IBM Security
Whitepaper – Thought Leadership

Mobilität für die Inhalte und Apps Ihres Unternehmens

Einfache und sichere mobile Kollaboration in Unternehmen

IBM

Mobile Strategie für ein neues Zeitalter

Frage: Verfügen Sie über eine effektive mobile Strategie?

Antwort: Über eine mobile Strategie? Sie meinen, ob Mitarbeiter über mobile Geräte auf E-Mail zugreifen können? Na klar haben wir das.

Wenn so Ihre Antwort lautet, sind Sie damit nicht allein. Bei der Kommunikation von Mitarbeitern außerhalb des Büros setzen viele Unternehmen weiterhin auf E-Mail als wichtigste App. Noch vor wenigen Jahren war dies tatsächlich ein großer Fortschritt. Doch lassen Sie uns ehrlich sein: Das Abrufen und Beantworten von E-Mail außerhalb des Büros ist nicht wirklich Arbeit. Im Idealfall werden ein paar Hindernisse beseitigt, Aufgaben verschoben oder der gute Schein gewahrt. In der Welt von heute bietet mobile Kollaboration jedoch viel mehr Potenzial: Sie kann für mehr Produktivität sorgen und eine Erledigung realer Aufgaben in nahezu Echtzeit ermöglichen. Viele Unternehmen befinden sich damit jedoch erst am Anfang und müssen noch eine effektive mobile Strategie planen und implementieren, um mit einfachem, geschützten Zugriff auf Unternehmensressourcen alle Chancen von Mobilität nutzen zu können.

In diesem Dokument untersuchen wir, wie sich Notebooks, Desktopcomputer und andere Endgeräte kontinuierlich überwachen lassen.

In diesem Whitepaper erfahren Sie, wie Sie:

- Ohne VPN auf einzelnen Geräten für sicheren mobilen Zugriff auf Unternehmensdaten sorgen können
- SharePoint, Windows-Dateifreigaben und Intranetsites mobil machen können
- Sensible Unternehmensdaten mit zuverlässigen Sicherheitsrichtlinien und DLP-Kontrollen schützen können
- Mobilen Zugriff gewährleisten können, ohne Änderungen an Ihrer Netzwerk- oder Firewall-Sicherheitskonfiguration vornehmen zu müssen
- Benutzern unterwegs eine Zusammenarbeit über persönliche Geräte ermöglichen können

Lesen Sie mehr, um zu erfahren, wie Sie Mitarbeitern Zugriff auf Ressourcen hinter der Firewall gewähren können, während Ihre Daten durch Autorisierungs-, Verschlüsselungs- und Containerisierungsrichtlinien geschützt werden.

Einfacher und sicherer Zugang

Hier eine einfache Aufgabe: Errichten Sie ein sicheres Haus, das Ihre unbezahlbaren Wertgegenstände zuverlässig schützt. Wie gehen Sie vor? Sie können zum Beispiel ein Haus ohne Fenster und Türen bauen – also ohne Ein- und Ausgang. Es wäre zwar äußerst sicher, aber nicht zum Leben geeignet. Sie können Ihr Haus aber auch mit Fenstern und Türen versehen, die hochwertige Schlösser und Sicherheitssysteme aufweisen, um ähnliche Sicherheit zu erreichen. Nun können Sie jedoch rein- und rausgehen, Besucher empfangen oder frische Luft hereinlassen, ohne einen Verlust von Wertgegenständen riskieren zu müssen.

Möglicherweise gleicht Ihre mobile Strategie einem Haus ohne Fenster und Türen. Oder einem Haus mit Fenstern und Türen, die sich aber nicht verriegeln lassen. Ihre Aufgabe besteht darin, Unternehmensinhalte zu schützen, diese jedoch gleichzeitig Benutzern zur Verfügung zu stellen, damit sie produktiv arbeiten können. Von Listen mit Kundenkontakten über Patientendaten, Finanzdaten und Personalakten sowie Unternehmens-Apps bis hin zu Sitzungsprotokollen – der Umfang der Informationen, auf die Benutzer zugreifen möchten, nimmt Tag für Tag zu. Eine Zugangssperre ist daher keine realistische Option. Sie brauchen Fenster und Türen – sowie ein Sicherheitssystem, das ausschließlich Befugten Einlass bietet.

Was passiert, wenn ein Mitarbeiter ein eigenes Smartphone oder Tablet für die Arbeit verwendet und Vertriebskontakte auf dieses Gerät lädt? Was ist, wenn er vertrauliche Finanzberichte an seine private E-Mail-Adresse sendet, um zuhause daran weiterarbeiten zu können, während die Kinder schlafen? Wie sähe es mit einem Verkäufer aus? Sie wollen Inhalte und Apps für eine effizientere Zusammenarbeit freigeben. Was geschieht jedoch, wenn das Projekt abgeschlossen ist?

Solche Szenarien gehören zum Alltag. Benutzer finden stets Wege, um an benötigte Informationen zu gelangen. Wenn Sie keine sicheren, zuverlässigen und einfachen Zugriffsmöglichkeiten bieten, werden unternehmenseigene Daten Risiken ausgesetzt.

Überlegungen zu Inhalten

Unternehmensinhalte werden in firmeneigenen Netzwerken wie Windows-Dateifreigaben, SharePoint, Intranetsites und Webanwendungen gespeichert. Für die Zusammenarbeit mit Kollegen, Partnern und Kunden erforderliche Informationen sind eingesperrt in interne Festplatten, Datenspeicher, Wissensdatenbanken, interne Wikis oder ERP-, SCM-, HRM-, CRM- und andere Managementsysteme sowie in unterschiedliche Prozesse.

Es stellt sich also folgende Frage: Wie können Sie dafür sorgen, dass mobile Mitarbeiter auch unterwegs Zugang erhalten – oftmals mit Geräten, die nicht Ihrem Unternehmen gehören?

Beim Schutz von Daten, internen Netzwerken und Dateifreigaben sowie anderen Systemen sollten Sie im Rahmen Ihrer mobilen Strategie folgende Aspekte berücksichtigen. Einige Punkte mögen selbstverständlich klingen, sollten aber dennoch erwähnt werden.

1. Benutzer müssen Inhalte bei Bedarf abrufen können – mittels eines Push- oder Pull-Verfahrens.
2. Benutzer dürfen – anhand von Kontext und Identität – ausschließlich Zugriff auf von ihnen benötigte Dokumente erhalten.
3. Daten müssen sich aktualisieren und auf allen betroffenen Geräten synchronisieren lassen.
4. Der Zugriff auf Daten muss für Benutzer einfach sein.
5. Der Schutz darf nicht teuer sein, auch wenn es sich um eine wichtige Investition handelt.
6. Die Pflege der Sicherheit darf keinen übermäßig hohen Arbeitsaufwand verursachen.
7. Aktive Daten müssen verschlüsselt und geschützt werden.
8. Daten dürfen das Unternehmen ohne Autorisierung nicht verlassen können.
9. In Apps erzeugte und gespeicherte Daten müssen rundum sicher sein.
10. Da private Geräte nicht dem Unternehmen gehören, können Sie nicht alles kontrollieren.

Eines der wichtigsten Ziele bei der Einrichtung einer zentralen Lösung für Cybersicherheit muss darin bestehen, Systeme mit Abwehrmaßnahmen so schnell zu schützen, wie Angreifer angreifen können.

Moderne Technologien

Lassen Sie uns einen Blick auf moderne Technologien sowie die Herausforderungen werfen, die bei der Unterstützung von Sicherheit und Produktivität auftreten können.

E-Mail

Zwar stellt E-Mail die App der Wahl für Kollaborationszwecke dar, ist eigentlich jedoch nur ein Tool unter vielen.

Es wurde nicht für Kollaborationsaufgaben entwickelt. E-Mail ermöglicht eine One-to-One- bzw. One-to-Many-Kommunikation, unterstützt jedoch keine Many-to-Many-Interaktionen, die Benutzer benötigen, um wirklich produktiv arbeiten zu können. Das führt bei Gruppen, die eigentlich zusammenarbeiten sollten, zur Entstehung von Silos.

Per E-Mail versendete Informationen veralten schnell – oft erhalten Benutzer eine Tabelle, die sie weiter bearbeiten, obwohl es inzwischen eine Version gibt, die deutlich aktueller ist.

Das größte Problem besteht darin, dass sich Daten kopieren, einfügen und weiterleiten lassen – auch an unerwünschte Empfänger oder Orte.

VPN

Anmeldungen per VPN stellen eine häufige Lösung zur Bereitstellung von Zugriff hinter einer Firewall dar.

Leider führen sie zu einer Beeinträchtigung des Benutzerkomforts. Wenn Benutzer die Wahl haben zwischen aktuellen Inhalten mit komplizierterem Zugriff sowie leicht zugänglichen Inhalten aus veralteten E-Mail-Anhängen, entscheiden sich viele Benutzer für die einfachere Methode.

VPNs sind mit geräteabhängigen Lizenzen verbunden, sodass die Kosten mit der Zeit hohe Summen erreichen können. Zudem verbrauchen VPNs Strom, wodurch sich die Akkulaufzeit mobiler Geräte verkürzt.

Da mobile Geräte für Verbindungen auf Drahtlostechnologie zurückgreifen, schreiben Sie wahrscheinlich Verschlüsselung vor. Hiermit gibt es jedoch Probleme beim Roaming. Lösungen, die auf übergeordnete Verschlüsselung setzen, weisen meist Lücken auf, wenn sich Benutzer zwischen verschiedenen Access Points bewegen (Roaming). Zum Glück gibt es einige Lösungen, mit denen sich diese Probleme bewältigen lassen.

Desktopvirtualisierung

Bei manchen Anwendungen können Sie auf mobilen Geräten einen Desktop anzeigen. So lassen sich alle Elemente eines Desktops auch auf Ihrem Smartphone oder Tablet aufrufen. Die Anwendungen sind jedoch kostspielig und bieten wenig Benutzerkomfort. Verfügbarkeit und Performance sind bei diesem Modell stark von der jeweiligen Netzwerkverbindung abhängig. Bildschirmgröße und -auflösung stellen eine weitere Herausforderung dar – dies gilt besonders für Smartphones mit kleinen Displays und Arbeitsbereichen. Anwendungen, die für eine Desktopumgebung optimiert wurden, lassen sich zwar durch Desktopvirtualisierung aufrufen. Das heißt jedoch nicht, dass sie auch benutzerfreundlich sind.

Außerdem muss die IT-Abteilung darauf achten, dass ausreichend Server- und Netzwerkressourcen vorhanden sind, um viele gleichzeitige Verbindungen von Geräten mit dem Netzwerk unterstützen zu können.

Dateifreigaben externer Anbieter

Mit Dateifreigaben externer Anbieter können Sie Dokumente in der Cloud speichern. Ein Problem ist hier jedoch die mangelnde Kontrolle. Inhalte lassen sich an beliebige Personen senden und von beliebigen Personen aufrufen. Außerdem können Schwierigkeiten bei der Versionskontrolle auftreten.

Eine weitere Herausforderung ist der geringe Benutzerkomfort. Benutzer wollen sich nicht mit neuer Software vertraut machen, um auf benötigte Inhalte zugreifen zu können. Bedenken Sie auch, wie lange es dauert, bis sich Benutzer mit der Software auskennen.

Dateifreigaben externer Anbieter können teuer werden: Je mehr Benutzer Sie haben, desto mehr Lizenzen brauchen Sie. Außerdem ist es möglich, dass sich vorhandene Investitionen wie Apps oder Content Stores nicht nutzen lassen.

Extern entwickelte und angepasste Apps

Wenn Sie Ihre Apps bei einem externen Entwickler einkaufen, sind Sie von diesem Anbieter abhängig. Möglicherweise weist die App keine Data Leak Prevention (DLP) auf.

Sie können versuchen, eigene Apps zu entwickeln, benötigen dann aber Mitarbeiter für den Support sowie für Anpassungen an neue Gerätetypen, Betriebssystemupdates usw.

Viele Sicherheitsexperten, hochrangige Regierungsvertreter für Internetsicherheit und Abgeordnete in Parlamenten drängen auf eine kontinuierliche Überwachung, automatisierte Überwachungstools sowie schnelle Reaktionen auf Angriffe, um staatliche Daten ausreichend schützen zu können.

Die Rolle von Richtlinien

Wenn Sie Benutzern den Zugriff auf Unternehmensressourcen über persönliche Geräte gestatten möchten, müssen Sie Richtlinien erstellen, um das Aufrufen und Verwenden Ihrer Daten angemessen zu regeln.

Vor dem Zugriff auf wichtige Daten können Sie eine Kennworteingabe durch Benutzer vorschreiben.

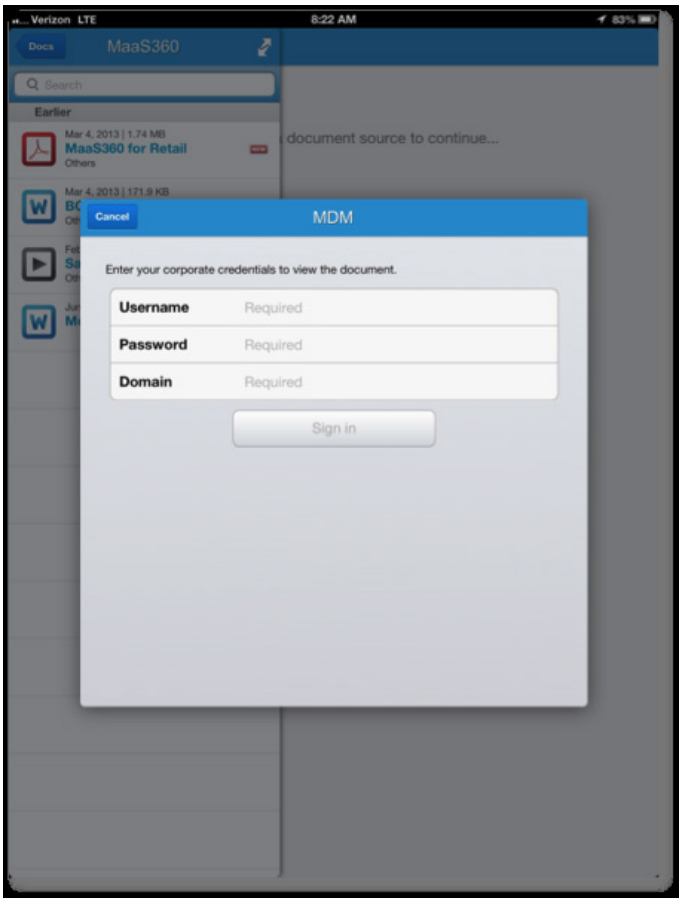

Abbildung 1: Eine Authentifizierungsanfrage

Außerdem können Sie das Kopieren und Einfügen von Text aus Dokumenten einschränken.

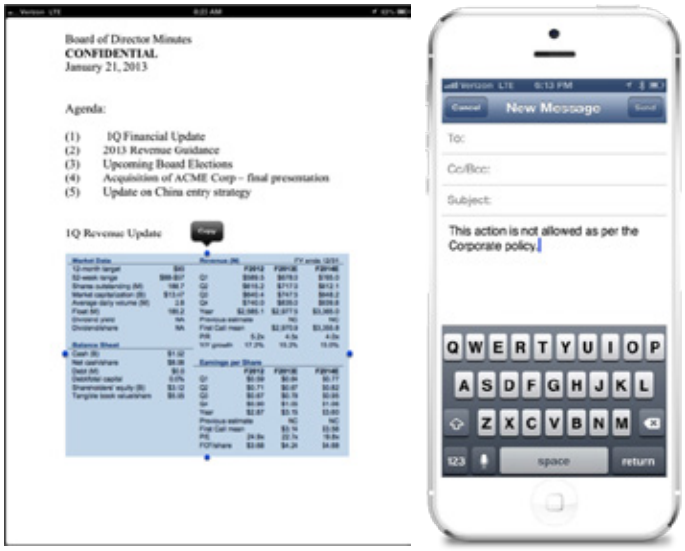

Abbildung 2: Kontrollen zum Verhindern von Datenlecks (wie Einschränkungen beim Kopieren und Einfügen)

IBM® MaaS360® Productivity Suite

Die MaaS360 Productivity Suite hilft Ihnen, den Herausforderungen moderner Technologien zu begegnen, und bietet verschiedene Möglichkeiten für den sicheren Abruf und Schutz ruhender Daten:

1. IBM® MaaS360® Secure Mobile Mail
2. IBM® MaaS360® Mobile Application Security
3. IBM® MaaS360® Secure Mobile Browser

MaaS360 verwendet einen Container für einen Dual-Persona-Ansatz – unternehmensspezifische Daten, Anwendungen und Inhalte werden auf dem Gerät in einem sicheren Bereich geschützt. Sie legen Kontrollen für den sicheren Bereich fest, damit E-Mails, Kontakte, Kalender, Apps (und Daten von Apps), Dokumente und Webseiten zuverlässig geschützt werden.

Abbildung 3: MaaS360 Productivity Suite und MaaS360 Content Suite

Die MaaS360 Productivity Suite nutzt Persona-Richtlinien zur Gewährleistung der Sicherheit auf allen Geräten eines Benutzers. Die Richtlinien werden im MaaS360 Portal erstellt und drahtlos auf die registrierten Geräte verteilt. So muss die IT-Abteilung Geräte nicht wirklich in der Hand halten.

Wenn ein Gerät die Kompatibilitätsanforderungen nicht erfüllt, das Projekt abgeschlossen ist oder der Verkäufer die Geschäftsbeziehung verlässt, können Sie den Container aus der Ferne löschen. Daten und Apps sind dann nicht mehr nutzbar.

Der Container verfügt über integrierte Sicherheitsfunktionen und mit FIPS 140-2 kompatible AES-256-Verschlüsselung. Vor dem Zugriff auf Daten können Sie eine Kennworteingabe durch Benutzer vorschreiben. Die Richtlinieneinstellungen lassen sich auf für das vollständige Löschen des Containers von Geräten mit Jailbreak oder Root verwenden. Das Gleiche ist möglich, wenn Geräte nicht innerhalb eines bestimmten Zeitraums registriert werden.

Außerdem können Sie verhindern, dass Dateien aus dem Container verschoben, kopiert oder gedruckt werden bzw. dass Inhalte eingefügt werden.

IBM® MaaS360® Content Suite

Die MaaS360 Content Suite bietet einen verschlüsselten Container sowie Produktivitätstools für das Verteilen, Anzeigen, Erstellen, Bearbeiten und Freigeben von Dokumenten auf mobilen Geräten, damit Unternehmen die nötige Kontrolle und Mitarbeiter den erforderlichen Zugang erhalten:

1. IBM® MaaS360® Mobile Content Management
2. IBM® MaaS360® Mobile Document Editor
3. IBM® MaaS360® Mobile Document Sync

MaaS360 Mobile Content Management bietet einen Container für mobile Dokumente mit leistungsstarken Funktionen für die Verwaltung des gesamten Informationslebenszyklus – zum Verteilen, Aktualisieren, Verwalten und Sichern von Dokumenten und somit für eine gemeinsame Bearbeitung von Inhalten. IT-Administratoren haben die Möglichkeit, Authentifizierung vorzuschreiben, das Kopieren und Einfügen zu beschränken und ausschließliche Leseberechtigungen zuzuweisen. Benutzer können auf im Unternehmen verteilte Daten und Datei-Repositorys wie SharePoint, Box und Google Drive zugreifen.

MaaS360 Mobile Document Editor verhindert Datenlecks, während Benutzer Dokumente erstellen, bearbeiten und speichern. Bei Bedarf können Benutzer Word-, Excel-, PowerPoint- und Textdateien unterwegs auf mobilen Geräten gemeinsam bearbeiten.

MaaS360 Mobile Document Sync erlaubt eine bequeme Synchronisierung von Inhalten auf allen verwalteten mobilen Geräten und somit eine nahtlose Erstellung und Bearbeitung von Dateien. Die IT-Abteilung kann Richtlinien für Inhalte durchsetzen, um das Kopieren und Einfügen einzuschränken sowie das Öffnen oder Freigeben von Daten in nicht verwalteten Anwendungen zu blockieren. Diese Kontrollen lassen sich auf alle Dokumente, eine Gruppe von Dokumenten oder einzelne Dokumente anwenden, damit Sie wertvolle Unternehmensdaten flexibel schützen können.

Für ein sicheres Content-Sharing finden sich in praktisch jedem Unternehmen vielfältige Einsatzmöglichkeiten – vom Vertrieb und Marketing über den operativen Betrieb bis hin zu den Finanzen:

- Zeigen Sie letzte Änderungen an einer Verkaufspräsentation an und geben Sie sie frei – direkt vor dem jeweiligen Kundengespräch
- Arbeiten Sie gemeinsam an den neuesten Finanzkennzahlen in einer Tabelle, bevor Sie in ein Flugzeug steigen
- Erörtern Sie Marketingbotschaften und leiten Sie sie an Kollegen weiter, während Sie im Café sitzen
- Verteilen Sie quartalsbezogene Finanzdokumente an den Aufsichtsrat und wählen Sie als Ablaufdatum für die Dokumente das Ende der Sitzung aus
- Teilen Sie Produktmaterialien in nahezu Echtzeit mit Vertriebsteams, damit diese nicht nach aktuellen Datenblättern oder Konkurrenzinformationen suchen müssen
- Stellen Sie sicher, dass Tablets in Einzelhandelsgeschäften über die neuesten Informationen zu Produkten und Lagerbestand verfügen

IBM® MaaS360® Gateway Suite

Die MaaS360 Gateway Suite ist eine Komponente, mit der all das möglich wird. Die Suite schützt aktive Daten durch nahtlosen und geschützten Zugriff von Mobilgeräten auf Inhalte und Intranet Ihres Unternehmens:

- Bieten Sie einfachen und sicheren mobilen Zugang zu Daten – auch ohne ein geräteeigenes VPN. So müssen sich Benutzer nicht jedes Mal im VPN anmelden, wenn sie Informationen benötigen.
- Sorgen Sie für Mobilität von SharePoint, Windows-Dateifreigaben, Intranetsites und Webanwendungen.
- Schützen Sie Daten mit effektiven Sicherheitsrichtlinien und DLP-Kontrollen.
- Änderungen an Netzwerk- oder Firewall-Sicherheitseinstellungen sind nicht erforderlich.

Abbildung 4: Datenströme mit MaaS360 Gateway

Mithilfe von Richtlinien können Sie Interaktionen der MaaS360 Productivity Suite mit Geräten Ihrer Benutzer genau konfigurieren. Beispielsweise können Sie URLs zu unternehmenseigenen Wikis, Bug-Tracking-Systemen usw. oder Unternehmensordnern festlegen, die sich über das MaaS360 Gateway aufrufen lassen und als Lesezeichen im MaaS360 Secure Mobile Browser erscheinen. Außerdem können Sie entscheiden, ob für Zugriff auf diese Speicherorte eine Authentifizierung erforderlich sein soll.

Das MaaS360 Gateway bestimmt darüber, welche Unternehmensressourcen angezeigt werden, wenn Benutzer auf den Datencontainer ihres Geräts zugreifen.

Kostenlose Testversion

MaaS360 lässt sich schnell und bequem testen – außerdem ist die Zeit, die Sie in die Anpassung von MaaS360 an Ihre Bedürfnisse investieren, lohnend angelegt. Wenn sich Ihr Unternehmen für MaaS360 entscheidet, wird Ihre Testumgebung automatisch zur Produktionsumgebung!

Sollten Sie sich für eine kostenlose Testversion von MaaS360 interessieren, klicken Sie hier. Legen Sie sofort los – die Einrichtung ist unkompliziert, Änderungen an der Infrastruktur sind nicht nötig. Testen Sie MaaS360 noch heute!

Abbildung 5: MaaS360 Produkte

Über IBM MaaS360

IBM MaaS360 ist eine Enterprise-Mobility-Management-Plattform, die bei mobilen Geschäften für hohe Produktivität und maximalen Datenschutz sorgt. Tausende von Unternehmen nutzen MaaS360 bereits als Grundlage für mobile Initiativen. MaaS360 ermöglicht eine umfassende Verwaltung mit zuverlässigen Sicherheitskontrollen für alle Benutzer, Geräte, Apps und Inhalte und unterstützt die Entwicklung einer optimalen mobilen Strategie. Wenn Sie weitere Informationen erhalten und IBM MaaS360 30 Tage lang kostenlos testen möchten, besuchen Sie www.ibm.com/maas360

Über IBM Security

Die Sicherheitsplattform von IBM stellt Sicherheitsinformationen bereit, damit Unternehmen ihre Mitarbeiter und Kunden, Daten, Anwendungen und Infrastruktur umfassend schützen können. Wir bieten Lösungen für Identitäts- und Zugriffsmanagement, Sicherheitsdaten- und Vorfallmanagement, Datenbanksicherheit, Anwendungsentwicklung, Risikomanagement, Endpunktmanagement, Intrusion Protection der nächsten Generation und vieles mehr an. IBM verfügt über eines der größten Forschungs-, Entwicklungs- und Bereitstellungsteams für Sicherheitslösungen weltweit. Weitere Informationen hierzu finden Sie im Internet unter www.ibm.com/security

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Hergestellt in den Vereinigten Staaten von Amerika,
März 2016

WGW03111-DEDE-01