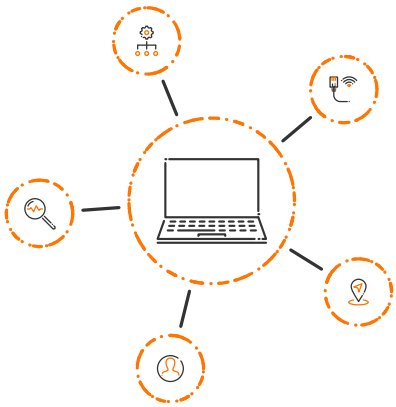
deviceTRUST

Zero Trust erfordert Device Trust

deviceTRUST erweitert Ihre Zero Trust Strategie um eine zusätzliche Sicherheitsebene. Umfangreiche Kontextinformationen und Aktionen über eine zentrale Schnittstelle für alle Bereitstellungsmethoden.

Nutzen Sie Ihre Endgeräte als weiteren Sicherheitsfaktor und bringen Sie Ihren Conditional Access auf die nächste Stufe!



Kontext als Faktor

deviceTRUST Kontextbasierte Sicherheit ist die entscheidende Ebene zum Schutz der Daten und Ressourcen eines Unternehmens. Sie reduziert die Kosten, die mit der Verwaltung und Sicherung digitaler Arbeitsplätze verbunden sind, während die Produktivität hoch bleibt.

Immer auf dem neuesten Stand

deviceTRUST ermöglicht es Ihnen, individuelle Kontexte für Ihre Endgeräte zu definieren. Verwenden Sie die gerätebezogenen Informationen, für die Definition eines immer aktuellen Kontexts. Die Endgeräte Ihrer Benutzenden werden dadurch zum nächsten Faktor!

Aktionen in Echtzeit

Basierend auf Ihrem Kontext, führt deviceTRUST die Aktionen aus, die Sie zum Schutz Ihres digitalen Arbeitsplatzes benötigen. Kontrollieren Sie den Zugriff auf Sitzungen und Anwendungen in Echtzeit und in jeder Situation. Sicherer Zugriff auf Ihre Daten!“

Einfach zu implementieren

Die Vorlagen von deviceTRUST helfen bei der Integration von Use Cases. Basierend auf realen Kundenszenarien und jahrelanger Erfahrung, eignen sie sich für eine einfache und schnelle Implementierung sowie individuelle Anpassungen. Sichern Sie Ihren digitalen Arbeitsplatz in wenigen Minuten“

Basierend auf Ihrem Kontext, führt deviceTRUST die Aktionen aus die Sie zum Schutz Ihrer digitalen Arbeitsplätze benötigen

Conditional Workspace Access

Der Conditional Workspace Access Ansatz dient zur Kontrolle von Zugriffen auf Ihre digitalen Arbeitsplätze.

Conditional Application Access

Mit dem Conditional Application Access legen Sie fest, auf welche Anwendungen die Benutzenden innerhalb ihrer digitalen Arbeitsumgebung zugreifen können.

Conditional Configuration

Conditional Configuration ermöglicht Ihnen die Konfiguration der digitalen Arbeitsplätze von Benutzenden, über den Standard Sicherheitsansatz.

deviceTRUST

Einsatzszenarien

Eine Lösung für alle Ihre kontextbezogenen Sicherheitsanforderungen!

Lokal
PC/Laptop

Als Lokales Szenario verstehen wir die Verwendung von deviceTRUST auf Windows-basierenden PCs oder Laptops. Mit nur einer Software-Komponente, dem deviceTRUST Agent, werden Kontext-Eigenschaften lokal ermittelt, und Aktionen lokal ausgeführt.

Remote
Multi-Session, VDI

Egal für welches Remoting-Produkt sie sich entscheiden, deviceTRUST bringt den Kontext in ihre digitalen Arbeitsplätze. Die deviceTRUST Client Extension ermittelt alle relevanten Kontext-Informationen auf den zugreifenden Geräten – BYO oder Managed Device.

SaaS
Software as a Service

SaaS-Applikationen sind Teil eines modernen, digitalen Arbeitsplatzes. Mit deviceTRUST können Sie den Kontext in das Microsoft Azure Active Directory bringen und Zugriffe auf AAD-angebundene SaaS-Applikationen steuern. deviceTRUST kann dabei sowohl bestehende Microsoft Intune-Konzepte ergänzen, als auch ganz ohne Microsoft Intune verwendet werden.

deviceTRUST-Komponenten

Basierend auf Ihrem Kontext führt deviceTRUST die Aktionen aus, die Sie zum Schutz Ihrer digitalen Arbeitsplätze benötigen

deviceTRUST
Console

Einfach zu bedienende Management-Oberfläche
Wir glauben, ein simples Management ist wichtig für eine sichere Implementierung. Die deviceTRUST Konsole bildet auf einfach Weise Ihre Realität und Anforderungen in Kontext-Definitionen ab.

deviceTRUST
Agent

Aktive Komponente für den digitalen Arbeitsplatz
Der deviceTRUST Agent ist unsere aktive Komponente für ihre digitalen Arbeitsplätze. Auf PCs, Laptops oder in ihrer Remoting-Umgebung bildet der deviceTRUST Agent den Kontext und führt Aktionen aus. Eine universelle Komponente für alle ihre Szenarien!

deviceTRUST
Client Extension

Passive Erweiterung für Remoting-Clients
Unsere deviceTRUST Client Extension unterstützt die BYO oder Managed Devices ihrer Nutzenden. Als vollständig passive Komponente dient sie dem Ermitteln, der von ihnen festgelegten Kontext-Informationen.

Sind Sie bereit, Ihre Zero-Trust-Strategie zu optimieren? Lassen Sie uns gemeinsam daran arbeiten!

Für weitere Informationen, kontaktieren Sie uns!

deviceTRUST GmbH
Hilpertstrasse 31
64295 Darmstadt

+49 6151 4936960
info@devicetrust.com
devicetrust.com

@deviceTRUST
devicetrust