

BeyondTrust Webinar "Sicher Arbeiten"

2. Dezember 2020

AVANTEC
Competence. Security. Trust.



Weil Sicherheit alles ändert.

Michael Scherzinger

IT Security Engineer | PAM Product Manager
scherzinger@avantec.ch

Agenda.

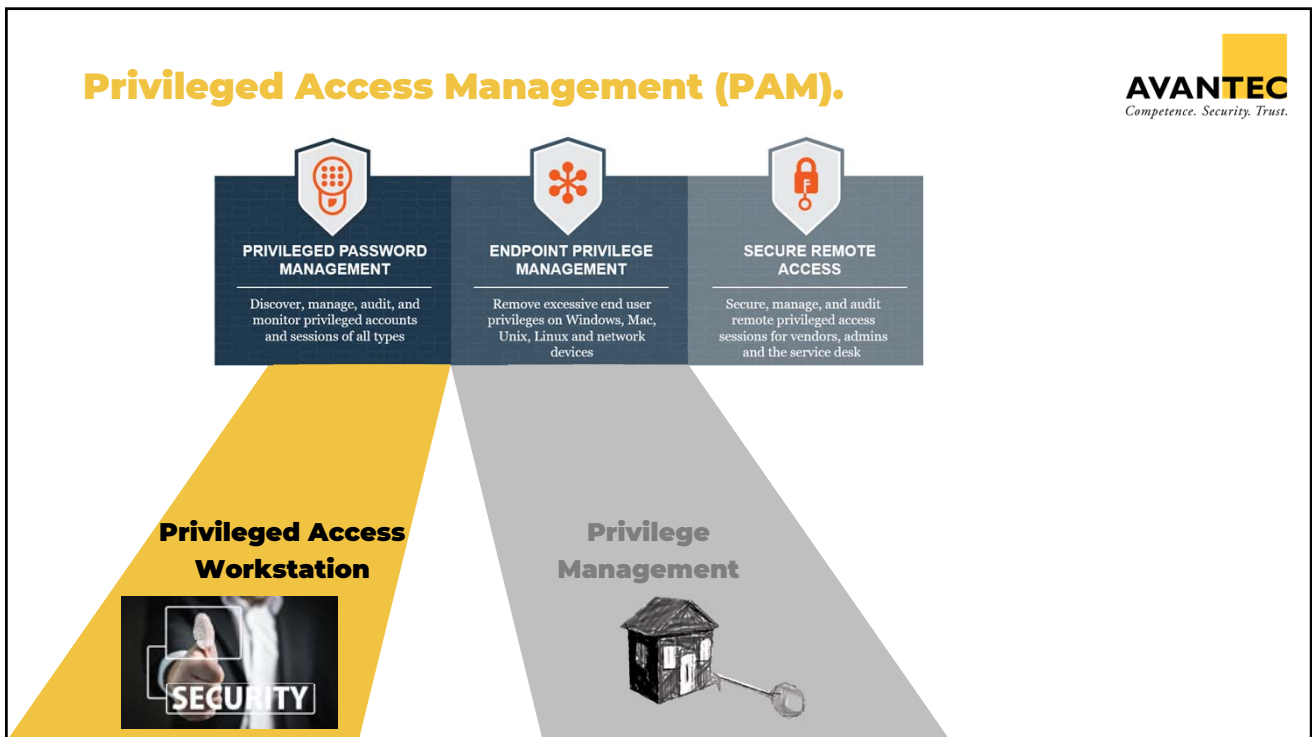
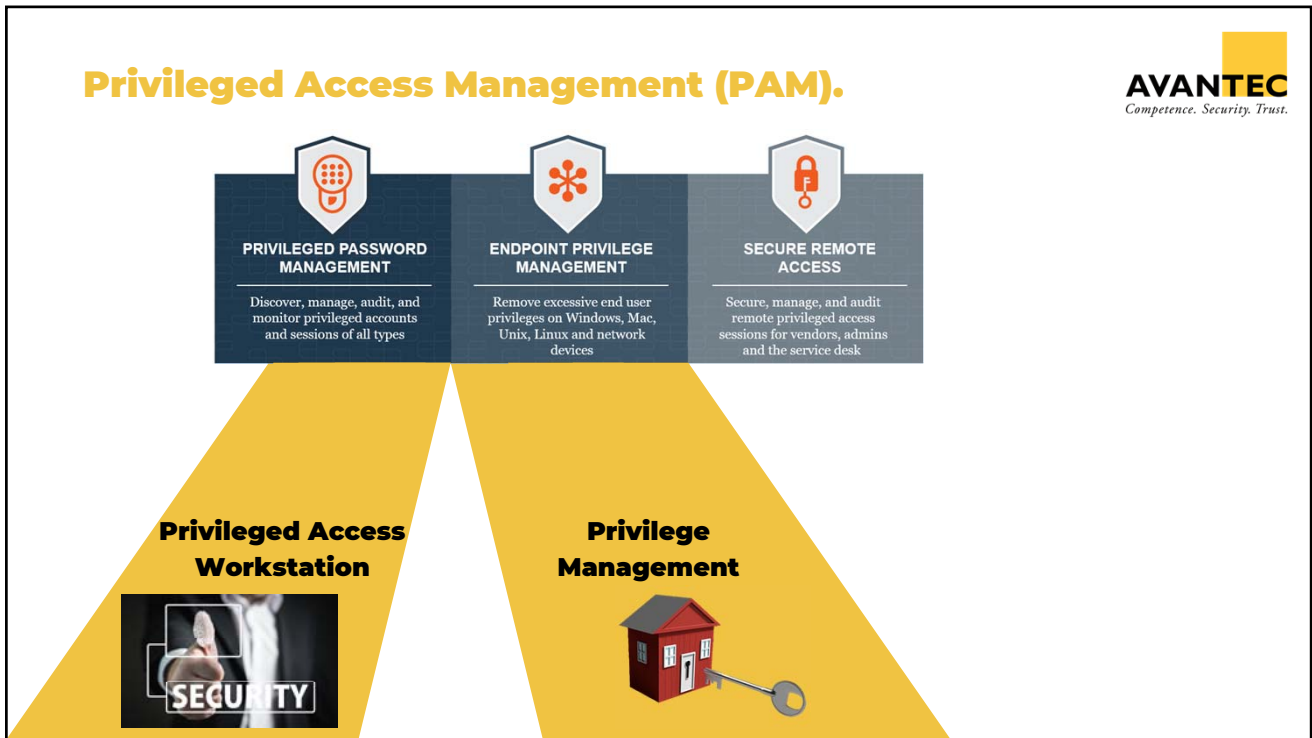
AVANTEC
Competence. Security. Trust.

- Begrüssung / Kennenlernen
- Privileged Access Workstation (PAW)
 - Herausforderungen / Anforderungen
 - Lösungsansatz
- Privilege Management
 - Herausforderungen / Anforderungen
 - Lösungsansatz
- Fragen

AVANTEC
Competence. Security. Trust.

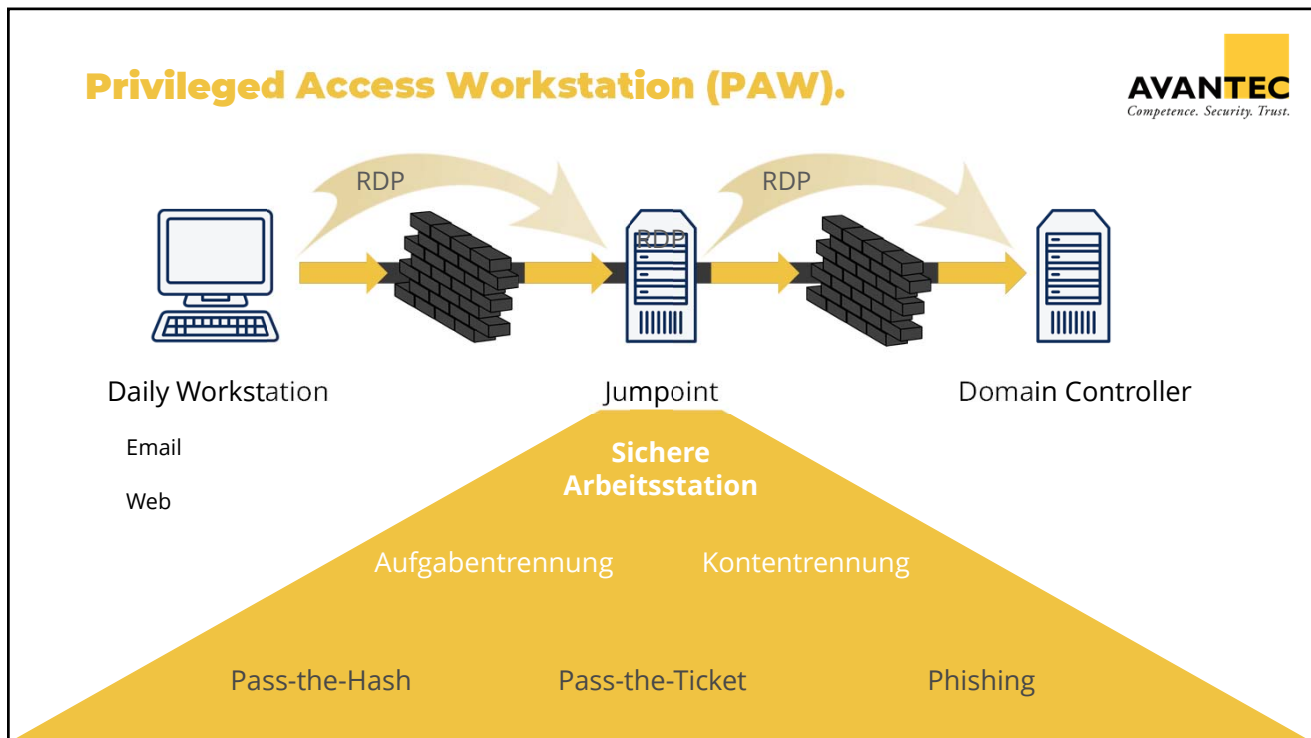
BeyondTrust Webinar "Sicher Arbeiten"

2. Dezember 2020

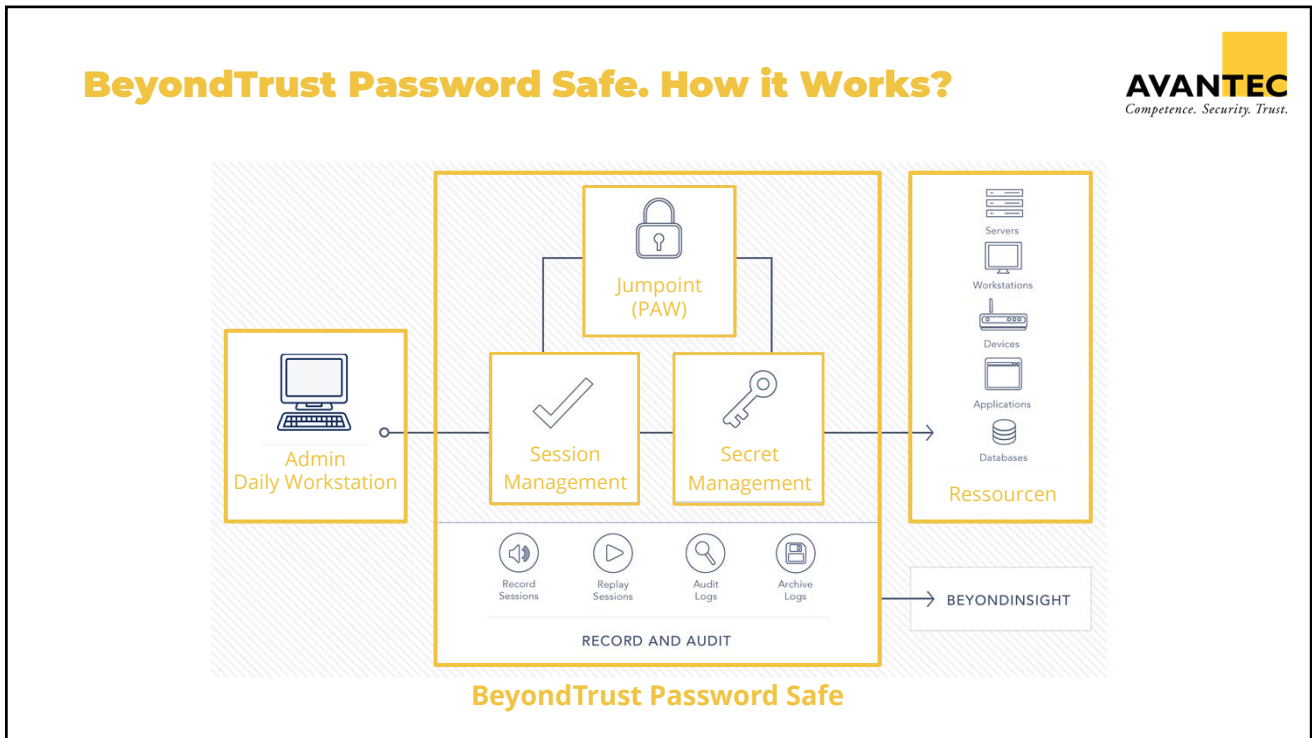


BeyondTrust Webinar "Sicher Arbeiten"

2. Dezember 2020



BeyondTrust Webinar "Sicher Arbeiten" 2. Dezember 2020



BeyondTrust Password Safe – Anforderungen.

AVANTEC
Competence. Security. Trust.

PAW Station

Session Management

Secret Management

- Sicherere Arbeitsstation
 - Schutz vor dem Internet
 - Schutz vor Phishing
 - Schutz vor Manipulation
- Kontentrennung
- Aufgabentrennung

Onboarding

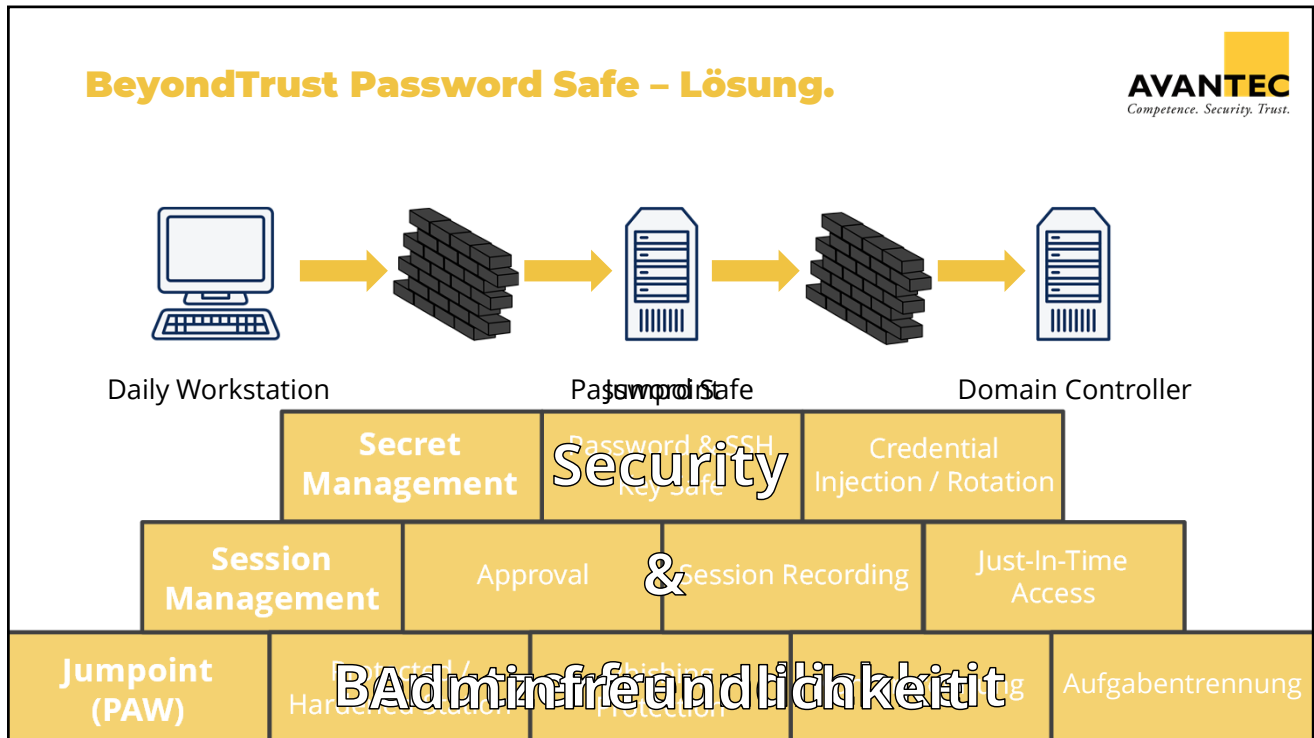
Secret Management

Key


Clipboard

BeyondTrust Webinar "Sicher Arbeiten"

2. Dezember 2020

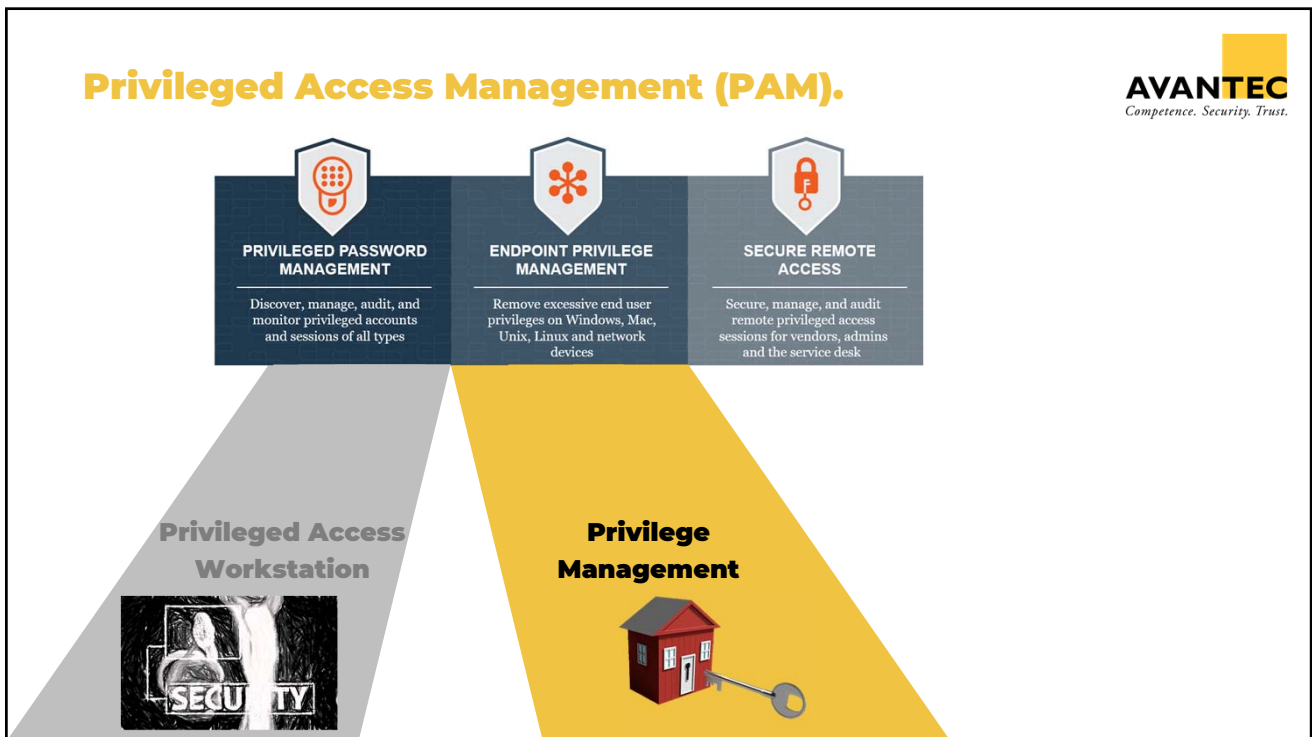
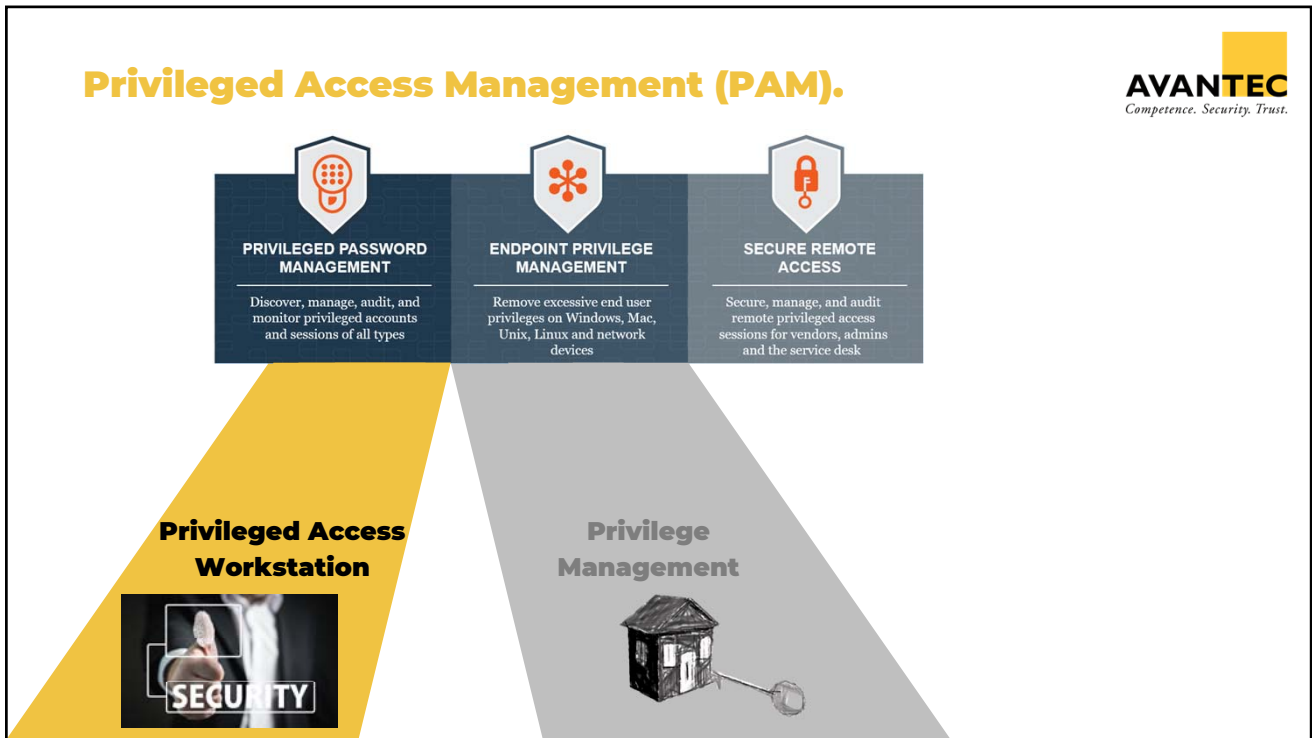


Demo.



BeyondTrust Webinar "Sicher Arbeiten"

2. Dezember 2020



BeyondTrust Webinar "Sicher Arbeiten"

2. Dezember 2020

Herausforderung: Schwachstelle.

AVANTEC
Competence. Security. Trust.



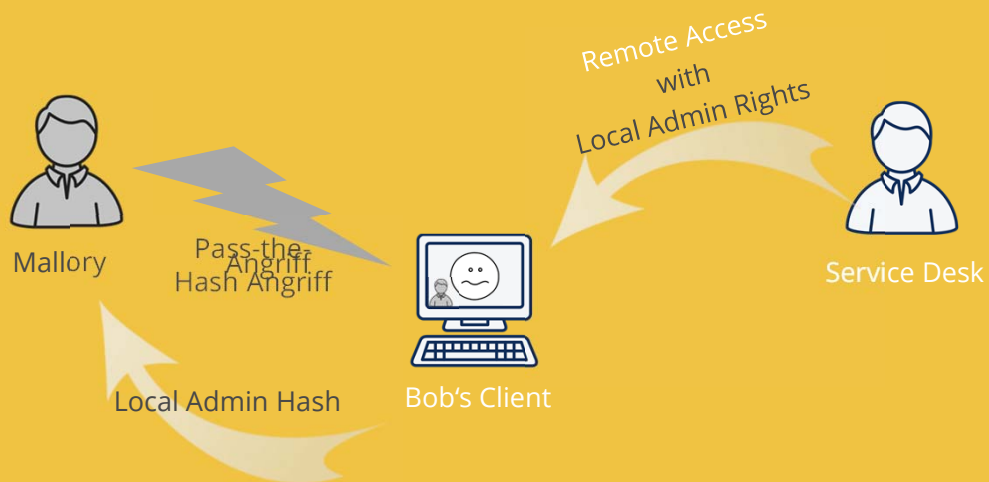
Internet Explorer

CVE's

Default User Rights

Herausforderung: Erhöhte Berechtigungen.

AVANTEC
Competence. Security. Trust.



AVANTEC
Competence. Security. Trust.

BeyondTrust Webinar "Sicher Arbeiten"

2. Dezember 2020

Herausforderung: Usability vs. Security.

AVANTEC
Competence. Security. Trust.

Beweglichkeit /
Benutzerfreundlichkeit

Beweglichkeit /
Benutzerfreundlichkeit

Beweglichkeit /
Benutzerfreundlichkeit



Schutz



Privilege Management

AVANTEC
Competence. Security. Trust.



Application Whitelisting

Modern Application Whitelisting
with Trusted Owner Principle



Manage Rights

Elevate Applications, not
Users




Enterprise Auditing & Reporting

- Analyze Use Behavior
- Track and Control Apps
- Auditing

AVANTEC
Competence. Security. Trust.

BeyondTrust Webinar "Sicher Arbeiten"

2. Dezember 2020




Application Whitelisting

with Trusted owner

60% – 80% Softwareverteilung (SCCM)

90% – 95% Softwareverteilung + **Privilege Management Templates**

5% - 10% Comp



- Application Informations
- Product Name
- Product version
- ...
- Path
- Source URL
- ...

Privilege Management



Application Whitelisting

Modern Application Whitelisting with Trusted Owner Principle



Manage Rights

Elevate Applications, not Users



Enterprise Auditing & Reporting

- Analyze Use Behavior
- Track and Control Apps
 - Auditing

BeyondTrust Webinar "Sicher Arbeiten"

2. Dezember 2020

Application Elevating with Access Token.

AVANTEC
Competence. Security. Trust.

The screenshot shows a Windows Command Prompt window with the following content:

```

Microsoft Windows [Version 10.0.17763.779]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\ui>whoami /user /groups /priv

USER INFORMATION
-----
User Name SID
-----
lab\ui 5-1-5-21-3797132838-3311603045-3969152827-1105

GROUP INFORMATION
-----
Group Name Type SID
-----
Everyone Well-known group 5-1-1-0
BUILTIN\Users Alias 5-1-5-32-545
NT AUTHORITY\INTERACTIVE Well-known group 5-1-5-4
CONSOLE LOGON Well-known group 5-1-5-11
NT AUTHORITY\Authenticated Users Well-known group 5-1-5-11
NT AUTHORITY\This Organization Well-known group 5-1-5-15
LOCAL Well-known group 5-1-2-0
Authentication authority asserted identity Well-known group 5-1-18-1
Mandatory Label\Medium Mandatory Level Label 5-1-16-8192

PRIVILEGES INFORMATION
-----
Privilege Name Description State
-----
SeShutdownPrivilege Shut down the system Disabled
SeChangeNotifyPrivilege Bypass traverse checking Enabled
SeUndockPrivilege Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
SeTimeZonePrivilege Change the time zone Disabled
  
```

Annotations on the image:

- User**: Points to the 'User Name' field in the USER INFORMATION section.
- Command: Whoami /user /groups /priv**: Points to the command entered in the Command Prompt.
- User Info ->**: Points to the USER INFORMATION section.
- User group info -> (User Token)**: Points to the GROUP INFORMATION section.
- Privileges Information ->**: Points to the PRIVILEGES INFORMATION section.
- Add local Admin privileges**: Points to the LOCAL group in the GROUP INFORMATION section.

Privilege Management for Windows & Mac Desktops



Application Whitelisting

Modern Application Whitelisting with Trusted Owner Principle



Manage Rights

Elevate Applications, not Users



Enterprise Auditing & Reporting

- Analyze Use Behavior
- Track and Control Apps
 - Auditing

AVANTEC
Competence. Security. Trust.

BeyondTrust Webinar "Sicher Arbeiten" 2. Dezember 2020

Demo.



Fragen.

