deviceTRUST

Context-awareness mit IGEL & deviceTRUST

Simple. Dynamic. Integrated.

Joint Solution

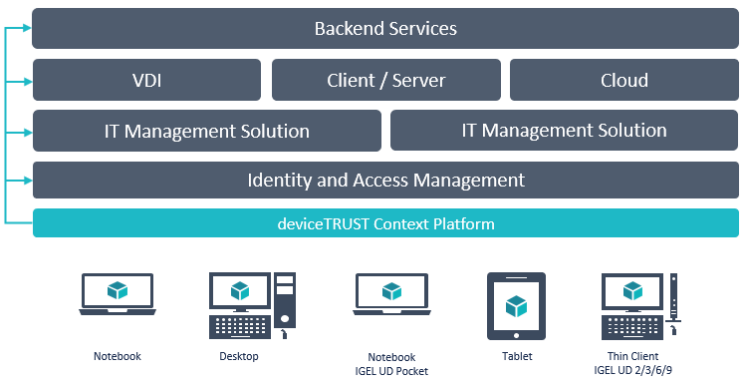
Moderne Arbeitssituationen stellen IT Abteilungen vor große Herausforderungen. Anwender arbeiten an unterschiedlichsten Orten, in diversen Netzwerken und mit verschiedensten Endgeräten. Trotzdem müssen alle Sicherheits-, Compliance- und regulatorische Vorgaben eingehalten werden. deviceTRUST bietet hierzu eine umfassende Lösung.

Mit seinen zum Patent angemeldeten Technologien stellt deviceTRUST mehr als 200 Hardware-, Software-, Netzwerk-, Sicherheits-, Performance- und Standorteigenschaften der genutzten IGEL Endpoints sowie weiterer Endgeräte 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.

Der deviceTRUST Client ist in dem IGEL-eigenen, Linux-basierten Betriebssystem IGEL OS (ab Version 10.04.100) vorinstalliert und lässt sich einfach über die IGEL Universal Management Suite (UMS) aktivieren.

Vorteile

- Erfüllung der Sicherheits-, Compliance- und regulatorischen Anforderungen durch Einbeziehung des Endgeräte- und Benutzerkontextes
- 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-of-Investment (ROI)



CITRIX Ready

deviceTRUST

E-Mail: info@devicetrust.com
https://devicetrust.com
Twitter: @deviceTRUST

IGEL

E-Mail: info@igel.com
https://www.igel.com
Twitter: @IGEL_Technology

deviceTRUST

Einfach

deviceTRUST stellt den Kontext des IGEL Endpoints innerhalb eines virtuellen Kanals für Citrix- und RDP-Sitzungen 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 IGEL Endpoint zur Laufzeit in der virtuellen Sitzung 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 IGEL Endpoints 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. Der deviceTRUST Client ist bereits in dem IGEL OS implementiert. 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 Endpoints in der virtuellen Sitzung und auf dem Endgerät können die Informationen von allen gängigen Managementwerkzeugen genutzt werden.

Durchgängiger Kontext: Der Kontext eines Endpoints 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 Endpoints ändert.

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

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

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

Verfügbare Eigenschaften: Über die deviceTRUST Richtlinie kann definiert werden, welche Eigenschaften des Endoints 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.

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.

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 Endpoints die Anforderungen nicht mehr erfüllt, kann deviceTRUST laufende Anwendungen beenden.

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

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 Endpoints nicht in das Reporting übernommen werden.

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

Unterstützte IGEL Endpoints: Durch Einbindung des deviceTRUST Client in die Firmware IGEL OS 10 steht deren Funktionalität auf allen IGEL Universal Desktop Thin Clients, IDEL UD Pocket, IGEL Zero Clients und mit dem IGEL Universal Desktop Converter konvertierten Endgeräten zur Verfügung.

Über IGEL

IGEL ist einer der führenden Anbieter leistungsfähiger Endpoint-Management-Lösungen, mit der Unternehmen ihre IT-Infrastruktur nachhaltig vereinfachen können. Die weltweit führenden Produkte, wie die IGEL Universal Management Suite, Thin und Zero Clients mit dem hauseigenen IGEL OS sowie All-in-One Thin Client-Lösungen, ermöglichen ein intelligentes und sicheres Endpoint-Management. Mit IGEL können Unternehmen all ihre Thin Clients über eine einzige Schnittstelle komfortabel steuern und verwalten. IT-Abteilungen können auf diese Weise mit weniger Aufwand mehr erreichen, die Total Cost of Ownership sowie Betriebskosten senken und ihr Unternehmen zukunftssicher gestalten. IGEL verfügt über 10 Niederlassungen weltweit und ist mit Partnern in über 50 Ländern vertreten.