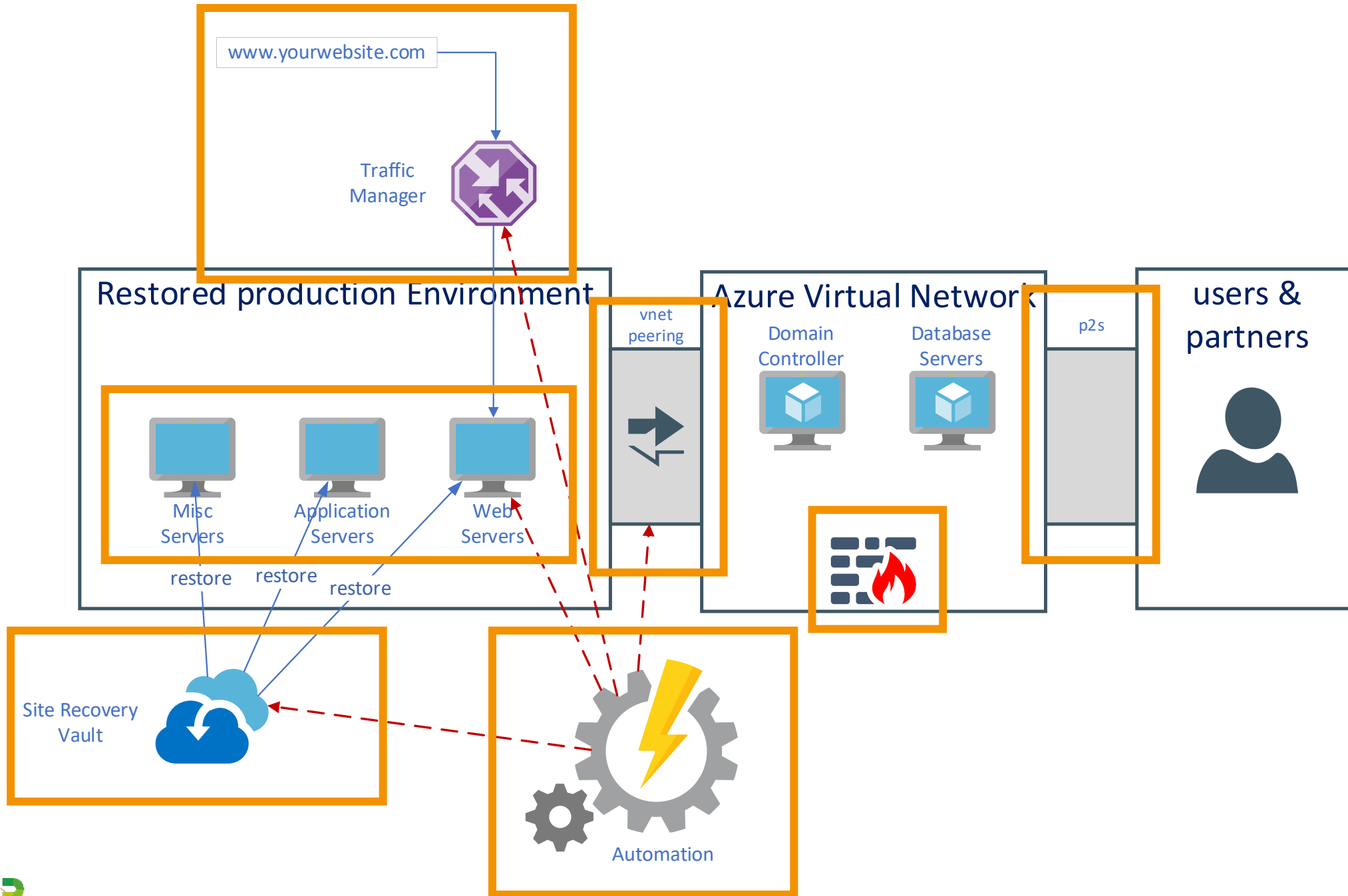 - ▶ Failover Office location connected to the LAN

Reference design

Azure Virtual Network

Domain Controller

Database Servers

Site Recovery Vault

www.yourwebsite.com

Traffic Manager

domain extend

load shipping

private connectivity
IPSec VPN
ExpressRoute

replication

replication

replication

Misc Servers

Application Servers

Web Servers

Domain Controller

Database Servers

Production Environment

www.yourwebsite.com

Traffic Manager

Restored production Environment

Azure Virtual Network

users & partners

vnet peering

Domain Controller

Database Servers

p2s

Misc Servers

Application Servers

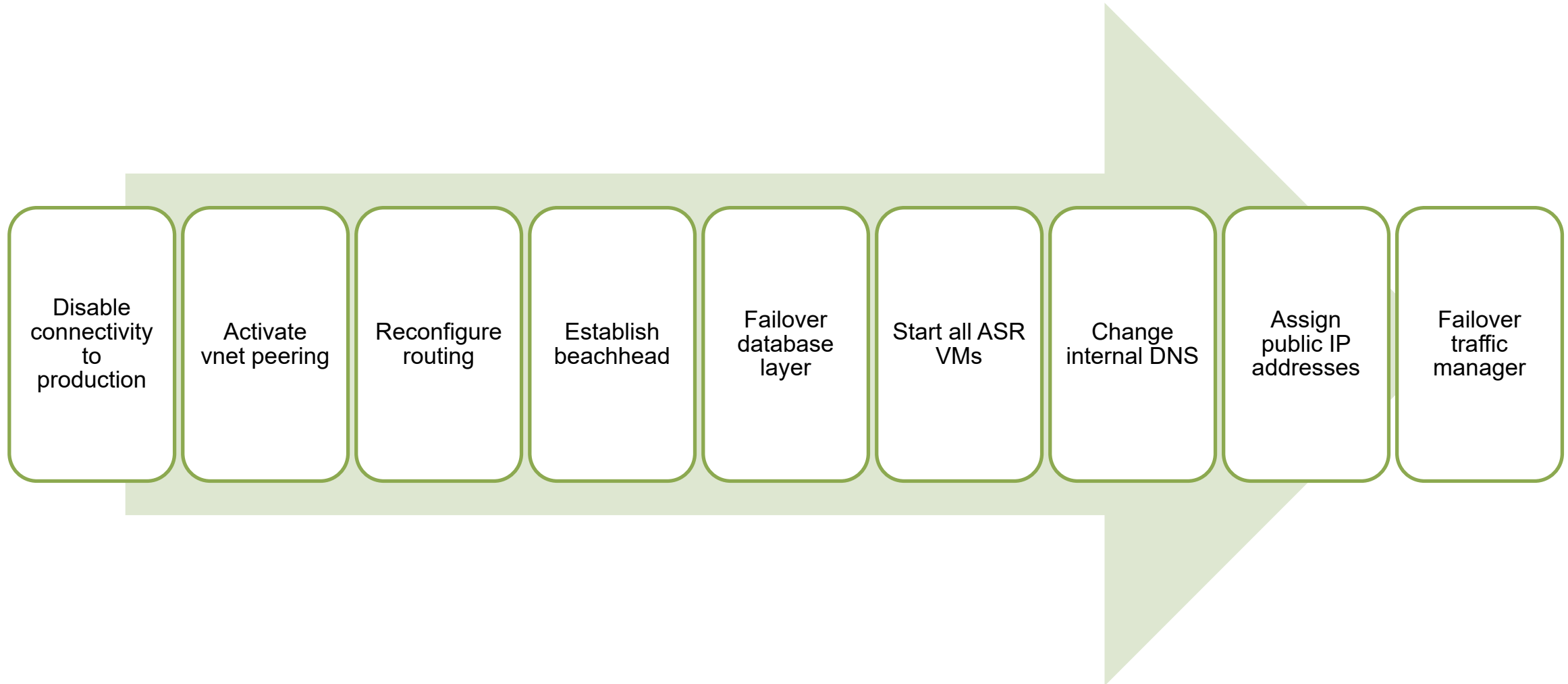Web Servers

restore

restore

restore

Site Recovery Vault

Automation

Runbook example – automated steps

KEY TAKEWAYS

Know what you're protecting against

Keep it simple

Map out network requirements

Check what the application has to offer

Recurrent testing

Go beyond the technical

Q&A

Thank you!

Contact us at:
hybridcloud@realdolmen.com