ASAVIE

OPTIMIEREN SIE DIE MOBILE DATENNUTZUNG IHRER MITARBEITER

Ein Leitfaden für Unternehmen zur effektiven Steuerung der Datennutzung auf mobilen Endgeräten

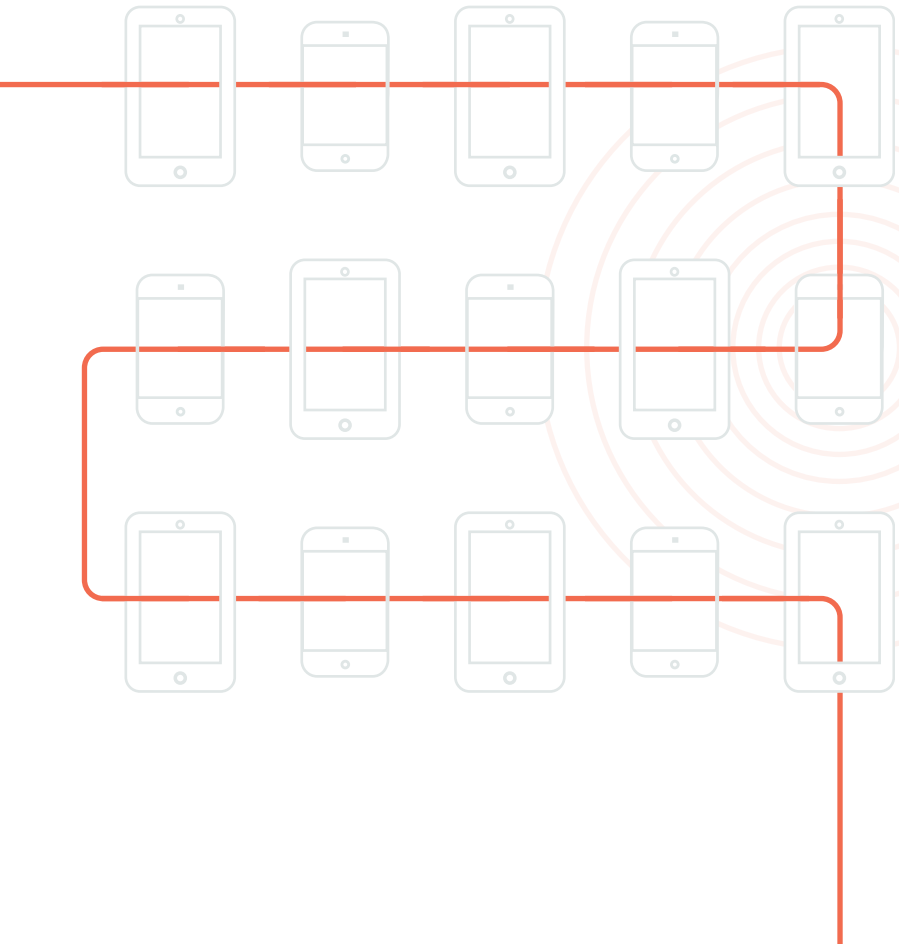
INHALT

ÜBERBLICK

Die Ausstattung von Mitarbeitern mit Mobilgeräten hat sich in den letzten fünf Jahren zu einem der wichtigsten Trends im Bereich Unternehmenskommunikation entwickelt der sich auch künftig noch weiter verstärken wird. Laut Citrix hat sich die Anzahl der in Unternehmen genutzten Geräte im letzten Jahr nahezu verdoppelt (Mobile Analytics Report, Februar 2015). Dabei steigt nicht nur das Datenaufkommen, sondern auch die Komplexität.

Datenverbindungen mit Mobilgeräten bedeuten längst nicht mehr nur „unterwegs E-Mails zu checken“. Video spielt eine immer größere Rolle, sowohl bei Telefonie und Konferenzen als auch beim Teilen von Inhalten. Unternehmensanwendungen werden zunehmend auch auf Mobilgeräten ausgeführt. Anbieter wie Microsoft, SAP, Oracle und IBM konzentrieren sich verstärkt auf die Entwicklung von Anwendungen für mobile Endgeräte und bedienen damit die steigende Nachfrage nach Fernzugriff auf wichtige Dienste.

IDC prognostiziert das Unternehmen in 2017 mindestens 25 % ihres Software-Budgets für die Entwicklung, Bereitstellung und Verwaltung von Anwendungen für mobile Endgeräte ausgeben werden. Die Herausforderung für Unternehmen besteht darin, die Produktivitätsvorteile durch die mobilen Endgeräte zu nutzen ohne dabei die Kosten für Datenverbindungen über 3G- und 4G-Netze linear zu steigern. Insbesondere IT-Abteilungen und Entwickler von Enterprise Mobility - Lösungen sind laut IDC bei der Vermittlung, Integration und Verwaltung sowie bei der Service-Orchestrierung gefordert. Sie müssen Möglichkeiten finden um die unzulässige, unsichere und unproduktive Nutzung von Datenverbindungen zu unterbinden.

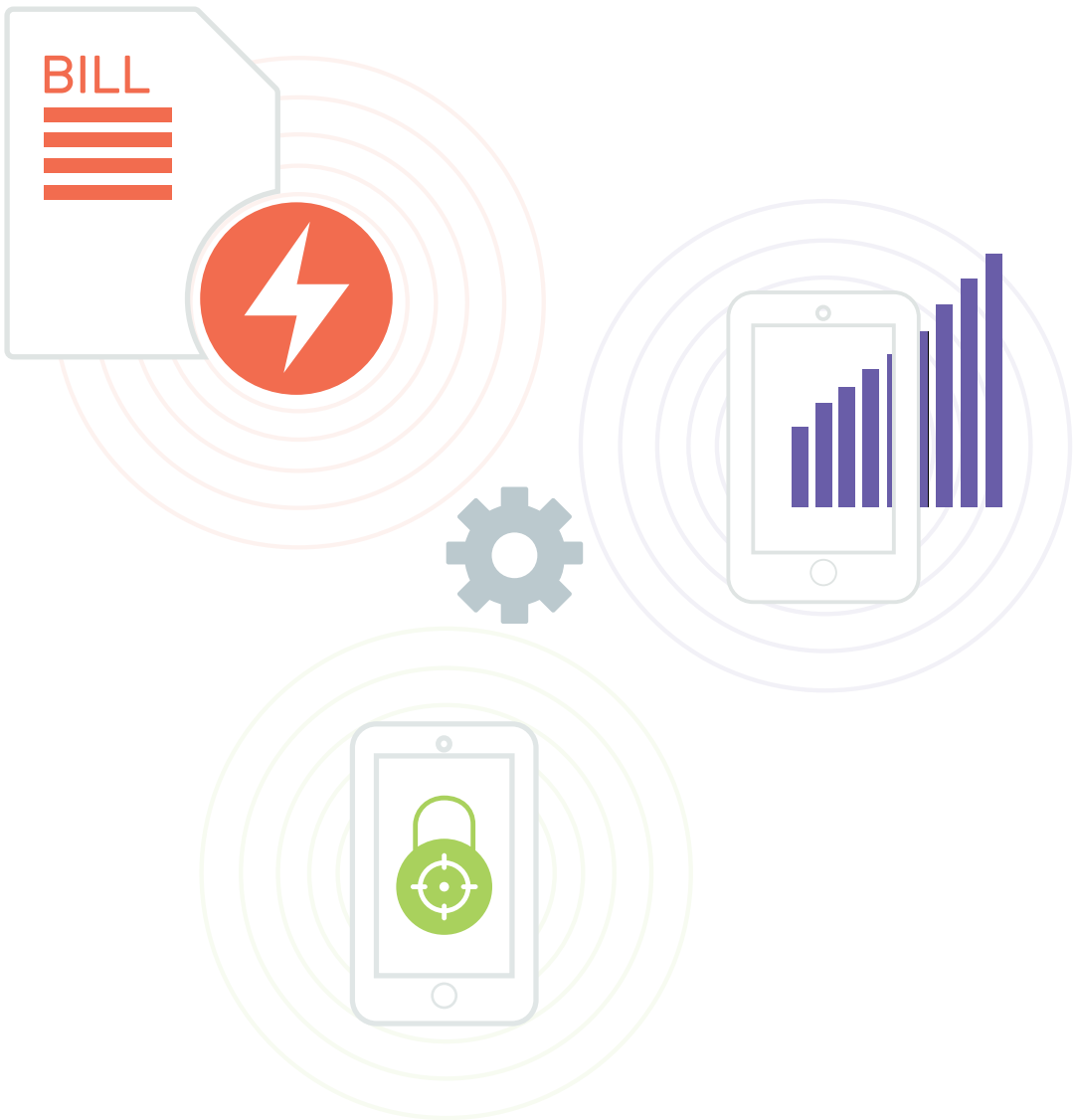


Die Anzahl der in Unternehmen genutzten mobile Geräte hat sich im letzten Jahr nahezu verdoppelt.

Im Mittelpunkt steht dabei “Wie” bzw. “Wo” die Daten genutzt werden und wie Unternehmen sich vor einem möglichen Rechnungsschock (“bill-shock”) in Folge des unkontrollierten Überschreitens vereinbarter Datenlimits schützen können. Wie aus verschiedenen Studien hervorgeht, nehmen Mitarbeiter bis zu 3 mobile Endgeräte mit auf Dienstreisen (Vodafone) und der Auslandsdatenverbrauch beträgt im Durchschnitt 18% Ihres Datenpaketes (Cisco). Dieses Anwenderverhalten erfordert eine effektive Steuerung der Datennutzung zur pro-aktiven Kostenkontrolle.

Hierfür gibt es bereits industrieerprobte Lösungen zur aktiven Regelung der Datennutzung mit denen das exponentielle Wachstum ohne Produktivitätsverlust zu bewältigen ist.

Das vorliegende Weißbuch stellt die verschiedenen technischen Ansätze vor und gibt damit Hilfestellung bei der Auswahl der für das Unternehmen am besten geeigneten, zukunftssicheren Lösung.



MÖGLICHKEITEN ZUR STEUERUNG DER MOBILEN DATENNUTZUNG

1 BROWSER-BASIERTES TOOL

Chrome, Firefox und Opera bieten browser-basierte Datenkomprimierung und -optimierung gemäß der IETF http/2.0-Spezifikation (über das SPDY-Protokoll von Google). Die Idee datenintensive Aufgaben mit Hilfe eines lokalen Protokolls in die Cloud zu verlagern ist grundsätzlich gut. Allerdings gibt es einige erhebliche Schwachstellen die verhindern daß Unternehmenskunden von einer wesentlichen Kostensenkung profitieren.

Das größte Defizit besteht darin, daß sich der App-Datenverkehr nicht überwachen lässt. Bei den Apps handelt es sich im Wesentlichen um Browser, die auf die Nutzung eines bestimmten Webdienstes zugeschnitten sind. Diese werden von browser-basierten Kontrollmechanismen in der Regel jedoch nicht erfasst. Aus diesem Grund sind browser-basierte Tools ungeeignet eine effektive Datenverbrauchskontrolle durchzusetzen.

Eine weitere Einschränkung besteht darin, daß browser-basierte Tools nur bei Smart Devices (Tablets und Smartphones) funktionieren nicht aber bei USB- Modems oder MiFi-Geräten und per Tethering übertragene Daten bleiben komplett unberücksichtigt. Desweiteren ist ein wachsender Anteil des Internetdatenverkehrs verschlüsselt oder bereits komprimiert. Browser-basierte Komprimierungstools sind daher im besten Fall ein nettes Plus, bilden aber keine sichere Kontrolle des gesamten Datenverkehrs ab.

RISIKO EINER UMGEHUNG

UNBEABSICHTIGT

hoch

Sämtliche außerhalb des „optimierten“ Browsers übertragen Daten werden nicht abgedeckt.

BEABSICHTIGT

hoch

Benutzer können eine andere SIM-Karte verwenden, einen anderen Browser installieren, Apps verwenden, ein VPN nutzen oder die Option zur sicheren Datenübertragung einfach deaktivieren. Es steht also eine Vielzahl von Möglichkeiten zur Verfügung, Datenverbindungen weiterhin unkontrolliert und uneingeschränkt zu nutzen. Ursachen für erhöhte Kosten wie sie z.B. durch Datennutzung entstehen lassen sich in Audit’s nicht ermitteln.

2 TOOLS VON GERÄTEHERSTELLERN

Mit Android 4 (Ice Cream Sandwich) für Mobilgeräte wurde ein rudimentäres Widget zur Datennutzung eingeführt und seitdem schrittweise verbessert. In ähnlicher Weise bietet iOS von Apple Informationen zur Datennutzung und die Möglichkeit, mobile Daten je nach genutzter App zu deaktivieren. Windows Phone bietet Cloud-gestützte Datenoptimierung.

Diese Tools weisen in der Regel auf das Ausschöpfen des monatlichen Datenkontingents hin, d.h. sie bieten Nutzern die Möglichkeit den eigenen Datenverbrauch selbst zu überwachen. Benutzerorientierte Tools sind jedoch für Unternehmen nur von geringem Wert, denn sie bieten keine übergeordneten Kontrollmöglichkeiten da Benutzer die Tools einfach deaktivieren und damit dem Unternehmen jede Transparenz entziehen können. Die Verwaltung von unterschiedlichen Benutzern mit mehreren Kontrollsystemen macht die einheitliche Durchsetzung von Regeln unmöglich.

Lösungen von Geräteherstellern bieten Endnutzern die Möglichkeit der Selbstkontrolle, sind aber für Unternehmen ungeeignet.

RISIKO EINER UMGEHUNG

UNBEABSICHTIGT

hoch

Benutzer können Datenlimits unbeabsichtigt zurücksetzen oder ändern. Sie missverstehen möglicherweise die bereitgestellten Informationen oder vergessen, beim Roaming-Zugriff die Einstellungen zu ändern.

BEABSICHTIGT

hoch

Benutzer können die SIM-Karte in ein anderes Gerät einsetzen, Warnungen ignorieren und Einstellungen ändern. Änderungen am Gerät lassen sich mühelos rückgängig machen. Die Datennutzung lässt sich, etwa zu Audit-Zwecken nicht zurückverfolgen.

3 MOBILE DEVICE MANAGEMENT

Viele Mobile Device Management (MDM)-Suites bieten eine Funktion zur Datenkontrolle – in der Regel in Form von Berichten über die Datennutzung sowohl an IT-Manager als auch an den Nutzer des mobile Endgerätes. MDM-Lösungen sind beim umfassenden Einsatz von Mobilgeräten zwar unverzichtbar, bieten jedoch keinerlei Möglichkeiten, die Datennutzung detailliert zu steuern. In der Regel stehen nur einfache Optionen zur Verfügung, beispielsweise: „Roaming: Ja/Nein“ oder „Daten: Ein/Aus“.

Darüberhinaus kann die Umsetzung von MDM-Maßnahmen auf iOS-Geräten unter Umständen völlig anders erfolgen als für Windows Phone. Der Abstraktionsgrad ist ein weiteres Problem. MDM-Lösungen können nicht zwischen dem Streaming von Netflix-Serien und dem Herunterladen einer PowerPoint- Präsentation unterscheiden. Sie unterbinden beides oder lassen beides zu. Dies ist eine grundlegende Schwäche aller heute verfügbaren Lösungen.

RISIKO EINER UMGEHUNG

UNBEABSICHTIGT

mittel

MDM-Dienste eignen sich gut um Berichte zur Nutzung von Datenverbindungen zu generieren, können die Nutzung bei der Verwendung von Standardregeln jedoch nicht einschränken. Strengere Regeln beeinträchtigen möglicherweise die erforderliche Nutzung der Geräte.

BEABSICHTIGT

mittel

Benutzer können SIM-Karten in andere Geräte einsetzen und sich sogar vom MDM abmelden. Richtig eingesetzt sind MDM-Dienste kaum zu umgehen, bieten jedoch wenig Möglichkeiten, die Datennutzung einzuschränken.

4 IN DER CLOUD GEHOSTETER PROXY

Einige Mobile Data Control (MDC) Lösungen basieren auf einem in der Cloud gehosteten Proxy-Server der in den Einstellungen für Datenverbindungen auf dem Mobilgerät angegeben wird. Dieses Konzept bietet gegenüber den zuvor beschriebenen Lösungen einige Verbesserungen, eignet sich jedoch trotzdem nicht für eine umfassende Kontrolle der Mobilgeräte eines Unternehmens.

Ein in der Cloud gehosteter Proxy-Server stellt eine Teillösung dar, mit der sich erhöhte Kosten wie sie etwa durch einen Rechnungsschock ("bill shock") entstehen weder verhindern noch nachvollziehen lassen. Außerdem ist dieses Proxy-basierte Konzept nicht für Windows Phone, Blackberry sowie USB-Modems und MiFi-Geräte geeignet. Proxy-Lösungen basieren auf der lokalen Gerätekonfiguration die mitunter nicht zwingend erforderlich ist, so daß sich Kontrollmechanismen beispielsweise durch die Nutzung eines VPN einfach umgehen lassen. Es ist für Nutzer verhältnismäßig einfach Proxy-Dienste zu umgehen in dem Sie die SIM-Karte eines beruflich genutzten Endgeräts einfach in ein privates Gerät einsetzen.

RISIKO EINER UMGEHUNG

UNBEABSICHTIGT

hoch

Cloud-Proxy-Dienste erfassen ausschließlich HTTP-Datenverkehr. Bei verschlüsselten Verbindungen sind sie wirkungslos. Der Test eines Proxy-Dienstes hat beispielsweise ergeben, dass dieser über 80 % des Datenverkehrs der 100 am häufigsten genutzten Apps nicht erfasst.

BEABSICHTIGT

hoch

Benutzer können eine andere SIM-Karte verwenden, einen anderen Browser installieren, Apps verwenden, ein VPN oder Tethering nutzen. Technisch versierte Benutzer haben zahlreiche Möglichkeiten, auf Daten zuzugreifen, die eigentlich blockiert werden sollen.

5 ANBIETEREIGENES NETZ

Viele Netzbetreiber bieten Kunden lediglich Gebührennachweise zur Kostenkontrolle. Solche Warnungen sind häufig mit anderen Maßnahmen wie einer Roaming-Sperre, der Anwendung eines Datenlimits oder der Drosselung der Verbindungsgeschwindigkeit verbunden.

Von den bisher vorgestellten Lösungen bietet jedoch nur die netzseitige Kontrolle eine wirkliche Möglichkeit der Kosten - und Volumenkontrolle. Der Netzbetreiber zählt die Daten-Pakete und Sessions, allerdings stellt er diese Informationen dem Kunden nur mit Zeitversatz zur Verfügung. Eine gewünschte zeitnahe Kontrolle durch den Anwender ist somit stark vom Netzbetreiber abhängig und wird in der Regel nicht angeboten.

So gut dieses Konzept in technischer Hinsicht sein mag, kann es doch nicht die Anforderungen von IT- und Einkaufsabteilungen erfüllen die aktuelle Daten sowie detaillierte Steuerungsmöglichkeiten benötigen. Hinweise des Anbieters werden in der Regel per SMS an das Endgerät gesendet. Damit erhält der Endbenutzer die Möglichkeit, „die Kosten zu akzeptieren“ und Datenverbindungen entgegen den Bestimmungen des Unternehmens zu nutzen. Darüber hinaus können weder Benutzer noch IT-Abteilungen detaillierte Entscheidungen darüber treffen welches Datenvolumen und welche Datentypen zu welchem Zeitpunkt zulässig sind.

Anbieterseitige Kontrollmechanismen sind für Endverbraucher gedacht und teilweise gesetzlich vorgeschrieben. Im Idealfall sollten Netzbetreiber diese Funktionen auch Unternehmen zur Verfügung stellen, was mit den netzseitigen Kontrollfunktionen technisch nicht realisierbar ist, so daß Unternehmen bis auf Weiteres mit überhöhte Kosten und überschrittenen Datenkontingenten rechen mussen. Unternehmen müssen sich bei der Abrechnung der Datenvolumen notgedrungen auf die Netzbetreiber verlassen, auch wenn sie sich mehr Einfluss auf die Nutzung von Datenverbindungen wünschen.

RISIKO EINER UMGEHUNG

UNBEABSICHTIGT

mittel

Benutzer beachten Kostenlimits bzw. SMS-Hinweise bei der Nutzung von MiFis oder USB-Modems unter Umständen nicht. Kostenhinweise sind oft nur allgemein formuliert und lassen sich einfach ignorieren.

BEABSICHTIGT

gleich Null

Angriffe auf das Datenkontrollmodul eines Netzbetreibers beschränken sich auf wenige Ausnahmefälle. Der Ansatz gilt aufgrund der vertrauenswürdigen Position des Netzbetreibers als zuverlässig.

6 SIM-KONTROLLE

Netzgestütze Datenkontrolle bietet die Gewissheit, dass alle in Rechnung gestellten Daten erfasst werden. Richtig effizient ist mobile Datensteuerung aber erst wenn detaillierte Informationen hinreichend abgebildet und Regeln durch automatisierte Mechanismen angewendet werden.

Kontrollmechanismen auf Ebene der SIM ermöglichen Zugang zu dem RADIUS Server des Netzbetreibers was Unternehmen erlaubt für jeden Mitarbeiter (bzw. jedes Gerät) eigene Regeln bezüglich Volumen und Art der zulässigen Daten festlegen. Alle aktuellen und künftigen mobilen Endgeräte werden ebenso unterstützt wie sämtliche SIM-fähigen Geräte z.B. Mobiltelefone, Tablets, MiFi und Datenkarten.

Die vom Netzbetreiber als Authentifzierungselement etablierte SIM-Karte ist dabei weder abhängig vom Betriebssystem des Endgerätes noch sind ständige Updates erforderlich.

RISIKO EINER UMGEHUNG

UNBEABSICHTIGT

Gleich Null

Die gesamte Mobilfunk-Datennutzung wird anhand von Kontrollmechanismen auf der SIM-Karte überwacht, so dass die aufgestellten Regeln auch dann greifen, wenn die SIM-Karte in ein anderes Gerät eingesetzt wird.
Die Nutzung von Datenverbindungen lässt sich nicht mit Hilfe von Apps, VPNs oder sonstigen Diensten verbergen.
Keine andere Lösung bietet derartige Einstellungsmöglichkeiten, die zudem unabhängig von der Geräteplattform anwendbar sind.

BEABSICHTIGT

Gleich Null

Angreifer können Kontrollmechanismen auf Ebene der SIM-Karte nicht umgehen – auch nicht mit physischem Zugriff auf das Mobilgerät. Die Kontrollmechanismen basieren auf derselben Datenquelle wie die Abrechnung des Netzbetreibers.

AUF EINEN BLICK: LÖSUNGEN ZUR STEUERUNG DER MOBILEN DATENNUTZUNG

	BROWSER	AUF GERÄT	MDM	PROXY	ANBIETER-EIGENES NETZ	SIM-BASIERT
CLOUD-BASIERT	Ja	Nein	Ja	Ja	Ja	Ja
ECHTZEITSTEUERUNG	Nein	Nein	Ja*	Nein	Ja	Ja
SCHUTZ VOR WECHSEL DER SIM-KARTE	Nein	Nein	Nein	Nein	Ja	Ja
UNTERBINDUNG VON TETHERING	Nein	?	Nein	Nein	Ja	Ja
REGELUNG DER BANDBREITE	Nein	Nein	Nein	Ja	Ja	Ja
iOS	Ja	Ja	Ja	Ja	Ja	Ja
ANDROID	Ja	Ja	Ja	Ja	Ja	Ja
WINDOWS	Ja	Ja	Ja	Nein	Ja	Ja
BLACKBERRY	Ja	Ja	Ja	Nein	Ja	Ja
MIFI	Nein	Nein	Nein	Nein	Ja	Ja
USB-MODEM	Nein	Nein	Nein	Nein	Ja	Ja
STEUERUNG DURCH ADMINISTRATOR	Nein	Nein	Ja	Ja	Nein	Ja

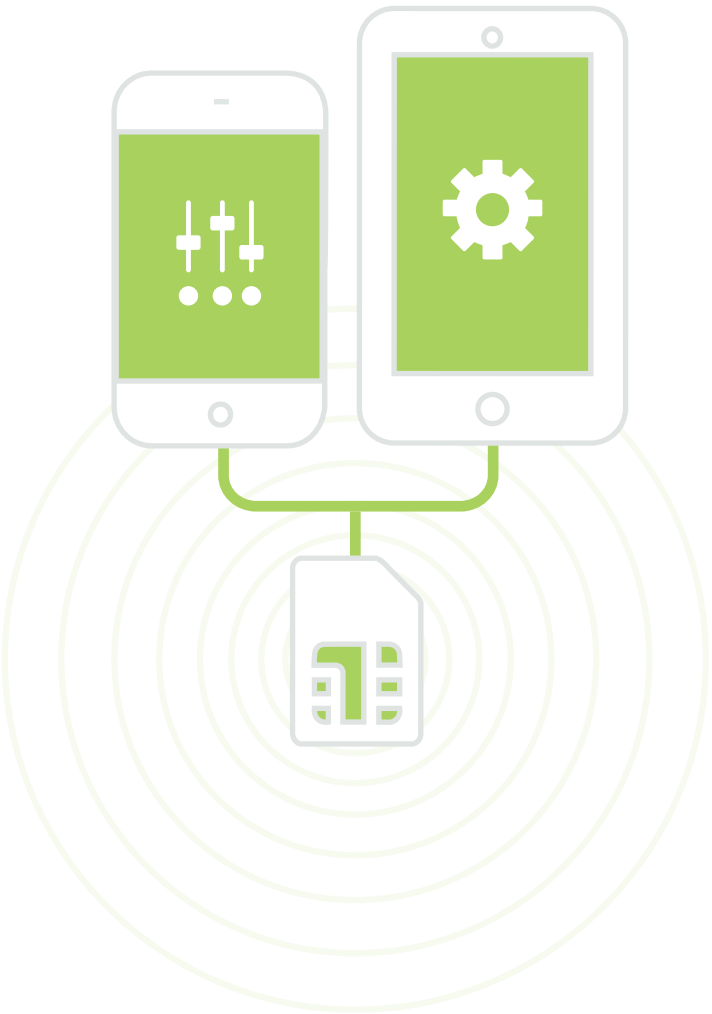
*Nur Daten ein/Daten aus

ZUSAMMENFASSUNG

Das rasante Wachstum bei der Nutzung von Datenverbindungen auf Mobilgeräten ermöglicht Unternehmen die Entwicklung neuer Arbeitsweisen, denn das stationäre Büro hat ausgedient da Mitarbeiter mit SIM-fähigen Endgeräten ihrer Tätigkeit jederzeit und von überall aus nachgehen können. Der Vorteil der höheren Produktivität stellt Firmen vor die Herausforderung das Risiko eines möglichen Rechnungsschocks durch überhöhte Datennutzung zu minimieren.

Dieses Weißbuch zeigt auf, dass die sicherste Lösung auf Ebene der SIM-Karte ansetzt. Der SIM-basierte Ansatz ermöglicht Unternehmen effektive Kontrolle, unabhängig von Plattform und Typ der Mobilgeräte. Die Regeln bleiben selbst bei einem Gerätewechsel bestehen. Bei ordnungsgemäßem Einsatz besteht keine Möglichkeit zur Manipulation der zentral verwalteten Einstellungen.

Die umfassenden Berichtsfunktionen liefern wertvolle Erkenntnisse über die Nutzung von Datenverbindungen.




MODA

Als weltweit führender Anbieter von Cloud-Services für Mobilfunkbetreiber hat Asavie mit Moda eine Software-as-a-Service (SaaS)-Lösung entwickelt, mit der sich Nutzungsregeln auf der SIM Karte anwenden und über ein Kundenportal festlegen lassen.
Moda erfüllt sämtliche Anforderungen für den Einsatz in Unternehmen:

CLOUD-DIENST

Hochgradig skalierbar bei geringen Investitionen in Infrastrukur und Systemintegration.

SIM-BASIERT

Funktioniert auf allen SIM-fähigen Geräten wie Mobiltelefonen, Tablets, MiFis und Datenkarten.

REGELN

Drosselung der Zugangsgeschwindigkeit z.B. den Zugriff auf datenintensive Streamingdienste.
Festlegung des Datenkontingents pro SIM, z.B. aus Datenpools.
Regelung des Aufrufs von Webseiten, Einrichten der Erlaubnis oder Verweigerung aus einem Pool von mehr als 1,25 Mrd. Webseiten übersichtlich gruppiert in 26 Kategorien.

ZONEN & GESCHWINDIGKEITEN KONTROLLIEREN

Individuelle Regeln für unterschiedliche Regionen verhindern das reisende Mitarbeiter beachtliche Roamingkosten verursachen.

ECHTZEIT MONITORING

Gewinnen Sie Einblick in die Datennutzung per SIM/Gruppe durch das umfangreiche Reporting.

GESCHÜTZT & MANIPULATIONSSICHER

Regeln lassen sich nicht umgehen und bleiben auf der SIM Karte auch bei Gerätewechsel aktiv. Such-, Sperr- und Löschfunktionen sorgen für den Schutz von Daten und Geräten.

ASAVIE

SIE MÖCHTEN MEHR ERFAHREN?

Unser Vertrieb informiert Sie gerne über Lösungen zur Kostensenkung/-kontrolle Ihrer Mobilfunk-Datenverbindungen.

Kontakt zu Asavie:
www.asavie.com/our-solutions/moda/

www.asavie.com

twitter.com/Asavie

linkedin.com/company/asavie-technologies