Secure Active Directory – a real world scenario

Fabian Böhm
13.11.2018

TEAL TECHNOLOGY CONSULTING
INTEGRITY ▪ PARTNERSHIP ▪ SUCCESS

Who is talking to you?

Fabian Böhm

- Co-founder & security consultant @TEAL
- 10+ years experience as consultant
- Focus on Microsoft Active Directory, public key infrastructures and cloud solutions

TEAL Technology Consulting GmbH

- Consulting company specialized in Microsoft & Linux infrastructure, cloud consulting and container management
- Founded in February 2017
- Currently 10 employees spread all over Germany

http://www.teal-consulting.de

info@teal-consulting.de

@TEAL_Technology

TEAL Technology Consulting GmbH

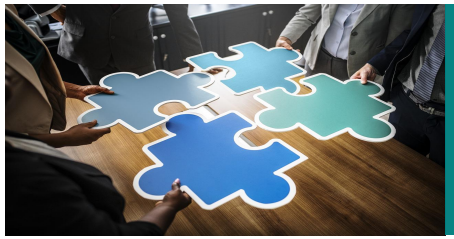
TEAL Technology Consulting GmbH

TEAL Technology Consulting GmbH

What is this talk about?

TEAL TECHNOLOGY CONSULTING
INTEGRITY ▪ PARTNERSHIP ▪ SUCCESS

Project Overview



Secure Solution

Lessons Learned

Q & A

Project Overview

What was the customer situation?

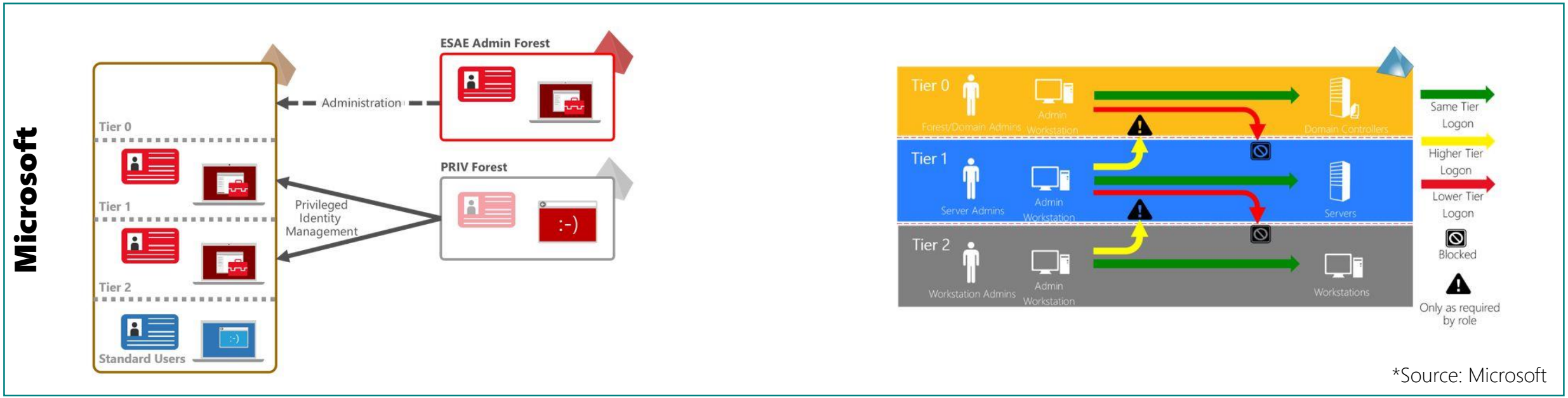
TEAL TECHNOLOGY CONSULTING
INTEGRITY ▪ PARTNERSHIP ▪ SUCCESS

- Customer situation
  - International insurance company – 40.000 employees worldwide
  - Till then little inter-affiliate collaboration
    - Each affiliate was responsible for it's own IT
    - Each affiliate had it's own identity / directory system
  - Cross-group collaboration should be massively increased
    - New international datacenter for shared services was to be implemented (20 affiliates in scope)
    - Global authentication service was necessary to enable seamless collaboration
    - In the future all applications were to use token based authentication –not all applications supported this

- Project: Global Authentication Service (GAS)
  - Implement this global authentication service for Kerberos as well as for token based authentication with best-practice security in a new co-located datacenter
  - Duration 9 month
  - Core team 5 FTE


Secure Solution

What is Microsoft's perspective?



*Source: Microsoft

- In it's ESAE documentation Microsoft focuses on securing Active Directory, clean source principal, tier model and administrative tools.
- But in reality much more needs to be considered…

What questions need to be answered?

TEAL TECHNOLOGY CONSULTING
INTEGRITY • PARTNERSHIP • SUCCESS

What qualification do my operators need?

How can we ensure short patching cycles?

How to train the Ops team properly?

Is the network service provider trustworthy?

Can we use the current monitoring solution?

Who will operate the solution?

How are the components working together?

What can we achieve within the given timeline?

What hardening settings must be applied?

How to classify systems into tiers?

What are the customers security requirements?

How are we going to deploy software?

What type of admin roles do we need to define?

Does the hardening break anything?

What Hypervisor should we use?

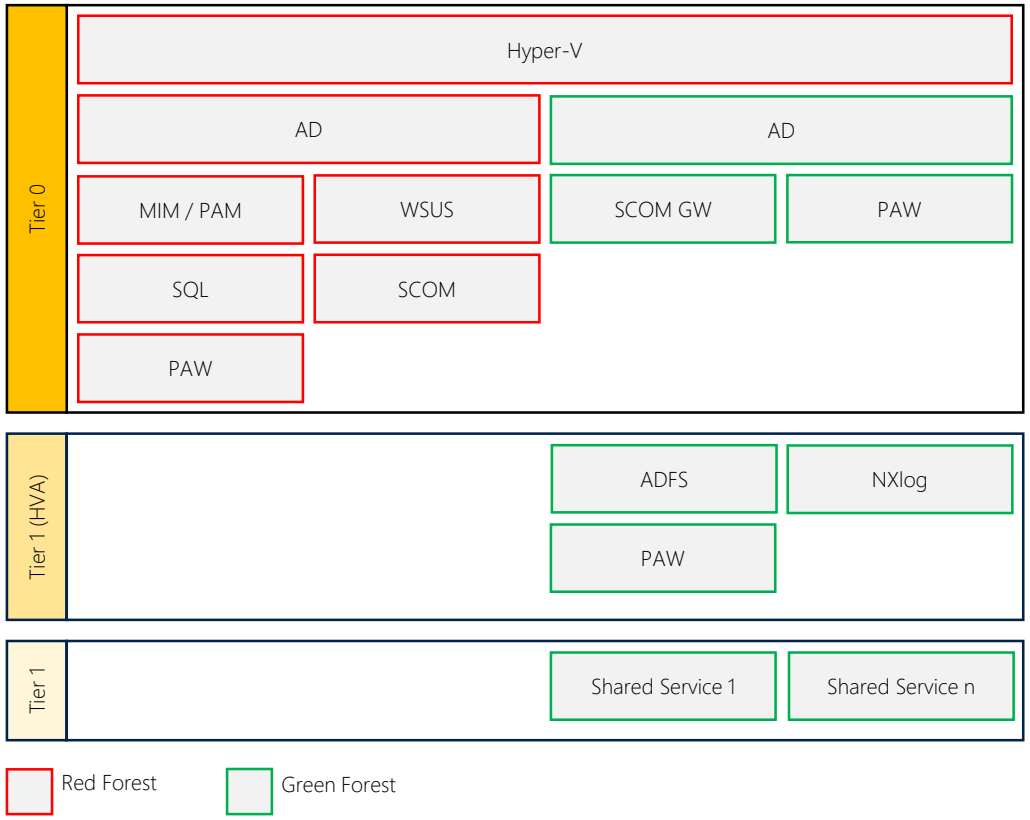
How do we enurese the security of our backups?

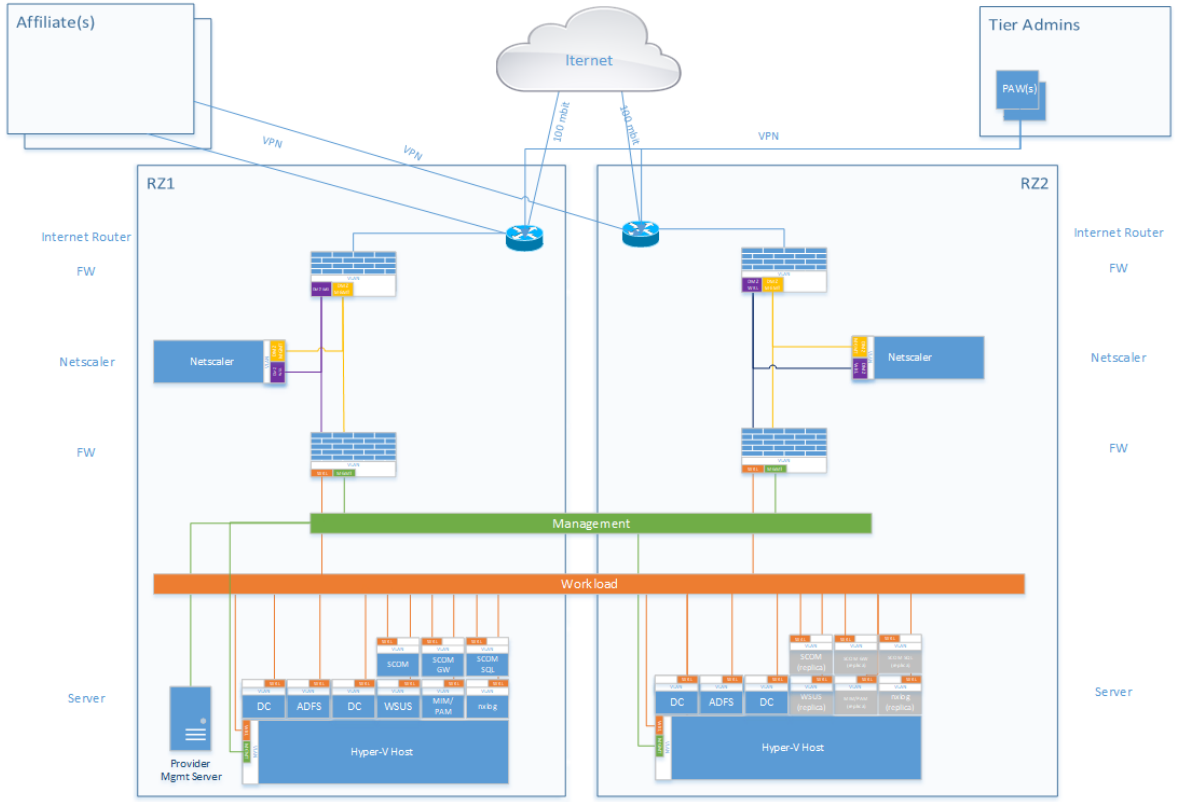
- It's a lot more to consider than just applying some hardening settings to DCs.
- Instead we analyzed the architecture bottom up starting with the physical security up to organizational controls

How does the customer architecture look like?

TEAL TECHNOLOGY CONSULTING
INTEGRITY ▪ PARTNERSHIP ▪ SUCCESS

Customer Solution





Lessons Learned

What have we learned about physical security?

TEAL TECHNOLOGY CONSULTING
INTEGRITY ▪ PARTNERSHIP ▪ SUCCESS

Requirement:
Secure physical access to Tier 0 systems

Customer situation:
Customer decided to outsource the housing for the GAS environment

Physical | Logical | Organizational

Our solution:

- Place server HW in dedicated racks or cages
- Spread servers across two locations
- Use biometric sensor to lock the rack
- Install surveillance camera to monitor the rack
- Only staff approved by the customer is allowed to get to the rack
- Nothing is done without a ticket approved by the customer
- Bios / ILO access is fully controlled by the Tier 0 team

What have we learned about physical security?

TEAL TECHNOLOGY CONSULTING
INTEGRITY ▪ PARTNERSHIP ▪ SUCCESS

Requirement:
Only approved staff (Tier 0) is allowed to monitor / administer the Tier 0 / Tier 1 systems

Customer situation:
Server Hardware, Network and security devices are operated by a service provider which is not part of the Tier 0 admin team

Our solution:

- Encrypt complete network traffic using IPSec
- If troubleshooting requires non encrypted traffic, only the Tier 0 team can temporary disable encryption. Troubleshooting is always done together with the Tier 0 team (4-eye-principal)
- Administrative access to BIOS/ ILO is only allowed by the Tier 0 team. Hardware provider has a read only account within ILO to get informed in case of a hardware failure
- All change activities must be pre-approved by the Tier 0 admin team

What have we learned about logical security?

TEAL TECHNOLOGY CONSULTING
INTEGRITY ▪ PARTNERSHIP ▪ SUCCESS

Requirement:
Administrative privileges must be assigned temporarily

Customer situation:
Customer wants an easy to use solution for JIT using MIM / PAM

Physical | Logical | Organizational

Our solution:

- The MIM / PAM End User portal does not work as expected, it's not usable
  - Option a) Develop your own custom portal
  - Option b) Use a custom PowerShell script to manage and request PAM roles
- Additional MIM learning:
  - During MIM/PAM installation TLS 1.0 and 1.1 must be allowed. After the solution is installed, TLS1.2 can be enforced again

What have we learned about logical security?

TEAL TECHNOLOGY CONSULTING
INTEGRITY ▪ PARTNERSHIP ▪ SUCCESS

Requirement :
Encrypt critical network traffic

Customer situation:
Project timeline and budget does not allow to design and built a new Tier 0 PKI

Physical | Logical | Organizational

Solution:

- Request certificates from a trusted public provider instead of installing an own PKI
- Implement certificate lifecycle process to exchange certificates after 2 years time
- In case of IPSec ensure that all certificates are signed by the same root CA or that the certificate has the IPSec OID within the template

What have we learned about organizational controls?

TEAL TECHNOLOGY CONSULTING
INTEGRITY ▪ PARTNERSHIP ▪ SUCCESS

Requirement :
Secure integrity of SW used in the environment

Customer situation:
Customer is currently downloading SW from all End User workstations without any integrity checking

Physical | Logical | Organizational

Our solution:

- Implement process to download and verify SW
- Option a): Vendor provides hash which can be compared after the software is downloaded
- Option b): If vendor does not provide a hash, download the software from two PAWs using two different internet breakouts and compare the checksum using a PowerShell script
- Exchange SW only via dedicated file shares which are cleaned-up every 24 hours

What have we learned about organizational controls?

TEAL TECHNOLOGY CONSULTING
INTEGRITY ▪ PARTNERSHIP ▪ SUCCESS

Requirement:
Operate Tier 0 systems only with internal staff

Customer situation:
Customer is organized in highly specialized teams (OS, virtualization, DBs etc.) in different departments. Engineering and operations are separated as well.

Physical | Logical | Organizational

Our solution:

- Build a cross functional team consisting of skills covering all required Tier 0 duties
- Choose solution components / products in regards to the skills of the admin team if possible (e.g. Hyper-V vs. VMWare)
- Invest in sufficient training of the Tier 0 team
- Automate as much as possible to relieve the Tier 0 team

What have we learned about organizational controls?

TEAL TECHNOLOGY CONSULTING
INTEGRITY ▪ PARTNERSHIP ▪ SUCCESS

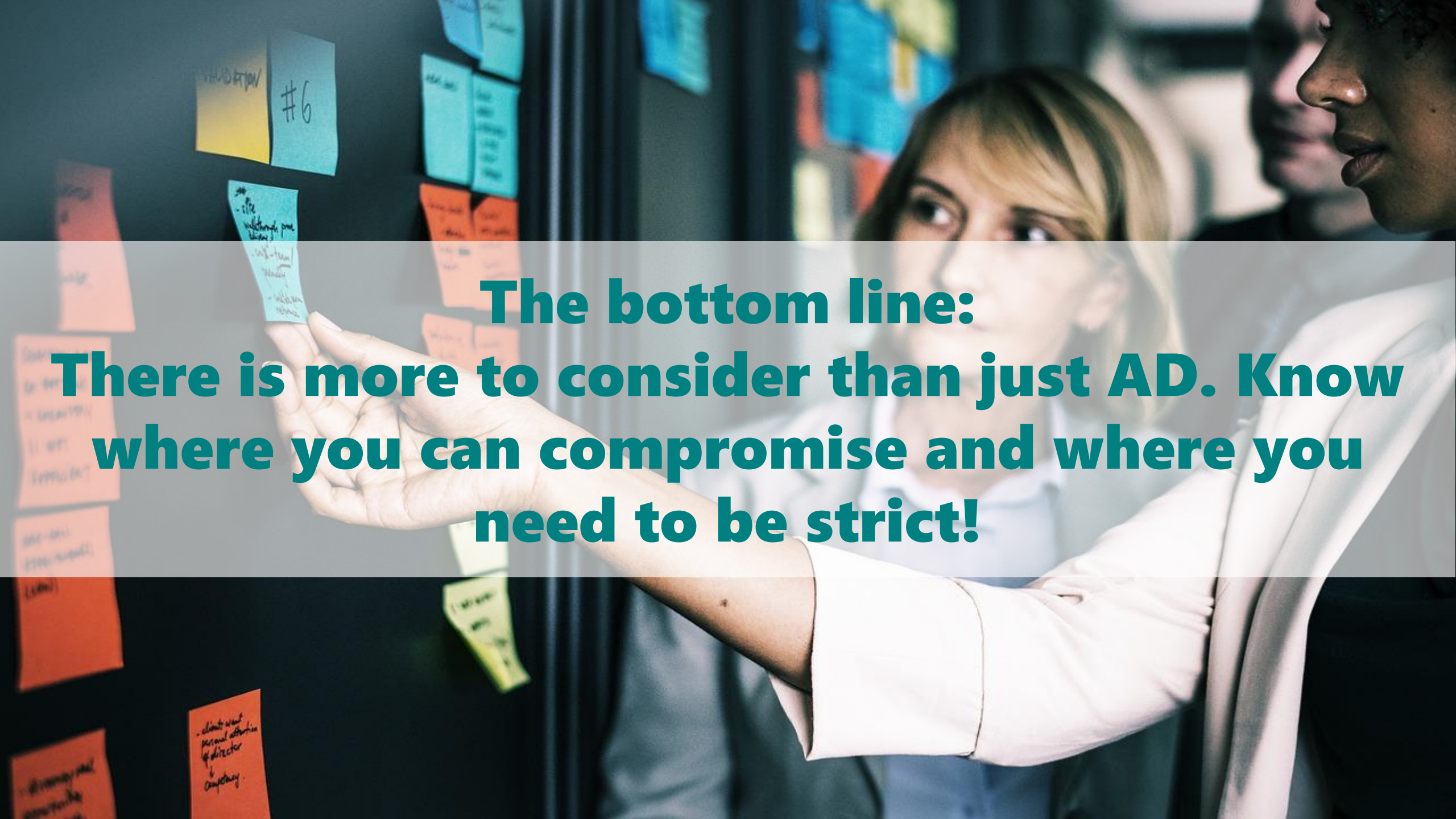
Requirement:
Keep your security measures up to date

Customer situation:
Customers think in projects. After the project the solution must be complete.

Physical | Logical | Organizational

Our solution:

- Define SPRINTs in which the Tier 0 team reviews existing procedures and introduces new security measures



The bottom line:
There is more to consider than just AD. Know where you can compromise and where you need to be strict!

Q & A