03 | 22 Sonderdruck für DeviceTRUST

IT Administrator
Das Magazin für professionelle System- und Netzwerkadministration

deviceTRUST

www.it-administrator.de

deviceTRUST

Trau! Schau! Wem?

von Thomas Bär und Frank-Michael Schlede

Quelle: vladimirfloyd – 123RF

Home Office und Remote-Work sind für die IT-Verantwortlichen häufig eher ein Albtraum, wenn in dieser Konstellation das Thema Sicherheit zur Sprache kommt. Die deutsche Softwarefirma deviceTRUST bietet einen Ansatz, die Geräte der Nutzer ständig auf Konformität mit den Unternehmensrichtlinien zu überwachen. Das funktionierte im Test für verschiedene Clients in unterschiedlichen Umgebungen sehr gut.

Die schöne neue IT-Welt, die uns die Covid-Pandemie in unterschiedlichsten Ausprägungen beschert, bürdet vor allen Dingen den IT-Abteilungen eine ganze Menge Mehrarbeit auf. War es schon zuvor nicht einfach, die Sicherheit und Konformität mit den Richtlinien des Unternehmens für die Endgeräte der Nutzer zu gewährleisten, so hat der Umzug vieler Mitarbeiter ins Home Office diese Problematik ein weiteres Mal verschärft.

Die Tatsache, dass in diesen Szenarien häufig auch private Endgeräte für die Arbeit direkt im Unternehmensnetzwerk und mit den Unternehmensdaten eingesetzt werden, verschärft die Problematik. Der vielgepriesene "Digital Workspace" stellt auf diese Weise viele neue Ansprüche an die Sicherheit des Unternehmensnetzwerks und der Daten darin.

Das in Darmstadt beheimatete Security-Unternehmen deviceTRUST widmet sich seit 2016 mit seiner Plattform gleichen Namens diesen Problemen. Der selbstgewählte Anspruch besteht darin, dass Anwender von jedem Ort und mit jedem Endgerät über beliebige Netzwerke sicher arbeiten können. Erreicht werden soll das durch den Einsatz der sogenannten kontextbasierten Sicherheit.

Was der Kontext leisten kann

Es gibt viele Gründe, warum bestimmte unternehmenskritische Anwendungen nur unter bestimmten Bedingungen zum Einsatz kommen dürfen. Dazu gehören unter anderem Sicherheits-, Compliance- und regulatorische Aspekte. Kontextinformationen, also alle Informationen über Nutzer, Gerät, Netzwerkanbindung und auch weitere Quellen, können helfen, diese Vorgaben zu erfüllen. Sie lassen sich sowohl während der Benutzeranmeldung beziehungsweise beim Entsperren mit Wiederverbinden mit dem digitalen Arbeitsplatz, aber auch während der Laufzeit einer solchen Sitzung erheben. Mithilfe dieser Informationen ist es dann grundsätzlich möglich, den Zugriff auf den Arbeitsplatz und auf die Anwendungen dynamisch zu steuern.

In den IT-Szenarien der Vergangenheit – ein Standort und ein Büro, von dem aus immer zugegriffen wurde – waren diese Dinge mithilfe eines rein rollenbasierten Zugriffs noch recht einfach zu verwalten. Heute laufen unterschiedliche Endgeräte von unterschiedlichen Standorten in ganz unterschiedlichen – auch öffentlichen – Netzwerken.

Bei der Plattform von deviceTRUST bilden deshalb ein oder mehrere logisch miteinander verknüpfte Kontexte die Grundlage für die bedingte Anwendungszugriffssteuerung. Je nach Kontext können IT-Verantwortliche dabei durch die Software jederzeit dynamische Microsoft-AppLocker-Regeln zur Anwendungszugriffssteuerung aktivieren und durchsetzen. Eine große Anzahl von verschiedenen Informationen steht zur Definition des Kontexts zur Verfügung und lässt sich auch logisch miteinander verknüpfen. Dazu gehört beispielsweise die Prüfung, ob der deviceTRUST-Client auf dem Endsystem verfügbar ist, oder der Test des Zugangs, also ob sich das Endgerät im Unternehmen oder außerhalb befindet. Aber auch der Einsatz von Geofencing ist möglich, sodass ein Anwender nur zugreifen kann, wenn er sich mit dem Endgerät im Inland befindet.

Im Bereich der Sicherheit können Informationen über Einschränkungen wie "Kein Zugriff über ein offenes nicht gesichertes WLAN" oder Eigenschaften aus dem Bereich der Gerätesicherheit wie "Aktualität der Antivirenlösung", "Firewall aktiv" oder "Gültigkeit der Zertifikate auf dem Gerät" zur Überprüfung dienen.

Weitere Kontextinformationen beziehen sich auf die Eigenschaften des Benutzer-

objekts aus dem Active Directory. Dazu zählen zum Beispiel der Firmenname, die Struktur der E-Mail-Adresse und Informationen über das genutzte Gerät (unternehmenseigenes oder privates Gerät). Aber auch Informationen, die aus SharePoint-Listen oder aus Textdateien stammen, sind für die Überprüfung des Kontexts einsetzbar.

Zusammenspiel der deviceTRUST-Kompenten

Die Software der deviceTRUST-Plattform setzt sich aus drei Komponenten zusammen: Konsole, Agent und Client Extension. Aus der Sicht der Administration ist dabei die Konsole zentral, denn hier konfigurieren Admins die gewünschten Einstellungen, Kontexte und Aktionen. Die Daten für diese Konfigurationen lassen sich dann sowohl in GPOs (Gruppenrichtlinienobjekten) oder in entsprechenden Konfigurationsdateien speichern.

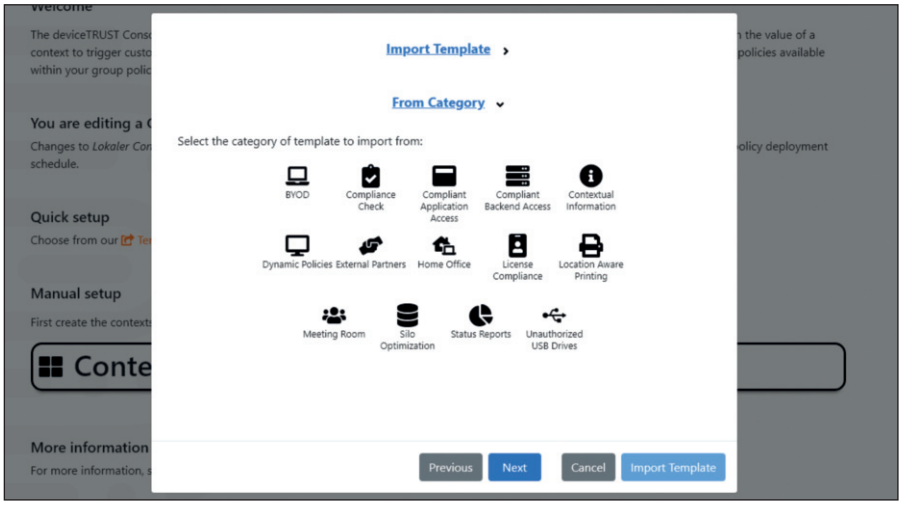

Bild 1: Die deviceTRUST-Konsole bietet den zentralen Zugriff für die Konfiguration und Administration und stellt Vorlagen bereit.

Fat Clients, also vollständige PC-Systeme mit Betriebssystem, oder auch Remote-Plattformen verwenden den deviceTRUST-Agenten. Dieses Programm wird dazu auf dem Endgerät oder dem Remoting-Host installiert, der den Anwendern die Sessions bereitstellt. Die Agentenkonfiguration erfolgt dabei über lokale Richtlinien oder Dateien. Der Agent fordert dabei beim Remote-Einsatz die Daten von den deviceTRUST-Client-Extensionen an, die auf der jeweils aktuellen Konfiguration basieren.

Die Erweiterungen müssen nach dem Einsatzprinzip der Plattform in Remote- und Device-as-a-Service-Szenarien (DaaS) auf den Clients installiert sein, damit die Software die vollständigen Kontextinformation erhalten und verarbeiten kann. Diese Extension, die keine zusätzliche Konfiguration erforderlich macht, sendet dann auf Anfrage die Daten an den Agenten. Es handelt sich dabei um eine rein passive Erweiterung für den Remote-Client, die standardmäßig keine Daten sammelt und nur auf die zentralen Konfigurationseinstellungen reagiert, die der deviceTRUST-Agent übermittelt. Die gesamte Kommunikation zwischen diesen einzelnen Komponenten findet immer innerhalb der bereits vorhandenen Umgebung statt. Für den Einsatz sind keine zusätzlichen Gateways, speziellen offenen Ports oder Firewall-Anpassung notwendig – das zeigte sich auch bei unseren Tests, auf die wir im weiteren Verlauf noch eingehen.

Schnelle Inbetriebnahme

Für unseren Test stellte uns der Anbieter eine Testumgebung zur Verfügung, die sich "Demobox" nennt. Ergänzend setzten wir einen Windows Server 2019 als virtuelle Maschine unter VMware Workstation auf. Auf diesem System installierten wir dann die deviceTRUST-Konsole, die als MSI-Datei sowohl mit 32 oder 64 Bit für Windows-Systeme bereitsteht. Der Anbieter stellt auch die entsprechenden Kommandozeilen-Optionen für eine "unattended"-Installation bereit, sodass Administratoren die Software mit ihren Methoden der Softwareverteilung ausrollen können.

Für ein sogenanntes "Fat Client"-Szenario mussten wir dann noch den deviceTRUST-Client auf dem entsprechenden Windows-System installieren. Dazu sind auf dem System lokale Administratorrechte und ein Neustart nach der Installation notwendig. Für die DaaS- und Remote-Szenarien wird der Agent auf dem entsprechenden Host-Rechner installiert, während auf den Endgeräten – beispielsweise unter Linux oder macOS – die jeweilige Client-Extension notwendig ist. Diese Erweiterung sendet dann die Kon-

deviceTRUST

Produkt
Software zur kontextbasierten Absicherung von Endgeräten.

Hersteller
deviceTrust
https://devicetrust.de/

Preis
deviceTRUST-Lizenzen gibt es mit einer Laufzeit von 12, 24, 36 oder mehr Monaten. Eine Subskription umfasst immer die Nutzung und Wartung sowie den Support für den gewählten Zeitraum. Die Lizenzierung erfolgt dabei per "Named User". Der Listenpreis für einen solchen Named User liegt bei einer Laufzeit von 12 Monaten bei 27,60 Euro pro Jahr. Dabei kann ein lizenzierter Benutzer beliebig viele unterschiedliche Endgeräte wie beispielsweise einen Firmenlaptop und ein BYOD-Gerät im Home Office verwenden. Für größere Lizenzmengen und längere Laufzeiten bietet das Unternehmen Rabatte an.

Systemvoraussetzungen
Agent, Konsole und die Client-Extension (32und 64 Bit) werden von Windows 8.x bis Windows 11 und von der Version 2012 bis zur Version 2022 des Windows Server unterstützt. Für macOS (10.12 bis 12), Ubuntu (18.04 LTS bis 21.10), iOS (11.x bis 15.x9) stehen ebenfalls Client-Extensions zur Verfügung. Das gilt auch für das Igel OS 10.3.500 und höher sowie für eLux RP (ein Thin-Client- und PC-Betriebssystem für VDI- und DaaS-Umgebungen) ab der Version 6.5.

Technische Daten
www.it-administrator.de/downloads/datenblaetter

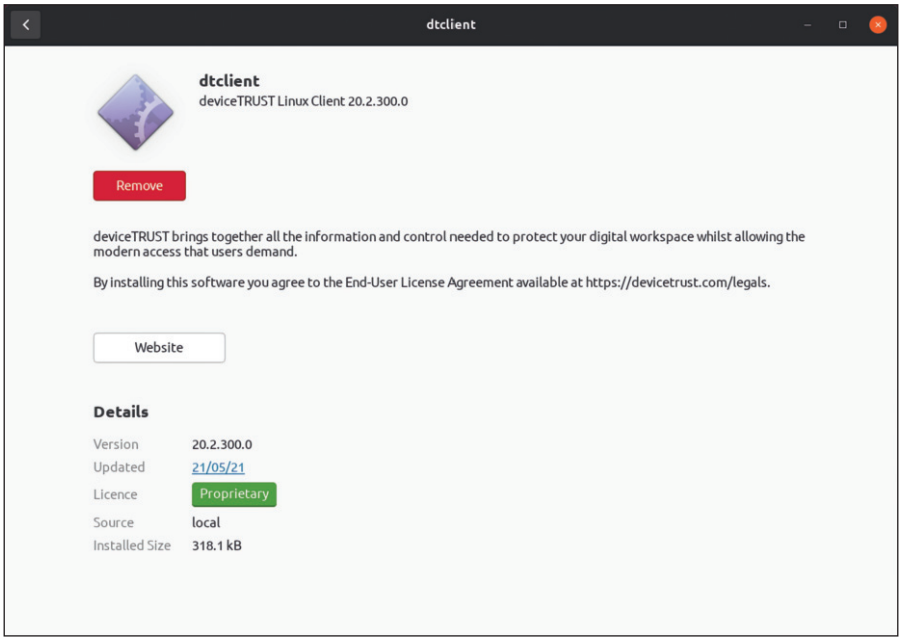

Bild 2: Linux-Systeme werden mithilfe der Client-Extension eingebunden: Diese sorgt dafür, dass die Kontextinformationen vom Nutzer und seinen Geräten zum Agent auf dem entsprechenden Host wandern.

textinformationen innerhalb des Kommunikationskanals des jeweiligen Remote-Protokolls an den Host-Rechner und den deviceTRUST-Agenten.

Ist die Konsole installiert, lässt sich auf dem entsprechenden System der Editor für lokalen Richtlinien, Gruppenrichtlinienobjekte oder dateibasierte Einstellungen verwenden. Die Konsole findet sich nach der Installation unter dem Pfad "%PROGRAMFILES% \ DEVICETRUST \ CONSOLE" als ausführbare Datei. Wir wählten in unserer Demo-Umgebung den Editor für lokale Richtlinien, in dem die Installation einen neuen Knoten unter dem Pfad "Computerkonfiguration \ deviceTRUST Console" angelegt hatte.

Administration nur auf Englisch

Dort fanden wir dann die gleiche Oberfläche, die uns auch in der ausführbaren Datei zur Verfügung gestellt wurde. Als ersten Schritt mussten wir hier nun einen gültigen Lizenzschlüssel eingeben. Durch einen Blick in die Ereignisanzeige des Windows-Betriebssystems ließ sich dann feststellen, ob eine gültige Lizenz für die Software vorhanden ist. Im Bereich "Anwendungs- und Dienstprotokolle" hat die Software dazu den Bereich "deviceTRUST" angelegt, in dem im Abschnitt "Admin" die Lizenzinformationen zu finden sind. Die Software protokolliert Ereignisse in der Windows-Ereignisanzeige. Gerade für die Lizenz hätten wir eine Rückmeldung des Programms nach der Installation für praktischer empfunden als die langwierige Suche danach in der Ereignisanzeige.

Die Konsole bietet eine grafische Oberfläche, über die sich fast alle Möglichkeiten und Fähigkeiten der Plattform einstellen lassen. In vielen Bereichen zeigt die Konsole zudem weitere Erläuterungen an. Wie die Online-Dokumentation auf der Webseite des Unternehmens sind auch in der Software alle Erläuterungen, Beschreibungen und Meldungen in englischer Sprache. Auf unsere Nachfrage hin sagte uns deviceTRUST, dass dies Missverständnisse und Probleme durch Übersetzungen vermeiden solle. Zudem sei es für die meisten Administratoren und Systemverantwortlichen durchaus normal, die Systeme in dieser Sprache zu betreuen. Die Meldungen für die Endnutzer lassen sich aber mit entsprechenden Anzeigen in deutscher Sprache ergänzen.

Leistungsfähige Kontexte

Die Kontextinformationen, die das System verwendet, legt immer der IT-Verantwortliche selbst fest. Gleiches gilt auch für die entsprechenden Aktionen, die an die Kontexte gebunden sind. Das Erstellen eines neuen Kontexts und der damit verbundenen Aktionen ist durch die übersichtliche Oberfläche und die darin integrierten Hilfen recht schnell und einfach erledigt. Die Zusammenhänge sind logisch und die Verknüpfungen werden durch bekannte Operatoren wie "equals" miteinander in Beziehung gesetzt. So sollte es erfahrenen Administratoren problemlos möglich sein, die gewünschten Konditionen für das eigene Netzwerk umzusetzen.

Eine Abfrage beispielsweise nach einer richtig konfigurierten Firewall (einschließlich der Überprüfung, ob diese für das "richtige" Netzwerk aktiv ist) ist auf diese Weise recht einfach anzulegen. Ein besonders großer Vorteil der deviceTRUST-Plattform besteht darin, dass

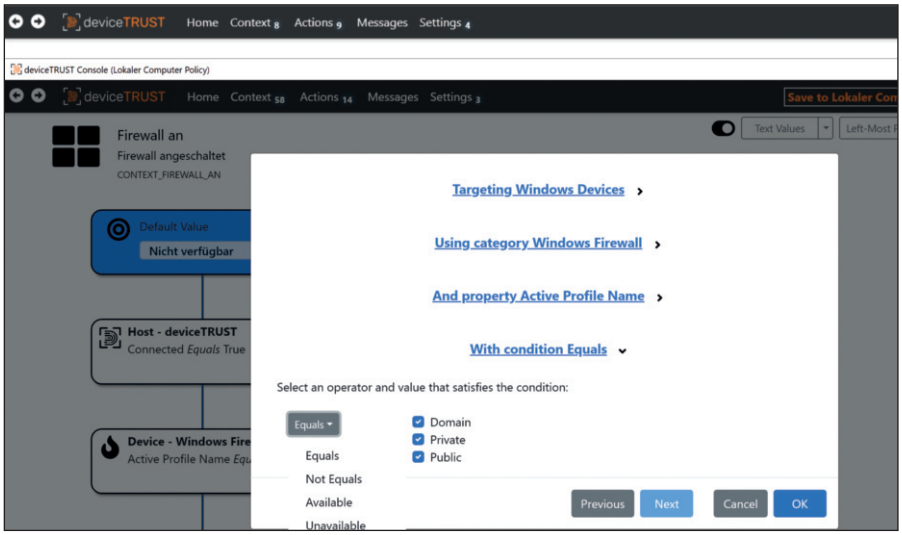

Bild 3: Über die GUI sind neue Kontexte schnell erstellt. Hier ein Beispiel zur Überprüfung der vorhandenen und richtig konfigurierten Firewall auf dem Client.

die Überprüfung des Kontexts immer dynamisch stattfindet. Das bedeutet am Beispiel von Geofencing: Befindet sich der Anwender mit seinem Gerät in einem Land, in dem er eine bestimmte sicherheitskritische Anwendung laut den Compliance-Regeln nutzen darf, kann er problemlos damit arbeiten.

Wechselt er aber während der aktiven Nutzung über die Landesgrenzen hinaus und ist es dann nicht mehr erlaubt, die Anwendung zu nutzen, wird deviceTRUST diese Verbindung unterbrechen und einen Zugriff nicht mehr zulassen. Ein Fall, der im Umfeld von Finanzdienstleistern und Banken sicher realistisch ist.

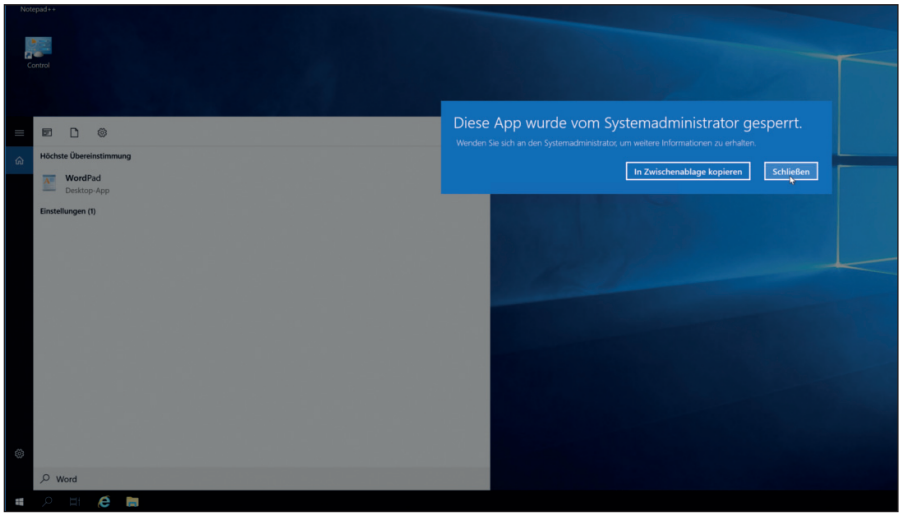

Bild 4: Das WordPad-Icon wurde durch deviceTRUST vom Desktop dynamisch entfernt, aber der Anwender kann immer noch versuchen, das Programm direkt aufzurufen – was jedoch scheitert.

Sehr praxisgerecht fanden wir auch die Templates, beispielsweise für die Zusammenarbeit mit externen Partnerfirmen. Diese Vorlagen erlauben, den Zugriff von externen Partnern auf eine Session und die Anwendungen zu kontrollieren. Dabei kann die Bedingung sich beispielsweise sowohl auf ein nicht-autorisiertes Endgerät als auch auf den nicht-autorisierten Zugriff in einem bestimmten Zeitraum (Arbeitszeit) oder etwa nach einer bestimmten Datei beziehen. In der jeweiligen Aktion kann ein Administrator dann wiederum festlegen, dem Nutzer den Zugriff komplett zu verweigern oder einen Hinweis darauf zu geben, wann ihm der Zugang gestattet ist.

So urteilt IT-Administrator

GUI für Kontextdefinition	7
Mitgelieferte Kontexte	8
Dokumentation und Hilfe	7
Unterstützung Protokolle	8
Anwendungszugriffssteuerung	7

Die Details unserer Testmethodik finden Sie unter www.it-administrator.de/testmethodik

Dieses Produkt eignet sich

optimal für große Organisationen, die viele Endanwender betreuen, die im Home Office oder mobil arbeiten, und zudem auch Partnerunternehmen gut kontrollierten Zugriff gewähren wollen.

bedingt für mittelgroße Unternehmen für Home Office und Remote-Work. Allerdings setzt ein schneller reibungsloser Einsatz voraus, dass bereits gewisse Vorbedingungen wie rollenbasierte Zugriffe zum Einsatz kommen. Ansonsten steigt die Lernkurve für die Administratoren an.

nicht für sehr kleine Unternehmen, da für sie der Aufwand der Einführung recht groß ist und hier vielfach auch ungeeignete Endgeräte (Windows-Home-Versionen) zum Einsatz kommen.

Fazit

Es erscheint zunächst erstaunlich, dass die Plattform den Firmen und ihren Anwendern eine so weitgehende und umfassende Kontrolle der Zugriffe mit verhältnismäßig wenigen Mitteln bieten kann. Uns hat es dabei besonders gut gefallen, dass es nicht notwendig ist, eine eigene neue Infrastruktur aufzusetzen. Der Einsatz setzt allerdings voraus, dass ein Unternehmen beispielsweise bereits einen rollenbasierten Zugriff am besten mit Zwei-Faktor-Authentifizierung verwendet und auch Techniken wie Active Directory einsetzt und pflegt. Diese Unternehmen dürften es aber als unbestreitbaren Vorteil der deviceTRUST-Plattform ansehen, dass sie beispielsweise beim Einsatz von Microsofts Virtual Desktops die Endgeräte nicht zwingend in das Azure Active Directory aufnehmen müssen. Dadurch ist dann auch ein Einsatz der Virtual Desktops von Microsoft mit privaten Endgeräten möglich.

Durch die Applocker-Technologie von Microsoft für die Zugriffskontrolle ist es dabei allerdings Voraussetzung, dass keine Windows-Clients der Home-Edition-Lizenz zum Einsatz kommen. Das sollte im professionellen Umfeld ebenfalls die Regel sein, kann aber gerade bei Home-Office-Szenarien mit BYOD-Geräten ein Problem darstellen.

Auch die Flexibilität der deviceTRUST-Software konnte überzeugen: Die breite Unterstützung der verschiedensten Remote-Protokolle erhöht die Chance, dass es der Unternehmens-IT recht schnell gelingen kann, ihre Endgeräte auch unter ganz unterschiedlichen Bedingungen wirkungsvoll zu kontrollieren. Hinzu kommt die recht übersichtliche und für IT-Profis einfache Konfiguration mit Hilfe der Richtlinien. Ganz sicher werden "kreative" Nutzer immer wieder Möglichkeiten finden, Endgeräte unabsichtlich oder mit Vorsatz so einzusetzen, dass es den Compliance-Regeln der eigenen Firma widerspricht.

Doch eine Lösung wie deviceTRUST gibt den IT-Verantwortlichen ein gutes Werkzeug in die Hand, viele der gängigen Fälle in Sachen Clientsecurity sicher und vor allen Dingen auch dynamisch zu verhindern. Dabei sehen wir es in Zeiten von Home Office und immer mobileren Anwendern als großen Vorteil dieser Plattform an, dass per "Named User" beliebig viele Endgeräte eingesetzt werden können. *(jp)*