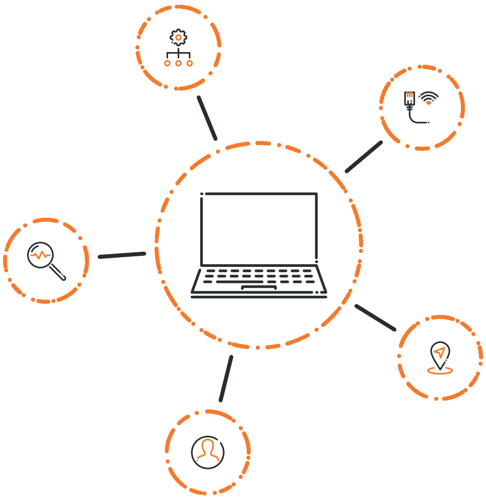
deviceTRUST

Zero Trust Requires Device Trust

deviceTRUST adds an additional level of security to your Zero Trust strategy. Rich context information and multiple actions via a central management interface across all deployment methods.

Use your devices as a security factor and bring your conditional access to the next level!



Context as a Factor

deviceTRUST Contextual Security is the layer to protect a company's data and resources and reduces the costs associated with managing and securing digital workspaces while keeping productivity high.

Always Up to Date

deviceTRUST allows you to define an individual context for your devices. Use the device-related information you need to define an always up-to-date context. Your users' devices become the next factor!

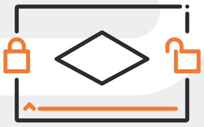
Actions in Real Time

Based on your Context, deviceTRUST runs the Actions you need to protect your environment. Control Access to Workspaces, Sessions, and Applications in Real-Time and every situation. Secure access to your data!

Easily implemented

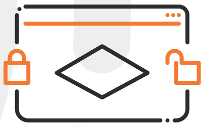
deviceTRUST's integrated templates assist with integrating use cases. Based on real-world customer scenarios and years of experience, they are valid for easy, quick implementation and individual customization. Secure your environment in minutes!

Based on your Context, deviceTRUST performs the Actions you need to protect your digital workspace



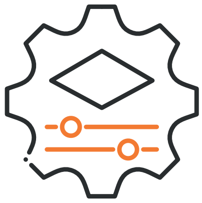
Conditional Workspace Access

Conditional Workspace Access approach to controlling access to your digital workspaces.



Conditional Application Access

With Conditional Application Access you can define the applications users can access inside their digital workspaces.



Conditional Configuration

Conditional Configuration allows you to configure the user's digital workspace beyond the standard security approach.

deviceTRUST

Deployment Scenarios

One solution for all your contextual security needs!

Local
PC/Laptop

We understand the use of deviceTRUST on Windows-based PCs or laptops as a local scenario. With just one software component – the deviceTRUST Agent – context properties are determined locally, and actions are also performed locally.

Remote
Multi-Session, VDI

The deviceTRUST Client Extension locates all relevant context information on the accessing devices – whether BYO or managed devices. The deviceTRUST Agent shapes the context and controls the remote session of the respective user. Thus, all your compliance and security requirements are met!

SaaS
Software as a Service

With deviceTRUST you can integrate the context into the Microsoft Azure Active Directory (AAD) and control access to AAD-connected SaaS applications. deviceTRUST can either extend existing Microsoft Intune concepts or be used entirely without Microsoft Intune.

deviceTRUST Components

Based on your Context, deviceTRUST performs the Actions you need to protect your digital workspace

deviceTRUST
Console

An Easy-to-Use Management Interface
We believe that a simple management is important for a secure implementation. The deviceTRUST Console maps your reality and requirements into contextual definitions in an easy way.

deviceTRUST
Agent

The Active Component for the Digital Workspace
The deviceTRUST Agent is our active component for your digital workspaces. It shapes the context and performs actions on PCs, laptops or in your remoting environment. A universal component for all your scenarios!

deviceTRUST
Client Extension

A Passive Extension for Remoting Clients
Our deviceTRUST Client Extension supports the BYO or managed devices of your users. As a completely passive component, it is used to locate the contextual information specified by you.

Are you ready to optimize your Zero Trust Strategy?
Let´s get in touch!

Contact us for more information!

deviceTRUST GmbH
Hilpertstrasse 31
64295 Darmstadt
Germany

☎ +49 6151 4936960
✉ info@devicetrust.com
🌐 devicetrust.com

@deviceTRUST
devicetrust