deviceTRUST

Use Cases

Umfangreiche Einsatzszenarien der deviceTRUST Lösung.

Einleitung

Sehen Sie sich die folgenden Kundenszenarien an und erfahren Sie, wie die kontextbasierte Sicherheitslösung von deviceTRUST eingesetzt werden kann, um Geschäftsanforderungen auf einfache Weise zu erfüllen, ohne Sicherheit, Compliance und gesetzliche Anforderungen zu gefährden.

Home Office

Anforderungen

- Mitarbeiter müssen in der Lage sein, uneingeschränkt mit allen erforderlichen Anwendungen, identisch wie innerhalb des Unternehmensnetzwerkes, aus ihrem Home Office heraus zu arbeiten.
- Die Mitarbeiter greifen hierbei jedoch von extern auf ihre virtuelle Arbeitsplatzumgebung zu, dabei hat die IT keinerlei Informationen, womit und von wo zugegriffen wird.
- Hieraus ergibt sich ein hohes Sicherheits- und Compliancerisiko für das Unternehmen, da die Rolle des Mitarbeiters im Unternehmen nicht ausreicht um die Zugriffe auf die virtuelle Arbeitsplatzumgebung sowie die Anwendungen zu steuern.

Lösung

Mit der kontextbasierten Sicherheit von deviceTRUST haben Unternehmen die Möglichkeit Home Office Zugänge zu ermöglichen, die alle Anforderungen seitens der IT Sicherheit, der Compliance und regulatorische Vorgaben erfüllen:

- Der deviceTRUST Compliance Check stellt grundsätzlich sicher, dass alle existierenden IT Sicherheits- und Compliancevorgaben erfüllt werden. Hierzu zählen zum Beispiel der Zustand der Sicherheitskomponenten, wie Firewall und Antivirus, aber auch die verwendeten Netzwerke sowie das Land aus welchem zugegriffen wird.
- Optional ermöglicht es deviceTRUST, falls erforderlich, das Home Office des Mitarbeiters zu validieren. Damit kann sichergestellt werden, dass Mitarbeiter nur aus validierten Umgebungen, wie ihrem Home Office oder ihrem Unternehmen, auf ihre virtuelle Arbeitsplatzumgebung zugreifen können. Unerlaubte Zugriffe, selbst mit gestohlenen Zugangsdaten, werden so sicher unterbunden.

Externe Partner

Anforderungen

- Mitarbeiter externer Partner sowie Lieferanten sollen Zugriff auf Anwendungen und Ressourcen erhalten, welche in der virtuellen Arbeitsplatzumgebung des Unternehmens bereitgestellt werden.
- Je nach Klassifizierung und Vertraulichkeit der Daten innerhalb der Anwendungen müssen die entsprechenden Sicherheits-, Compliance und regulatorischen Vorgaben bei den Zugriffen eingehalten werden.
- Die Endgeräte sind hierbei der Unternehmens-IT unbekannt und neben der Rolle des Benutzers sind keine weiteren Informationen verfügbar, die es ermöglichen Anwendungen und Ressourcen entsprechend den Vorgaben für externe Partner bereit zu stellen.

Lösung

Mit der kontextbasierten Sicherheit von deviceTRUST haben Unternehmen die Möglichkeit Anwendungen und Ressourcen über die virtuelle Arbeitsplatzumgebung externen Partnern, entsprechend den Vorgaben, zur Verfügung zu stellen:

- deviceTRUST ermöglicht es bei Zugriffen von Mitarbeitern externer Partner einen Compliance Check des genutzten Endgerätes durchzuführen, ohne diese Endgeräte verwalten zu müssen. Zugriffe werden somit nur gestattet, wenn das Endgerät alle Sicherheits- und Compliancevorgaben erfüllt.
- Dieser Compliance Check kann an die verschiedenen Anforderungen der Unternehmen individuell angepasst werden. Hierzu stehen sowohl Informationen über das genutzte Endgerät, die genutzte Netzwerkverbindung als auch des Standortes zur Verfügung.

Lizenz-Compliance

Anforderungen

- Unternehmensanwendungen, die per Endgerät lizensiert sind (z.B. Microsoft Project oder Microsoft Visio) werden auf virtuellen Arbeitsplatzumgebungen für ein dedizierten Kreis von Anwendern zur Verfügung gestellt.
- Hierbei ist es erforderlich, dass die Lizenzbedingungen der jeweiligen Hersteller eingehalten werden und die entsprechenden Anwendungen ausschließlich genutzt werden können, wenn der Anwender ein lizensiertes Endgerät nutzt.
- Da in virtuellen Arbeitsplatzumgebungen das von den Anwendern genutzte Endgerät nicht eindeutig zu identifizieren ist, kann nicht sichergestellt werden, dass Anwender nur mit lizensierten Endgeräten diese Anwendungen in der virtuellen Arbeitsplatzumgebung ausführen können.
- Somit ist eine lizenzkonforme Nutzung der Anwendungen nicht bzw. nur mit hohem finanziellem Aufwand möglich.

Lösung

Mit der kontextbasierten Sicherheit von deviceTRUST haben Unternehmen die Möglichkeit endgerätebasierte Anwendungen lizenzkonform über virtuelle Arbeitsplatzumgebungen zur Verfügung zu stellen:

- deviceTRUST ermöglicht es, Endgeräte beim Zugriff auf die virtuelle Arbeitsplatzumgebung eindeutig zu identifizieren.
- Basierend auf dieser Identifizierung wird der Zugriff auf die Anwendung lizenzkonform erlaubt oder verhindert.
- Dabei wird die lizenzkonforme Anwendungsnutzung auditsicher protokolliert.

Silo Optimierung

Anforderungen

- Anwender greifen auf ihre virtuelle Arbeitsplatzumgebung von unterschiedlichen Lokationen zu. Hierzu zählen sowohl Zugriffe von innerhalb des Unternehmens als auch von außerhalb auf Reisen oder aus dem Home Office.
- Die vorhandenen Sicherheits-, Compliance und auch regulatorischen Vorgaben schreiben vor, dass einzelne Anwendungen innerhalb der virtuellen Arbeitsplatzumgebung nur bei Zugriffen aus bestimmten Szenarien, z.B. innerhalb des Unternehmens, genutzt werden dürfen.
- Hierbei reicht die Rolle des Mitarbeiters nicht aus, um für das jeweilige Zugriffsszenario die korrekten Anwendungen und Ressourcen bereit zu stellen.
- Ein gängiger Workaround ist der Aufbau mehrerer Anwendungssilos für jedes Zugriffsszenario. Der Anwender muss sich somit je nach Situation mit der Richtigen virtuellen Arbeitsplatzumgebungen verbinden.
- Dies führt zu einem erhöhten administrativen Aufwand und Kosten sowie einer schlechteren Benutzererfahrung.

Lösung

Mit der kontextbasierten Sicherheit von deviceTRUST haben Unternehmen die Möglichkeit die Anzahl der virtuellen Arbeitsplatzumgebungen drastisch zu reduzieren:

- deviceTRUST ermöglicht es Unternehmen sehr einfach unterschiedliche Zugriffsszenarien innerhalb einer virtuellen Arbeitsplatzumgebung bereitzustellen.
- Dies führt zu deutlich geringeren Betriebskosten der virtuellen Arbeitsplatzumgebungen und einem reduzierten Administrationsaufwand.
- Die Anwender verbinden sich nur noch mit einer virtuellen Arbeitsplatzumgebung unabhängig ihres Zugriffsszenarios. Hierbei werden alle Sicherheits-, Compliance und regulatorische Vorgaben weiterhin eingehalten.

Compliance Check

Anforderungen

- Unternehmen ermöglichen es ihren Anwendern mit unterschiedlichen Endgeräten auf ihre virtuelle Arbeitsplatzumgebung zuzugreifen, um dort produktiv mit ihren Anwendungen und Ressourcen zu arbeiten.
- Hierbei sollen die Anwender sowohl durch die IT verwaltete als auch der IT unbekannte Endgeräte nutzen.
- Da beim Zugriff lediglich die Rolle des Benutzers bekannt ist, jedoch keine Informationen über den Zustand des genutzten Endgerätes vorliegen, kann ein den Sicherheits- und Compliancevorgaben entsprechender Zugriff auf die virtuelle Arbeitsplatzumgebung nicht sichergestellt werden.

Lösung

Mit der kontextbasierten Sicherheit von deviceTRUST haben Unternehmen die Möglichkeit Anwendungen und Ressourcen über die virtuelle Arbeitsplatzumgebung ihren Anwendern entsprechend den Vorgaben zur Verfügung zu stellen:

- deviceTRUST ermöglicht es bei Zugriffen von Anwendern einen Compliance Check des genutzten Endgerätes durchzuführen, jedoch ohne diese Endgeräte verwalten zu müssen. Zugriffe werden somit nur gestattet, wenn das Endgerät alle Sicherheits- und Compliancevorgaben erfüllt.
- Dieser Compliance Check kann an die verschiedenen Anforderungen der Unternehmen individuell angepasst werden. Hierzu stehen Informationen über das genutzte Endgerät, die genutzte Netzwerkverbindung und auch des Standortes zur Verfügung.

Bring Your Own Device (BYOD)

Anforderungen

- Unternehmen ermöglichen es ihren Anwendern mit privaten Endgeräten auf ihre virtuelle Arbeitsplatzumgebung zuzugreifen, um dort produktiv mit ihren Anwendungen und Ressourcen zu arbeiten.
- Da beim Zugriff lediglich die Rolle des Benutzers bekannt ist, jedoch keine Informationen über den Zustand des genutzten Endgerätes vorliegen, kann ein den Sicherheits- und Compliancevorgaben entsprechender Zugriff auf die virtuelle Arbeitsplatzumgebung nicht sichergestellt werden.

Lösung

Mit der kontextbasierten Sicherheit von deviceTRUST haben Unternehmen die Möglichkeit ihren Anwendern den Zugriff auf die virtuelle Arbeitsplatzumgebung mit privaten Endgeräten sicher zu ermöglichen:

- deviceTRUST ermöglicht es bei Zugriffen von Anwendern einen Compliance Check des genutzten Endgerätes durchzuführen, ohne diese Endgeräte verwalten zu müssen. Zugriffe werden somit nur gestattet, wenn das Endgerät alle Sicherheits- und Compliancevorgaben erfüllt.
- Dieser Compliance Check kann an die verschiedenen Anforderungen der Unternehmen individuell angepasst werden. Hierzu stehen Informationen über das genutzte Endgerät, die genutzte Netzwerkverbindung als auch des Standortes zur Verfügung.

Compliant Anwendungszugriff

Anforderungen

- Viele Branchen, wie Gesundheitswesen, Versicherungen, Behörden und Finanzwesen, haben für die Zugriffe auf die virtuellen Arbeitsplatzumgebungen und der darin verfügbaren Anwendungen strenge Compliance sowie regulatorische Vorgaben.
- Die Vorgaben regeln klar welche Anwendungen in welchen Zugriffsszenarien genutzt werden dürfen.
- Hierbei muss zum Beispiel zwischen internem und externem Zugriff, Zugriffen aus unterschiedlichen Ländern, der Netzwerksicherheit oder des genutzten Endgerätes unterschieden werden können.
- Die Rolle des Benutzers ist hierbei nicht ausreichend, um diese Anforderungen entsprechend den Vorgaben umzusetzen.

Lösung

Mit der kontextbasierten Sicherheit von deviceTRUST haben Unternehmen die Möglichkeit die Zugriffe auf Anwendungen innerhalb des virtuellen Arbeitsplatzes entsprechend den Compliance und regulatorischen Vorgaben umzusetzen:

- deviceTRUST ermöglicht es sehr einfach unterschiedliche Zugriffsszenarien innerhalb einer virtuellen Arbeitsplatzumgebung bereitzustellen.
- Die Kontrolle der Anwendungszugriffe wird hierbei nicht nur bei der Anmeldung und dem Wiederverbinden, sondern auch während der Sitzungslaufzeit durchgeführt.
- Dabei wird die Anwendungsnutzung Compliant und auditsicher protokolliert.

Unerlaubte USB Laufwerke

Anforderungen

- Anwender der virtuellen Arbeitsplatzumgebung müssen in der Lage seine Dateien mit einen an ihrem Endgerät eingesteckten USB Speichersticks auszutauschen.
- Dieser Datentransfer darf aus Sicherheitsgründen jedoch ausschließlich mit USB Speichersticks erfolgen die von dem Unternehmen autorisiert sind.
- Innerhalb der virtuellen Arbeitsplatzumgebungen gibt es standardmäßig keine Möglichkeit nur die Nutzung dedizierter USB Speichersticks definierter Hersteller zu erlauben.

Lösung

Mit der kontextbasierten Sicherheit von deviceTRUST haben Unternehmen die Möglichkeit, nur autorisierte USB Speichersticks innerhalb der virtuellen Arbeitsplatzumgebung für die Anwender freizugeben:

- deviceTRUST ermöglicht die eindeutige Identifikation eines USB Speichersticks durch die Nutzung der Eigenschaften des USB Speichersticks (z.B. Hersteller-ID, Produkt-ID sowie Seriennummer).
- Diese eindeutige Identifikation des USB Speichersticks ermöglicht jederzeit eine dynamische Zugriffssteuerung sowohl in der virtuellen Arbeitsplatzumgebung als auch am lokalen Endgerät.

Compliant Backend Zugriff

Anforderungen

- Die Administration und Wartung von zentralen IT Systemen, wie z.B. Datenbanken, Fileserver oder Mailsystemen, erfolgt durch Mitarbeiter des Unternehmens oder externe Dienstleister.
- Hierbei erfolgen die Zugriffe auf die Systeme meist über eine Microsoft RDP Remote Verbindung die von unterschiedlichen Endgeräten aufgebaut werden.
- Bei den Microsoft RDP Remote Verbindungen stehen keine Informationen über das genutzte Endgerät, den Sicherheitsstatus des Endgerätes, die genutzte Netzwerkverbindung oder die Lokation des Administrators zur Verfügung.
- Da es sich um unternehmenskritische Systeme handelt, müssen diese Zugriffe immer entsprechend den Sicherheits- und Compliancevorgaben des Unternehmens erfolgen.

Lösung

Mit der kontextbasierten Sicherheit von deviceTRUST haben Unternehmen die Möglichkeit Administratoren und externen Dienstleistern schnell und kosteneffizient Zugriff auf Backend Server zu gewähren und dabei alle Sicherheitsanforderungen einzuhalten:

- deviceTRUST ermöglicht es bei Zugriffen von Administratoren einen Compliance Check des genutzten Endgerätes durchzuführen, ohne diese Endgeräte verwalten zu müssen. Zugriffe werden somit nur gestattet, wenn das Endgerät alle Sicherheits- und Compliancevorgaben erfüllt.
- Dieser Compliance Check kann an die verschiedenen Anforderungen der Unternehmen individuell angepasst werden. Hierzu stehen Informationen über das genutzte Endgerät, die genutzte Netzwerkverbindung sowie des Standortes zur Verfügung.

Lokationsabhängiges Drucken

Anforderungen

- Drucken in virtuellen Arbeitsplatzumgebungen stellt nach wie vor eine große Herausforderung dar, denn Mitarbeiter arbeiten an verschiedenen Endgeräten und Lokationen innerhalb des Unternehmensgebäudes.
- Für den Mitarbeiter wird der Standarddrucker auf Basis seiner Rolle definiert. Dokumente werden somit häufig nicht auf dem Drucker ausgedruckt, der dem Mitarbeiter am nächsten ist.
- In Folge dessen erhält der Mitarbeiter nicht sein erforderliches Dokument und Dokumente mit personenbezogenen Daten können unter Umständen auf den falschen Druckern ausgedruckt werden.

Lösung

Mit der kontextbasierten Sicherheit von deviceTRUST haben Unternehmen die Möglichkeit sowohl die verfügbaren Netzwerkdrucker als auch Standarddrucker innerhalb der virtuellen Arbeitsplatzumgebung entsprechend der Lokation des Endgerätes zu definieren:

- deviceTRUST ermöglicht es, die Lokation des Endgerätes beim Zugriff auf die virtuelle Arbeitsplatzumgebung eindeutig zu identifizieren.
- Basierend auf dieser Identifizierung werden beim Anmelden und Wiederverbinden die verfügbaren Netzwerk- und Standarddrucker dynamisch definiert.
- Anwender nutzen somit immer den nächstgelegenen verfügbaren Drucker.

Meeting Raum

Anforderungen

- Zur Absicherung der virtuellen Arbeitsplatzumgebungen werden innerhalb der Benutzersitzungen nach z.B. 10 Minuten Leerlaufzeit Bildschirmschoner aktiviert.
- Befindet sich ein Anwender in einem Meetingraum ist die Aktivierungszeit für den Bildschirmschoner sehr oft zu kurz bemessen, da beispielsweise während einer Präsentation länger mit den Teilnehmern diskutiert wird. Der Anwender ist gezwungen während seines Meetings den Bildschirmschoner durch Passworteingabe zu entsperren.
- In virtuellen Arbeitsplatzumgebungen gibt es heute keine Möglichkeit, dynamisch den Aktivierungszeitraum des Bildschirmschoners anzupassen.

Lösung

Mit der kontextbasierten Sicherheit von deviceTRUST haben Unternehmen die Möglichkeit den Aktivierungszeitraum des Bildschirmschoners entsprechend des Standortes des Endgerätes dynamisch anzupassen:

- Anwender erhalten nun dynamisch eine Bildschirmschonerkonfiguration innerhalb der virtuellen Arbeitsplatzumgebung, welche ihren Anforderungen gerecht werden.
- Gleichzeitig werden weiterhin die Sicherheitsanforderungen des Unternehmens eingehalten.

Dynamische Policies

Anforderungen

- In lokalen und virtuellen Arbeitsplatzumgebungen werden Policies unterschiedlicher Hersteller, wie z.B. Microsoft, Citrix und VMware, für das Management der Benutzerumgebung genutzt.
- Über diese Policies werden beispielsweise Einstellungen für Bildschirmschoner, Sitzungsleerlaufzeit, Verfügbarkeit von lokalen Laufwerken und Druckern in der virtuellen Arbeitsplatzumgebung des Anwenders gesteuert.
- Das Setzen dieser Policy-Einstellungen erfolgt überwiegend statisch auf Basis der Gruppenmitgliedschaften des Anwenders, und wird den heutigen Anforderungen einer dynamischen Arbeitsweise des Anwenders nicht mehr gerecht.

Lösung

Mit der kontextbasierten Sicherheit von deviceTRUST haben Unternehmen die Möglichkeit, in lokalen und virtuellen Arbeitsplatzumgebungen, Policy-Einstellungen dynamisch den heutigen Anforderungen des Anwenders anzupassen:

- In der virtuellen Arbeitsplatzumgebung wird der Bildschirmschoner nur dann aktiviert, wenn das Endgerät die Anforderungen an einen sicheren Bildschirmschoner nicht erfüllt.
- Die Sitzungsleerlaufzeit zum Trennen oder Abmelden einer Benutzersitzung kann nun auf Basis der Lokation des Endgerätes und des Anwenders dynamisch definiert werden.
- Lokale Ressourcen, wie Laufwerke und Drucker, sind in der virtuellen Arbeitsplatzumgebung nur dann nutzbar, wenn z.B. das genutzte Endgerät durch das Unternehmen verwaltet und abgesichert ist. Unternehmensfremde Endgeräte können weiterhin genutzt werden, jedoch stehen keine lokalen Ressourcen zur Verfügung.