deviceTRUST

# Kontextbasierte Sicherheit

## Die einzige Möglichkeit Ihre digitalen Arbeitsplätze zu schützen!

Mitarbeiter arbeiten heutzutage von unterschiedlichen Geräten und unterschiedlichen Orten. Ein sicherer Arbeitsplatz ist dabei nur möglich, wenn alle kontextbezogenen Informationen zusammengeführt und auf dem neuesten Stand gehalten werden.

### Identität

Mit unserer Active Directory-Integration können wir alle Eigenschaften abrufen, die Sie zur Beschreibung Ihrer Benutzer benötigen und diese Ihrem Kontext hinzuzufügen.

### Sicherheitstatus

deviceTRUST ermöglicht es, den Sicherheitsstatus des Gerätes über verschiedene Eigenschaften zu definieren.

### Endpoint

Informationen über das Gerät des Benutzers sind der Schlüssel zu unserem Ansatz. deviceTRUST kann bis zu 400 verschiedene Eigenschaften Ihrer Geräte auswerten.

### Netzwerk

deviceTRUST erlaubt tiefe Einblicke in die Netzwerkverbindung des Geräts und kann diese je nach Anforderungen unterschiedlich behandeln.

### Standort

Mit deviceTRUST kann der Gerätestandort ermittelt werden. Beginnend mit dem Herkunftsland bis hin zur Straße und Hausnummer, wenn gewünscht.

### Zusätzliche Quellen

deviceTRUST bietet eine multifunktionale Scripting-Engine. Verwenden Sie PowerShell, VBScript oder Batch-Skripte, um Daten aus Quellen wie Textdateien oder Datenbanken abzurufen.

# Ein leistungsstarkes Set an Echtzeitaktionen sorgt für einen dauerhaft sicheren digitalen Arbeitsplatz

### Conditional Access

Mit dem Conditional Access steuern Sie die Zugriffe auf Ihre digitalen Arbeitsplätze, unabhängig davon, ob diese lokal als Fat Client, remote oder über die Cloud bereitgestellt werden.

### Conditional Application Access

Mit Conditional Application Access können Sie definieren, auf welche Anwendungen Benutzer innerhalb ihrer digitalen Arbeitsplätze zugreifen können.

### Conditional Configuration

Conditional Configuration ermöglicht Ihnen, den digitalen Arbeitsplatz des Benutzers über den Standard-Sicherheitsansatz hinaus zu konfigurieren.

deviceTRUST

# Sichere, zukunftsfähige digitale Arbeitsplätze

Arbeiten mit bestehender Benutzerauthentifizierung

Kein Endgeräte Management erforderlich

Nur Software - keine zusätzliche Infrastruktur erforderlich

Keine Abhängigkeit von rollenbasierten Zugriffskonzepten

Nutzung vorhandener Zugriffstechnologien

Unterstützung von lokalen, Cloud- oder Hybridumgebungen

# Kontextbezogene Sicherheitsrichtlinien verwalten und anwenden

**deviceTRUST Konsole**

In der deviceTRUST Konsole erstellen Sie Ihre Konfigurationen, um Kontexte und Aktionen sowie zusätzliche Einstellungen zu definieren.

**deviceTRUST Host**

Fat Clients oder Remote-Plattformen verwenden den deviceTRUST Host, um Aktionen auszuführen.

**deviceTRUST Client**

In Remote-Szenarien wird der deviceTRUST Client auf der Client-Seite installiert, um die vollständigen Kontextinformationen zu erhalten.

# Reporting

deviceTRUST ermöglicht die volle Kontrolle über die gesammelten Daten. Sie können jeden einzelnen Wert erfassen oder verhindern. Ebenso können Sie kontrollieren, ob Daten gespeichert werden, wenn ja, wo und zu welchem Zweck:

- Windows Event Log
- E-Mail senden
- ELK Stack, Splunk

## Kontaktieren Sie uns für weitere Informationen!

deviceTRUST GmbH
Hilpertstrasse 31
64295 Darmstadt
Deutschland

Telefon: +49 6151 4936960
E-Mail: info@devicetrust.com

LinkedIn
Twitter