

AVANTech-Day 2026



IT-Security Deep Dive



AVANTech-Day 2026



Automatisierung von Sicherheitslösungen gezeigt an BeyondTrust PRA

Michael Brändli

Security Engineer,
AVANTEC



AVANTech-Day 2026



...seit Juni 2019 bei der **AVANTEC AG** (FLS Team)

...seit Mai 2023 im **PAM & Access Security Team**

Michael Brändli

Security Engineer,
AVANTEC



Inhalt

- Die Reise
- Kurze Einführung BeyondTrust PRA
- Zu konfigurierende Komponenten
 - Mögliches Problem
- Automatisierung
- Demo
- Kunden Case – Viega (Dominic Welsch)
- Q&A

Die Reise



Kurze Einführung PRA

Privileged Remote Access

 **BeyondTrust**
Platform



CLOUD | HYBRID | ON-PREMISES | OT

Kurze Einführung PRA

Privileged Remote Access



Privileged Remote Access



Remote Support

Kurze Einführung PRA

Privileged Remote Access

Interne IT

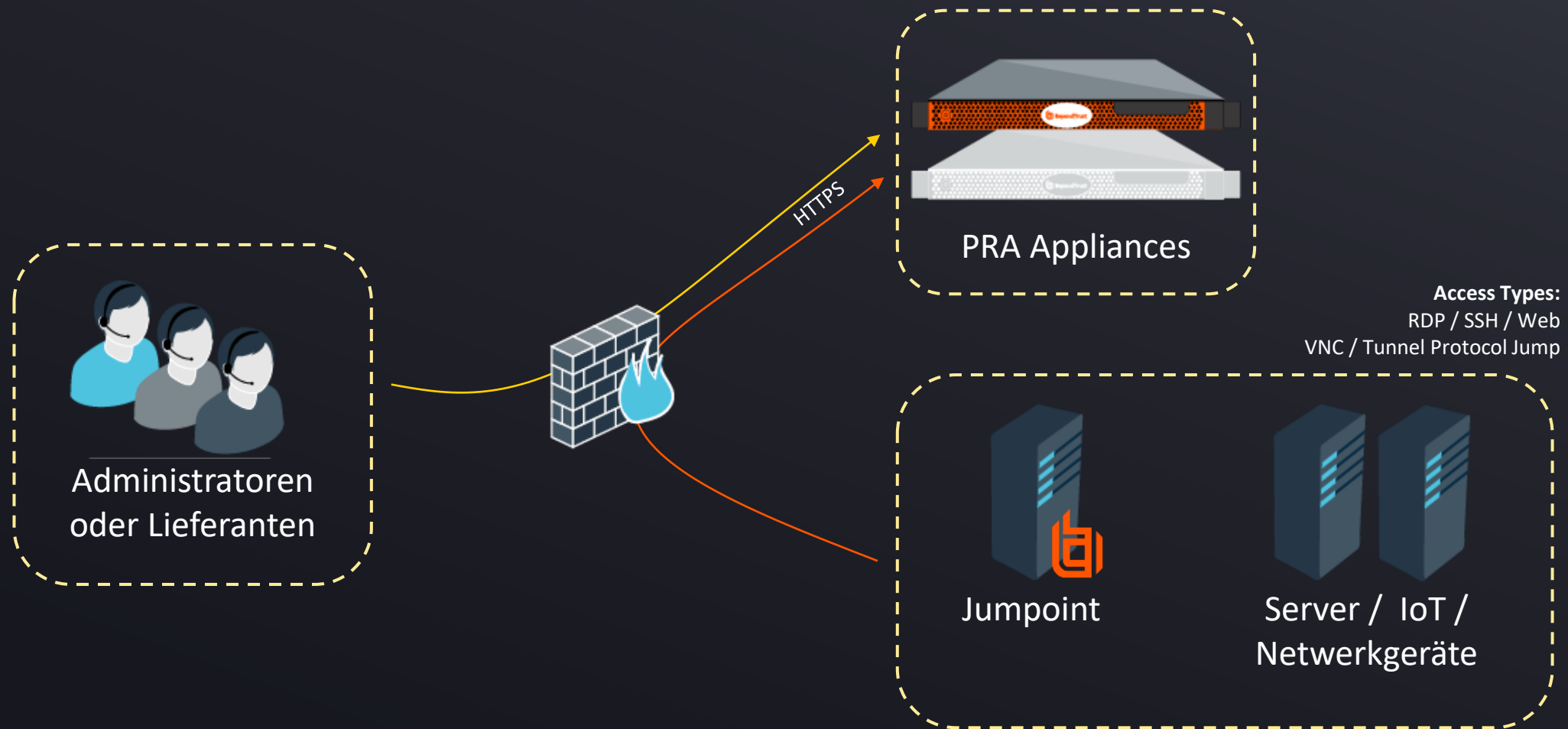


Lieferanten



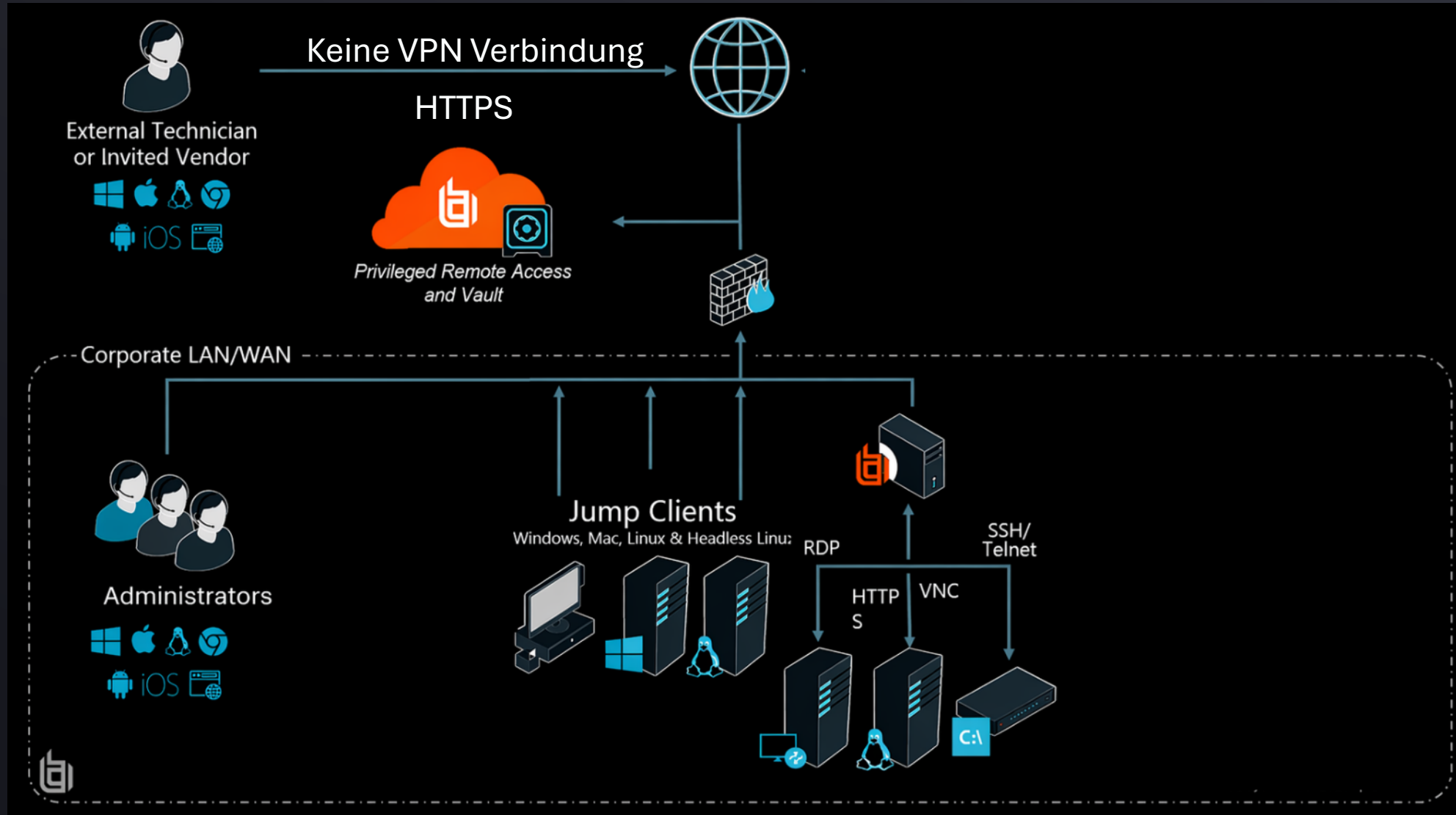
Kurze Einführung PRA

Privileged Remote Access



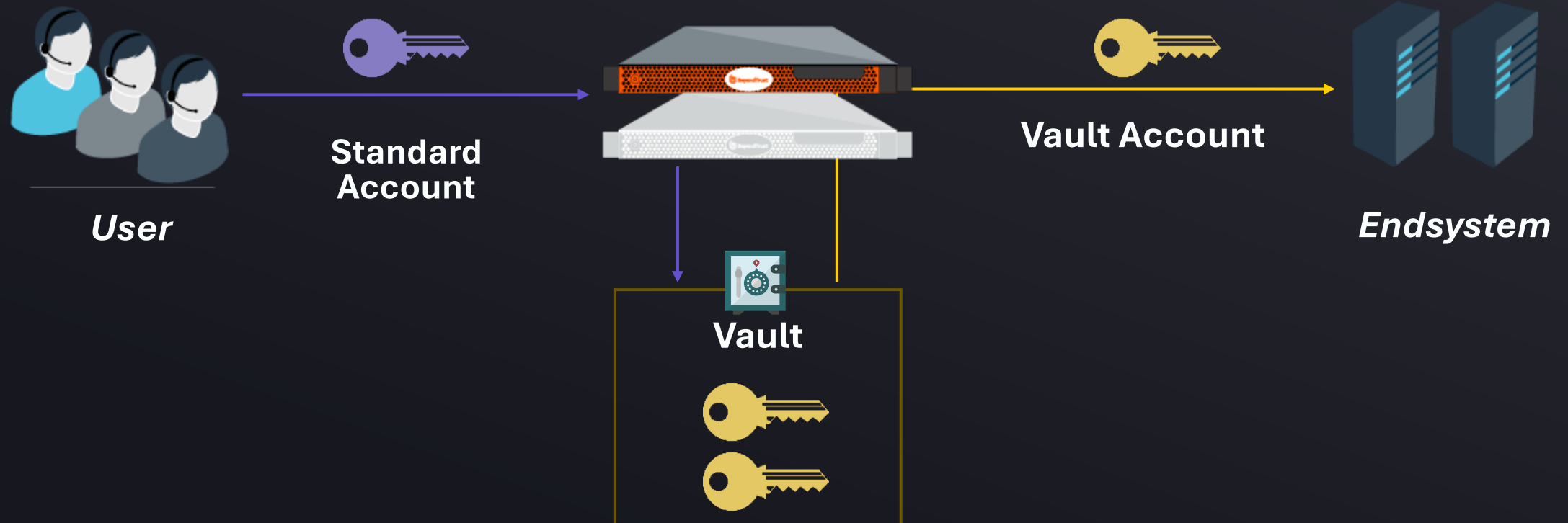
Kurze Einführung PRA

Privileged Remote Access



Kurze Einführung PRA

Privileged Remote Access - Accountwechsel



Zu konfigurierende Komponenten

Einmalig

Was	Beschreibung
Date & Time	Zeit & Datum
Access Session Logging Settings	Recording der Access Sessions
Jump Client Installer	MSI für Jump Client Installation
Jumpoint (Gateway)	Installation Jumpoint(s)
Domain Onboarding	Anbinden von On-Prem AD / EntraID
Email Configuration	Versand von Mails (Session Invite, System Info...)
Site Configuration	Mind. Passwortlänge, Standard IdP. ...

Zu konfigurierende Komponenten

Wiederkehrend pro User / Endsystem / Zugriff

Was	Beschreibung
(Erstellung & Zuweisung) User	Anlegen der Standard User
(Erstellung & Zuweisung) Teams	Teams-Funktionalität (Member, Lead, Manager)
(Erstellung & Zuweisung) Jump Client / Jump Item	Anbindung Endsystem
(Erstellung & Zuweisung) Jump Groups	Logische Sortierung der Endsysteme Berechtigten auf Endsysteme
(Erstellung & Zuweisung) Jump Policy	Berechtigungen, bevor eine Session startet
(Erstellung & Zuweisung) Session Policy	Berechtigungen während einer Session
(Onboarding & Zuweisung) Vault Account	Vault Account für Zugriff auf das Endsystem
(Erstellung & Zuweisung) Group Policy	Zentraler Ort für Zuweisung der Berechtigungen

Zu konfigurierende Komponenten



Automatisierung?



Automatisierung

- Alle Informationen stehen (bereits) im AD / EntraID
- Allgemeine Security Group für Provisionierung auf PAM-Lösung
- Zuweisung von User zu Endsystemen über Security Groups
- Ableiten von Standard Account auf Vault Account
 - max_muester@mbr.lab -> adm_max_muester@mbr.lab
- Attribute für
 - Internal / External
 - Team: Member / Lead / Manager

Ziel: Alle zu konfigurierenden Info's müssen irgendwo stehen 😊

Automatisierung

Max Muster Properties

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile		COM+
General	Address	Account	Profile
	Telephones	Organization	

Max Muster

First name: Max Initials: MM

Last name: Muster

Display name: Max Muster

Description:

Office: Internal

Telephone number: Other...

E-mail: Other...

Web page: Other...

OK Cancel Apply Help

Max Muster Properties

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile		COM+
General	Address	Account	Profile
	Telephones	Organization	

User logon name: muster @mbr.lab

User logon name (pre-Windows 2000): MBR\muster

Logon Hours... Log On To...

Unlock account

Account options:

- User must change password at next logon
- User cannot change password
- Password never expires
- Store password using reversible encryption

Account expires:

Never

End of: Freitag .22. Mai 2026

OK Cancel Apply Help

ADM Muster Properties

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile		COM+
General	Address	Account	Profile
	Telephones	Organization	

User logon name: adm_muster @mbr.lab

User logon name (pre-Windows 2000): MBR\adm_muster

Logon Hours... Log On To...

Unlock account

Account options:

- User must change password at next logon
- User cannot change password
- Password never expires
- Store password using reversible encryption

Account expires:

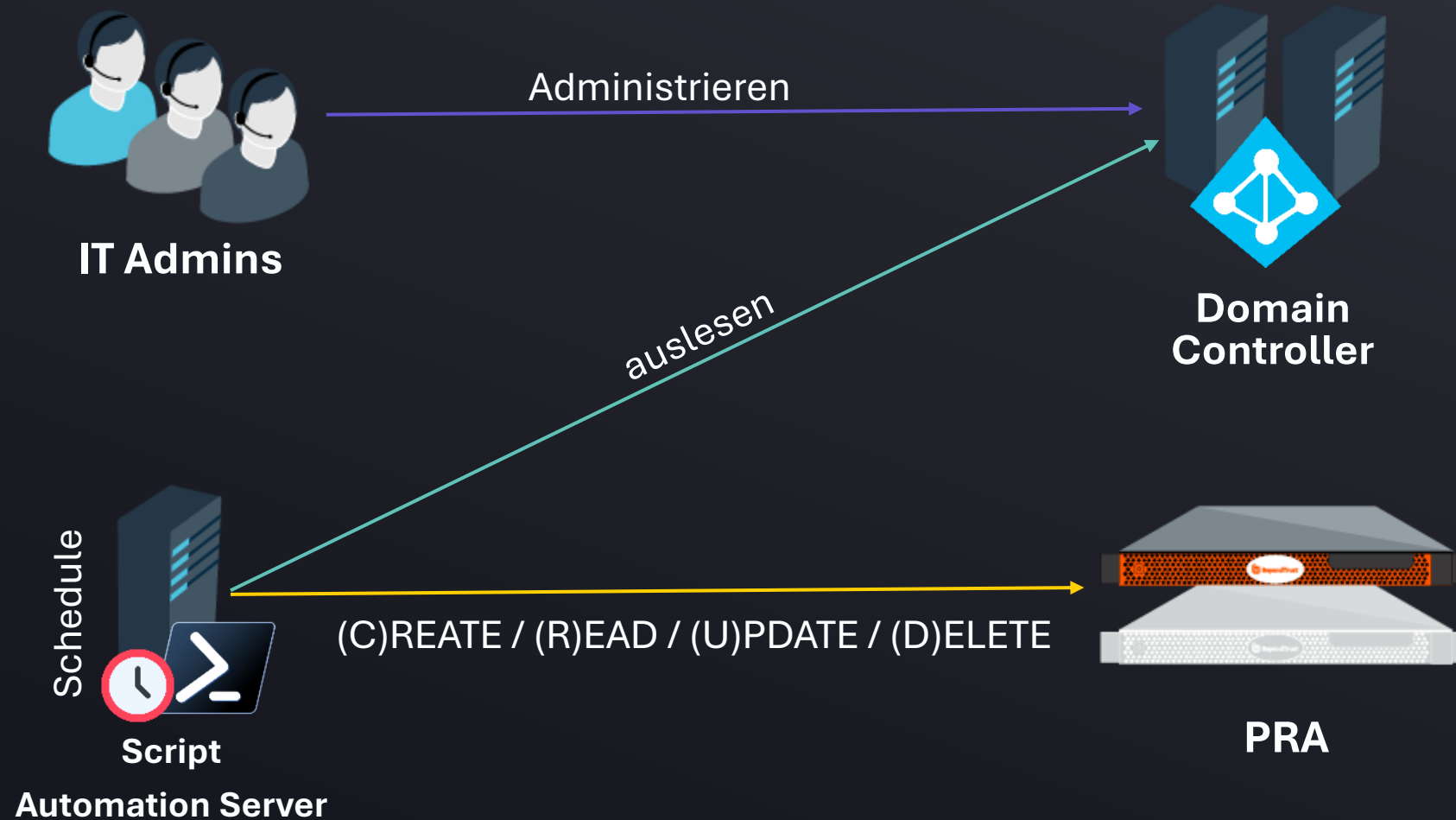
Never

End of: Freitag .22. Mai 2026

OK Cancel Apply Help

Name	Type	Description
SCRIPT	Security Group - Global	
g.pra.users	Security Group - Global	General PAM Provisioning Group
DC	Security Group - Global	

Automatisierung



SRA PS Module

Was ist das?

- Custom PowerShell Module von AVANTEC
- Wiederverwendbares Paket
 - Funktionen
 - Cmdlets
 - Variablen
- (Fast) ganze SRA API abgebildet



SRA PS Module

Was ist das?

Overview

Jump Clients

Jump Items

Jump Groups

Jumpoints

Jump Policy

Teams

Users

Session Policies

Group Policies

Security Providers

Vault Account

Vault Endpoint

Vault Account Group

Vault Account Policy

Vendors

Endpoint Automation

Miscellaneous

BeyondTrust Privileged Remote Access

Configuration APIs

Configuration API Version:
1.12

Base URL:
https://pra.test.avantec.ch/api/config/v1

Overview

The BeyondTrust Privileged Remote Access Configuration APIs provide a way to programmatically configure the system.

Authentication

The BeyondTrust Privileged Remote Access Configuration APIs require OAuth 2 credentials for authentication. The **API Configuration** page. The account must have permission to access the Configuration API. Copy the client ID and secret to be generated using this client ID and secret and then submitted with each API request.

NOTE: The **OAuth Client Secret** cannot be viewed again after the API Account has been saved, saving the account immediately invalidates any OAuth tokens associated with the account. Any new tokens generated will require the new client secret.

Create a token

Create a token by sending an HTTP POST request to the URL of your BeyondTrust Privileged Remote Access Configuration API.

```
https://pra.test.avantec.ch/oauth2/token
```

The OAuth client ID and client secret associated with the API account should be Base64 encoded and included in the request headers.

```
Authorization: Basic <base64-encoded "client_id:secret">
```

Include the following POST body in the request:

PAM-AS / BeyondTrust PRA / SRA-PS-Module

Files

Search files (*.vue, *.rb...)

Classes

adding vault account to group policy added
Michael Brändli authored 1 week ago

Name	Last commit	Last update
Authentication.ps1	Object conversion 2.0 -> faster object processing	6 months ago
EndpointAutomation.ps1	endpoint automation implemented	3 months ago
GroupPolicy.ps1	adding vault account to group policy added	1 week ago
JumpGroup.ps1	Object conversion 2.0 -> faster object processing	6 months ago
JumpItem.ps1	Pester test 2.0	2 months ago
JumpPolicy.ps1	Object conversion 2.0 -> faster object processing	6 months ago
Jumpoint.ps1	improve getnode issues with jumpoints	2 months ago
PublicPortal.ps1	Object conversion 2.0 -> faster object processing	6 months ago
RepStatus.ps1	Object conversion 2.0 -> faster object processing	6 months ago
SecurityProvider.ps1	Object conversion 2.0 -> faster object processing	6 months ago
SessionPolicy.ps1	Object conversion 2.0 -> faster object processing	6 months ago
Team.ps1	Object conversion 2.0 -> faster object processing	6 months ago
User.ps1	Object conversion 2.0 -> faster object processing	6 months ago
Utils.ps1	improve auth flow	2 months ago
VaultAccount.ps1	vaultaccount improvements	2 months ago
VaultAccountGroup.ps1	Pester test 2.0	2 months ago
VaultAccountPolicy.ps1	Object conversion 2.0 -> faster object processing	6 months ago
VaultEndpoint.ps1	Object conversion 2.0 -> faster object processing	6 months ago
Vendor.ps1	Object conversion 2.0 -> faster object processing	6 months ago

SRA PS Module

Was ist das?

```
PS C:\Script> Import-Module .\sra-ps\  
PS C:\Script> Get-Module
```

ModuleType	Version	PreRelease	Name	ExportedCommands
Manifest	1.0.1.0		ActiveDirectory	{Add-ADCentralAccessPolicyMember, Add-ADComputerServiceAccount, Add-ADDomainControllerPass...
Manifest	7.0.0.0		Microsoft.PowerShell.Management	{Add-Content, Clear-Content, Clear-Item, Clear-ItemProperty...}
Manifest	7.0.0.0		Microsoft.PowerShell.Security	{ConvertFrom-SecureString, ConvertTo-SecureString, Get-Acl, Get-AuthenticodeSignature...}
Manifest	7.0.0.0		Microsoft.PowerShell.Utility	{Add-Member, Add-Type, Clear-Variable, Compare-Object...}
Script	2.4.5		PSReadLine	{Get-PSReadLineKeyHandler, Get-PSReadLineOption, Remove-PSReadLineKeyHandler, Set-PSReadLi...
Script	0.0.3		sra-ps	{Get-EndpointAutomationEndpoint, Get-EndpointAutomationJob, Get-EndpointAutomationJobExecu...

```
PS C:\Script> Get-GroupPolicy -All
```

```
id : 1  
name : PRA - Auditor - Direct  
perm_access_allowed : False  
access_perm_status : not_defined  
perm_share_other_team : False  
perm_invite_external_user : False  
perm_session_idle_timeout : -1  
perm_extended_availability_mode_allowed : False  
perm_edit_external_key : False  
perm_collaborate : False  
perm_collaborate_control : False  
perm_jump_client : False
```

The screenshot shows the BeyondTrust Privileged Remote Access console. The left sidebar contains navigation options like Status, Consoles & Downloads, My Account, Configuration, Jump, Vault, Console Settings, Users & Security (highlighted), Reports, Localization, and Management. The main area is titled 'Users & Security' and has tabs for Users, Access Invite, Security Providers, Vendors, Session Policies, Group Policies (selected), and Kerberos Keytab. Below the tabs are 'Cancel' and 'Save' buttons. The 'Edit Policy' section shows 'Policy Name' as 'PRA - Auditor - Direct'. Under 'Available Members', 'Local' is selected as the 'Security Provider' and 'Admin (admin)' is listed. The 'Policy Members' section has a search bar and 'Add', 'Remove', and 'Remove All' buttons.

SRA PS Module

Warum? PowerShell <-> AD Integration



Active Directory

SRA PS Module

Warum? – Pagination



SRA PS Module

Warum? – Anzahl Zeilen Code

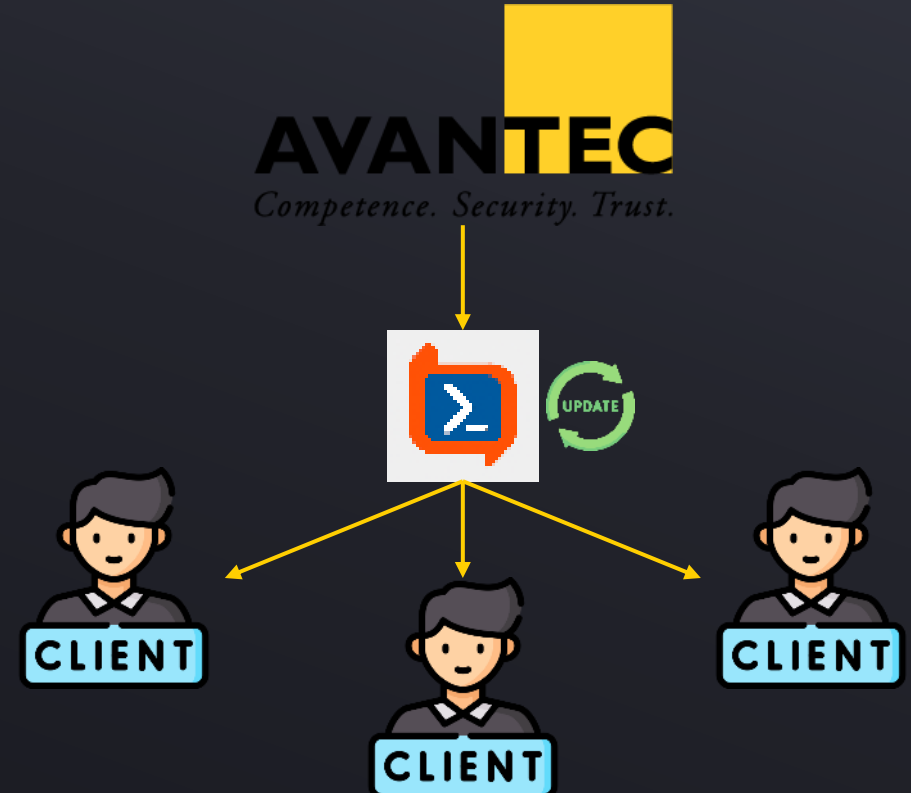
```
1 # Get all Group Policies from PRA
2 $GroupPolicies_PRA_Current_State = @()
3 #Pagination, get last page for response
4 $URL = 'https://' + $ApplianceURL + '/api/config/v1/group-policy'
5 try {
6     $AllGPFfromPRA = Invoke-WebRequest $URL -Method 'GET' -Headers $headers -UseBasicParsing
7 } catch {
8     $_ | Out-File -FilePath $ErrorLog -Append
9 }
10 $LastPage = [int]$AllGPFfromPRA.Headers["X-BT-Pagination-Last-Page"][0]
11
12 # Get all the Group Policies from PRA and save them in $GroupPolicies_PRA_Current_State
13 for ($counter = 1; $counter -le $LastPage; $counter++)
14 {
15     $URL = 'https://' + $ApplianceURL + '/api/config/v1/group-policy?per_page=100&current_page=' + $counter + ''
16     try {
17         $response = Invoke-RestMethod $URL -Method 'GET' -Headers $headers
18     } catch {
19         $_ | Out-File -FilePath $ErrorLog -Append
20         Write-Host "$(Get-Date) Error occurred while retrieving group policies from PRA" -ForegroundColor Red
21         "Error occurred while retrieving group policies from PRA" | Out-File -FilePath $ErrorLog -Append
22         exit
23     }
24     $response | ForEach-Object {
25         $GroupPolicies_PRA_Current_State += $_
26     }
27 }
```



```
PS C:\Script> Get-GroupPolicy -All
id
name
perm_access_allowed
```

SRA PS Module

Warum? – Hersteller Update



SRA PS Module

Warum? – Verschlüsselung der Secrets

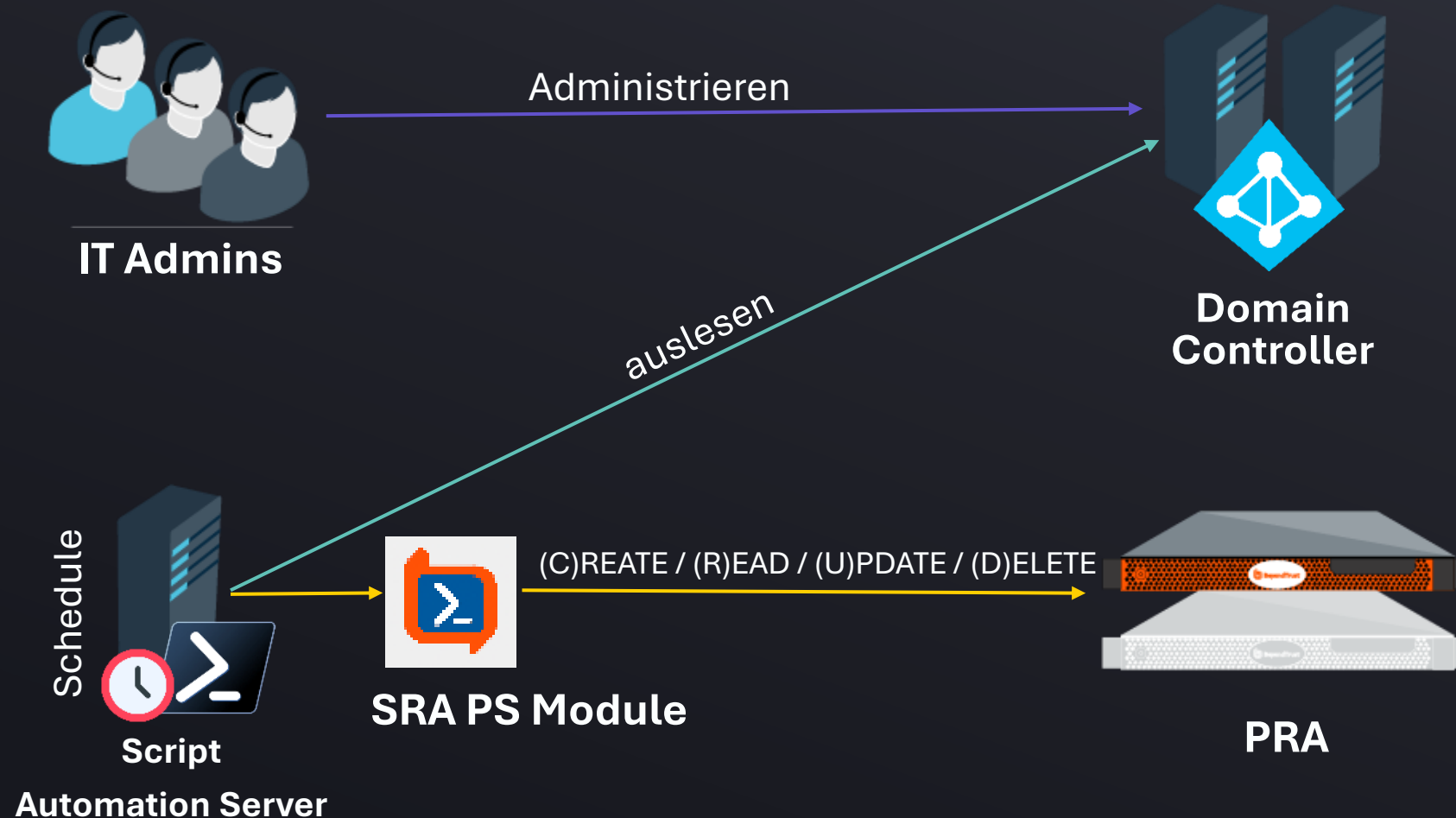
```
$Base64AuthString = [Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes("${ClientId}:${ClientSecret}"))
```

```
$SecureAuth = ConvertTo-SecureString -String $Base64AuthString
```



```
sra_api_key.txt - Notepad
File Edit Format View Help
This key can only be used by the user (Administrator) and computer(SCRIP), which created it was created on. This is the
encrypted
key:0100000d08c9ddf0115d1118c7a00c04fc297eb01000000e94ba82b865acf46b3da437b60c50ec0000000002000000000106600000001000020
00000034d955bfc63de2411af96285e006e80e04339b722fe9a87e8bb8c05fe23824bd00000000e80000000020000200000009989af8197d13fe2780f
8d84ecccf7fa6ce3a0e7697f6db19ea8e9840ee75fc5f0000000e0a33f480fbc2e1ae728117d12c9275764f24b73bc7ccae674859c2222048c68f59753
1bbea655aa7d8f6c08905299a40065e14ed8b2439f9bc147de237670a48cf4159b5301d1f166722f0ea10cf596d5040889da843994f39dea0fe0836a28
fa0db63a0b3f5a5b588f3ca8456fda33f2143c34874371acfbf84583fb6dc7d6ed77799ee8bdf7cefad9ace5bfe40f51d9a56c7512de234c14eb69a4b3
bc587e3b232e261aabf87c9cae12421830a29007f6561270255ece8c1bedca545fd6cc3dd2bae9d639650936c3f0209fe5d37d427c50383da620229909
8c6bfea401a5d56ef9adc26631fefa643275fa5434cf400000005e78be574bf1a81ae1303f08c7cd908776a77e520f1c6b7b723fe96781e90394654617
1c37cca1c373248a809eeeeaf049fb1805ca830f4c7fba7d01c9e0b52c
```

Automatisierung mit SRA PS Module

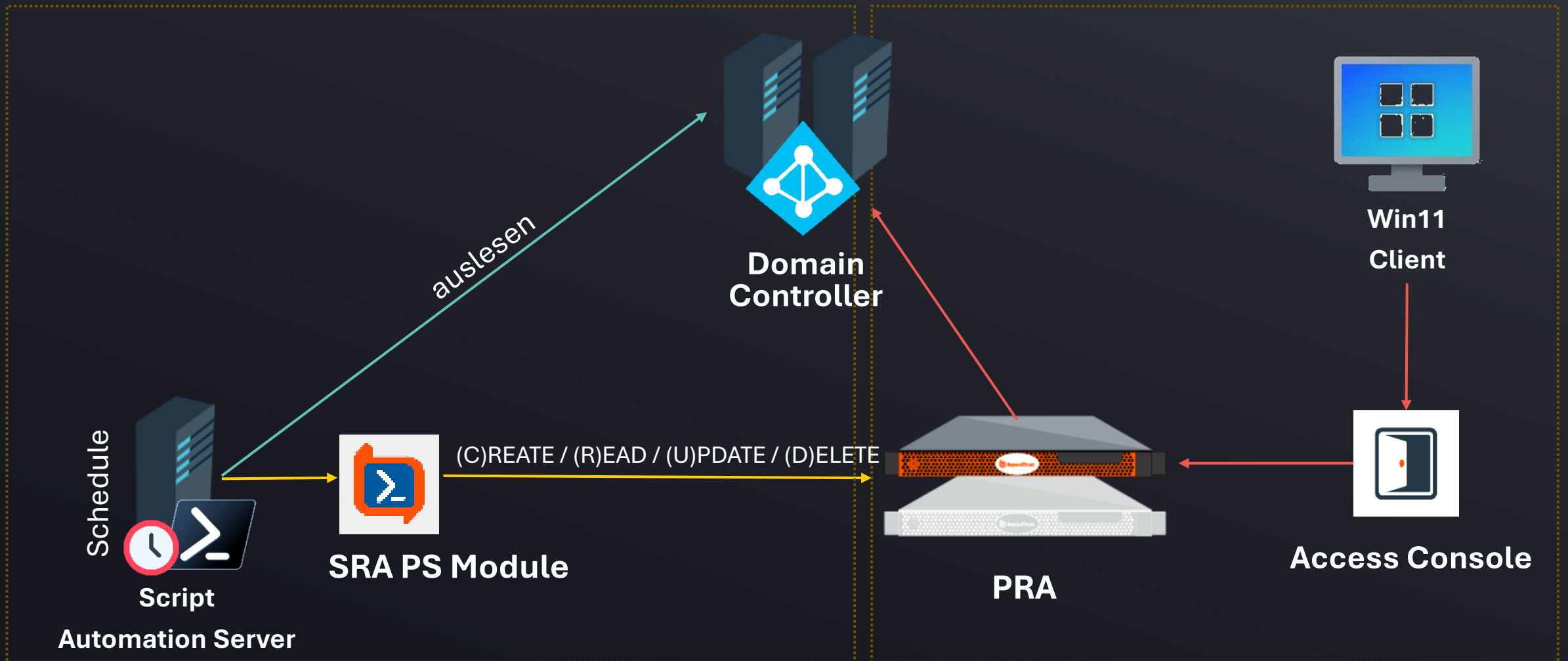




DEMO

DEMO

Aufbau



AVANTech-Day 2026



Dominic Welsch

IT Team Lead Network & Security
Viega



Viega - TBD

Kunden Case

- TEIL DOMINIC WELSCH



Viega – was wurde automatisiert?

Kunden Case

- Provisionierung von User & Gruppen – SCIM
- Erstellung und Zuweisung von:
 - Endsystemen (Jump Items)
 - Jump Policy & Session Policy
 - Group Policies
- Differenzierung zwischen internen und externen Mitarbeiter
 - Andere Jump & Session Policy

The logo for Viega, featuring the word "viega" in a bold, lowercase, sans-serif font. The text is white and is set against a black rectangular background.

Viega – ein paar Zahlen

Kunden Case

Was?	EMEA	US	<u>Total</u>
Users	220	30	<u>250</u>
Jump Items / Jump Groups	390	227	<u>617</u>
Group Policies	1506	344	<u>1850</u>



Stand: 05.05.2026

GIBT ES NOCH FRAGEN?



**BESTEN DANK
FÜR IHRE
AUFMERKSAMKEIT!**



Nächste Session 13:00

Session 2

Was ist PAM mit Zero Standing Privileges (ZSP)?

Produkt:  BeyondTrust

Referenten: Michael Scherzinger, Jessica Warland

Frei, 4. OG

Kontrolle und Schutz im Zeitalter von KI – Der Zscaler-Ansatz für GenAI Security

Produkt:  zscaler

Referent: Jonas Kugler

Odermatt, 4. OG

Disaster Recovery im Cloud-Zeitalter

Produkt:  zscaler

Referent: Matthias Geiser

Lehmann Steingruber, 5. OG

How to secure AI – Ein strategischer Überblick

Produkte: Diverse

Referent: Georg Hegyi

Cancellara, 4. OG