deviceTRUST

Contextualizing IT *Simple. Dynamic. Integrated.*

Produktdatenblatt

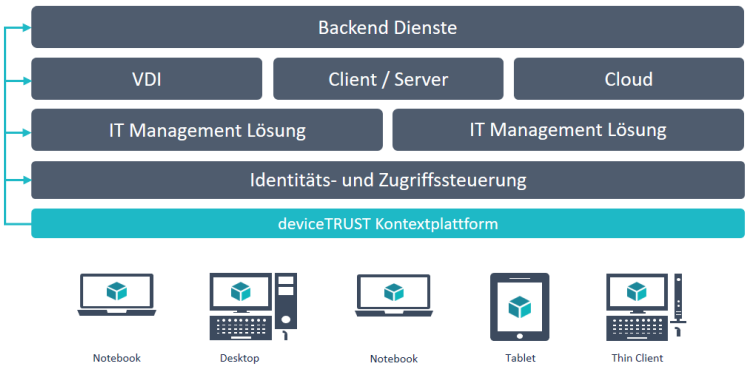
deviceTRUST bietet die zentrale Kontextplattform für Unternehmen, die es Anwendern ermöglicht von jedem Ort, mit jedem beliebigen Endgerät, über jedes Netzwerk und zu jeder Zeit mit ihrem digitalen Workspace zu Arbeiten und gibt den IT-Abteilungen gleichzeitig die erforderlichen Informationen und Kontrolle zur Einhaltung aller Sicherheits-, Compliance- und regulatorischer Vorgaben.

Mit seinen zum Patent angemeldeten Technologien stellt deviceTRUST mehr als 200 Hardware-, Software-, Netzwerk-, Sicherheits-, Performance- und Standort-eigenschaften bereit. deviceTRUST lässt sich problemlos in jede bestehende Workspace-Management-Lösung integrieren und benötigt keine zusätzliche Infrastruktur. Der Kontext ist immer aktuell und jede Änderung löst eine definierbare Aktion aus.

deviceTRUST - Contextualizing IT

Vorteile

- **Erfüllung der Sicherheits-, Compliance- und regulatorischen Anforderungen durch Einbeziehung des Endgeräte- und Benutzerkontextes in die Unternehmensrichtlinien**
- **Eine zentrale Kontextplattform - umfangreicher und detaillierter Kontext**
- **Nahtlose Integration in bestehende Management- und Reporting-Lösungen**
- **Keine zusätzliche Infrastruktur erforderlich - Einfache und schnelle Implementierung**
- **Lizenzierung auf Subscription-Basis**
- **Sofortiger Return on Investment (ROI)**



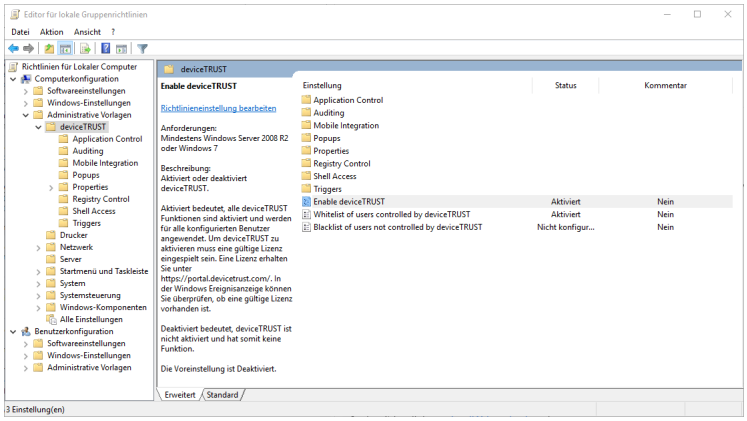
deviceTRUST

Telefon: +49 (6162) 8015950
E-Mail: info@devicetrust.com
https://devicetrust.com
Twitter: @deviceTRUST

deviceTRUST

Contextualizing IT *Simple. Dynamic. Integrated.*

Einfach



deviceTRUST stellt den Kontext des Endgerätes innerhalb der virtuellen Sitzung als auch auf dem Endgerät bereit. Durch das intelligente Verfahren der Bereitstellung kann dieser Kontext einfach genutzt werden. Dies garantiert eine nahtlose Unterstützung von internen und externen Netzwerkzugriffen, integriert sich transparent in bestehende VPN-Lösungen und erfordert keine zusätzliche Infrastruktur, was die Implementierung einfach macht.

Dynamisch

deviceTRUST stellt sicher, dass jede Änderung des Kontexts eines Endgerätes zur Laufzeit in der virtuellen Sitzung und auf dem Endgerät verfügbar ist und somit der wirkliche Status durchgehend bekannt ist. Mittels der dynamischen Trigger können diese übermittelten Änderungen genutzt werden, um aktiv darauf zu reagieren. Für größtmögliche Flexibilität sind die Trigger in der Lage, frei definierbare Aktionen, wie z.B. Skripte, auszuführen.

Integriert

Der Kontext des Benutzers und des Endpunkts wird in das Microsoft Event Log geschrieben, was eine einfache Integration in bestehende SIEM- und Reporting-Lösungen ermöglicht.

Funktionen

Keine Infrastruktur: deviceTRUST erfordert keine zusätzliche Infrastruktur. Dies ermöglicht eine schnelle und effektive Installation und sorgt für niedrige Implementierungs- und Betriebskosten.

Intuitives Management: Die Konfiguration und Verwaltung von deviceTRUST erfolgt selbsterklärend mittels Microsoft Active Directory Gruppenrichtlinien.

Einfacher Start: Über Gruppenmitgliedschaft lässt sich granular definieren, für welche Benutzer deviceTRUST genutzt werden soll.

Nahtlose Integration: Durch die intelligente Bereitstellung der Eigenschaften eines Endgerätes in der virtuellen Sitzung und auf dem Endgerät können die Informationen von allen gängigen Managementwerkzeugen genutzt werden.

Durchgängiger Kontext: Der Kontext eines Endgerätes steht während der gesamten Laufzeit der Benutzersitzung immer aktuell zur Verfügung. Dies stellt sicher, dass jederzeit die Sicherheits- und Compliancevorgaben eingehalten werden, auch wenn sich der Status des Endgerätes ändert.

Eigenschaften auf dem Endgerät verfügbar: Alle Eigenschaften die den Kontext des Endgerätes darstellen sind ebenfalls auf dem Endgerät verfügbar und können so einfach von z.B. Access Gateways als auch lokal auf dem Endgerät genutzt werden.

Benutzerbenachrichtigung: In Abhängigkeit des Kontexts des Endgerätes können dem Benutzer situationsabhängig Benachrichtigungen angezeigt werden.

Mehrsprachige Unterstützung: Alle in der deviceTRUST Konfiguration verfügbaren Benutzernachrichten können mehrsprachig angezeigt werden.

Conditional Access: Kontrollieren des Zugriffs auf die virtuelle Sitzung je nachdem, ob ein deviceTRUST Client installiert ist oder abhängig von definierten Eigenschaften des Endgerätes. Entspricht das Endgerät nicht Ihren Vorgaben kann die virtuelle Sitzung für den Benutzer gesperrt werden. Sowohl bei der Anmeldung als auch während der laufenden Sitzung.

Detaillierte Informationen: deviceTRUST stellt mehr als 400 Hardware, Software, Netzwerk, Security, Performance, Drucker und Lokationseigenschaften in der virtuellen Sitzung, sowie über 200 Eigenschaften am Endgerät zur Verfügung.

deviceTRUST

Contextualizing IT *Simple. Dynamic. Integrated.*

Verfügbare Eigenschaften: Über die deviceTRUST Richtlinie kann definiert werden, welche Eigenschaften des Endgerätes von deviceTRUST bereitgestellt werden sollen. Eigenschaften die Sie nicht benötigen werden von deviceTRUST nicht ermittelt und stehen somit weder auf dem Endgerät noch in der virtuellen Sitzung zur Verfügung. Zusätzlich ist es jetzt möglich zu definieren auf welche Veränderungen der Eigenschaften am Endgerät mit den Triggern reagiert werden soll.

Geolocation: deviceTRUST ermöglicht es, den Standort eines Endgerätes unabhängig der genutzten Netzwerkverbindung zur Verfügung zu stellen. Damit können regulatorische Vorgaben in Bezug auf standortbasierten Applikationszugriff eingehalten werden.

Hinweis: *Geolocation erfordert die Integration mit einem Standortanbieter und kann Gegenstand von Drittanbieterbedingungen sein.*

Detaillierte Sicherheitsinformationen: deviceTRUST bietet eine Vielzahl von detaillierten Informationen über den Sicherheitsstatus des Endgerätes. Der Status von Windows Update, Windows Defender und der Windows Firewall kann abgerufen werden, um z.B. den Zugriff auf die virtuelle Sitzung zu kontrollieren oder um Zugriff auf Anwendungen zu gewähren oder zu verweigern.

Intelligente Trigger: Zur Anpassung der Benutzersitzung verfügt deviceTRUST über Trigger, die Aktionen bei Logon, Logoff, Disconnect, Reconnect, Desktop Starting, Desktop Ready sowie einem Property Change im Kontext des angemeldeten Benutzers, als auch im System-Kontext ausführen können.

Einfache Installation: Alle Komponenten lassen sich mittels Softwareverteilung installieren. Der Client kann für alle Benutzer oder pro Benutzer installiert werden.

Microsoft® AppLocker Unterstützung: Abhängig vom Kontext des Benutzers und des Endgerätes kann deviceTRUST dynamisch Microsoft® AppLocker so konfigurieren, dass der Zugriff auf Anwendungen gewährt oder verweigert wird, z. B. zur Erfüllung der Lizenzbestimmungen.

Application Termination: Wenn der Kontext des Benutzers und des Endgerätes die Anforderungen nicht mehr erfüllt, kann deviceTRUST laufende Anwendungen beenden.

Double-hop Support: Alle Kontextinformationen des Benutzers und des Endgerätes sind innerhalb aller Sessions des Benutzers verfügbar (Multi-Hop).

Auto Update Client: Der deviceTRUST Client kann durch den Benutzer über einen Downloadlink heruntergeladen werden. Neue Versionen des Clients können automatisch und ohne Benutzereingriff installiert werden.

Sichere Kommunikation: Zusätzlich zur Verschlüsselung durch das zugrundeliegende Remoting-Protokoll wird die gesamte Kommunikation mit einem 2048-Bit-RSA-Schlüssel und einer 256-Bit-AES-GCM-Stream-Chiffre verschlüsselt.

Umfangreiches Reporting: deviceTRUST übermittelt alle Informationen strukturiert als Events in das Microsoft Event Log. Dies erlaubt eine nahtlose Integration und Nutzung mit den vorhandenen Reporting-Lösungen. Es ist möglich granular zu definieren, welche Eigenschaften eines Endgerätes nicht in das Reporting übernommen werden.

Attraktives Lizenzmodell: deviceTRUST wird pro Benutzer unabhängig der Anzahl der genutzten Endgeräte lizensiert. Das attraktive Subscription basierende Lizenzmodell vermeidet hohe Investitionskosten.

Anforderungen

Unterstützte Windows Betriebssysteme (32-bit & 64-bit):

- Microsoft Windows 7
- Microsoft Windows 8.x
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

Unterstützte Mobile Betriebssysteme:

- Apple iOS 8.x / 9.x / 10.x / 11.x

Unterstützte IGEL Betriebssysteme:

- IGEL OS 10.3.500 oder höher

Unterstützte Remoting Technologien:

- Microsoft Remote Desktop Protocol (RDP)
- Citrix Independent Computing Architecture (ICA)
- Amazon WorkSpaces PC-over-IP (PCoIP)