

device**TRUST**



Online-Event: Homeoffice ? Aber sicher!

device**TRUST**

Online-Event: Homeoffice? Aber sicher!

- 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



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



Warum deviceTRUST



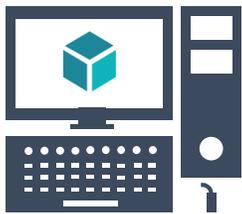
Digitaler Arbeitsplatz

Unternehmens
-desktops

Unternehmens
-anwendungen

Unternehmens
-ressourcen

On-Premises, Cloud und Lokal



PC / Thin Client



Unternehmen

Warum deviceTRUST



Digitaler Arbeitsplatz

Unternehmens
-desktops

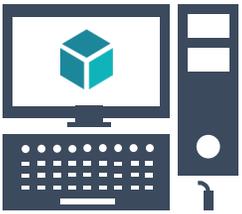
Unternehmens
-anwendungen

Unternehmens
-ressourcen

On-Premises, Cloud und Lokal

Sicherheits-, Compliance- und regulatorische Anforderungen

Benutzerauthentifizierung



PC / Thin Client



Unternehmen

Digitaler Arbeitsplatz

Unternehmens
-desktops

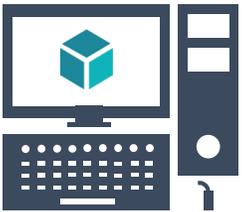
Unternehmens
-anwendungen

Unternehmens
-ressourcen

On-Premises, Cloud und Lokal

Sicherheits-, Compliance- und regulatorische Anforderungen

Benutzerauthentifizierung



PC / Thin Client



Unternehmen



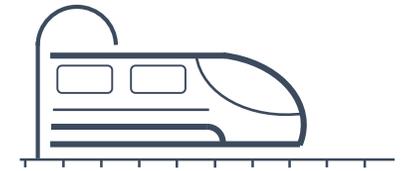
Managed / BYOD



Home Office



Externe Partner



Mobil

Warum deviceTRUST



Digitaler Arbeitsplatz

Unternehmens
-desktops

Unternehmens
-anwendungen

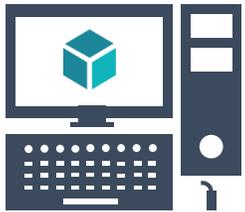
Unternehmens
-ressourcen

On-Premises, Cloud und Lokal

Sicherheits-, Compliance- und regulatorische Anforderungen

deviceTRUST Kontextbasierte Sicherheit

Benutzerauthentifizierung



PC / Thin Client



Unternehmen



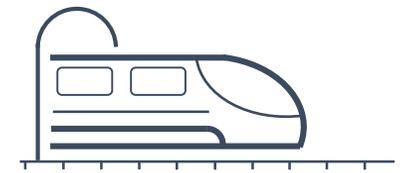
Managed / BYOD



Home Office

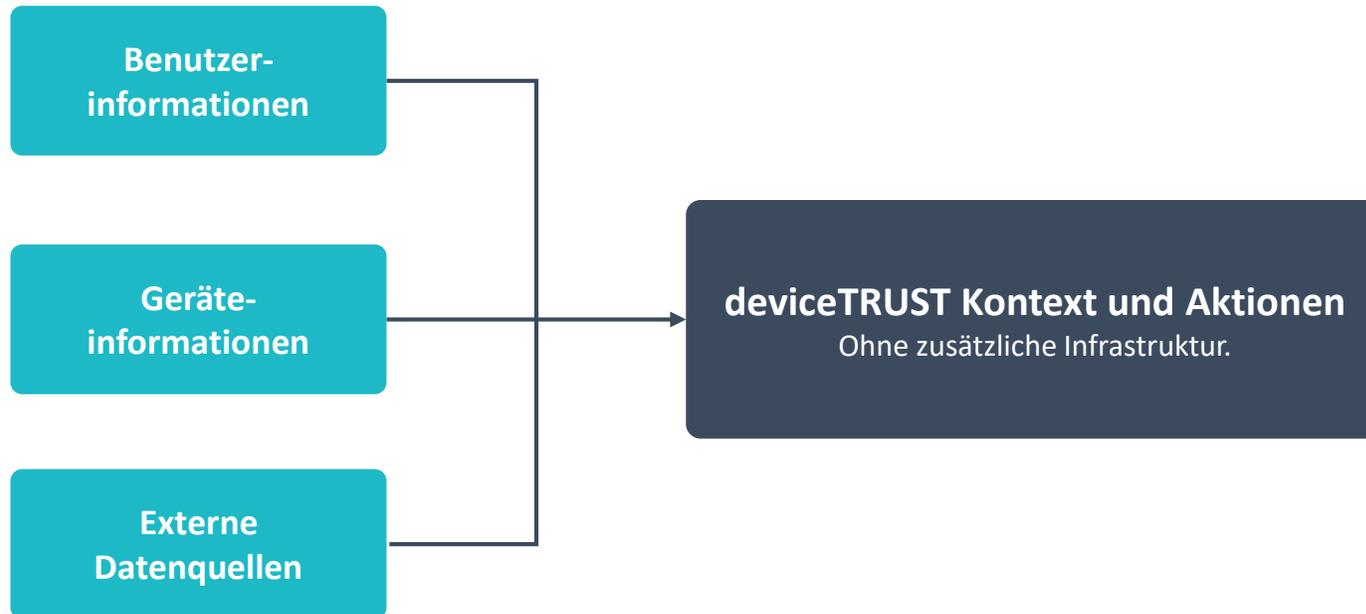


Externe Partner



Mobil

deviceTRUST Kontext und Aktionen
Ohne zusätzliche Infrastruktur.





Home Office Use Case

- 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 Compiancerisiko für das Unternehmen, da die Rolle des Mitarbeiters im Unternehmen nicht ausreicht, um die Zugriffe auf den virtuellen Arbeitsplatz sowie die Anwendungen zu steuern.

Demo: Compliance Check

Option 1: Compliance Check

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

Option 1: Compliance Check



The screenshot displays the 'Context' management page in the deviceTRUST application. The page includes a navigation bar with 'Home', 'Context', 'Actions', 'Messages', and 'Settings'. Below the navigation, there is a 'Context' section with an explanatory paragraph: 'Create the contexts that are important to your business. Each context is evaluated using properties from the remote device or the local host. They are assigned a value which can be acted upon by a task.' A search filter is present above a list of contexts. A dashed box highlights the 'Create new context' button. The list of contexts includes: Access Mode, Country, Detected Home Office, deviceTRUST Client, Remote Controlled, Security State, Validated Home Office, and WiFi Secure. Each context entry has a toggle switch and a delete icon.

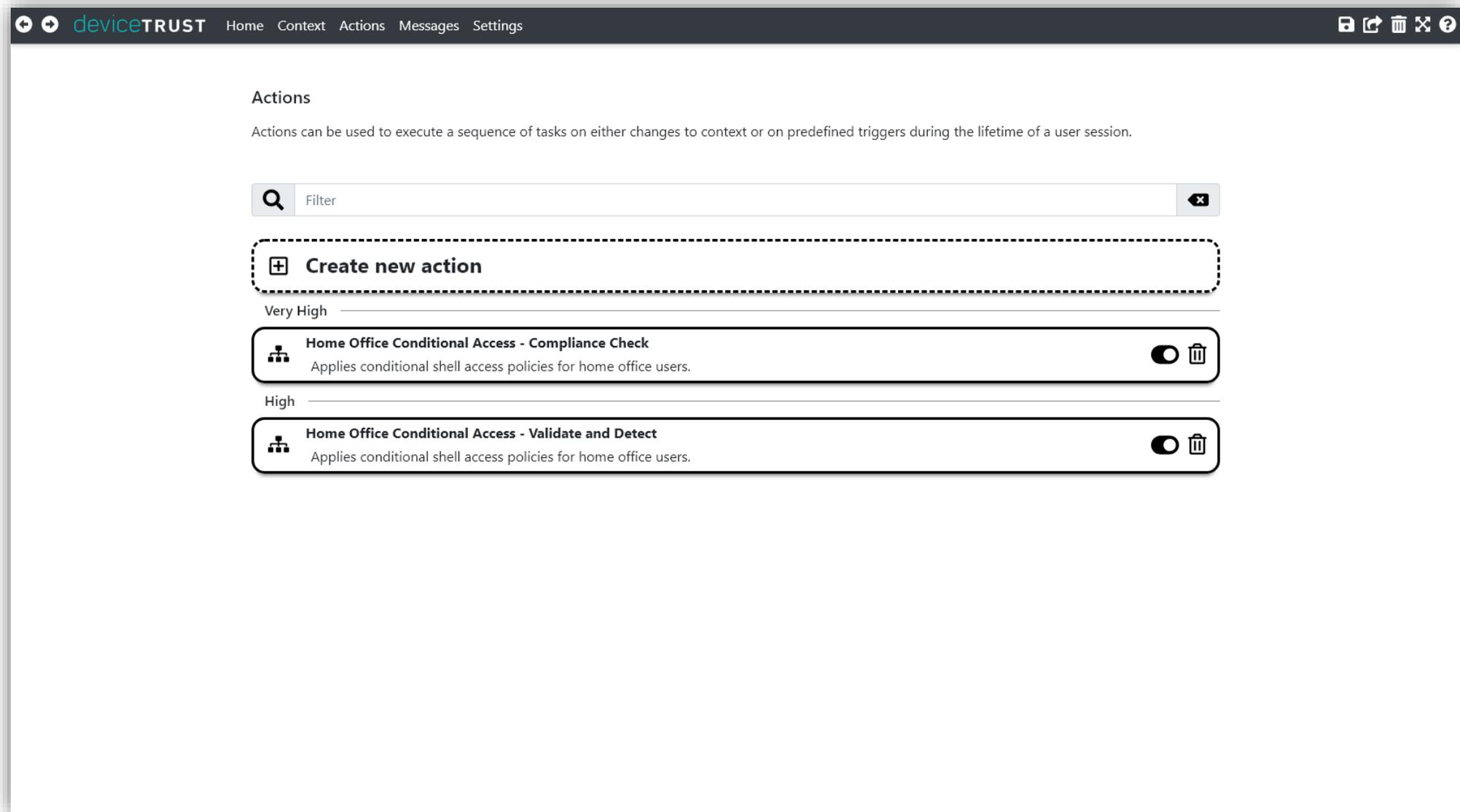
Context Name	Description	Toggle	Delete
Access Mode	Determines whether the remote device is internal or external to the corporate network.	On	Yes
Country	Determines the country in which the remote device is located.	On	Yes
Detected Home Office	Determines the detected home office of the user.	On	Yes
deviceTRUST Client	Determines the availability of the deviceTRUST Client on the remote device.	On	Yes
Remote Controlled	Determines whether the remote device is remote controlled.	On	Yes
Security State	Determines the security status of the remote device.	On	Yes
Validated Home Office	Determines the validated home office of the user.	On	Yes
WiFi Secure		On	Yes

Demo: Validieren und Erkennen

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



The screenshot shows the 'Actions' page in the deviceTRUST interface. At the top, there is a navigation bar with the 'deviceTRUST' logo and menu items: Home, Context, Actions, Messages, and Settings. On the right side of the navigation bar are icons for save, share, delete, and help. Below the navigation bar, the page title 'Actions' is displayed, followed by a descriptive sentence: 'Actions can be used to execute a sequence of tasks on either changes to context or on predefined triggers during the lifetime of a user session.' A search bar with a magnifying glass icon and the placeholder text 'Filter' is located below the description. A dashed-line box highlights a button with a plus sign and the text 'Create new action'. Below this, the page is organized into sections based on priority. The 'Very High' section contains one action: 'Home Office Conditional Access - Compliance Check', which is currently disabled (indicated by a grey toggle switch) and has a trash icon to its right. The description for this action is 'Applies conditional shell access policies for home office users.' The 'High' section contains one action: 'Home Office Conditional Access - Validate and Detect', which is also disabled and has a trash icon. Its description is 'Applies conditional shell access policies for home office users.'

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

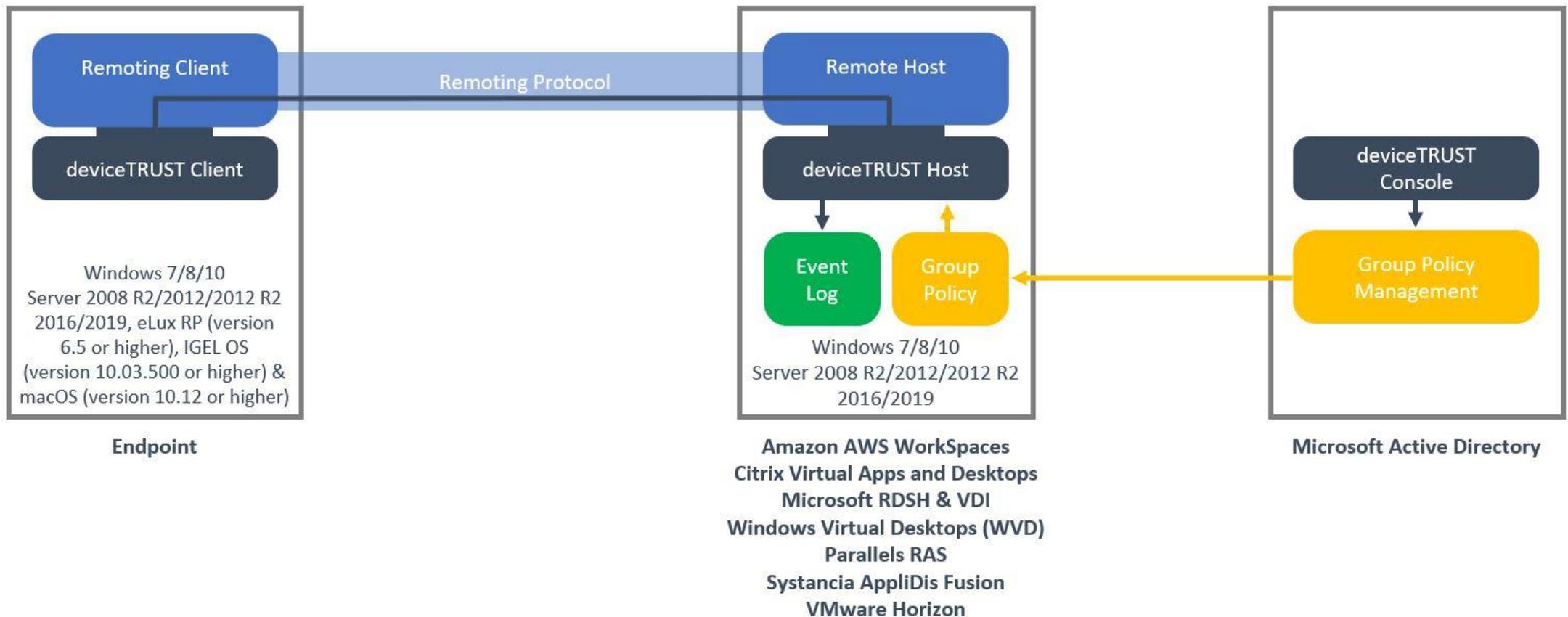


- Amazon WorkSpaces PC-over-IP (PCoIP)
- Citrix Independent Computing Architecture (ICA)
- Citrix High Definition Experience (HDX)
- Microsoft Remote Desktop Protocol (RDP)
- Microsoft Windows Virtual Desktops (WVD)
- VMware Horizon View BLAST
- VMware Horizon View PC-over-IP (PCoIP)
- VMware Horizon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

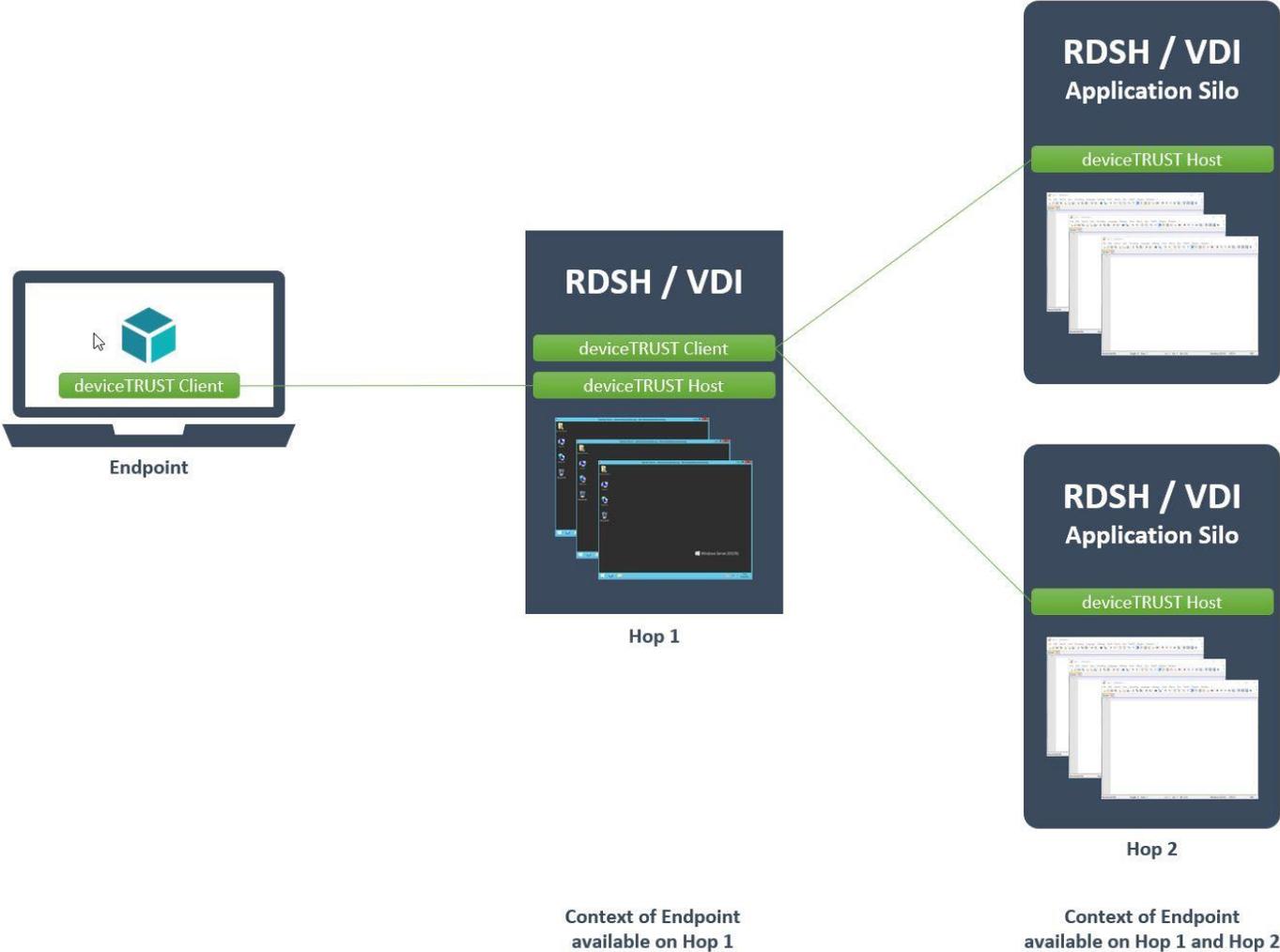
deviceTRUST Architektur - Keine Infrastruktur erforderlich!



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



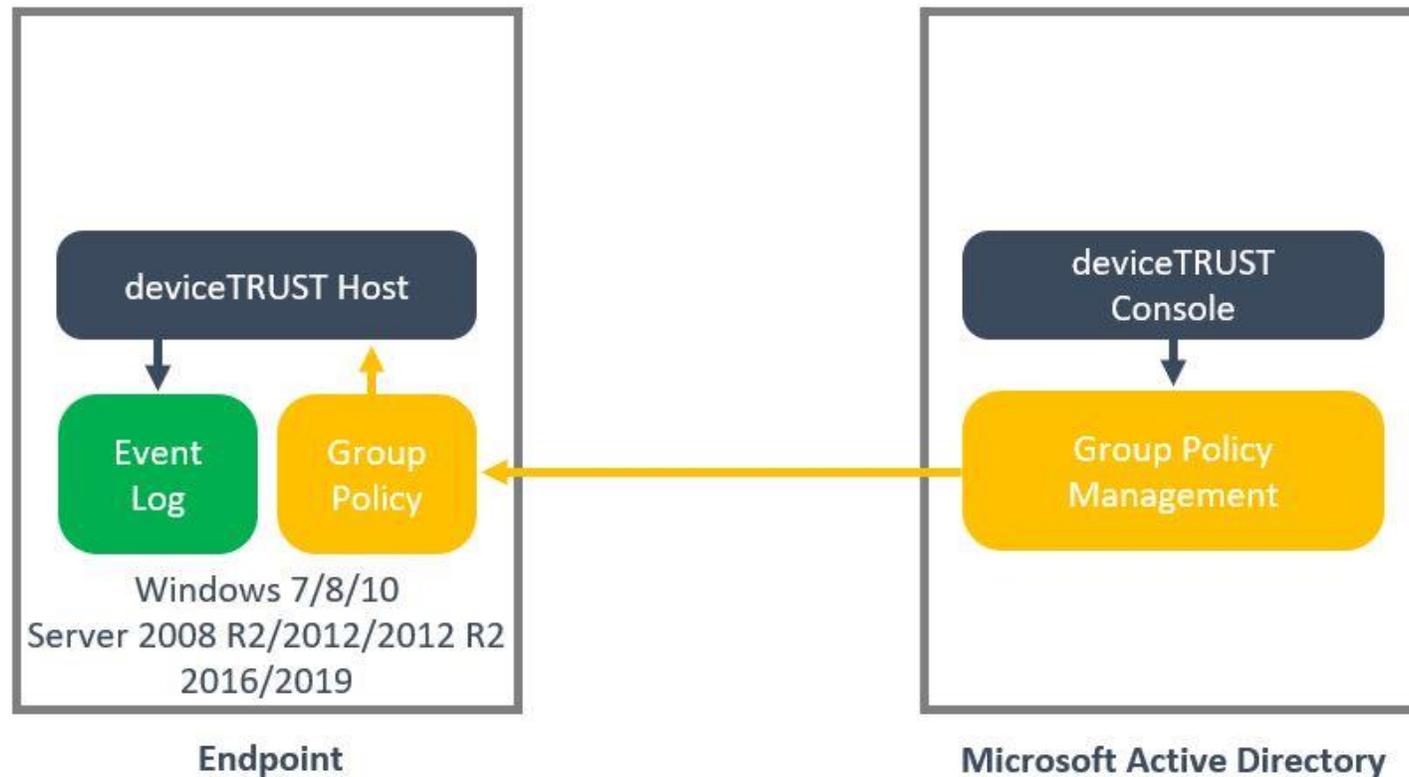
deviceTRUST Architektur - Keine Infrastruktur erforderlich!



deviceTRUST Architektur - Keine Infrastruktur erforderlich!



deviceTRUST Architecture Diagram for Windows Endpoints



Digitaler Arbeitsplatz

Unternehmens
-desktops

Unternehmens
-anwendungen

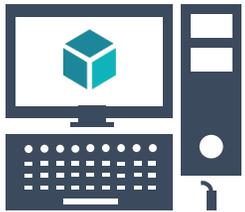
Unternehmens
-ressourcen

On-Premises, Cloud und Lokal

Sicherheits-, Compliance- und regulatorische Anforderungen

deviceTRUST Kontextbasierte Sicherheit

Benutzerauthentifizierung



PC / Thin Client



Unternehmen



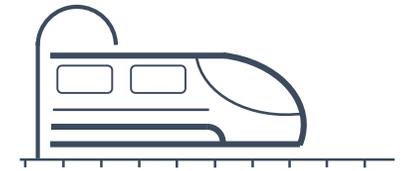
Managed / BYOD



Home Office



Externe Partner



Mobil





deviceTRUST Kontextbasierte Sicherheit

Benutzerauthentifizierung



- 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

Marc Stieber



marc.stieber@devicetrust.com

+49 (171) 8370900



Sascha Göckel



sascha.goeckel@devicetrust.com

+49 (151) 20522308



Möchten Sie noch weitere Informationen über unsere Lösung:

Internet: <https://devicetrust.com>

E-Mail: sales@devicetrust.com

Twitter: @deviceTRUST