deviceTRUST

Online-Event: Homeoffice ? Aber sicher!

deviceTRUST

Online-Event: Homeoffice? Aber sicher!

Über uns

- Deutscher Softwarehersteller gegründet 2016
- Marktführer für kontextbasierte Sicherheit digitaler Arbeitsplätze
- Kunden in allen Branchen und Größen
- Kooperationen mit den führenden IT-Resellern
- Starke Allianzen mit führenden Lösungsanbietern

Hauptsitz des Unternehmens
HUB31, Darmstadt DE

Starke Partner

Als deutscher Softwarehersteller im Bereich der IT-Sicherheit gehören wir zum Portfolio starker europäischer Investoren:

High-Tech Gründerfonds

HESSEN HessenKapital

TFH

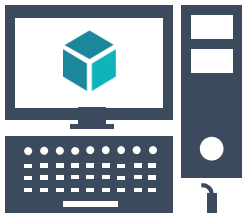
TFH III Technologiefonds Hessen GmbH

Warum deviceTRUST

Digitaler Arbeitsplatz

Unternehmens -desktops	Unternehmens -anwendungen	Unternehmens -ressourcen

On-Premises, Cloud und Lokal



PC / Thin Client

Unternehmen

Warum deviceTRUST

Digitaler Arbeitsplatz

Unternehmens -desktops

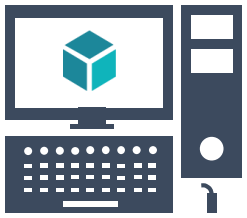
Unternehmens -anwendungen

Unternehmens -ressourcen

On-Premises, Cloud und Lokal

Sicherheits-, Compliance- und regulatorische Anforderungen

Benutzerauthentifizierung



PC / Thin Client

Unternehmen

Warum deviceTRUST

Digitaler Arbeitsplatz

Unternehmens -desktops

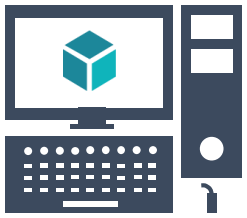
Unternehmens -anwendungen

Unternehmens -ressourcen

On-Premises, Cloud und Lokal

Sicherheits-, Compliance- und regulatorische Anforderungen

Benutzerauthentifizierung



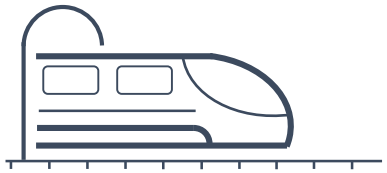
PC / Thin Client

Unternehmen

Managed / BYOD

Home Office

Externe Partner



Mobil

Warum deviceTRUST

Digitaler Arbeitsplatz

Unternehmens -desktops

Unternehmens -anwendungen

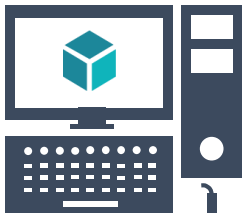
Unternehmens -ressourcen

On-Premises, Cloud und Lokal

Sicherheits-, Compliance- und regulatorische Anforderungen

deviceTRUST Kontextbasierte Sicherheit

Benutzerauthentifizierung



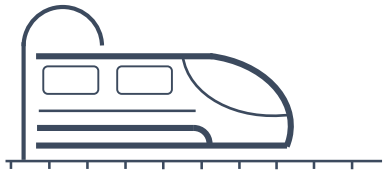
PC / Thin Client

Unternehmen

Managed / BYOD

Home Office

Externe Partner

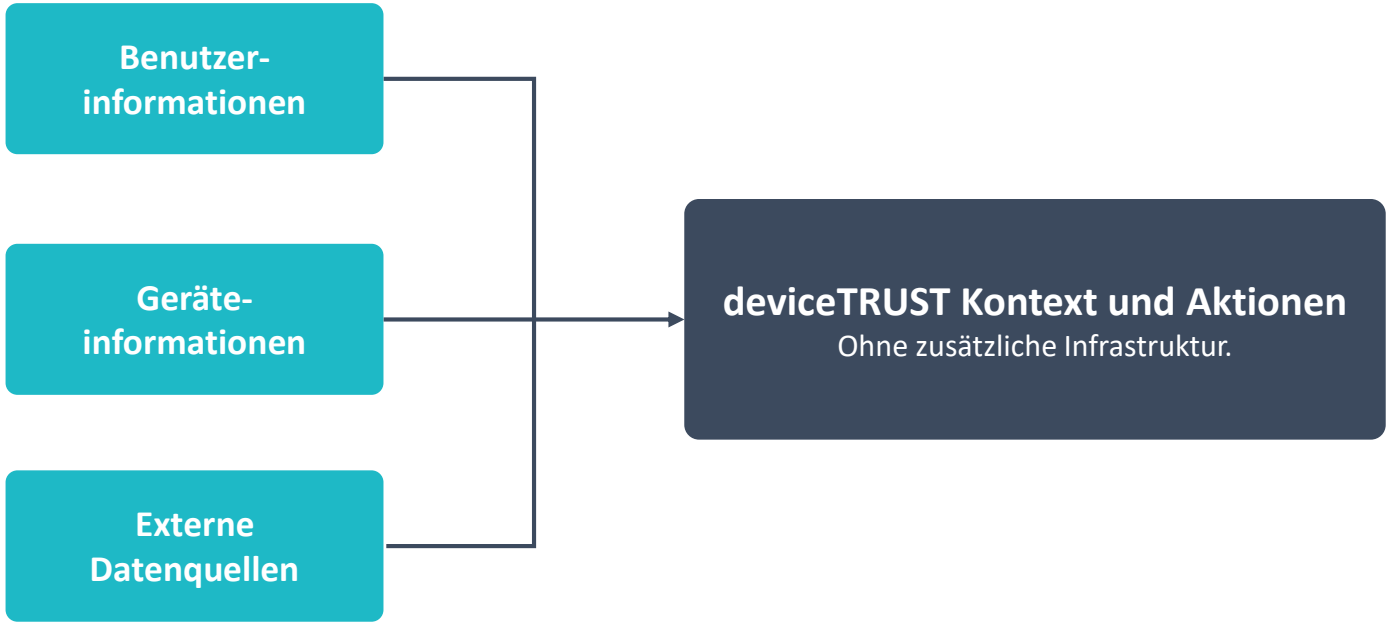


Mobil

deviceTRUST Kontextbasierte Sicherheit

deviceTRUST Kontext und Aktionen
Ohne zusätzliche Infrastruktur.

deviceTRUST Kontextbasierte Sicherheit



deviceTRUST Kontextbasierte Sicherheit

deviceTRUST

Home Office Use Case

Home Office

- Mitarbeiter müssen in der Lage sein, uneingeschränkt mit allen erforderlichen Anwendungen, identisch wie innerhalb des Unternehmensnetzwerkes, aus ihrem Home Office heraus zu arbeiten.
- Die Mitarbeiter greifen hierbei jedoch von extern auf ihren virtuellen Arbeitsplatz zu, dabei hat die IT keinerlei Informationen womit und von wo zugegriffen wird.
- Hieraus ergibt sich ein hohes Sicherheits- und Compliancerisiko für das Unternehmen, da die Rolle des Mitarbeiters im Unternehmen nicht ausreicht, um die Zugriffe auf den virtuellen Arbeitsplatz sowie die Anwendungen zu steuern.

deviceTRUST

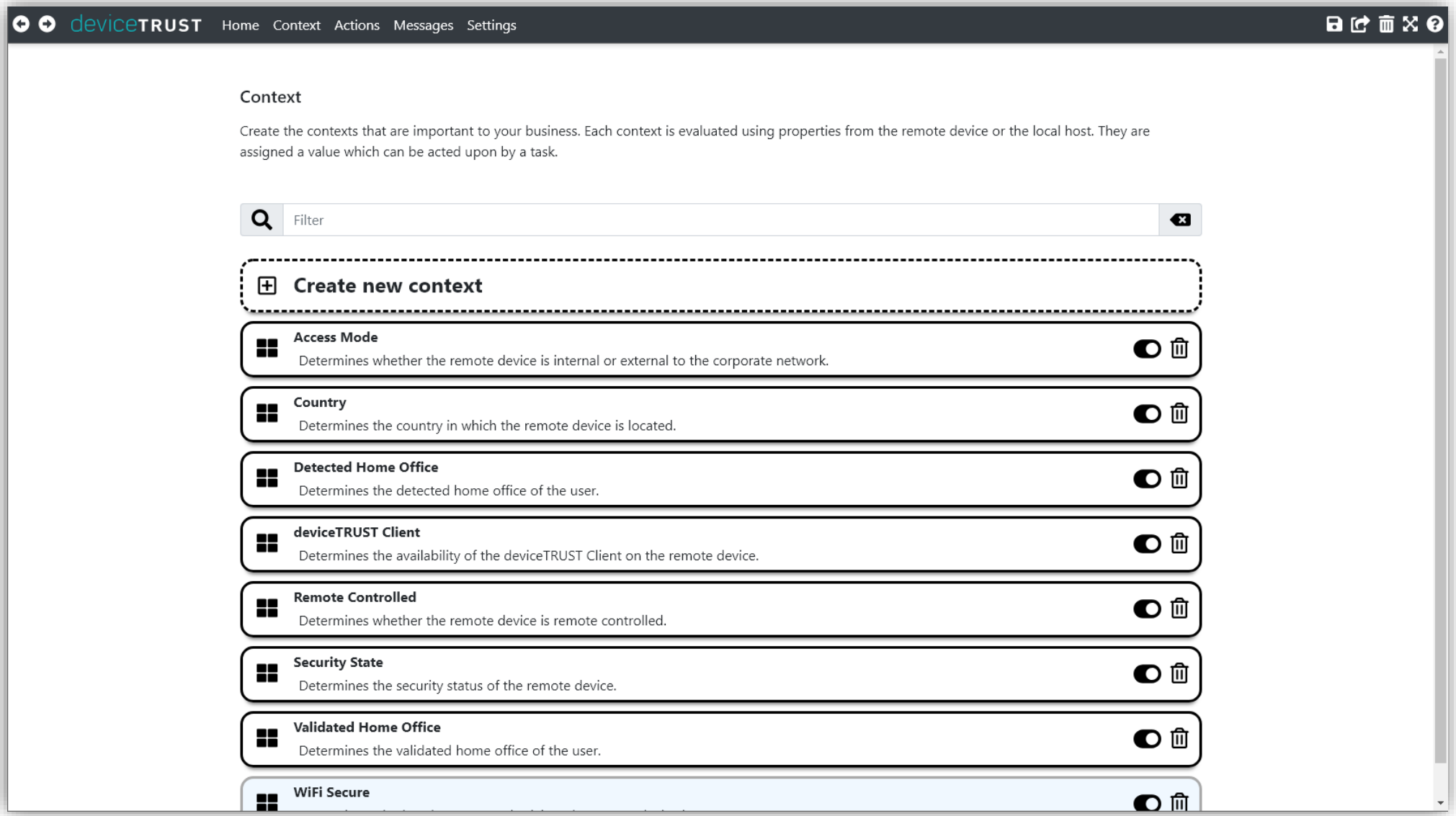
Demo: Compliance Check

Home Office

Option 1: Compliance Check

- Zugriffsmethode
- Authorisiertes Land
- Sicheres Netzwerk (Kein ungesichertes WLAN)
- Benutzerrechte
- Endgerätezugriff (Endgerät wird nicht “ferngesteuert”)
- Unternehmensgerät / BYOD
- Sicheres Endgerät
- …

Option 1: Compliance Check



deviceTRUST

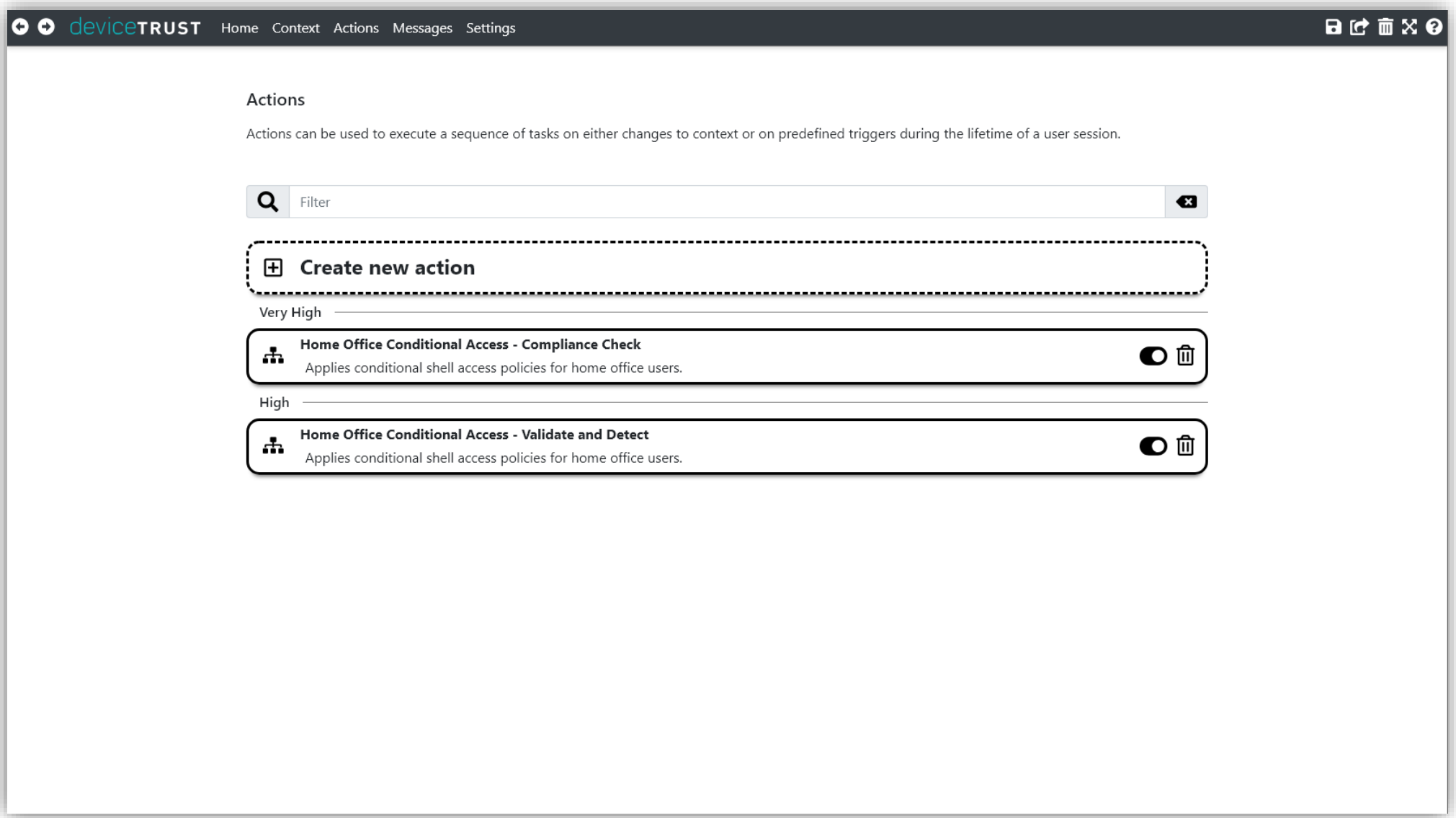
Demo: Validieren und Erkennen

Home Office

Option 2: Validieren und Erkennen

- Validierung der aktuellen Home Office Umgebung
- Erkennen der aktuellen Umgebung und sicherstellen, dass es sich um das Home Office handelt

Option 2: Validieren und Erkennen



Richtlinien Varianten

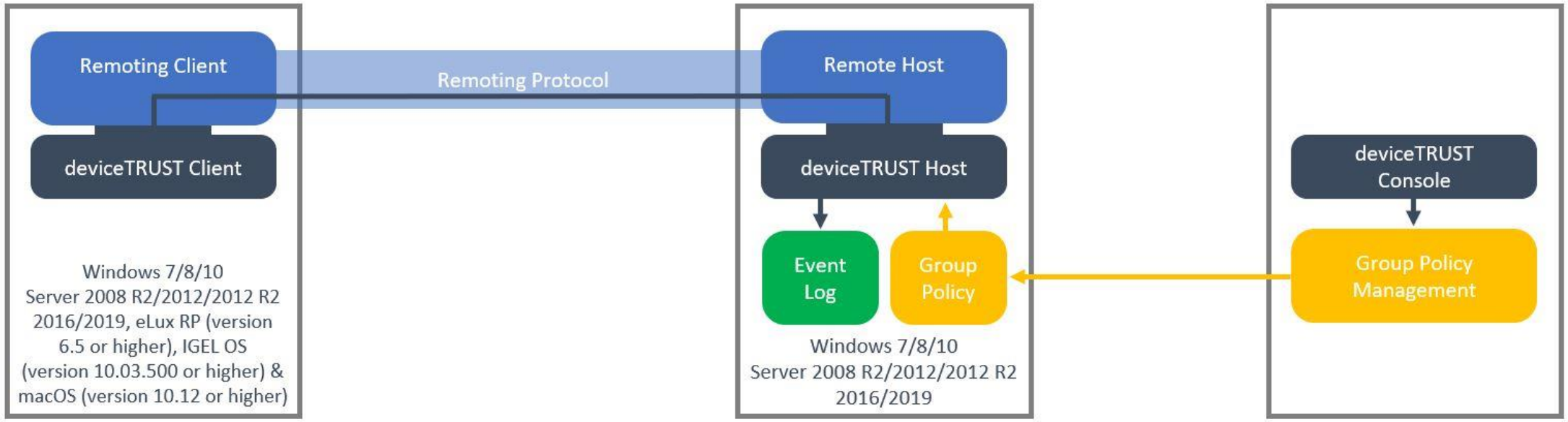
Variante	Unternehmensnetzwerk	Validiertes Home Office	Extern
Use Case 1	Vollzugriff	Vollzugriff	Kein Zugriff
Use Case 2	Vollzugriff	Vollzugriff	Eingeschränkter Zugriff (z.B. bestimmte Applikationen unterbinden)

Unterstützte Remoting-Protokolle

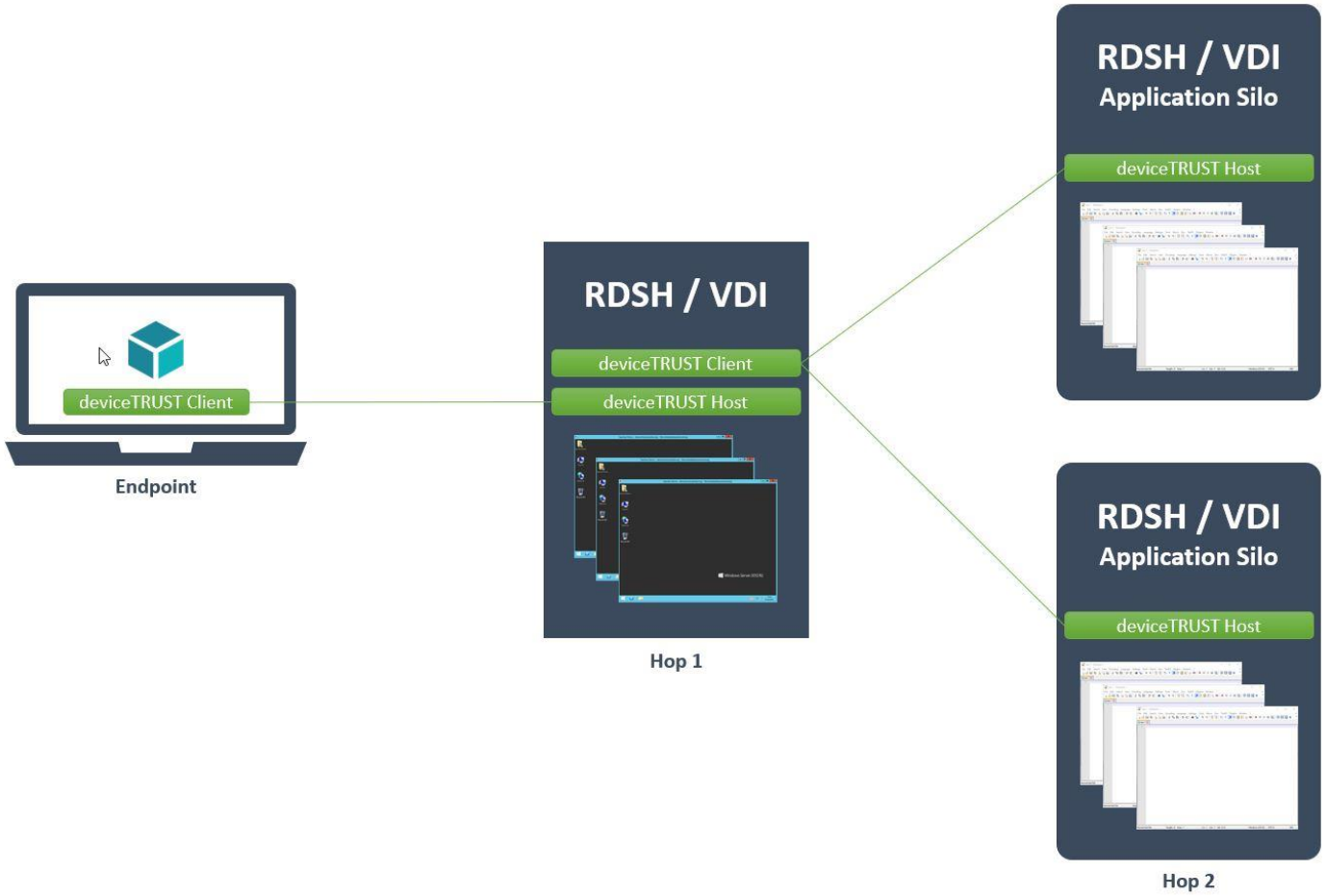
- Amazon WorkSpaces PC-over-IP (PCoIP)
- Citrix Independent Computing Architecture (ICA)
- Citrix High Definition Experience (HDX)
- Microsoft Remote Desktop Protocol (RDP)
- Microsoft Windows Virtual Desktops (WVD)
- VMware Horizon View BLAST
- VMware Horizon View PC-over-IP (PCoIP)
- VMware Horizon View Microsoft Remote Desktop Protocol (RDP)

deviceTRUST Architektur - Keine Infrastruktur erforderlich!

deviceTRUST Architecture Diagram for Windows, eLux RP, IGEL OS & macOS Endpoints

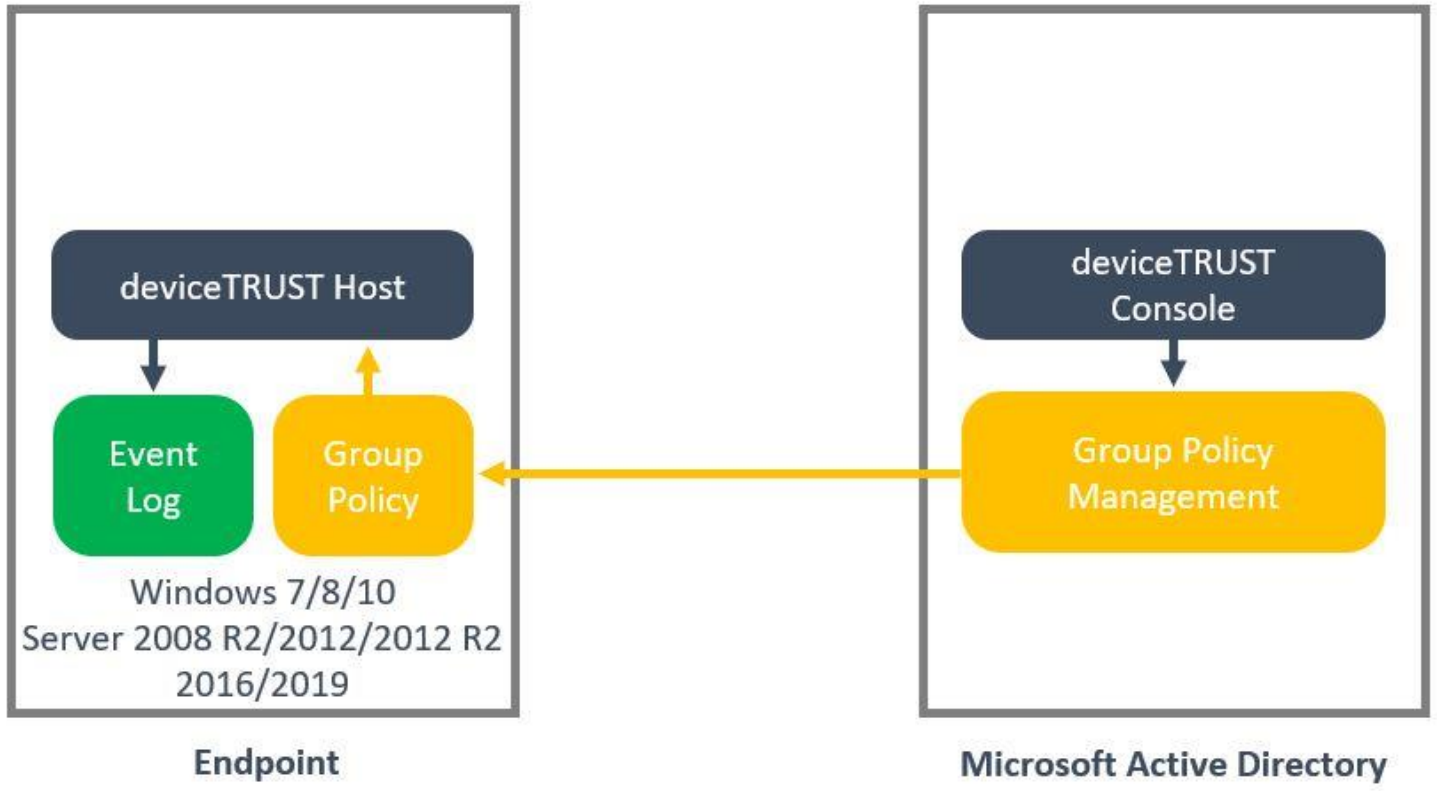


deviceTRUST Architektur - Keine Infrastruktur erforderlich!



deviceTRUST Architektur - Keine Infrastruktur erforderlich!

deviceTRUST Architecture Diagram for Windows Endpoints



Zusammenfassung

Digitaler Arbeitsplatz

Unternehmens -desktops

Unternehmens -anwendungen

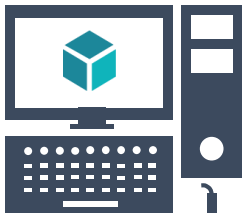
Unternehmens -ressourcen

On-Premises, Cloud und Lokal

Sicherheits-, Compliance- und regulatorische Anforderungen

deviceTRUST Kontextbasierte Sicherheit

Benutzerauthentifizierung



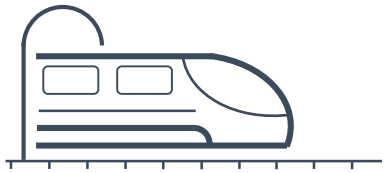
PC / Thin Client

Unternehmen

Managed / BYOD

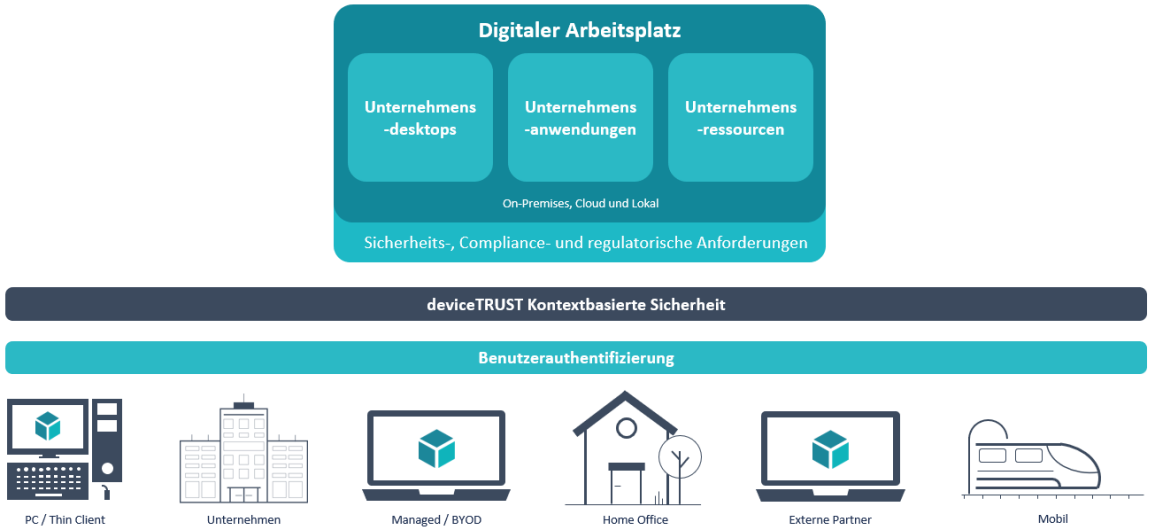
Home Office

Externe Partner



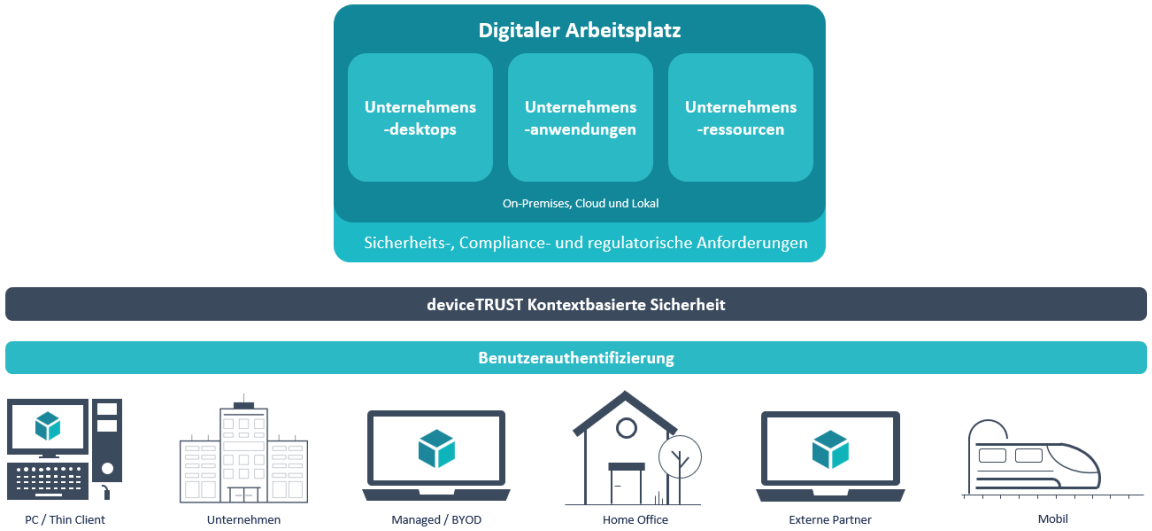
Mobil

Use Cases



- Home Office
- Externe Partner
- Lizenz-Compliance
- Silo Optimierung
- Compliance Check
- Bring your own Device (BYOD)
- Compliant Anwendungs-zugriff
- Unerlaubte USB Laufwerke
- Compliant Backend Zugriff
- Lokations-abhängiges Drucken
- Meeting Raum
- Dynamische Policies

Alleinstellungsmerkmale



- Keine Ablösung der vorhandenen Benutzerauthentifizierung
- Keine zusätzliche Infrastruktur notwendig
- Nutzung vorhandener Zugriffstechnologien
- Integration in vorhandene Managementlösungen
- Kein Endgeräte Management erforderlich

✓ Geringe Betriebsaufwände
✓ Schnelle Implementierung
✓ Plattform-übergreifend
✓ Zukunftssicher

Ihre Kontakte

Marc Stieber

marc.stieber@devicetrust.com

+49 (171) 8370900

Sascha Göckel

sascha.goeckel@devicetrust.com

+49 (151) 20522308

Vielen Dank

Möchten Sie noch weitere Informationen über unsere Lösung:

Internet:	https://devicetrust.com
E-Mail:	sales@devicetrust.com
Twitter:	@deviceTRUST