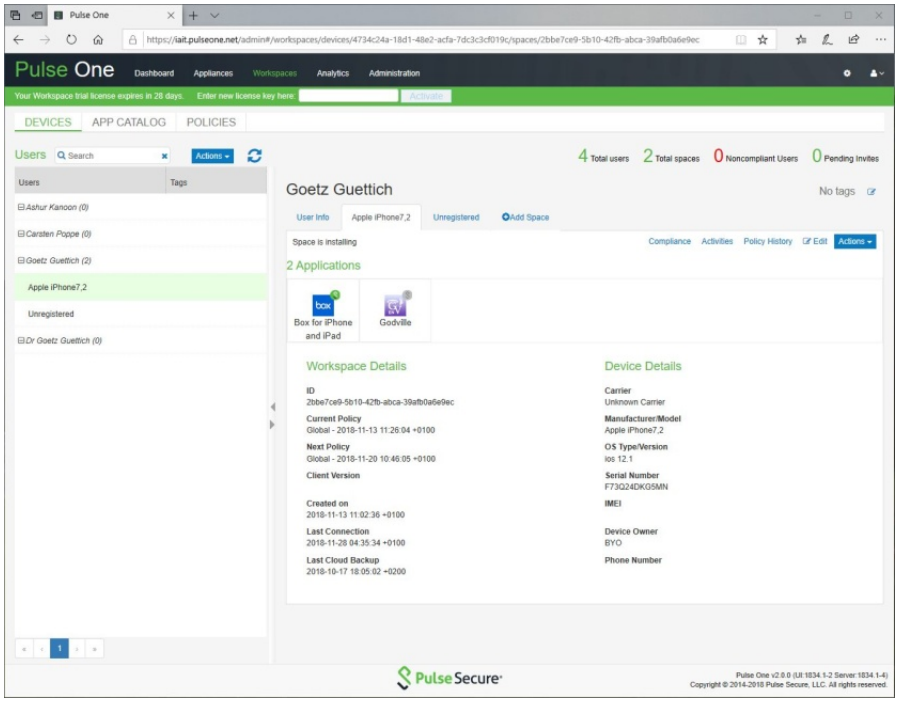
Einfaches Mobile Device Management

Dr. Götz Güttich

Mit Pulse Workspace bietet PulseSecure IT-Administratoren ein Mobility Management-Werkzeug, mit dem sie nach Aussagen des Herstellers eine umfassende Kontrolle über ihre mobile IT-Umgebung erhalten, ohne dabei die Privatsphäre der Gerätenutzer zu beeinträchtigen. Wir haben uns im Testlabor angesehen, was die Lösung in der Praxis leistet.



Pulse Workspace mit dem hinzugefügten iPhone

Pulse Workspace verfügt über eine App Management-Funktion, mit der die zuständigen Mitarbeiter dazu in der Lage sind, einen Unternehmens App-Katalog anzulegen und die Apps dann gruppenweise an die Anwender zu verteilen. In manchen Fällen lassen sich die Apps sogar vorkonfigurieren, um das Deployment an Endanwender zur vereinfachen.

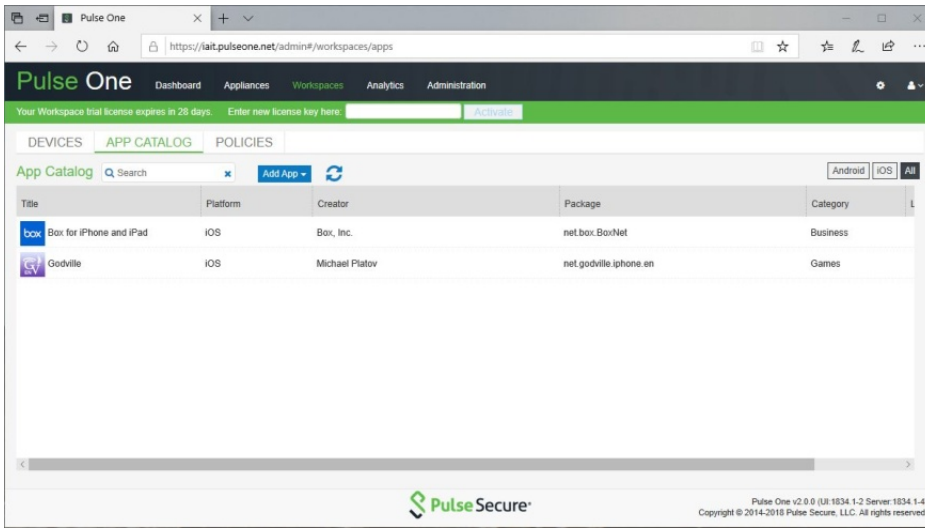
Gleichzeitig stellt eine Workspace Separation sicher, dass die Privatsphäre der User und ihre normale Benutzererfahrung nicht beeinträchtigt werden. Da Unternehmensverzeichnisdienste in das Produkt integriert werden können, müssen die Administratoren die Benutzerkonten im Betrieb nicht mehrfach pflegen.

Die Cloud-basierte Lösung unterstützt mobile Endgeräte unter Android und iOS. Sie wird über eine zentrale Management-Konsole verwaltet und bietet neben dem App-Katalog unter anderem auch die Option, die Parameter für E-Mail- und VPN-Verbindungen automatisch auf die Geräte zu verteilen. Darüber hinaus steht auch eine Funktion zur Verfügung, mit der die IT-Mitarbeiter Zugriff auf unmodifizierte Anwendungen in den offiziellen Apple App- und Google Play-Stores erlauben können. Auf diese Weise sind die Benutzer in der Lage, auch Apps wie Microsoft Office und ähnliches einzusetzen.

Die Lösung ermöglicht zudem das Festlegen von Compliance-Vorgaben, die die Geräte erfüllen müssen. Auf diese Weise besteht etwa die Option, keine Geräte mit aktivem USB-Debugging zuzulassen oder Produkte mit Jailbreak zu blockieren. Darüber hinaus lassen sich auch Vorgaben zur Verschlüsselung und zur Komplexität des PIN-Codes machen. Das Teilen von Daten gilt als besonders wichtiges Thema im Zusammenhang mit mobilen Geräten im Unternehmen. Deswegen bietet Pulse Workspace granular einstellbare Data Sharing-Policies in Kombination mit selektiven Wipe-Funktionen. Die für die tägliche Arbeit benötigten Verbindungen lassen sich darüber hinaus auf App-Basis konfigurieren. Auf diese Weise ist es beispielsweise möglich, über ein per-app VPN auf das Netzwerk des Unternehmens zuzugreifen und Cloud-Verbindungen über ein Policy-basiertes Split-Tunneling zu realisieren.

Der Test

Im Test verwendeten wir eine virtuelle Pulse Connect Secure-Appliance (PCS), um den VPN-Zugriff in unser Netz zu realisieren. Zum Verwalten von Pulse Workspace setzten wir eine kostenlose 60 Tage-Testversion der zentralen, cloud-basierten Management-Konsole namens Pulse One ein. Als mobiler Test-Client kam ein iPhone 6 unter iOS 12.1 ins Spiel.



Der App Catalog von Pulse Workspace

Zuerst nahmen wir die PCS-Appliance in Betrieb und konfigurierten sie so, dass VPN-Zugriffe in unser Testnetz möglich waren. Danach verbanden wir sie mit der Cloud-basierten Management-Konsole Pulse One und banden dort unser mobiles Endgerät in die Konfiguration ein. Anschließend erstellten wir einen App-Katalog, fügten diesem Anwendungen hinzu und installierten diese dann auf dem Endgerät.

Zusätzlich verteilten wir eine E-Mail- und eine VPN-Konfiguration. Zum Schluss sahen wir uns an, wie die tägliche Arbeit mit dem Produkt ablief, nahmen die Log- und Analysefunktionen der Lösung unter die Lupe und sperrten das Gerät testweise aus der Ferne.

Installation

Auf die Inbetriebnahme der PCS-Appliance gehen wir an dieser Stelle nicht genauer ein, da sie detailliert in der Dokumentation beschrieben wird und den Rahmen dieses Artikels sprengen würde. Es genügt zu sagen, dass wir etwa eine halbe Stunde bis zum Aufbau unserer ersten VPN-Verbindung benötigten und dass das Setup keinen Administratoren vor unüberwindliche Schwierigkeiten stellt.

Für den Test verwendeten wir eine Trial-Version von Pulse One. Diese steht unter https:// www. pulsesecure.net/ trynow/ pulse-one- short- form- demo/ ?source zur Verfügung. Nachdem wir sie aktiviert hatten, war es im nächsten Schritt erforderlich, zunächst einmal unsere PCS-Appliance zum System hinzuzufügen.

Dazu wechselten wir in Pulse One nach "Appliances / Appliances" und selektieren dort den Befehl "Add Appliance". Anschließend fragte uns das System nach einem Namen für die Appliance und teilte uns einen Registration Host und einen Registration Code mit. Diese beiden Codes trugen wir zum Schluss in der Pulse One-Konfiguration im Management-Interface der PCS-Appliance ein. Anschließend meldete sich die Appliance bei Pulse One an und stand für unseren Test zur Verfügung.

Das Einbinden des mobilen Clients

Um nun unser iPhone in unsere Testumgebung zu integrieren, mussten wir im ersten Schritt eine Apple MDM Push-Zertifikat zu unserer Workspace Management-Konsole hinzufügen. Dieses versetzt Pulse Workspace in die Lage, Policies, Updates und Aktionen auf die verwalteten iOS-Geräte zu pushen. Das Einfügen des Zertifikats gestaltet sich verhältnismäßig einfach.

Wenn die Administratoren nach „Settings / Apple“ wechseln, haben sie die Möglichkeit, den Reiter „Apple MDM Cert“ aufzurufen. Dort können sie dann einen Signing Request (CSR) herunterladen, den sie dann im nächsten Schritt auf dem Apple Push Certificates-Portal hochladen müssen. Da der Link zu diesem Portal bereits direkt in die Apple MDM Cert-Page integriert wurde, lässt sich diese direkt aufrufen und die zuständigen Mitarbeiter müssen nicht erst nach der dazugehörigen URL suchen.

Bei dem Portal mussten wir uns zunächst mit unserer Apple-ID anmelden, danach konnten wir in den Bereich „Create a new Certificate“ wechseln, die Nutzungsbedingungen akzeptieren und unseren CSR hochladen. Daraufhin bot uns das Portal eine PEM-Datei mit dem neuen Zertifikat zum

Download an. Dieses luden wir dann in der Pulse One-Konsole hoch, danach war der Vorgang abgeschlossen. Im Test nahm er keine Minute in Anspruch.

Jetzt fügten wir als nächstes unser iPhone zu unserer Umgebung hinzu. Dazu loggten wir uns erneut bei dem Pulse One-Portal ein, wechselten nach „Workspaces“ und selektierten das (zuvor mit Benutzernamen und Mail-Adresse angelegte) Test-Benutzerkonto, dem wir das iPhone zuordnen wollten. Dann klickten wir auf „Add Space“ und aktivierten die Funktion, die dem Benutzer eine Willkommens E-Mail auf seinem Mail-Account zukommen lässt. Alternativ kann man die Willkommensbotschaft auch als SMS verschicken.

Nachdem die Mail auf unserem iPhone eingegangen war, klickten wir auf den darin enthaltenen Registrierungslink, woraufhin das System in den Apple App Store wechselte und auf dem Smartphone die Pulse Secure-App einspielte. Danach starteten wir diese App und gaben auf dem Willkommensbildschirm unsere E-Mail-Adresse und den in der Willkommensmail enthaltenen Aktivierungsschlüssel an.

Jetzt mussten wir nur noch das BYOD-Policy-Agreement akzeptieren, der App erlauben, den Workspace zu installieren und dem Zertifikat vertrauen. Damit war der Prozess abgeschlossen und das iPhone erschien anschließend in der Übersicht der verwalteten Geräte.

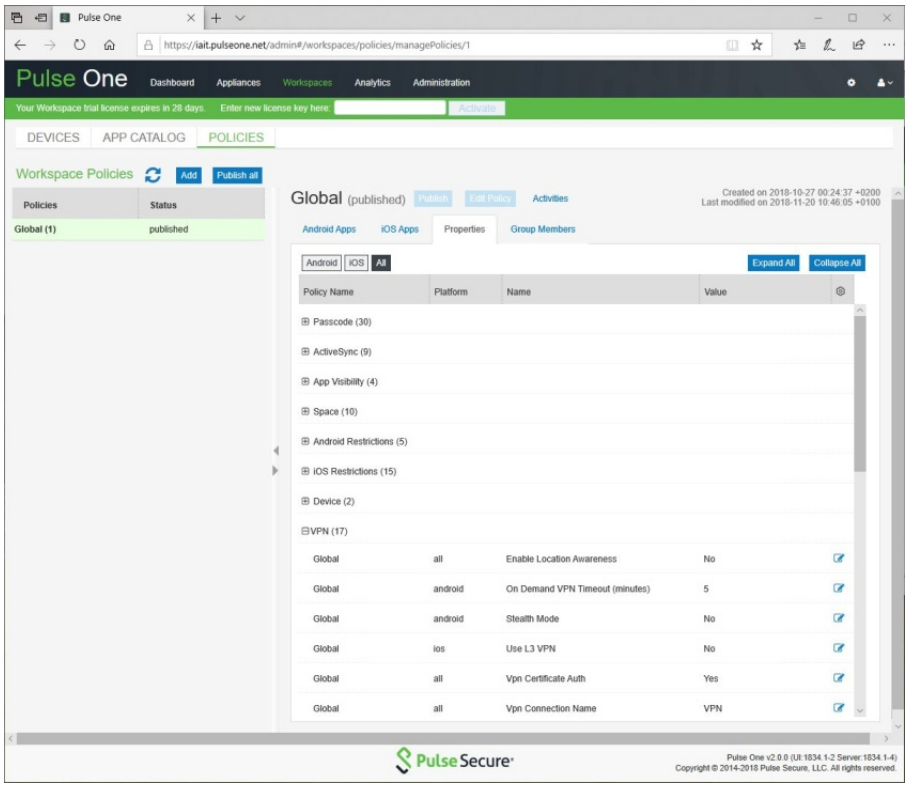
Die Arbeit mit den Profilen

Nachdem wir jetzt ein Gerät zum Verwalten in unsere Umgebung eingefügt hatten, konnten wir uns daran machen, die Funktionalität von Pulse Workspace unter die Lupe zu nehmen. Dazu fügten wir erst einmal zum Testen die Client App des Cloud-Webspeichers „Box“ zu unserem Profil hinzu und verteilten sie auf das iPhone.

Dazu steht unter Workspaces der Reiter „App Catalog“ zur Verfügung. Dort selektierten wir den Befehl „Add App from Store“, wählten über die Suchfunktion die Box App aus, erlaubten direkten Netzwerkzugriff (statt „Per App VPN“) und klickten auf „Add“. Danach fand sich die App in der Liste des App-Katalogs wieder. Jetzt mussten wir nur noch auf den Reiter „Policies“ wechseln und die App zu unserer aktiven Policy hinzufügen. Nach einem Klick auf „Publish“ wurde die App auf das iPhone geladen. Auch hier ging der Prozess wieder schnell von der Hand und war nach wenigen Minuten abgeschlossen.

Das Verteilen eines Mail-Profils

Um nun die Konfiguration unseres Mail-Kontos auf das iPhone zu übertragen, gingen wir ähnlich vor. Wir wählten wieder unsere Policy aus und wechselten nach „Properties / iOS POP/IMAP“. Dort konnten wir anschließend die Konfigurationsdaten wie IMAP- und SMTP-Server, Authentifizierung, Verschlüsselung, verwendete Ports und so weiter eingeben. Nach dem nächsten Veröffentlichen der Policy wurden die Angaben auf das iPhone übertragen und wir mussten dort nur noch unsere Mail-Passwort eingeben, um das Mail-Konto zu der Mail-App hinzuzufügen.

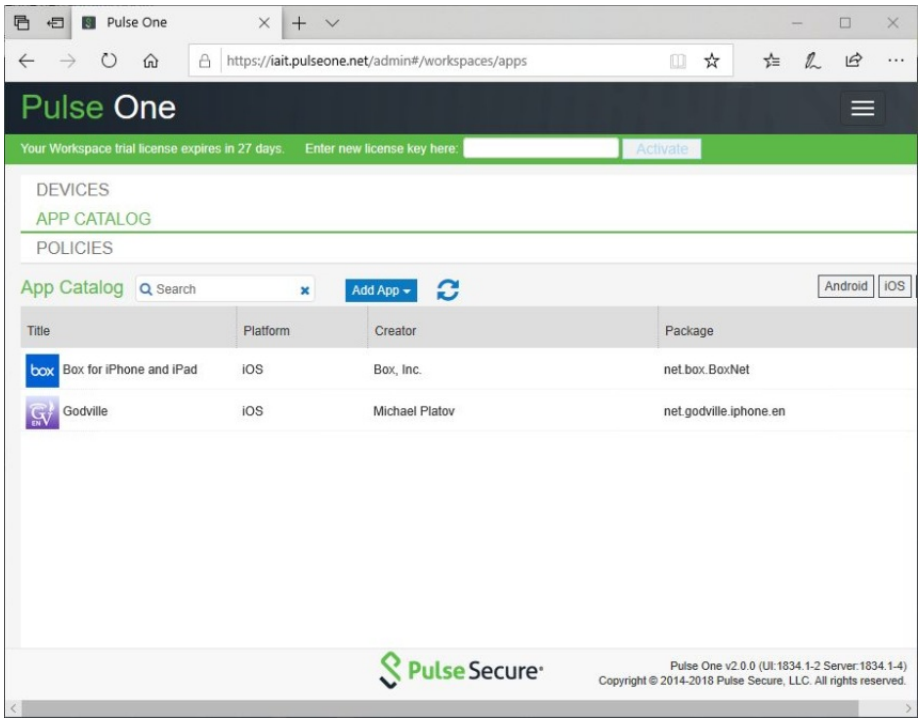


Die Policies bieten den zuständigen Mitarbeitern die Möglichkeit, eine Vielzahl von Parametern auf den Endpoints zu konfigurieren

VPN-Verbindungen

Nachdem wir die Apps und Mail-Konten auf unser Endgerät ausgebracht hatten, richteten wir zum Schluss noch eine VPN-Verbindung über die zuvor erwähnte PCS-Appliance in unser Testnetzwerk ein, um die Datenübertragungen zwischen dem im

Test verwendeten mobilen Endpoint und den Assets bei uns im Netz abzusichern. Das funktioniert so ähnlich wie das Verteilen der Mail-Zugangsdaten. Zu-



Der App Katalog von Pulse Workspace

nächst einmal wechselten wir unter "Workspaces / Policies" auf die von uns verwendete Test-Policy und trugen dort unter "Properties / VPN" den VPN-Host (also unsere PCS-Appliance), den Namen des VPNs und ähnliches ein. Anschließend verteilten wir die neuen Informationen wieder über den Button "Publish" auf unser Endgerät. Nachdem die Policy verteilt worden war, konnten wir auf unserem iPhone eine VPN-Verbindung aufbauen, uns bei dem VPN einloggen und auf die Assets in unserem Testnetzwerk zugreifen. Bei Bedarf prüft ein Host Checker, ob der verwendete Endpoint die vorgegebenen Compliance-Regeln erfüllt.

Die Analysewerkzeuge von Pulse Workspace

Wenden wir uns nun den Dashboards, Logs und Analysefunktionen von Pulse Workspace zu. Unter "Dashboard / Workspaces" finden sich Informationen zu den zehn am meisten und am wenigsten benutzten Apps sowie der Zahl der Benutzer und der Workspaces, der blockierten Spaces, der Geräte, die nicht den Compliance-Vorgaben entsprechen und vieles mehr.

Darüber hinaus informieren Grafiken über die vorhandenen Geräte mit ihren Betriebssystemen, die Carrier und die Hersteller. Unter "Analytics" haben die zuständigen Mitarbeiter Gelegenheit, sich über die Login-Versuche bei der PCS-Appliance, die Appliance Health und die Appliance-Aktivitäten zu informieren.

Der Eintrag "App Visibility" gibt im Gegensatz dazu unter anderem darüber Aufschluss, welche der im App-Katalog aufgeführten Anwendungen in welchen Workspaces installiert wurde und welche Versionen der App dabei zum Einsatz gekommen sind. Außerdem gibt es auch noch die Option, unter "Workspaces / Devices" ein verwaltetes Gerät auszuwählen und über den Eintrag "Activities" ein Log einzusehen, das Informationen über das Verteilen der Policies, die Compliance und so weiter gibt. Es ist für Administratoren also kein Problem, über alle wesentlichen Punkte auf dem Laufenden zu bleiben.

Der Abschluss des Tests

Zum Abschluss des Tests simulierten wir noch ein verlorenes Phone. Selektiert der Administrator unter "Workspaces / Devices" das betroffene Gerät, so kann er verschiedene Aktionen durchführen, wie beispielsweise "Delete Workspace", "Revoke VPN Certificate", "Wipe Workspace" oder auch "Lock Device". Nachdem wir den "Lock Device"-Befehl aufgerufen hatte, war das iPhone, wie zu erwarten war, anschließend sofort gesperrt und ließ sich erst durch ein "Reset Passcode" wieder zum Leben erwecken.

Fazit

Pulse Workspace konnte uns im Test überzeugen. Die Arbeit mit dem App Catalog und den Profilen gestaltet sich einfach, die Lösung bringt die wichtigsten Sicherheitsfunktionen wie Lock- und Wipe-Device mit und die Analyse- und Log-Funktionen sorgen dafür, dass die Administratoren immer wissen, was in ihrer Umgebung abläuft. IT-Mitarbeiter, die auf der Suche nach einer Management-Lösung für mobile Geräte sind, sollten auf jeden Fall einen Blick auf das Produkt werfen. Aufgrund der einfachen Bedienung und der nützlichen Funktionen verleihen wir dem Produkt das Attribut "IAITested and recommended".