Securing your infrastructure with JEA

Miriam Wiesner

miriam.wiesner@microsoft.com
Premier Field Engineer - Secure Infrastructure

Twitter: @miriamxyra
LinkedIn: miriamwiesner
Blogs: https://miriamxyra.com
https://aka.ms/miriam

2018

Securing your infrastructure with JEA

Miriam Wiesner

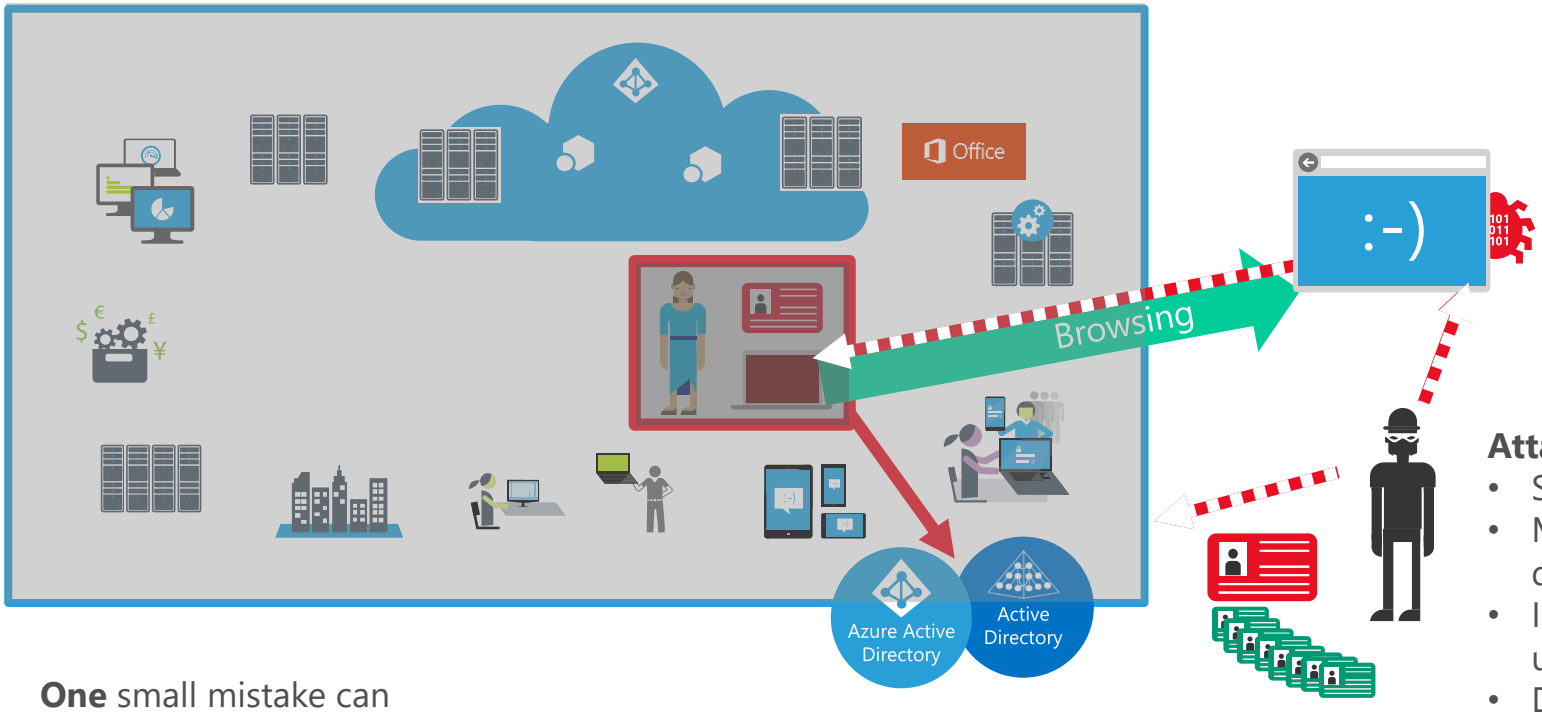
Agenda

- Current Threat Landscape
- Just Enough Administration
  - Use Cases
  - How does it work? – Demo
  - Planning for the deployment
- Risks and misconfiguration
- JEA FAQ – most common concerns
- Further mitigations besides JEA

Typical Attack Timeline & Observations

Identity is the new security "perimeter" under attack

Active Directory and Administrators control all the assets



One small mistake can lead to attacker control

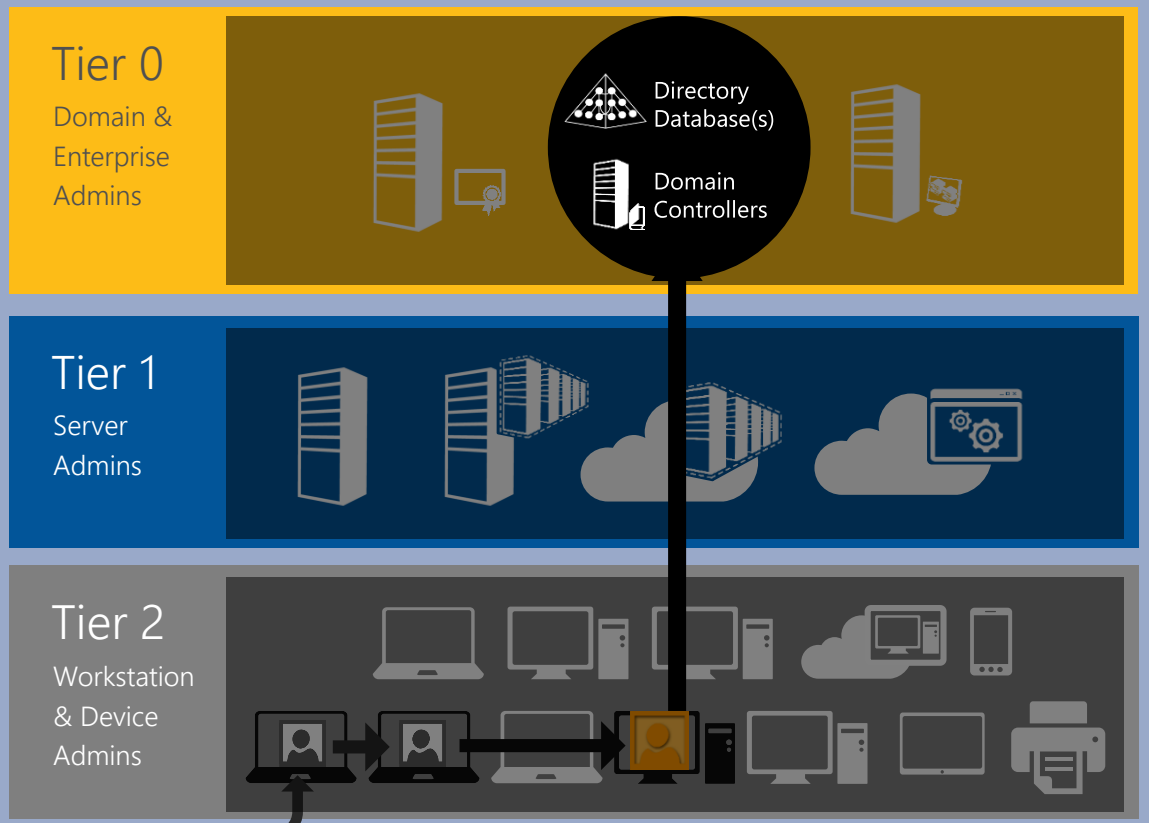
Attackers Can

- Steal any data
- Modify documents
- Impersonate users
- Disrupt business operations

Typical Attack Chain

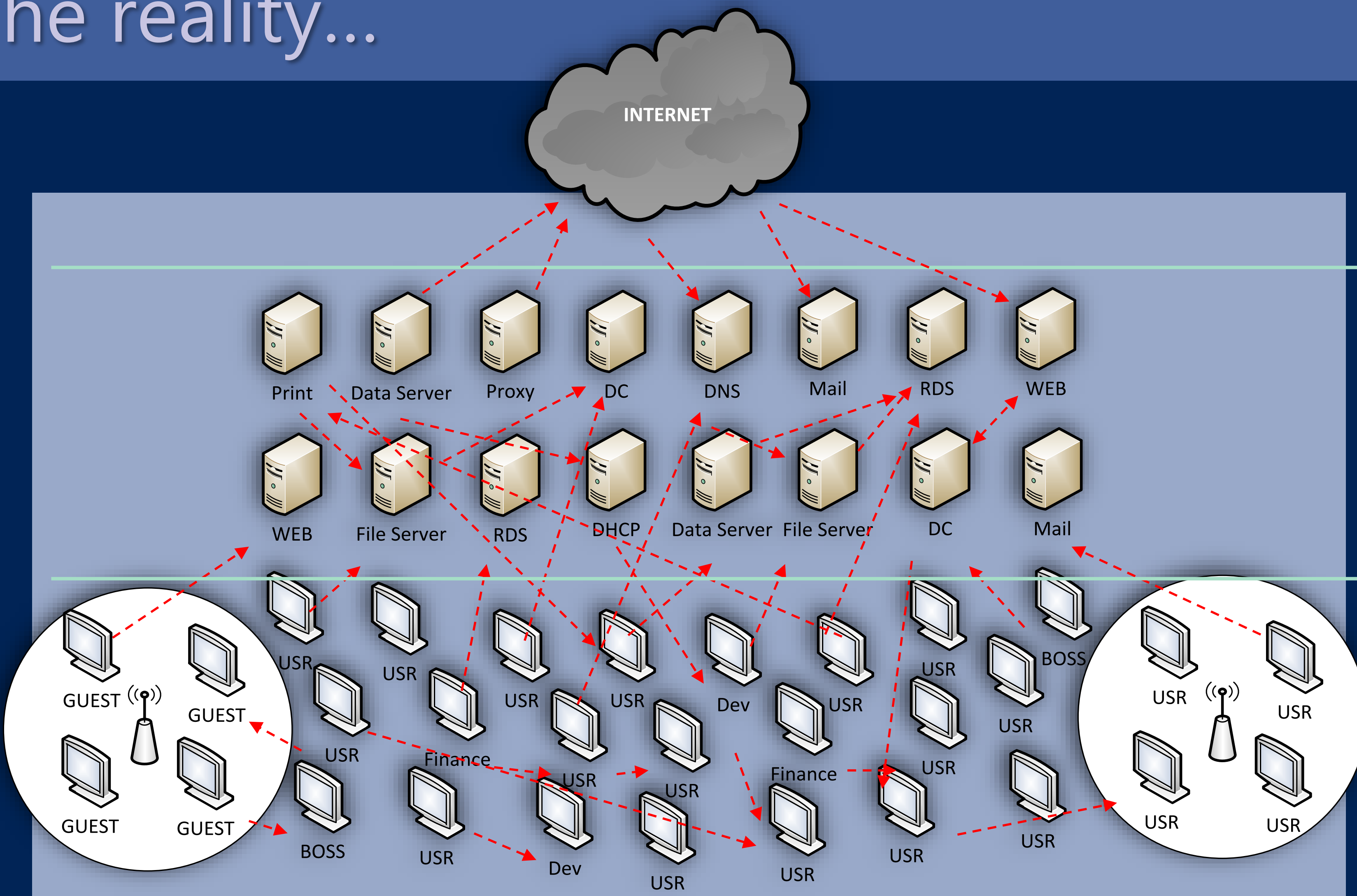
24-48 Hours

1. Beachhead (Phishing Attack, etc.)
2. Lateral Movement
   a. Steal Credentials
   b. Compromise more hosts & credentials
3. Privilege Escalation
   a. Get Domain Admin credentials
4. Execute Attacker Mission
   a. Steal data, destroy systems, etc.
   b. Persist Presence



PowerShell Conference EU 2018

The reality…

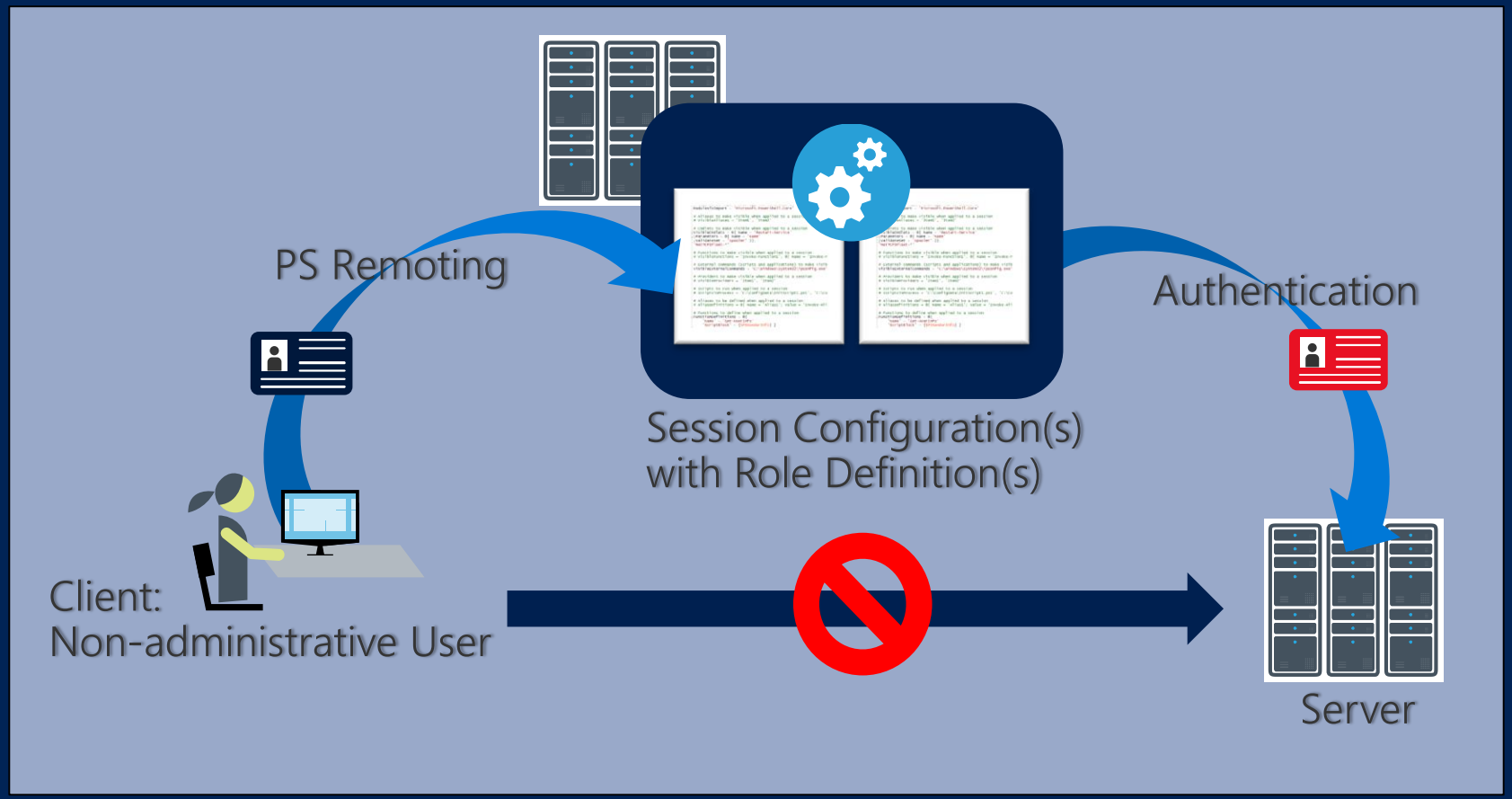



KEEP
CALM
AND
USE
JEA

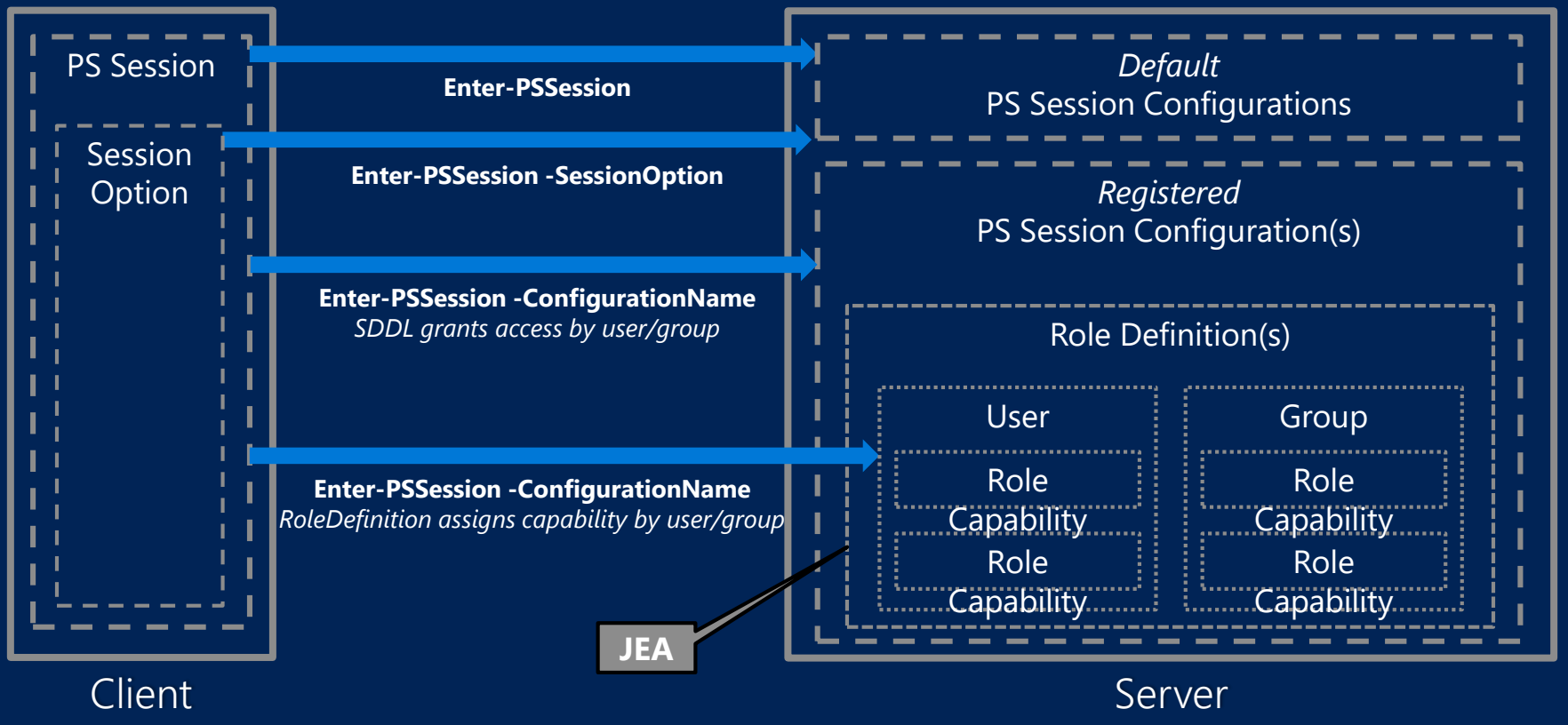
Use Cases

- High privileged operations outsourced
  - Junior Administrators
  - Supporter
  - Server Operators
- Service Accounts
- Client Help Desk
- Multi-Tenant Administration
- Auditing
- Lower trust system operations
- Securing “in-Tier” Credentials
- …and many more…

JEA functionality



Remoting Configuration Layers and JEA



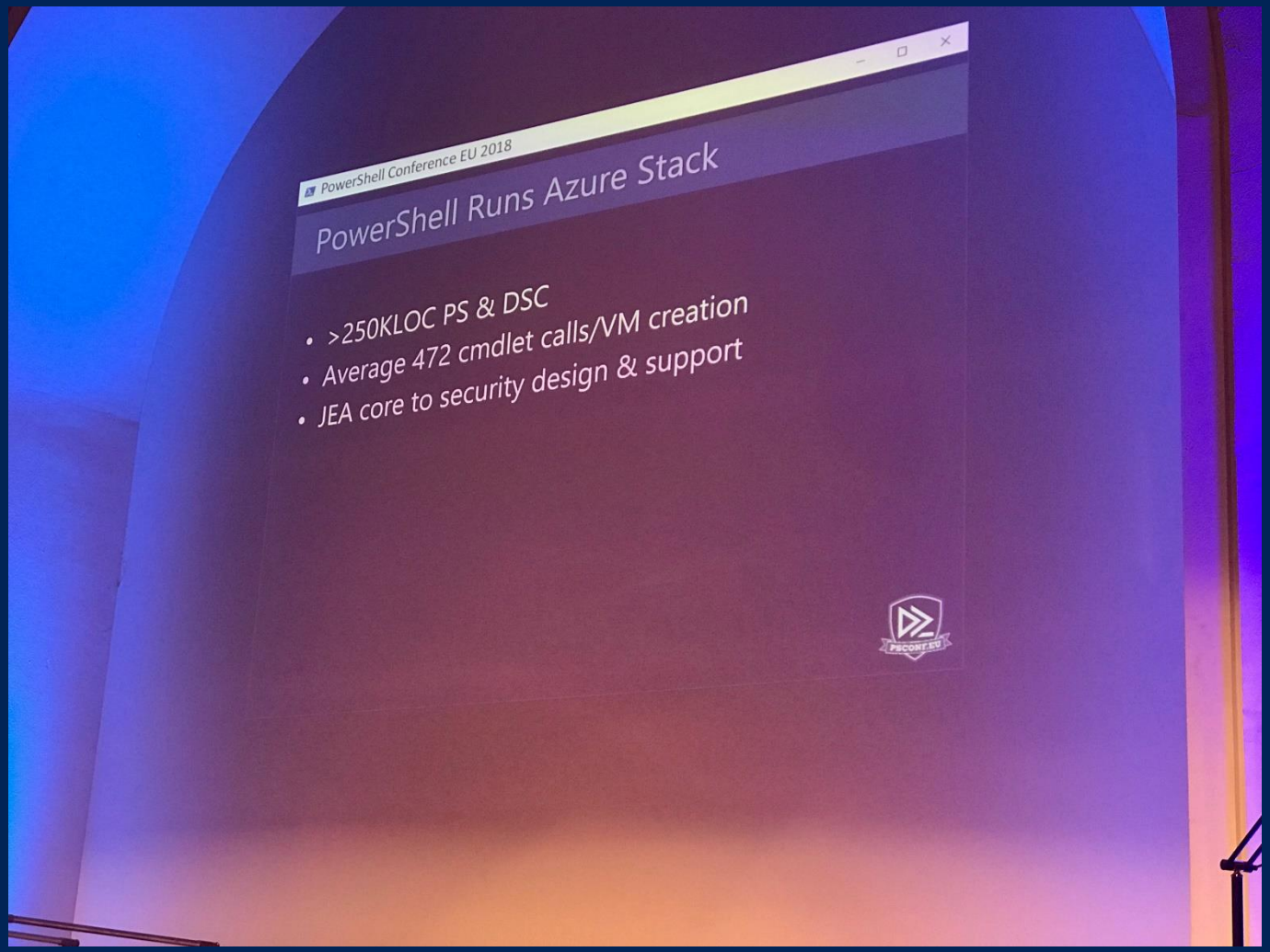
Demo

Planning for the deployment

Prerequisites

PowerShell 6 Core:
Everywhere

PowerShell Runs Azure Stack



How to deploy JEA

Identify and Define

Session Capability File

- Identify users & groups
- Identify the commands used

Restrict

Role Capability File

- Restrict the scope of Cmdlets
- Create custom functions

Deploy

- Syntax Check: session conf file
- Deploy via DSC

Test and Correct

Risks and misconfiguration

Risks of misconfiguration

- Granting the connecting user admin privileges to bypass JEA
  - `PS> Add-LocalGroupMember -Member 'CONTOSO\jdoe' -Group 'Administrators'`
  - `Add-ADGroupMember, Add-LocalGroupMember, net.exe, dsadd.exe`
- Running arbitrary code, such as malware, exploits, or custom scripts to bypass protections
  - `PS> Start-Process -FilePath '\\san\share\malware.exe'`
  - `Start-Process, New-Service, Invoke-Item, Invoke-WmiMethod, Invoke-CimMethod, Invoke-Expression, Invoke-Command, New-ScheduledTask, Register-ScheduledJob`
- Wildcard configuration is evil
- Be careful when using the JEA helper tool

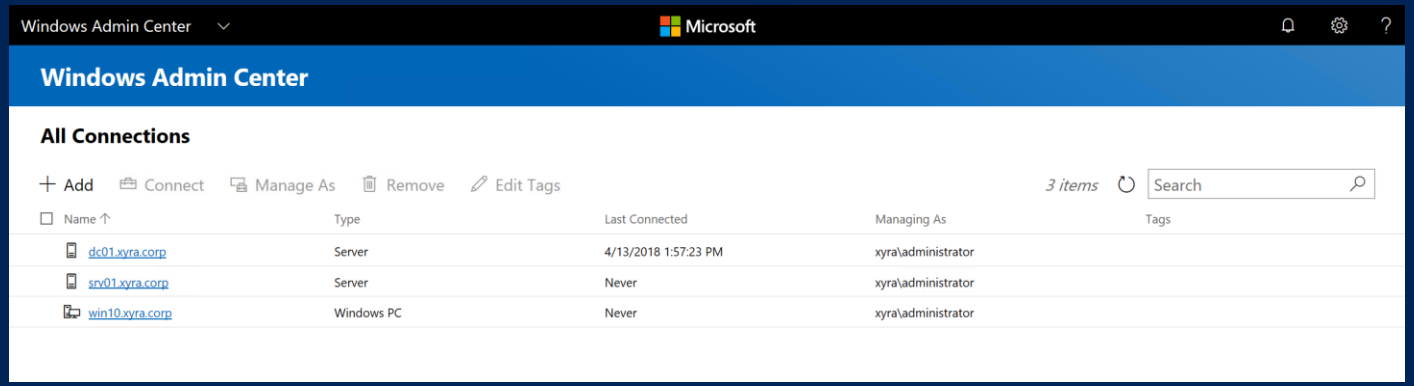
Securing your configuration

- Use **signing** to protect role capability files from tampering.
- **Secure** transcript files and event logs following the guidance in the blog post "PowerShell ♥ the Blue Team".

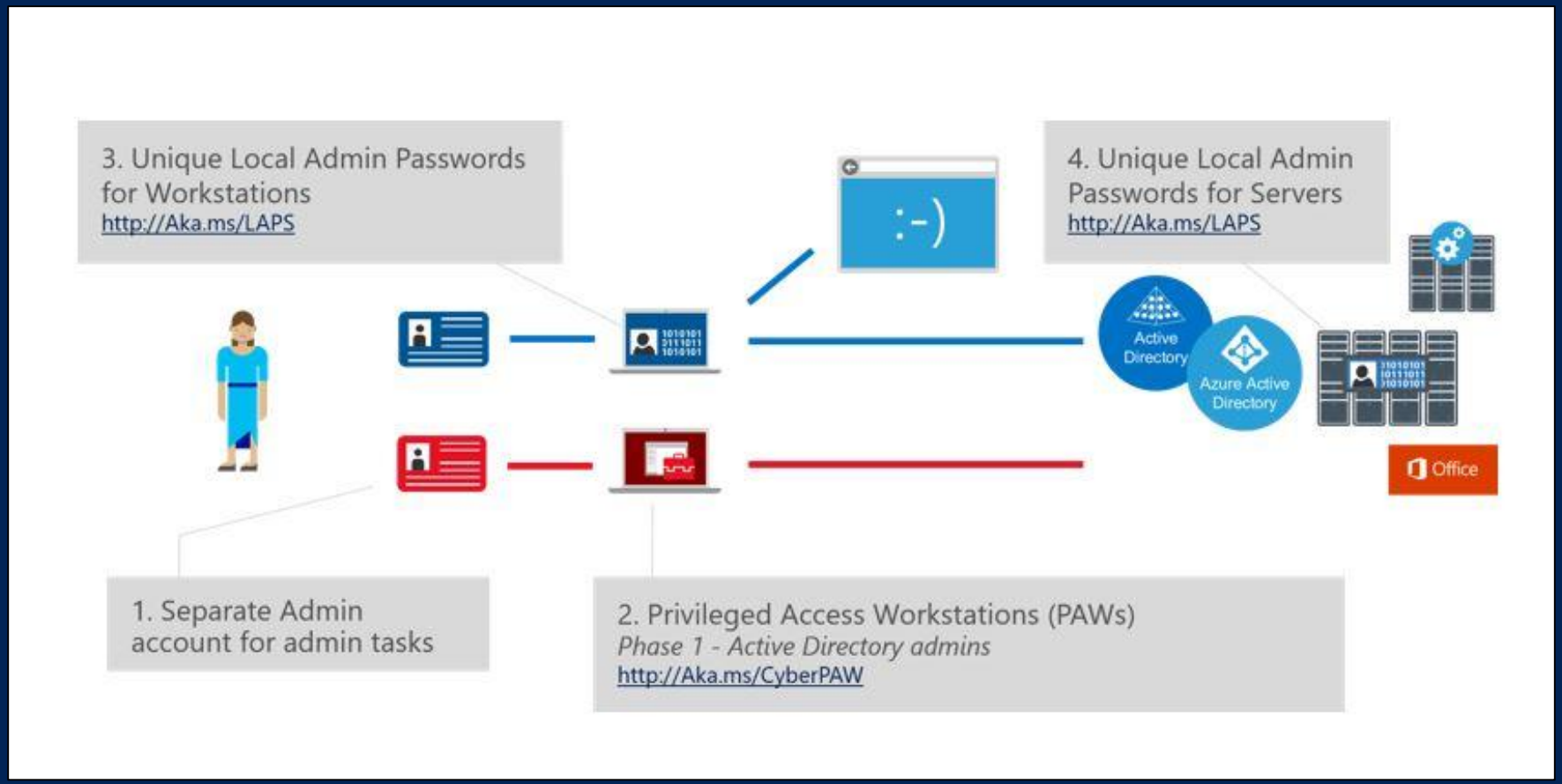
None of this matters if you do not take away admin rights and remote desktop access to the servers!

Most common concerns about JEA

- Oh, it's difficult to implement
  - Yes it is, but we are working on it
  - Feel free to submit your role template configs
- ...is there a GUI?
  - Windows Admin Center (formerly Project Honolulu)

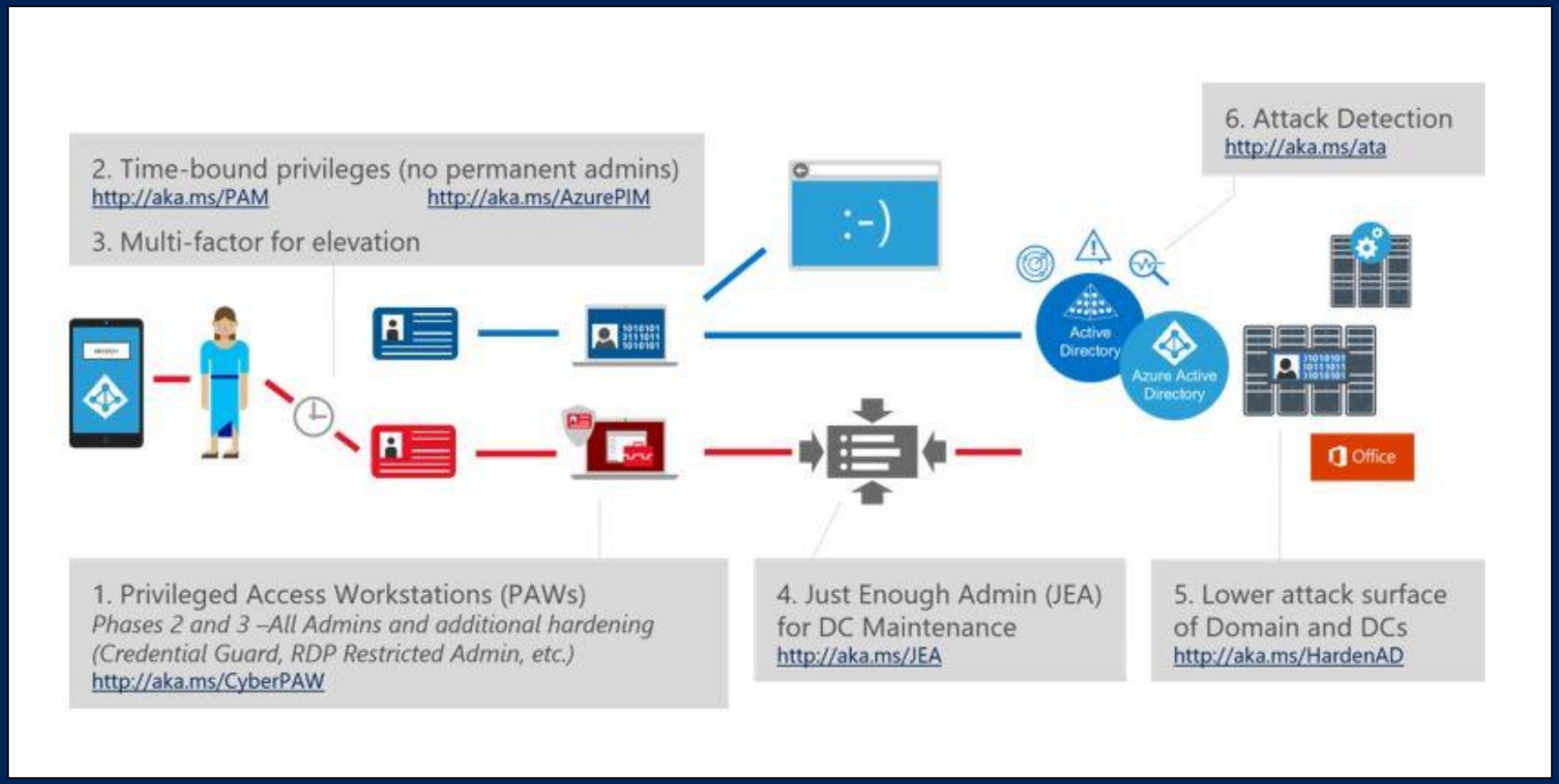


Further Security Mitigations – Step 1



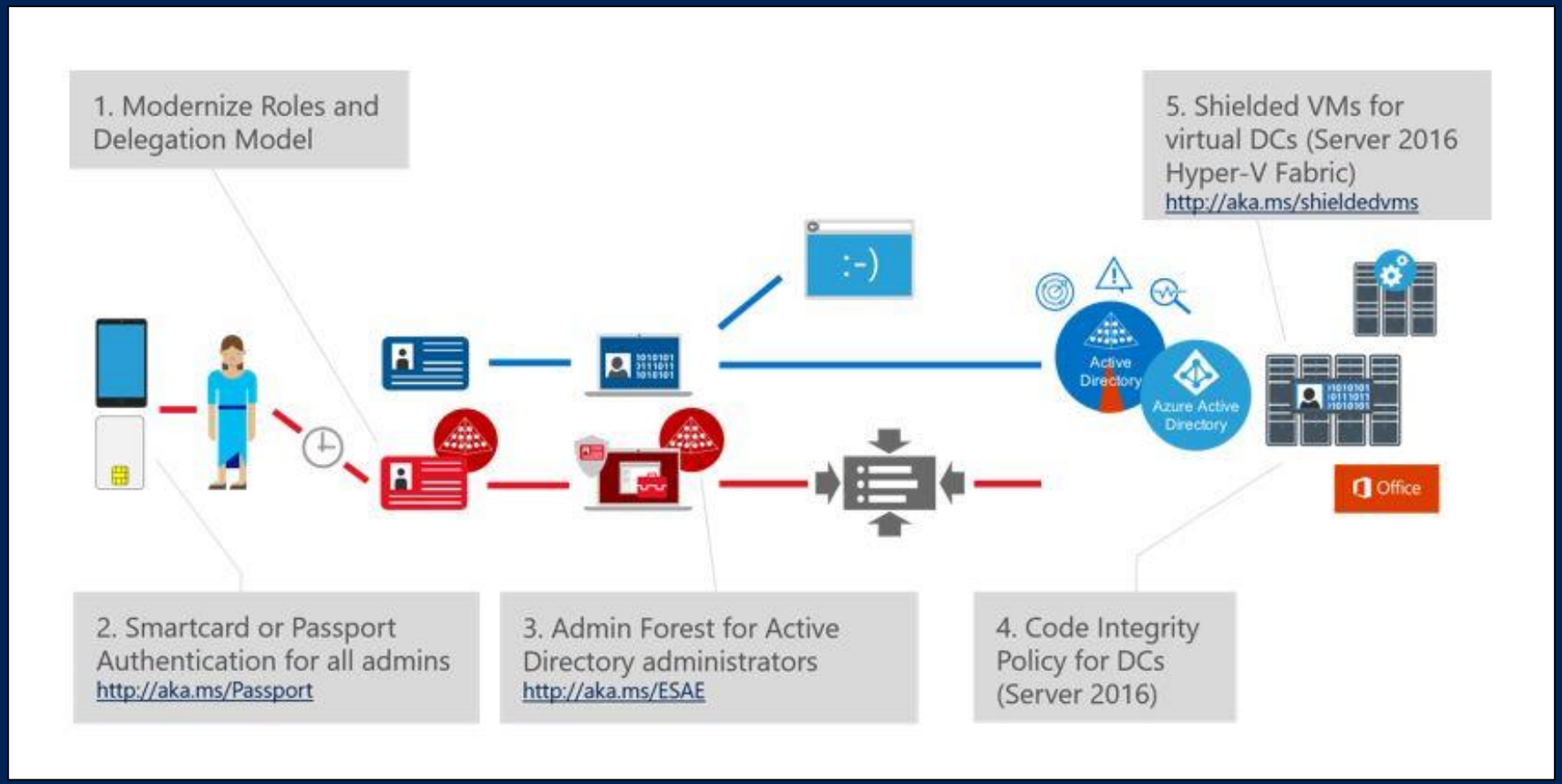
Securing privileged access: http://aka.ms/privsec

Further Security Mitigations – Step 2



Securing privileged access: http://aka.ms/privsec

Further Security Mitigations – Step 3



Securing privileged access: http://aka.ms/privsec

Summary

- JEA helps you securing your environment – but do not use JEA as your only security barrier
- Also secure the usage of non-administrators having „JEA delegated“ rights
- Check carefully if the configured commands allow privilege escalation
- Secure your important files (JEA config files, transcripts, scripts, …) from tampering
- None of this matters if you do not take away admin rights and remote desktop access to the servers!

Next Steps

- Now: 15 min break

- Grab a coffee
- Stay here to enjoy next presentation
- Change track and switch to another room

- Ask me questions or meet me in a breakout session room afterwards

Questions?