TECH UPDATE

EXPERTENWISSEN FÜR IHRE IT-STRATEGIE

braincon
IT-EXPERTS. NOTHING ELSE.

Digital Workplace Security: Citrix EUC state of the art

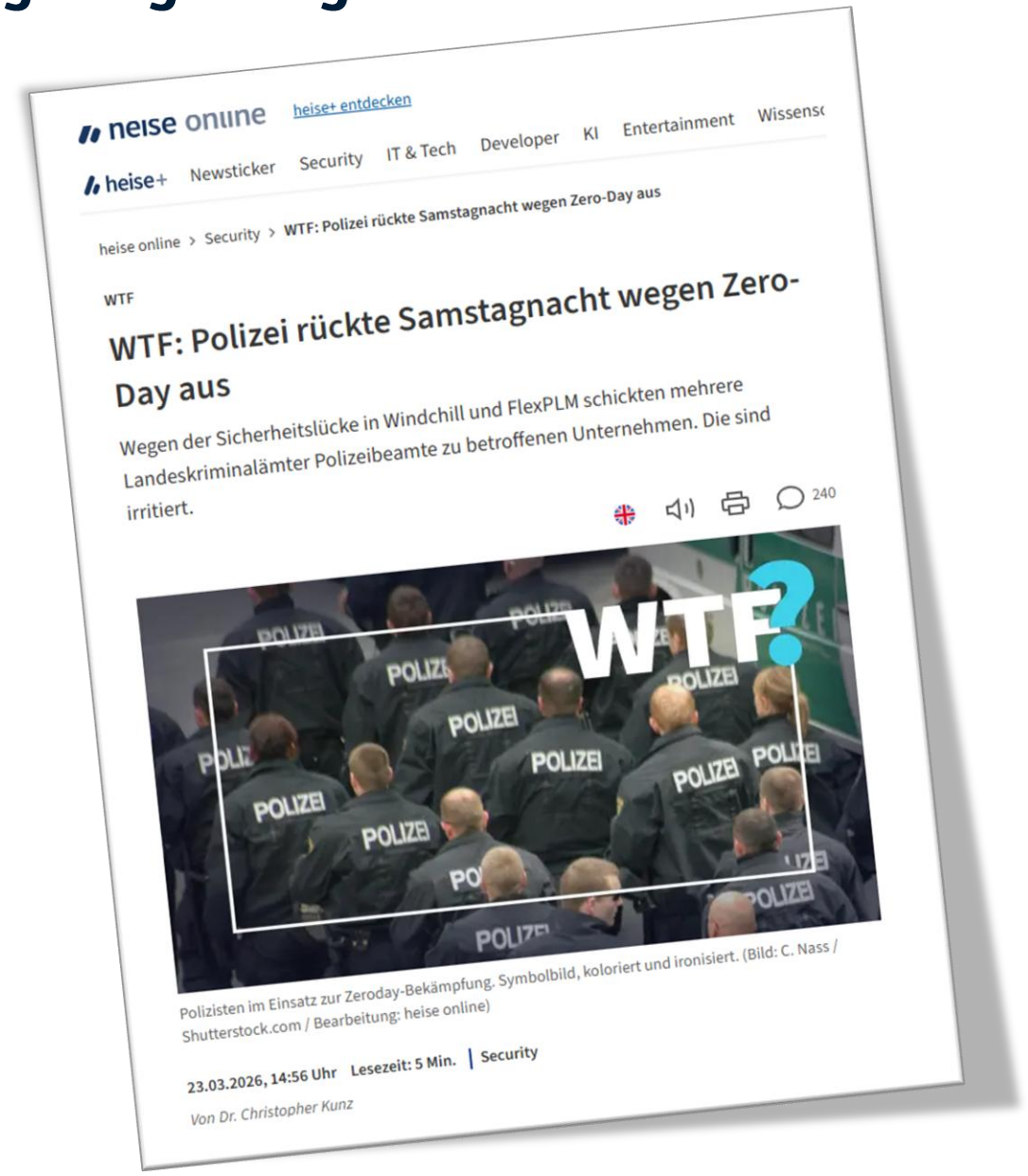
Markus Zehnle
Lead Solution Expert

Tobias Zurstegen
Senior Solution Expert

Warum sind Remoting Umgebung besonders kritisch?

Warum sind Remoting Umgebung besonders kritisch?

Warum sind Remoting Umgebung besonders kritisch?



heise online heise+ entdecken

heise+ Newsticker Security IT & Tech Developer KI Entertainment Wissens

heise online > Security > WTF: Polizei rückte Samstagnacht wegen Zero-Day aus

WTF

WTF: Polizei rückte Samstagnacht wegen Zero-Day aus

Wegen der Sicherheitslücke in Windchill und FlexPLM schickten mehrere Landeskriminalämter Polizeibeamte zu betroffenen Unternehmen. Die sind irritiert.

240

Polizisten im Einsatz zur Zeroday-Bekämpfung. Symbolbild, koloriert und ironisiert. (Bild: C. Nass / Shutterstock.com / Bearbeitung: heise online)

23.03.2026, 14:56 Uhr Lesezeit: 5 Min. | Security

Von Dr. Christopher Kunz

Warum sind Remoting Umgebung besonders kritisch?

BLEEPINGCOMPUTER

NEWS ▾ TUTORIALS ▾ WEBINARS DOWNLOADS ▾ DEALS ▾ VPNS ▾

Search Site

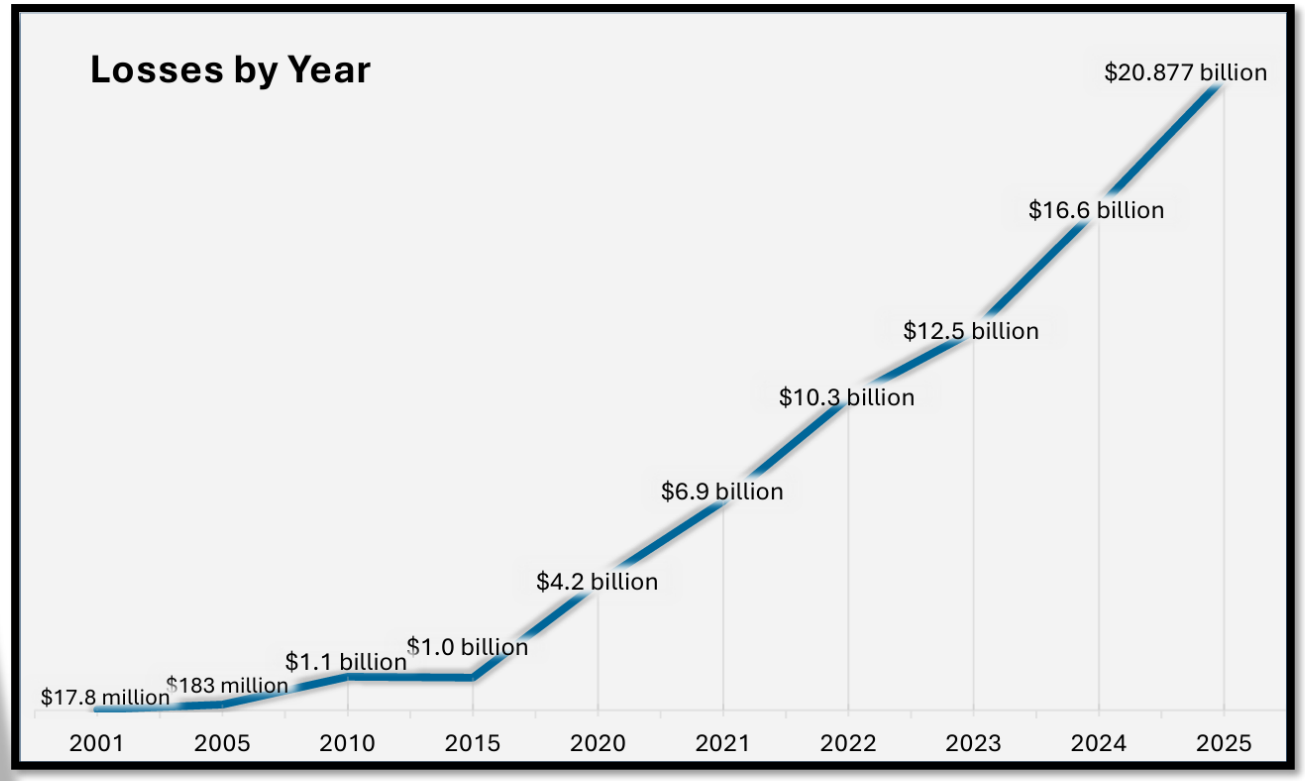
Home > News > Security > FBI: Americans lost a record $21 billion to cybercrime last year

FBI: Americans lost a record $21 billion to cybercrime last year

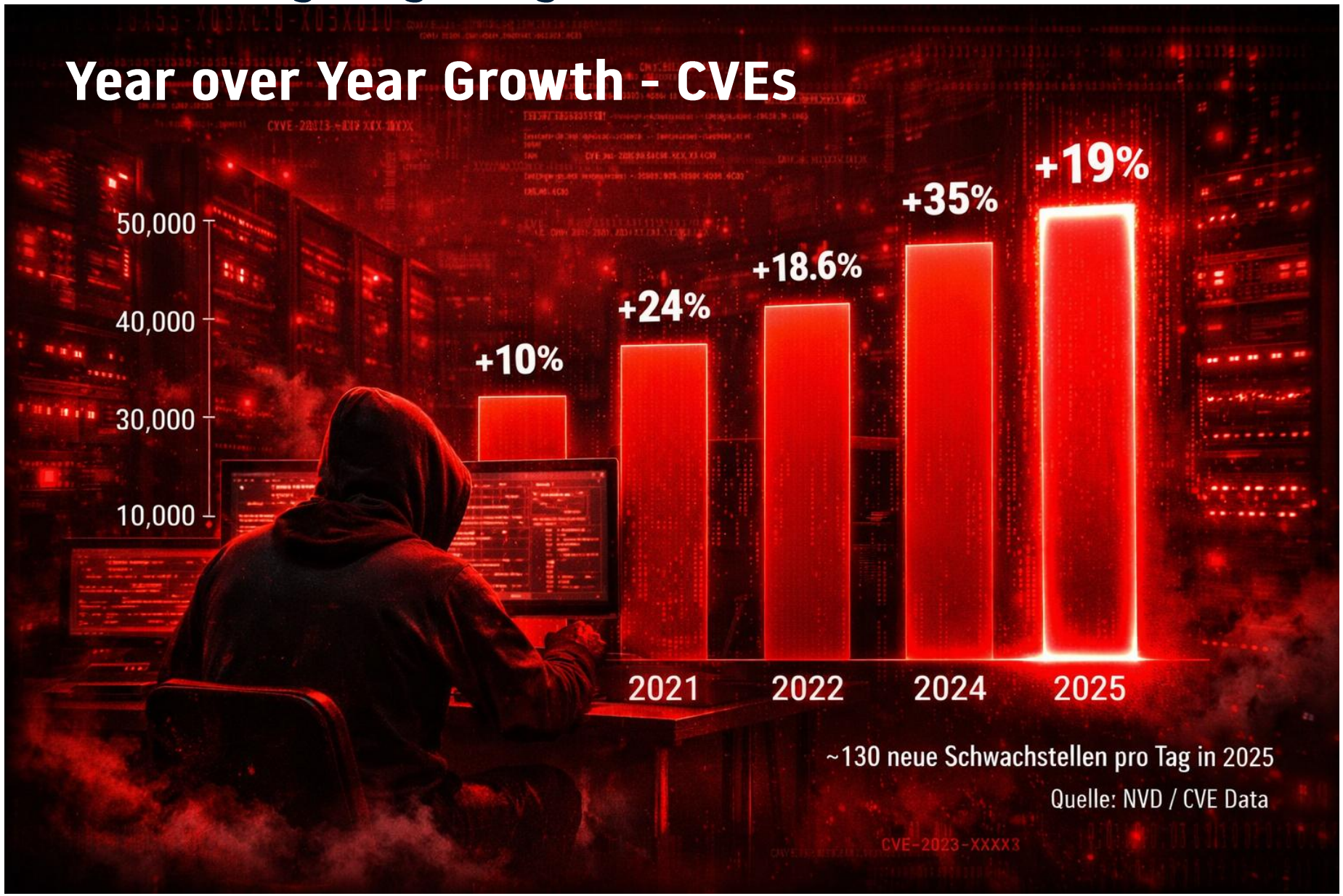
By Bill Toulas

April 7, 2026 04:41 PM 0

U.S. victims lost nearly $21 billion to cyber-enabled crimes last year, driven primarily by investment scams, business email compromise, tech support fraud, and data breaches, the Federal Bureau of Investigation says.



Warum sind Remoting Umgebung besonders kritisch?

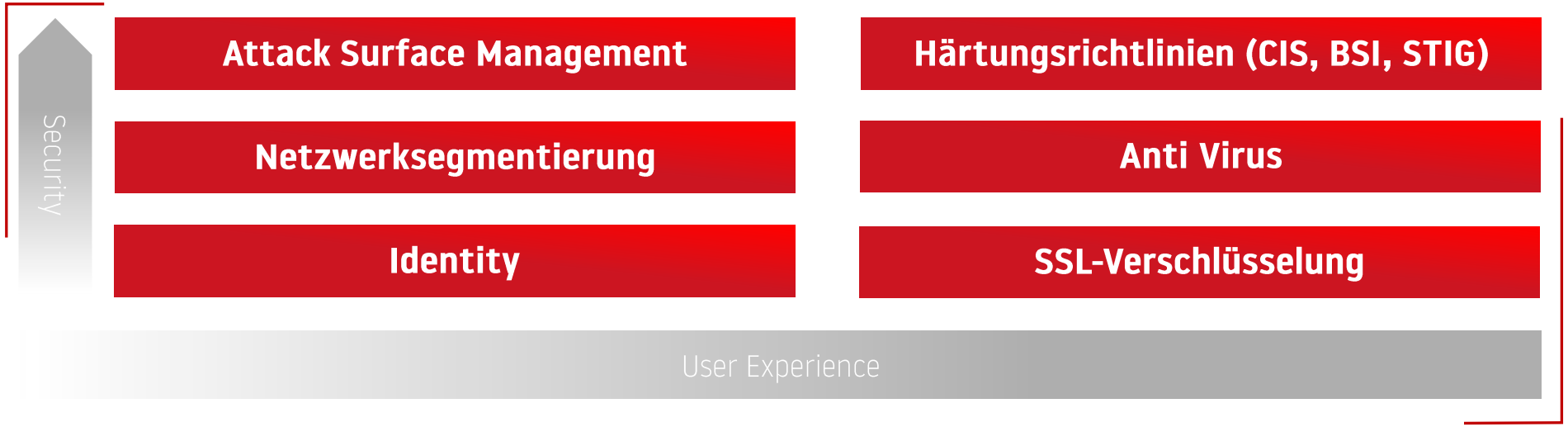


Warum sind Remoting Umgebung besonders kritisch?

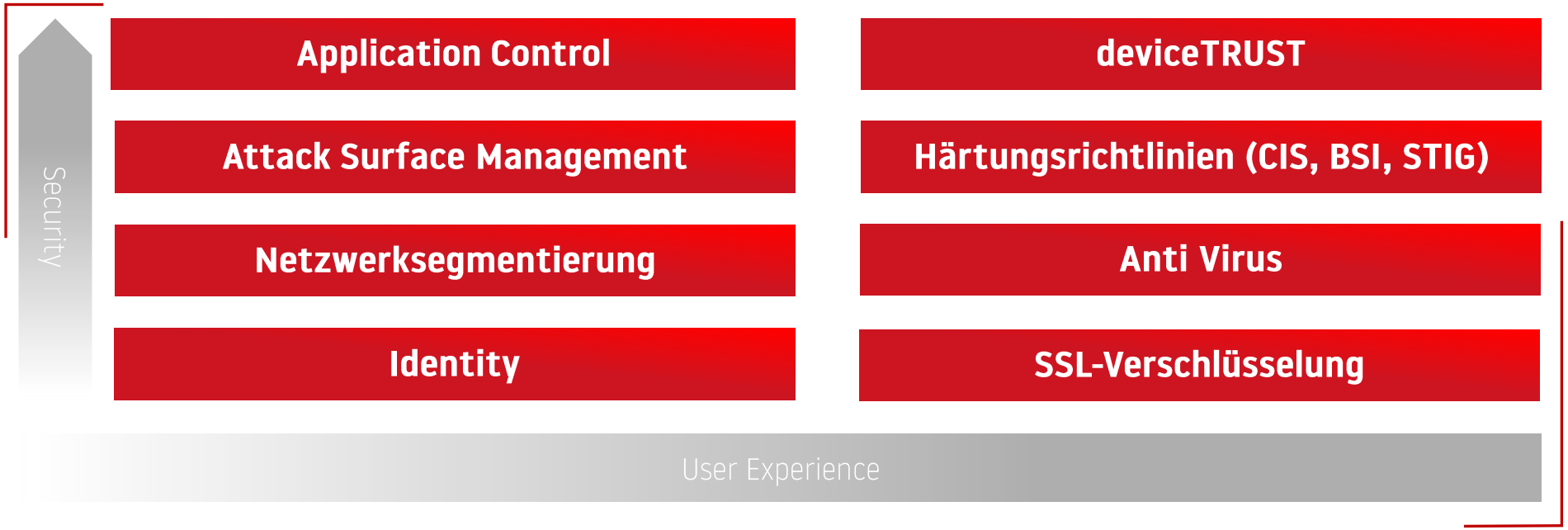
- Zentrale Bereitstellung
- Identität ist kritisch
- Externe Zugriff
- Multi-User Systeme
- Patch- und Zero Day Risiko
- Datenabfluss
- Ransomware Multiplikator
- Hohe Privilegien Konzentration bei Administratoren

End-User Computing – Security Framework

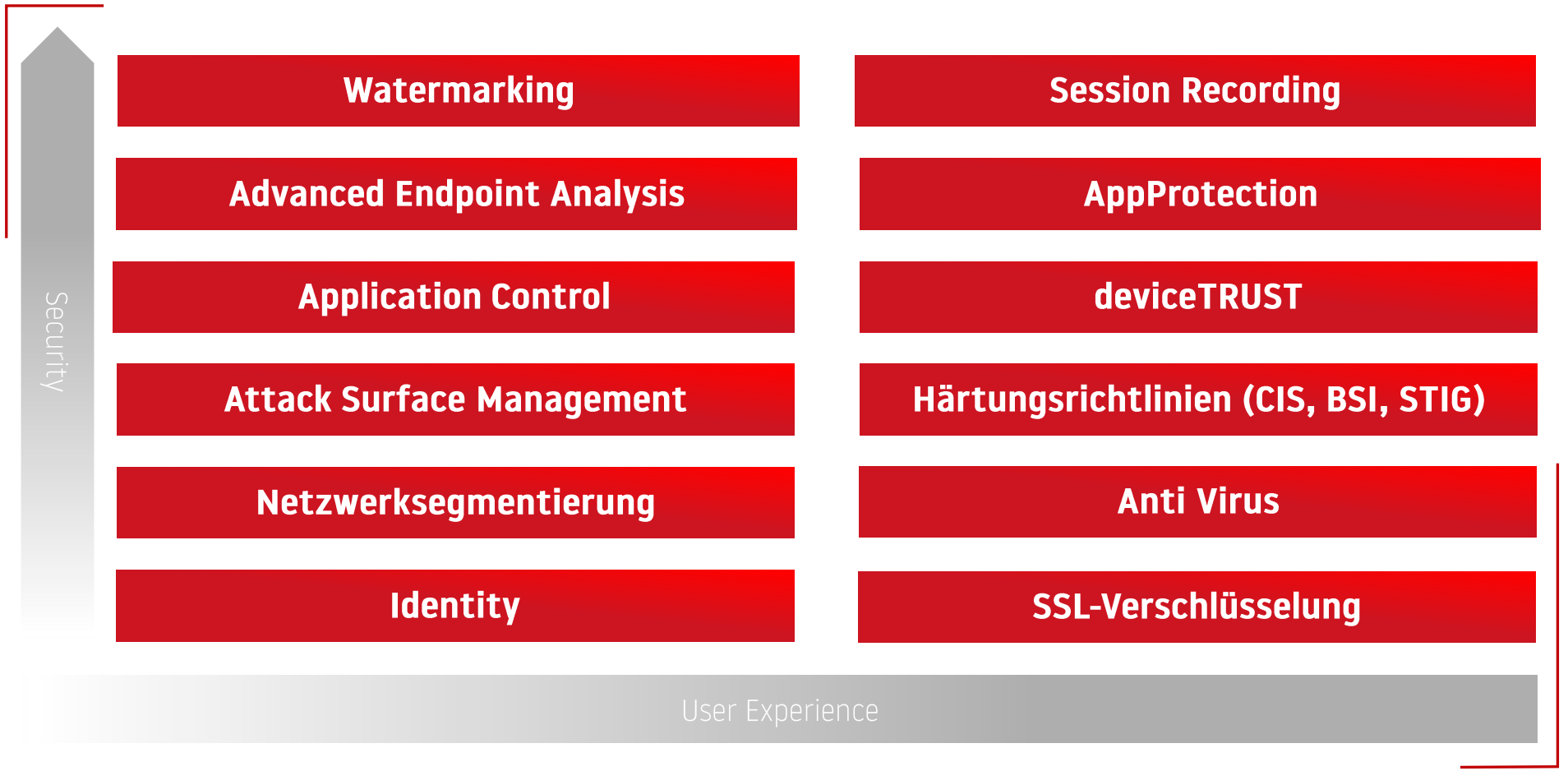
End-User Computing – Security Framework



End-User Computing – Security Framework



End-User Computing – Security Framework



Security Baseline zur Systemhärtung

- Härtung von Systemen
- Reduzierung der Angriffsflächen
- Schutz vor Fehlkonfiguration
- Hersteller Unabhängigkeit
- Einheitlicher Sicherheitsstandard
- Compliance & Audit Fähigkeit
- Reproduzierbarkeit
- Automatisierung

Security Baseline zur Systemhärtung

- Härtung von Systemen
- Reduzierung der Angriffsflächen
- Schutz vor Fehlkonfiguration
- Hersteller Unabhängigkeit
- Einheitlicher Sicherheitsstandard
- Compliance & Audit Fähigkeit
- Reproduzierbarkeit
- Automatisierung

CIS (Benchmarks)

Security Baseline zur Systemhärtung

- Härtung von Systemen
- Reduzierung der Angriffsflächen
- Schutz vor Fehlkonfiguration
- Hersteller Unabhängigkeit
- Einheitlicher Sicherheitsstandard
- Compliance & Audit Fähigkeit
- Reproduzierbarkeit
- Automatisierung

CIS (Benchmarks)

BSI (SiSyPHuS)

Security Baseline zur Systemhärtung

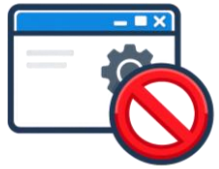
- Härtung von Systemen
- Reduzierung der Angriffsflächen
- Schutz vor Fehlkonfiguration
- Hersteller Unabhängigkeit
- Einheitlicher Sicherheitsstandard
- Compliance & Audit Fähigkeit
- Reproduzierbarkeit
- Automatisierung

CIS (Benchmarks)

BSI (SiSyPHuS)

STIGs (Security Technical Implementation Guides)

Application Control



Anwendungssteuerung

Application Control

Anwendungssteuerung

Code-Integrität

Application Control

Anwendungssteuerung

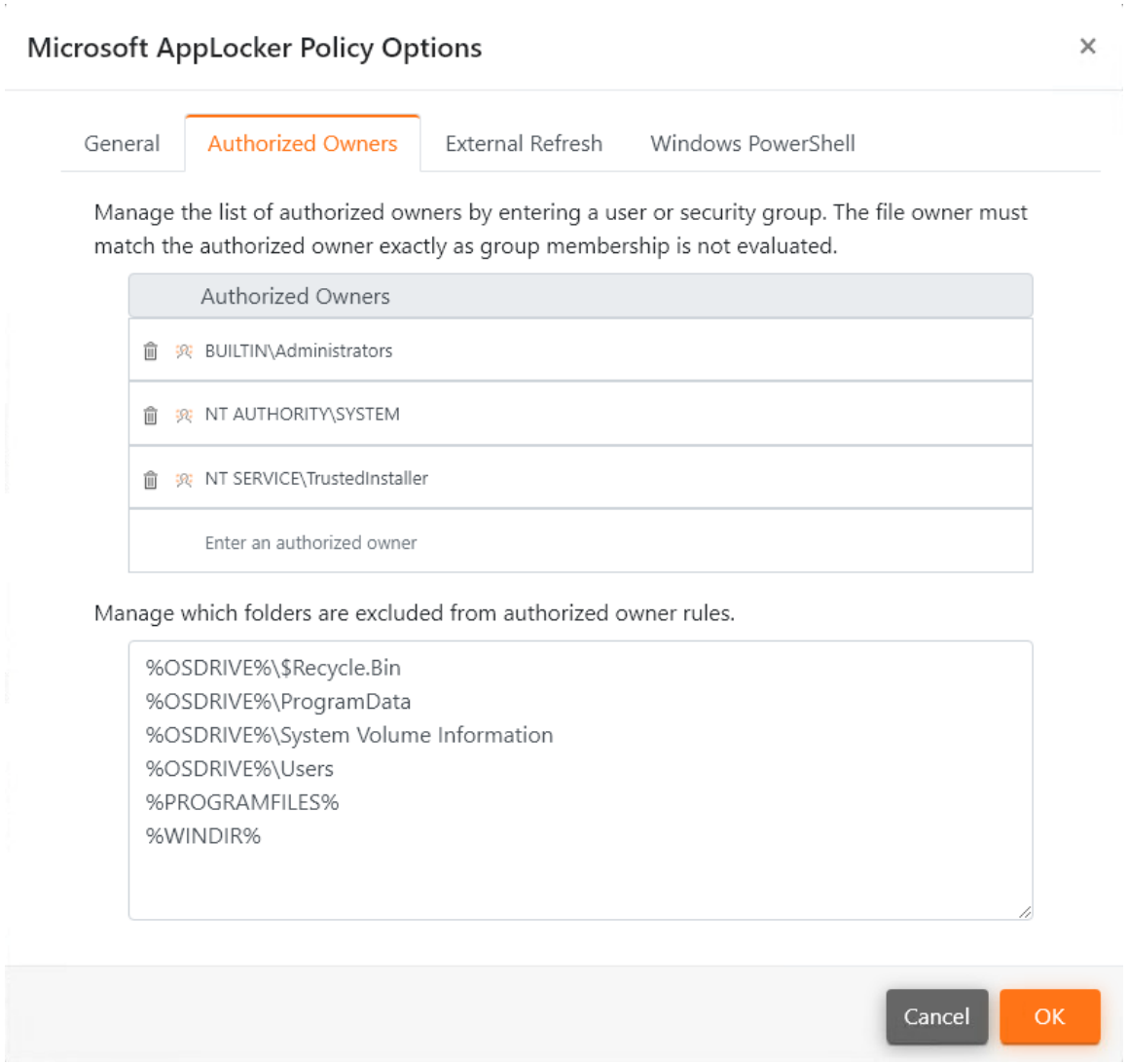
Code-Integrität

Audit & Compliance

Whitelisting

AppLocker mit deviceTRUST

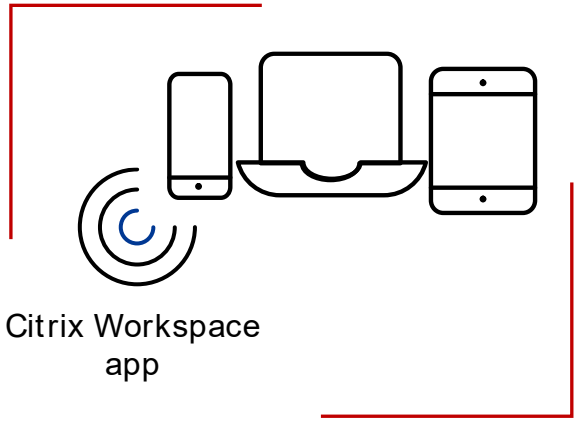
- Zentrales Managed u.a. Automatischer Start des Application Identity Services
- EventLog Größe
- „Authorized Owner“ für eine automatisierte Erstellung der Allow List inkl. Ordnerausnahmen
- Erweiterung der Standard-Umgebungsvariablen



Microsoft Defender Attack Surface Reduction

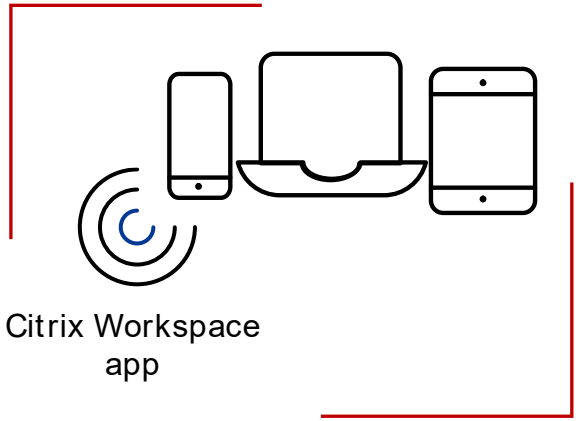
- Blockierung typischer Angriffstechniken auf Basis Microsoft Defender for Endpoint
- Beispiele:
  - Office- u. Adobe Anwendungen dürfen keine untergeordneten Prozesse erstellen
  - Win32-API-Aufrufe aus Office-Makros blockieren
  - Prozessstart über PSExcec u. WMI blockieren
  - Ausführung potenziell verschleierter Skripte blockieren

deviceTRUST Funktionsweise



Endgerät

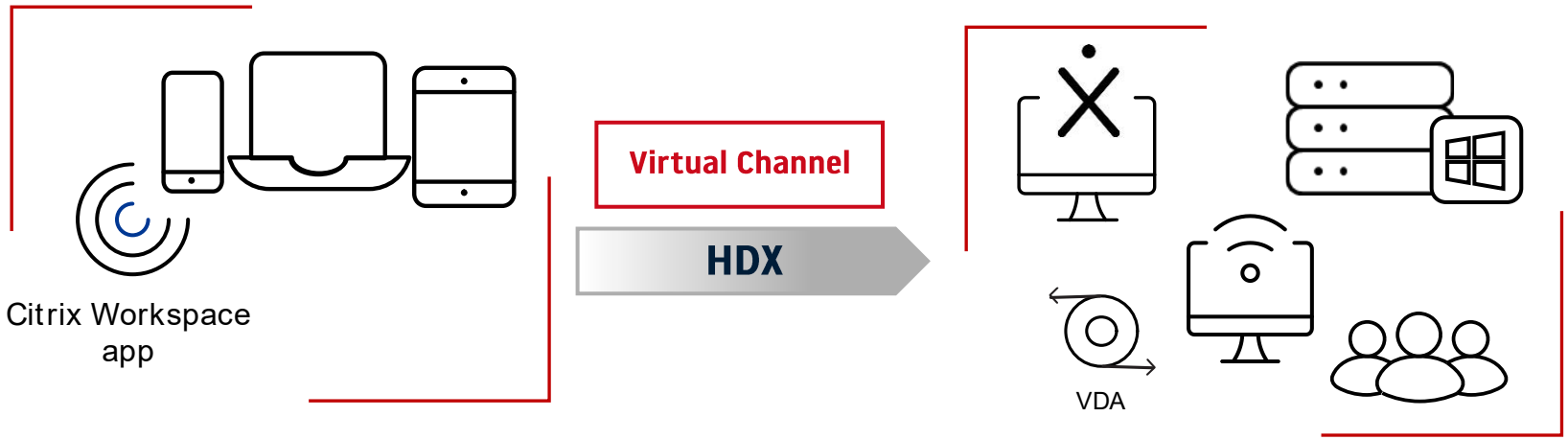
deviceTRUST Funktionsweise



Eigenschaften

Endgerät

deviceTRUST Funktionsweise

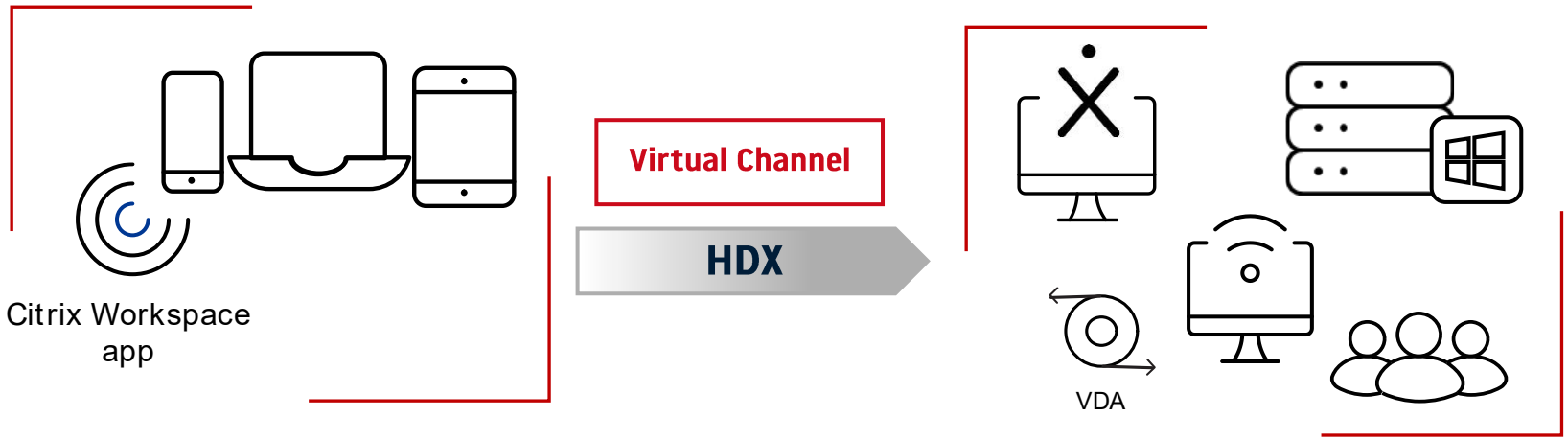


Eigenschaften

Endgerät

Remoting

deviceTRUST Funktionsweise



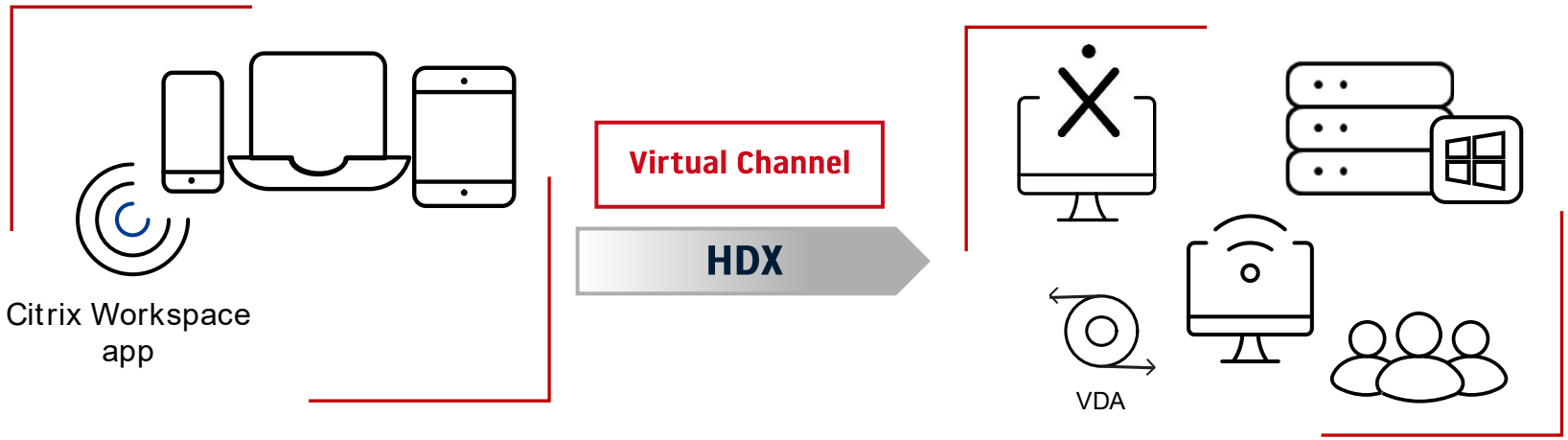
Eigenschaften

Endgerät

Kontext

Remoting

deviceTRUST Funktionsweise



Eigenschaften

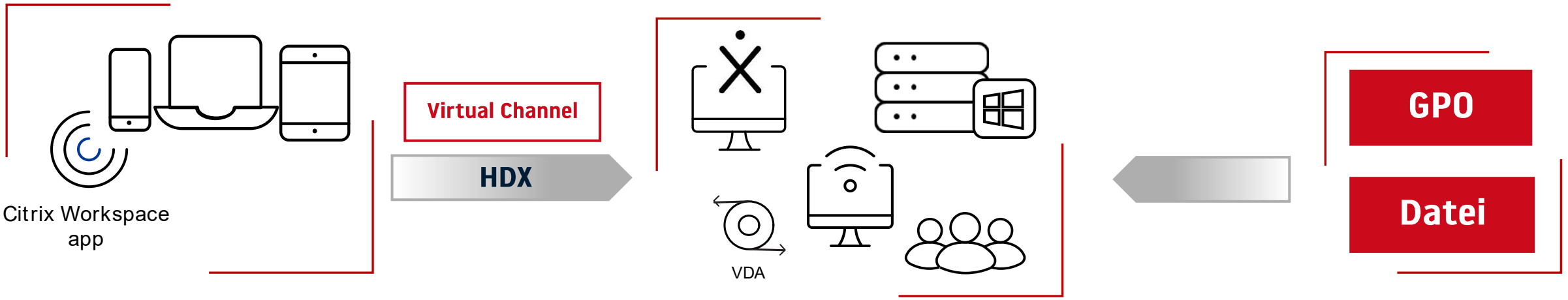
Endgerät

Aktionen

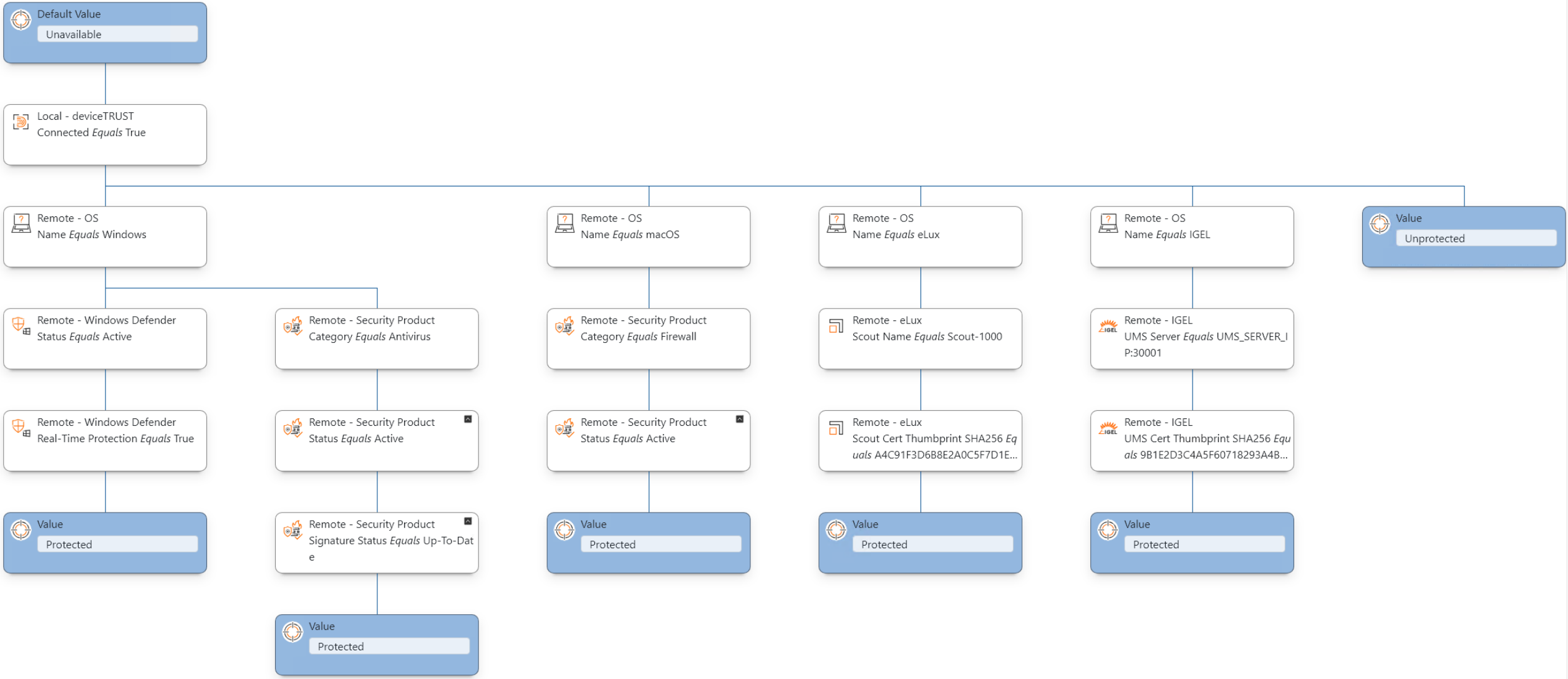
Kontext

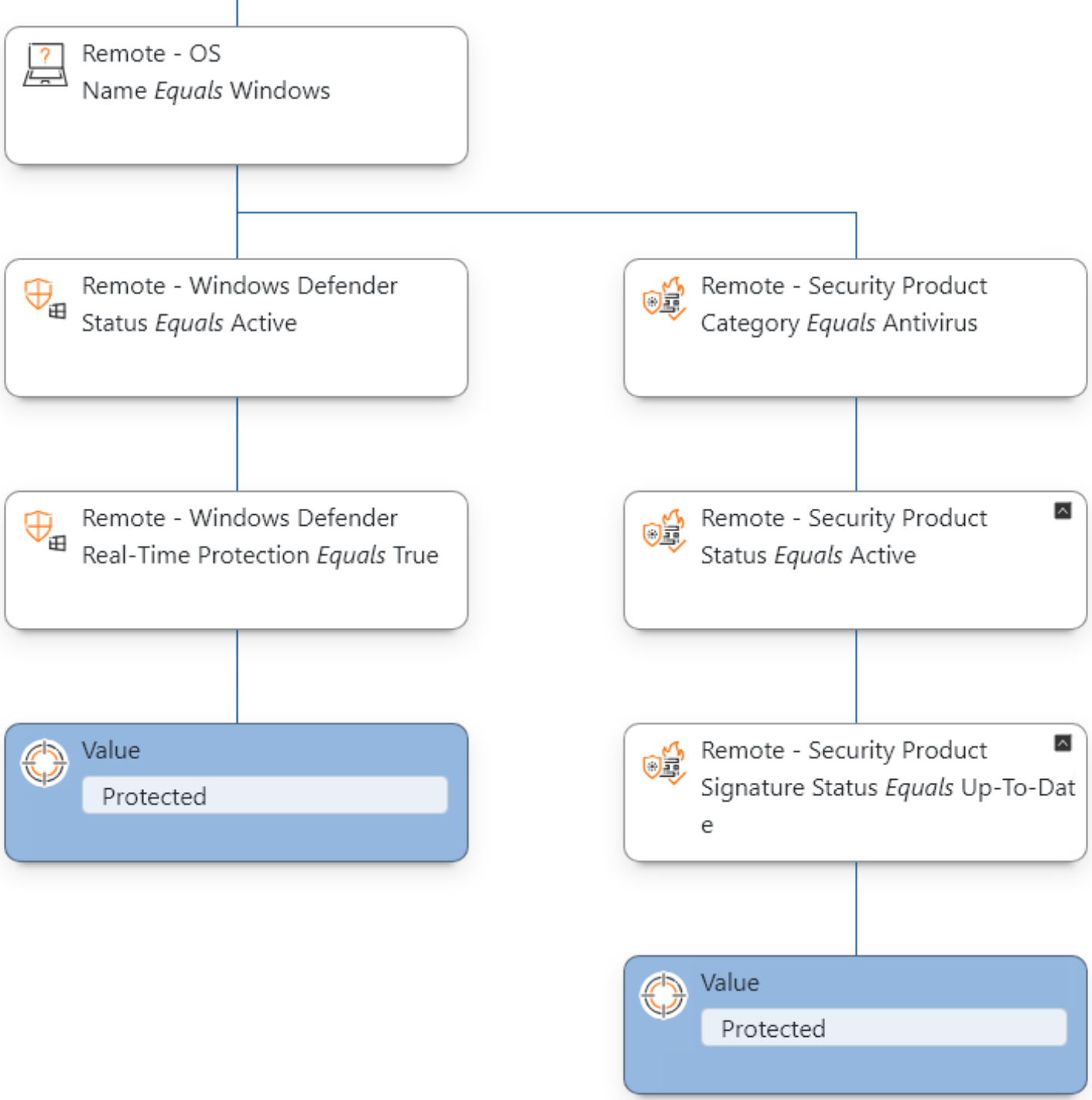
Remoting

deviceTRUST Funktionsweise



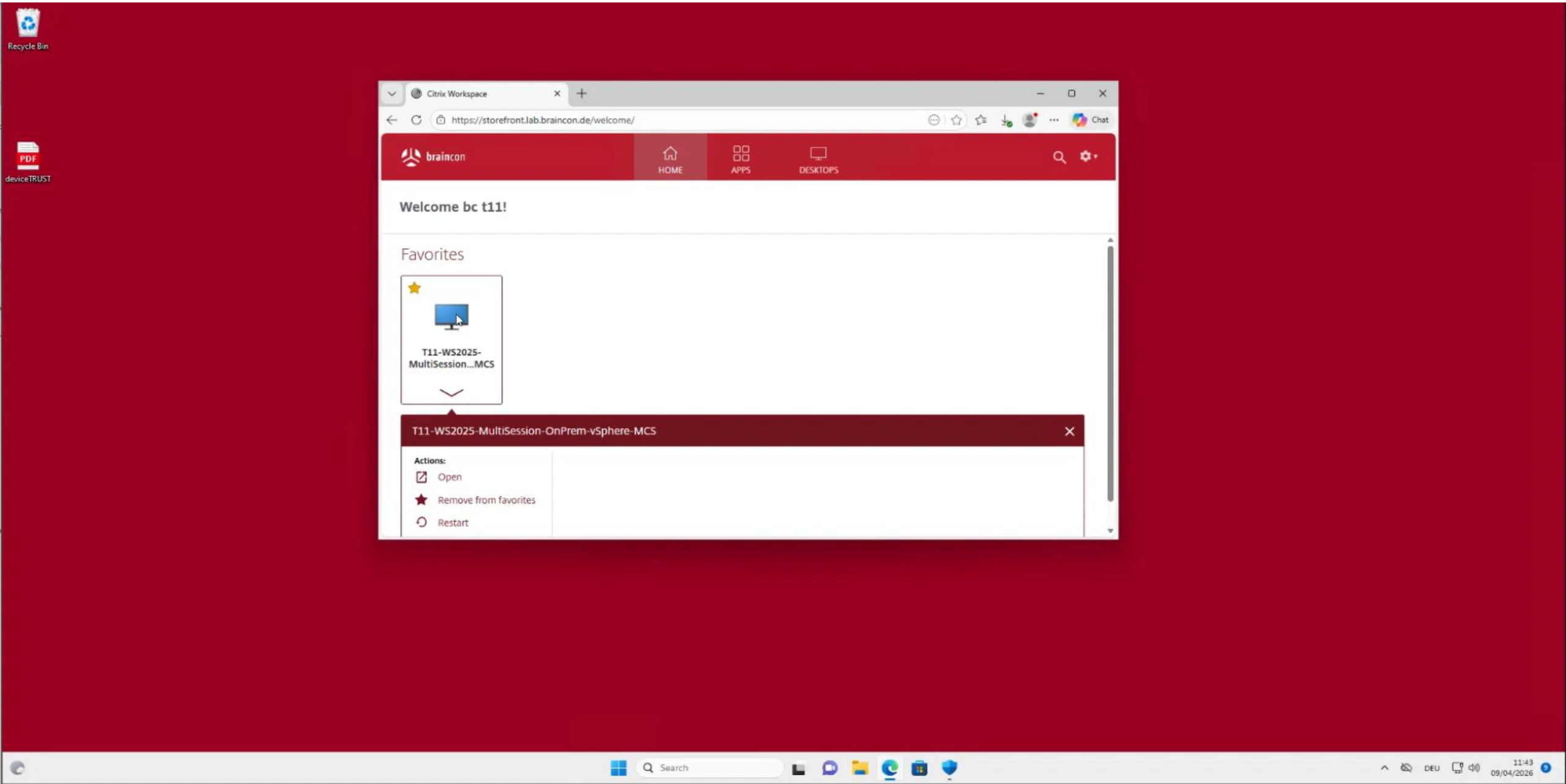
deviceTRUST Console - Eigenschaften und Kontexte




Remote - OS
Name *Equals* Windows
Remote - Windows Defender
Status *Equals* Active
Remote - Security Product
Category *Equals* Antivirus
Remote - Windows Defender
Real-Time Protection *Equals* True
Remote - Security Product
Status *Equals* Active
Value
Protected
Remote - Security Product
Signature Status *Equals* Up-To-Dat
e
Value
Protected

Demo

Demo


Recycle Bin
deviceTRUST
Citrix Workspace
https://storefront.lab.braincon.de/welcome/
Chat
braincon
HOME
APPS
DESKTOPS
Welcome bc t11!
Favorites
T11-WS2025-MultiSession...MCS
T11-WS2025-MultiSession-OnPrem-vSphere-MCS
Actions:
Open
Remove from favorites
Restart
Search
DEU
11:43
09/04/2026

deviceTRUST Logging

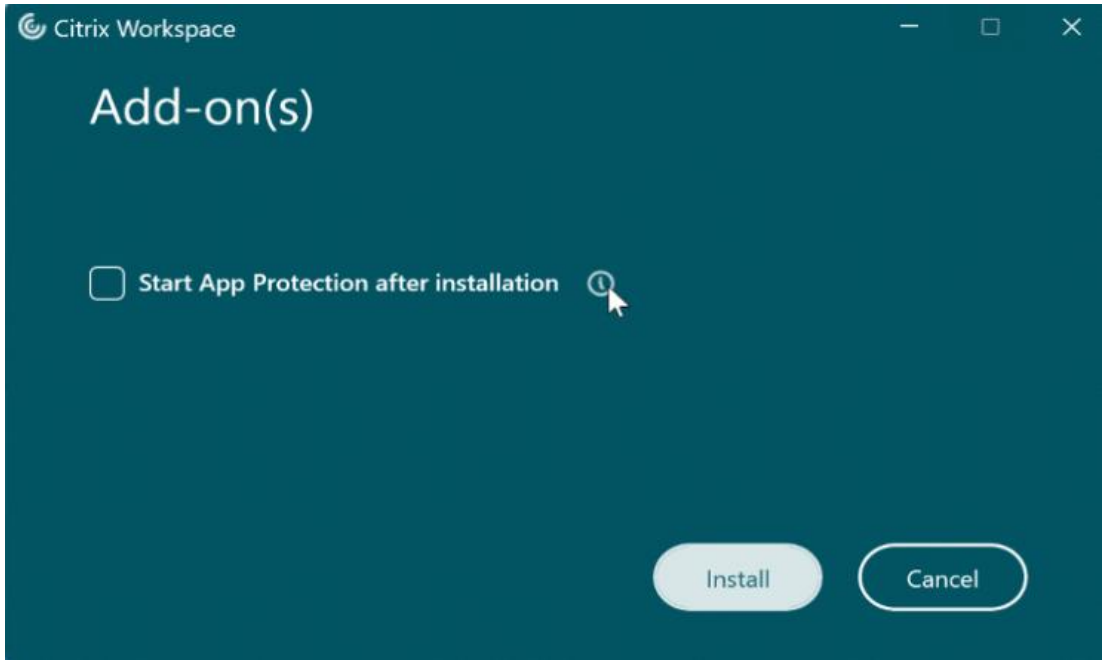
- Logging auf Seite des Agents per
  - Windows Event Log
  - Windows Registry
  - Umgebungsvariablen
  - Web-Request

```
Contexts:
CONTEXT_CORPORATE_DEVICE=True
CONTEXT_DEVICETRUST_CLIENT=Available
CONTEXT_OS_UPDATE=Check Required
CONTEXT_SECURITY_STATE=Unprotected
CONTEXT_THREAT_DETECTION=Safe
```

```
LOCAL_REMOTECONTROL_REMOTE_PLATFORM=Windows
LOCAL_REMOTECONTROL_REMOTE_VERSION=24.2.3001.9
REMOTE_DEVICETRUST_VERSION=23.1.300.0
REMOTE_DOMAIN_ID=S-1-5-21-2694324719-1286008975-1193932117
REMOTE_DOMAIN_JOIN=Domain
REMOTE_OS_NAME=Windows
REMOTE_SECURITYPRODUCT_0_CATEGORY=Antispyware
REMOTE_SECURITYPRODUCT_0_STATUS=Active
REMOTE_SECURITYPRODUCT_1_CATEGORY=Antivirus
REMOTE_SECURITYPRODUCT_1_STATUS=Active
REMOTE_SECURITYPRODUCT_2_CATEGORY=Firewall
REMOTE_SECURITYPRODUCT_2_STATUS=Active
REMOTE_WINDOWSDEFENDER_BEHAVIORTHREATS=0
REMOTE_WINDOWSDEFENDER_LASTFULLSCAN=2025-06-20T09:23:37.185Z
REMOTE_WINDOWSDEFENDER_LASTQUICKSCAN=2026-03-26T11:16:47.991Z
REMOTE_WINDOWSDEFENDER_REALTIMEPROTECTION=false
REMOTE_WINDOWSDEFENDER_SIGNATURETHREATS=0
REMOTE_WINDOWSDEFENDER_STATUS=Active
REMOTE_WINDOWSUPDATE_CRITICAL=Unavailable
REMOTE_WINDOWSUPDATE_LASTSEARCH=Unavailable
REMOTE_WINDOWSUPDATE_SECURITY=Unavailable
```

Citrix App Protection

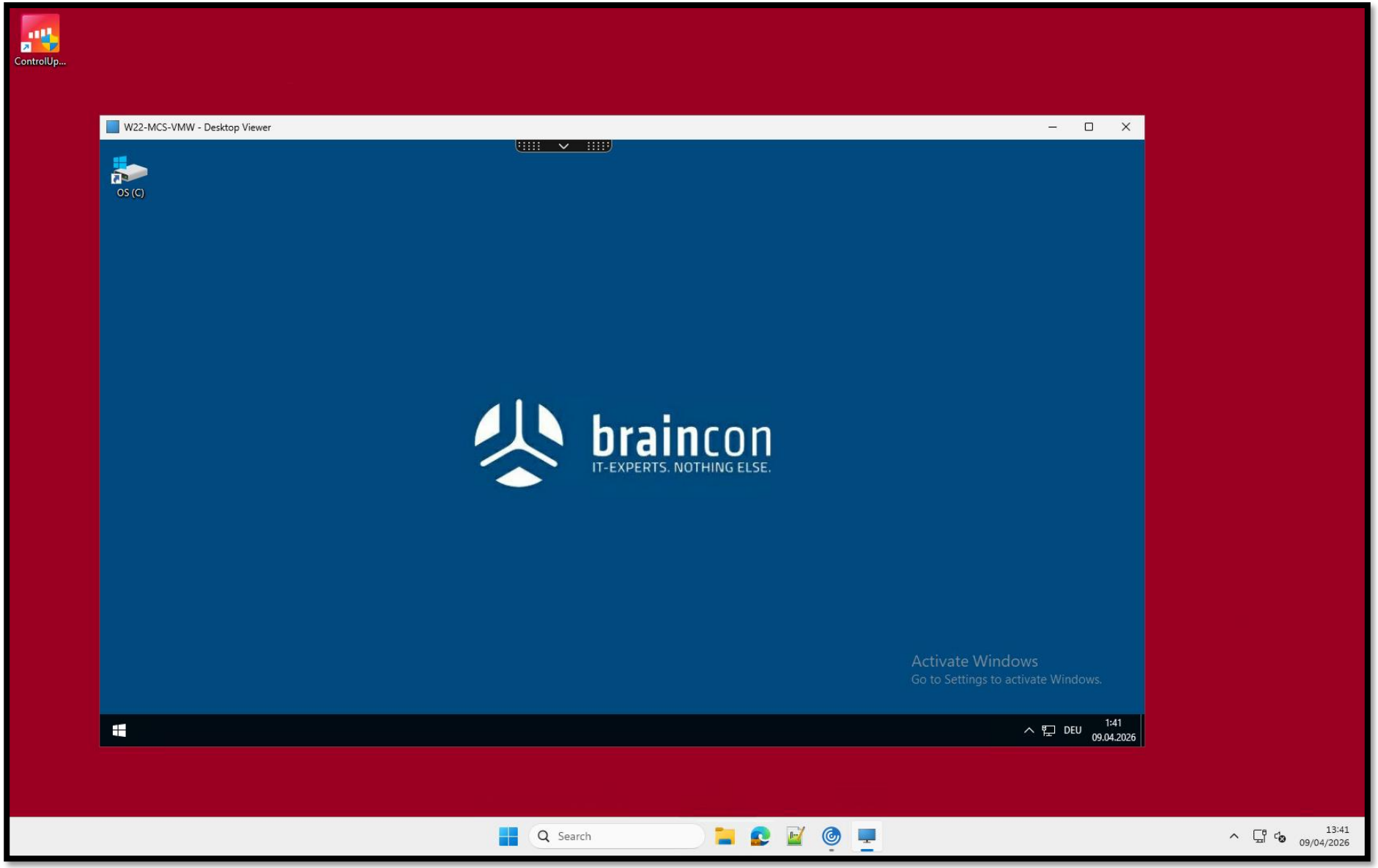
- Anti-Screen Capture
- Anti-KeyLogging
- für:
  - Citrix Sign In Windows
  - Citrix Workspace App HDX Session
  - Self-Service Store (Windows)
  - Web and SaaS Citrix Enterprise Browser
  - Citrix Secure Private Access



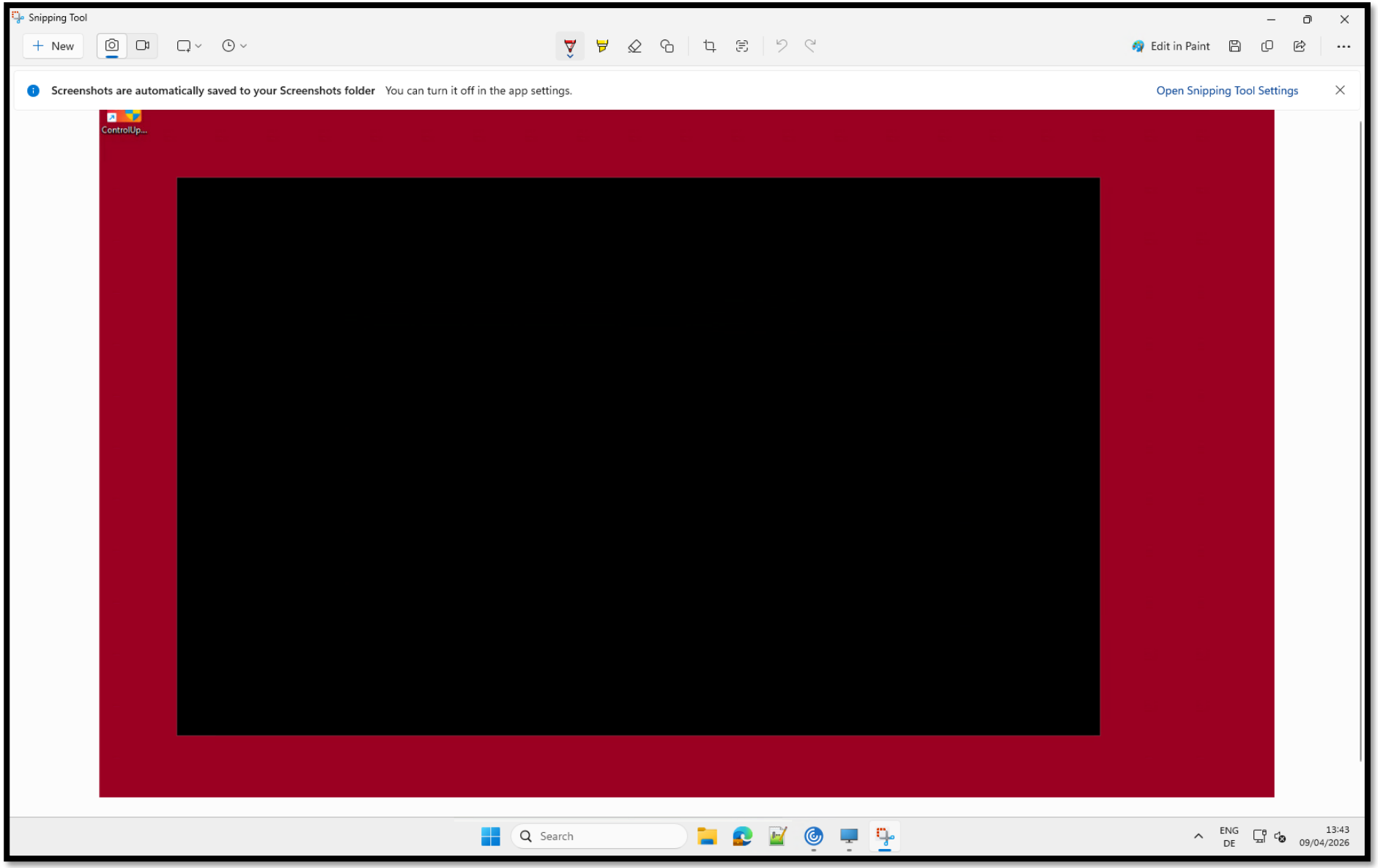
Demo

Screenshot Tool

App Protection – Ansicht User



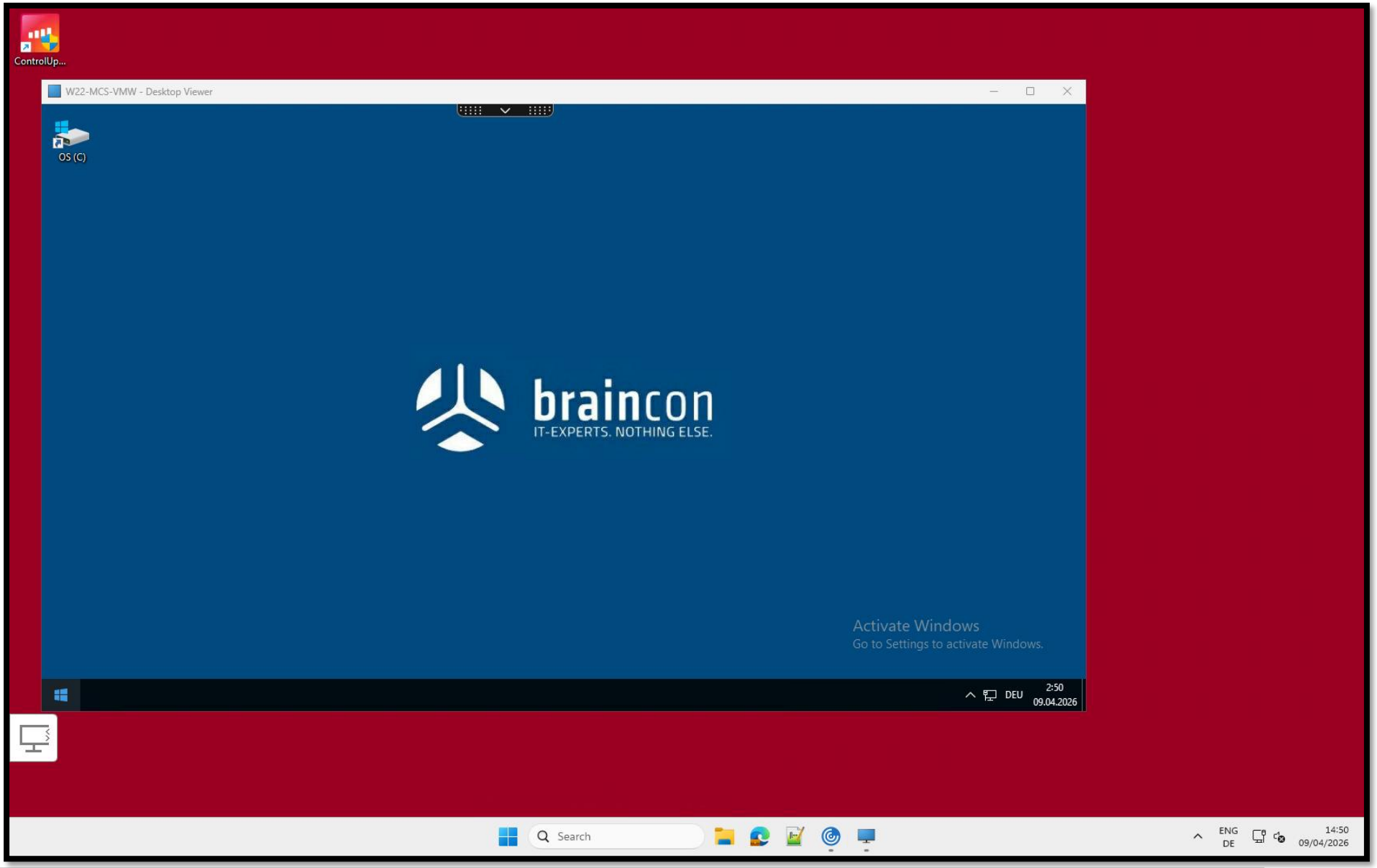
App Protection – Ansicht User Screenshot Tool



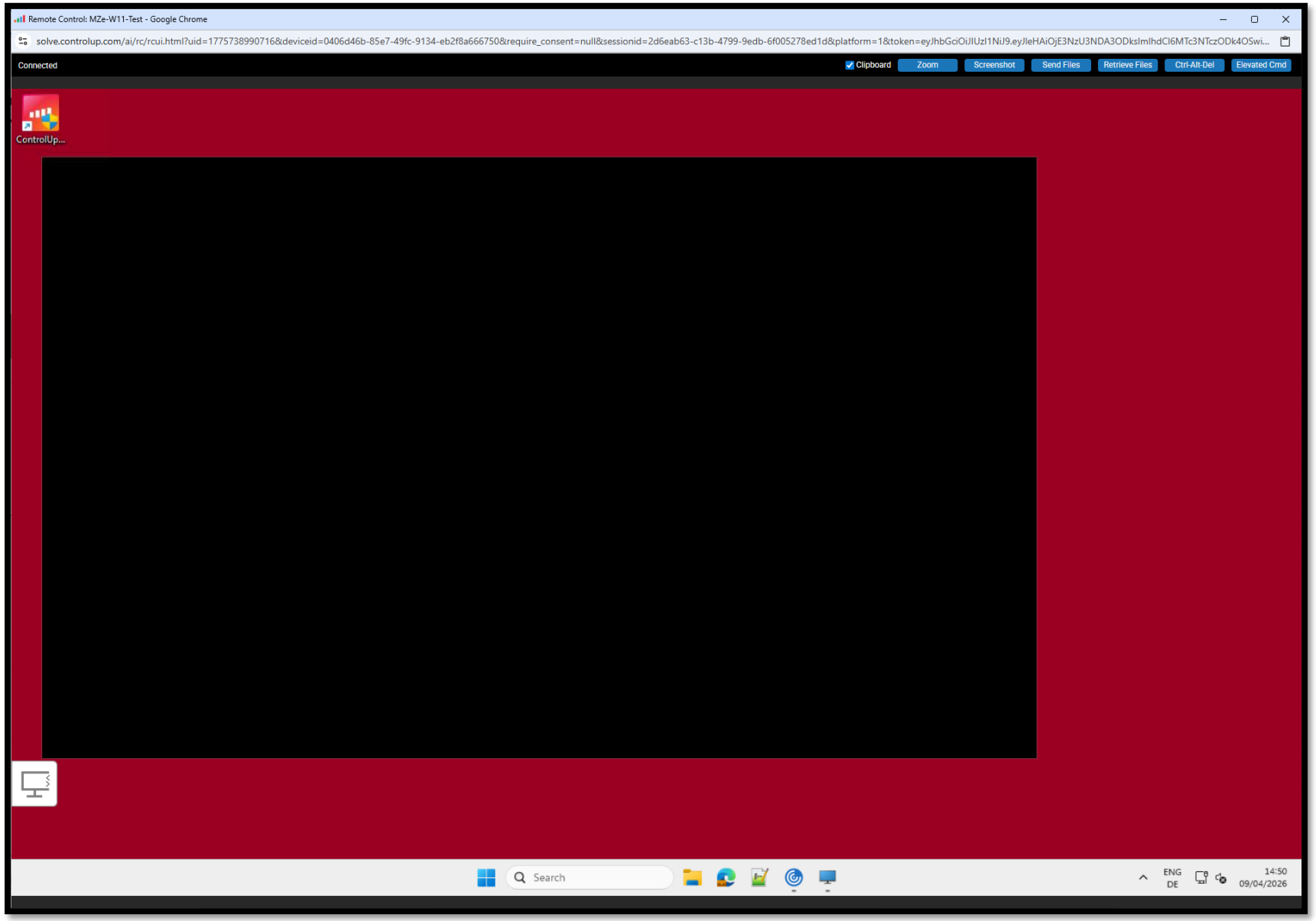
Demo

Remote Help

App Protection – Remote Help – Ansicht Benutzer



App Protection – Remote Help – Ansicht “Helfer”



Session Recording

IT-Admin Sitzungen

Externe Mitarbeiter

Kritische Ereignisse

Session Recording

Start bei bestimmten Parametern

Aufzeichnung der Benutzersitzung

IT-Admin Sitzungen

Externe Mitarbeiter

Kritische Ereignisse

Session Recording

E-Mail Alerting

SIEM Integeration

AI-Insights

Start bei bestimmten Parametern

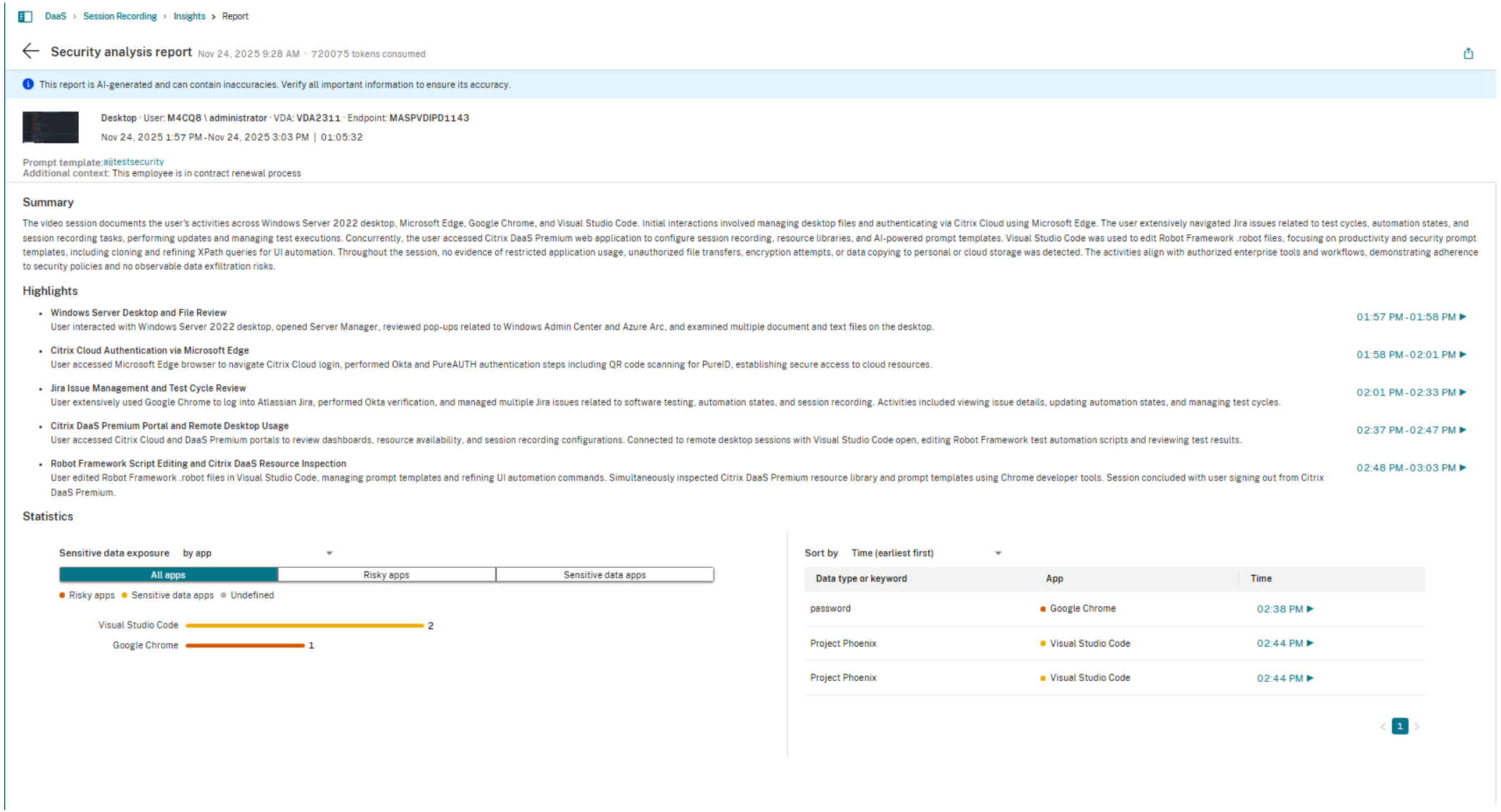
Aufzeichnung der Benutzersitzung

IT-Admin Sitzungen

Externe Mitarbeiter

Kritische Ereignisse

Session Recording – AI-Insights



Security analysis report

Nov 24, 2025 9:28 AM · 720075 tokens consumed

This report is AI-generated and can contain inaccuracies. Verify all important information to ensure its accuracy.

Desktop · User: **M4CQ8 \ administrator** · VDA: **VDA2311** · Endpoint: **MASPVDIPD1143**

Nov 24, 2025 1:57 PM - Nov 24, 2025 3:03 PM | 01:05:32

Prompt template: aijtestsecurity
Additional context: This employee is in contract renewal process

Summary

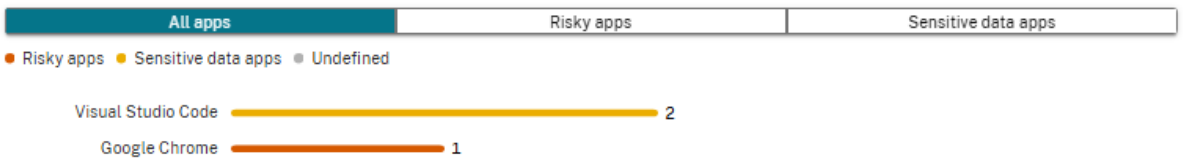
The video session documents the user's activities across Windows Server 2022 desktop, Microsoft Edge, Google Chrome, and Visual Studio Code. Initial interactions involved managing desktop files and authenticating via Citrix Cloud using Microsoft Edge. The user extensively navigated Jira issues related to test cycles, automation state session recording tasks, performing updates and managing test executions. Concurrently, the user accessed Citrix DaaS Premium web application to configure session recording, resource libraries, and AI-powered prompt templates. Visual Studio Code was used to edit Robot Framework .robot files, focusing on productivity and security templates, including cloning and refining XPath queries for UI automation. Throughout the session, no evidence of restricted application usage, unauthorized file transfers, encryption attempts, or data copying to personal or cloud storage was detected. The activities align with authorized enterprise tools and workflows, demonstrating ac to security policies and no observable data exfiltration risks.

Highlights

- **Windows Server Desktop and File Review** — 01:57 PM - 01:58
  User interacted with Windows Server 2022 desktop, opened Server Manager, reviewed pop-ups related to Windows Admin Center and Azure Arc, and examined multiple document and text files on the desktop.
- **Citrix Cloud Authentication via Microsoft Edge** — 01:58 PM - 02:01
  User accessed Microsoft Edge browser to navigate Citrix Cloud login, performed Okta and PureAUTH authentication steps including QR code scanning for PureID, establishing secure access to cloud resources.
- **Jira Issue Management and Test Cycle Review** — 02:01 PM - 02:33
  User extensively used Google Chrome to log into Atlassian Jira, performed Okta verification, and managed multiple Jira issues related to software testing, automation states, and session recording. Activities included viewing issue details, updating automation states, and managing test cycles.
- **Citrix DaaS Premium Portal and Remote Desktop Usage** — 02:37 PM - 02:47
  User accessed Citrix Cloud and DaaS Premium portals to review dashboards, resource availability, and session recording configurations. Connected to remote desktop sessions with Visual Studio Code open, editing Robot Framework test automation scripts and reviewing test results.
- **Robot Framework Script Editing and Citrix DaaS Resource Inspection** — 02:48 PM - 03:03
  User edited Robot Framework .robot files in Visual Studio Code, managing prompt templates and refining UI automation commands. Simultaneously inspected Citrix DaaS Premium resource library and prompt templates using Chrome developer tools. Session concluded with user signing out from Citrix DaaS Premium.

Statistics

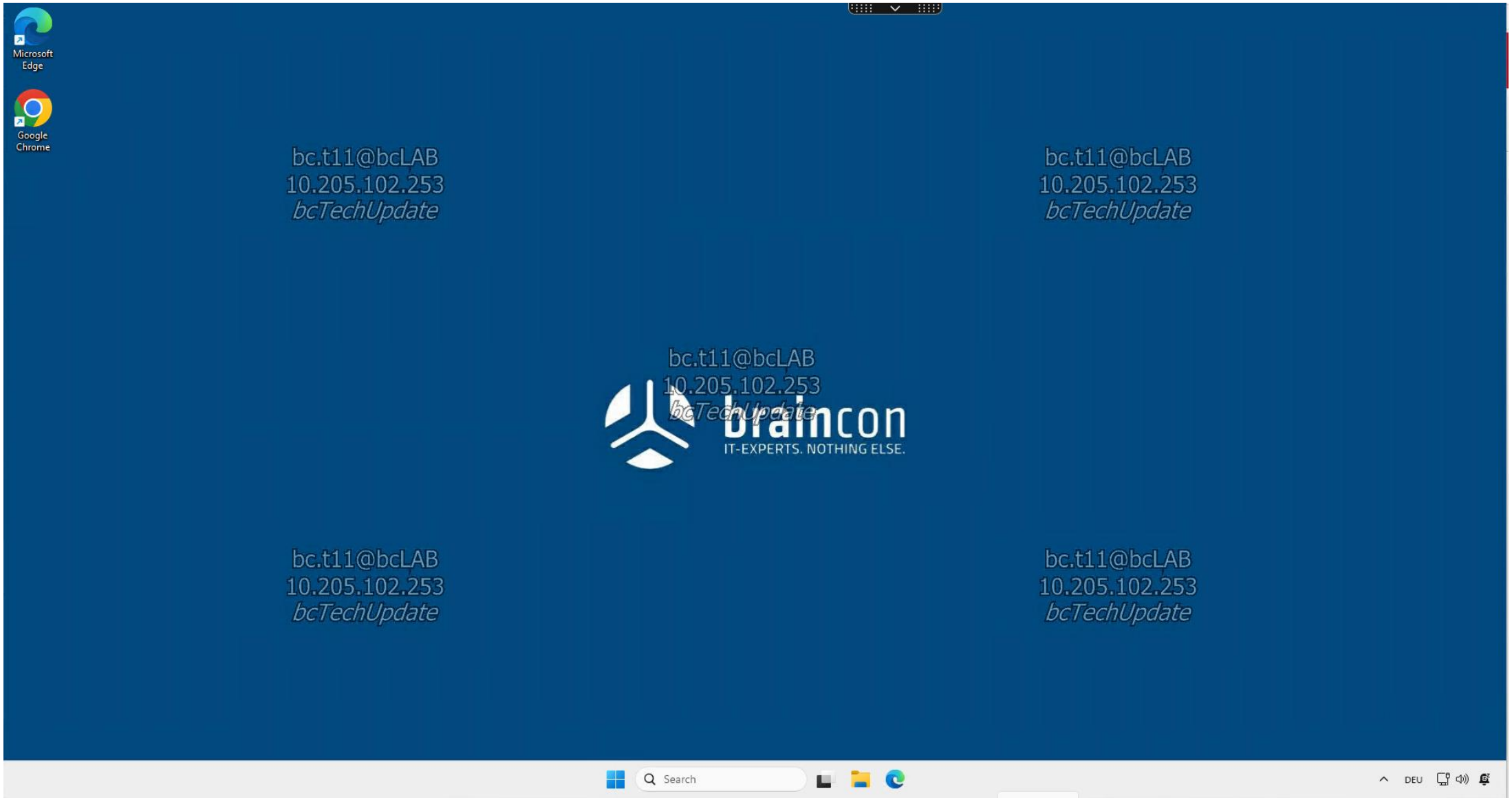
Sensitive data exposure by app



Sort by Time (earliest first)

Data type or keyword	App	Time
password	Google Chrome	02:38 PM ▶
Project Phoenix	Visual Studio Code	02:44 PM ▶
Project Phoenix	Visual Studio Code	02:44 PM ▶

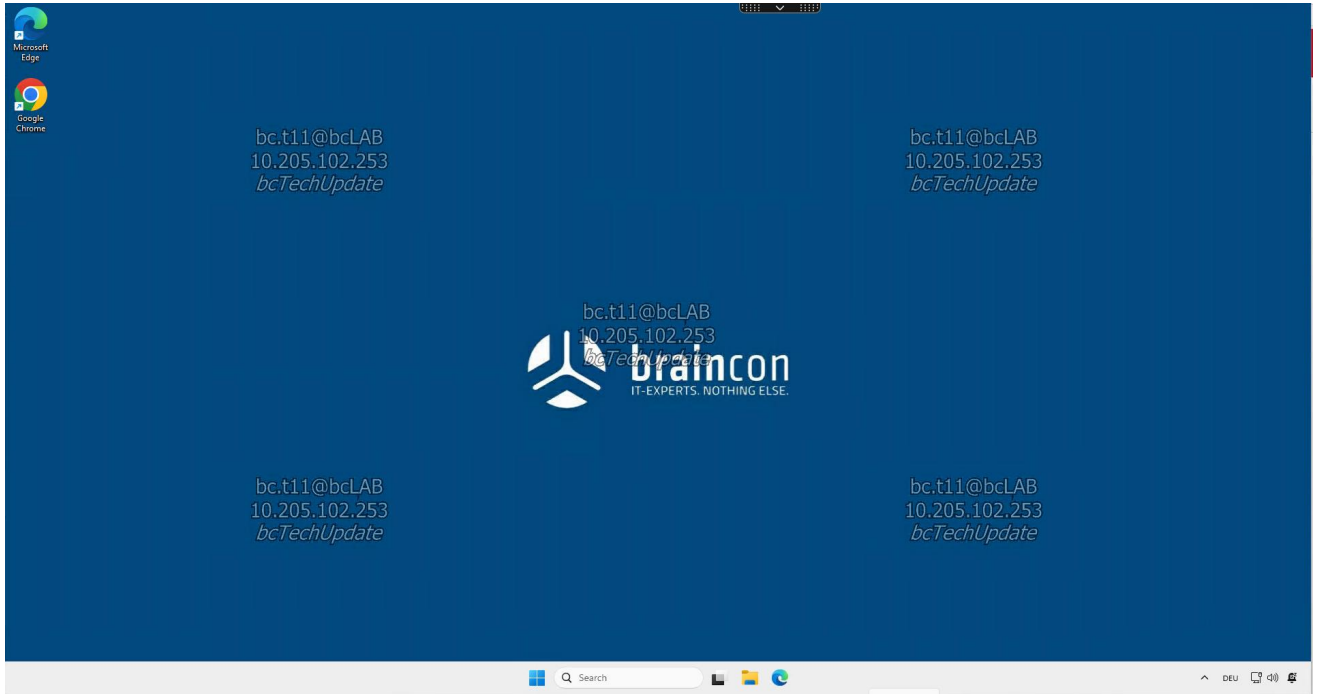
Session Watermarking




Braincon
IT-EXPERTS. NOTHING ELSE.

Session Watermarking

- Wasserzeichen wird in die Citrix Sitzung integriert
- Performance Unterschied ist in der Regel minimal
- Deutlich höhere Bandbreite
- Wasserzeichen in der Citrix Sitzung
  - Eigener Text
  - Client IP-Adresse
  - Zeit Verbindungsaufbau
  - Benutzername
  - VDA Hostname
  - VDA -P-Adresse



Übersicht

Produkt	Lizenz
AppLocker	Ab Windows Server 2022 bzw. Windows 10 2004 Bestandteil aller Editionen

Übersicht

Produkt	Lizenz
AppLocker	Ab Windows Server 2022 bzw. Windows 10 2004 Bestandteil aller Editionen
ASR	Microsoft Defender for Endpoint (lizenziert über die angemeldeten Benutzer) oder Microsoft Defender for Endpoint for Servers

Übersicht

Produkt	Lizenz
AppLocker	Ab Windows Server 2022 bzw. Windows 10 2004 Bestandteil aller Editionen
ASR	Microsoft Defender for Endpoint (lizenziert über die angemeldeten Benutzer) oder Microsoft Defender for Endpoint for Servers
BSI	Kostenlos

Übersicht

Produkt	Lizenz
AppLocker	Ab Windows Server 2022 bzw. Windows 10 2004 Bestandteil aller Editionen
ASR	Microsoft Defender for Endpoint (lizenziert über die angemeldeten Benutzer) oder Microsoft Defender for Endpoint for Servers
BSI	Kostenlos
CIS	PDFs kostenlos, GPOs kostenpflichtig

Übersicht

Produkt	Lizenz
AppLocker	Ab Windows Server 2022 bzw. Windows 10 2004 Bestandteil aller Editionen
ASR	Microsoft Defender for Endpoint (lizenziert über die angemeldeten Benutzer) oder Microsoft Defender for Endpoint for Servers
BSI	Kostenlos
CIS	PDFs kostenlos, GPOs kostenpflichtig
deviceTRUST	Citrix UHMC & Citrix Platform

Übersicht

Produkt	Lizenz
AppLocker	Ab Windows Server 2022 bzw. Windows 10 2004 Bestandteil aller Editionen
ASR	Microsoft Defender for Endpoint (lizenziert über die angemeldeten Benutzer) oder Microsoft Defender for Endpoint for Servers
BSI	Kostenlos
CIS	PDFs kostenlos, GPOs kostenpflichtig
deviceTRUST	Citrix UHMC & Citrix Platform
Session Recording	Citrix UHMC & Citrix Platform

Übersicht

Produkt	Lizenz
AppLocker	Ab Windows Server 2022 bzw. Windows 10 2004 Bestandteil aller Editionen
ASR	Microsoft Defender for Endpoint (lizenziert über die angemeldeten Benutzer) oder Microsoft Defender for Endpoint for Servers
BSI	Kostenlos
CIS	PDFs kostenlos, GPOs kostenpflichtig
deviceTRUST	Citrix UHMC & Citrix Platform
Session Recording	Citrix UHMC & Citrix Platform
Session Recording AI Insights	Open-AI API Tokens
Session Watermarking	Beliebige Citrix Lizenz

DANKE

Fragen? Gerne!

braincon GmbH

+49 6071 180 300
info@braincon.de
www.braincon.de

Region Rhein-Main

Altheimer Straße 4
64807 Dieburg

Region Rhein-Ruhr

Lise-Meitner-Straße 1-13
42119 Wuppertal

braincon
IT-EXPERTS. NOTHING ELSE.

The Digital Workplace Experts!

Modern. Secured. Managed.