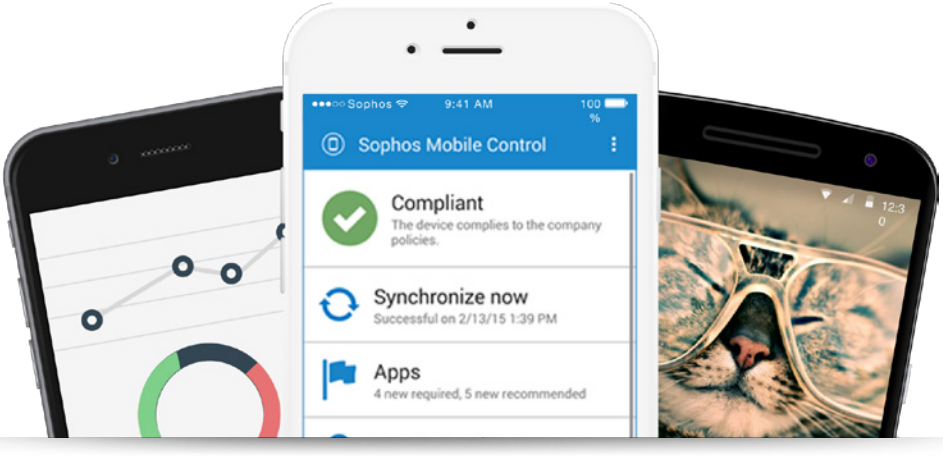
SOPHOS
Security made simple.



Container-Lösungen einfach nutzen – mit Sophos Mobile Control

Smartphones und Tablets sind aus dem Unternehmensalltag nicht mehr wegzudenken. Zum flexiblen Arbeiten werden immer mehr private (Bring Your Own Device, BYOD) oder vom Unternehmen ausgegebene Geräte (Choose Your Own Device, CYOD) genutzt. Als Folge befinden sich auf den mobilen Geräten meist sowohl geschäftliche als auch private Daten. Unternehmen benötigen hier einen pragmatischen Ansatz: Die geschäftlichen Daten müssen sicher sein, gleichzeitig muss die Privatsphäre der Nutzer gewahrt bleiben.

Die Vorteile von Container-Lösungen

Mit Containern lassen sich Unternehmensdaten auf mobilen Geräten ganz einfach schützen – egal, wem das betreffende Gerät gehört. Container-Lösungen erstellen auf Smartphones und Tablets abgetrennte, sichere Bereiche, in denen die Nutzer auf Unternehmensdaten zugreifen können. Container sind passwortgeschützt und verschlüsselt. So schützen und isolieren sie Daten vor unbefugten Zugriffen, Malware, anderen Anwendungen und Systemressourcen. Außerdem ermöglichen Container den Nutzern, auf dem Gerät ihrer Wahl zu arbeiten, und geben der IT gleichzeitig die Kontrolle über Daten, die von Rechts wegen in ihren Zuständigkeitsbereich fallen.

Container ermöglichen nicht nur einen sicheren Zugriff auf Unternehmensdaten, sondern vereinfachen auch den Schutz und die Verwaltung mobiler Geräte. Die IT hat die volle Kontrolle über den Container, kann Unternehmensdaten löschen und Richtlinien erstellen, die steuern, wann und wo Benutzer auf Unternehmensressourcen zugreifen dürfen. Mit dem Container lassen sich auch verschiedene Geräteplattform-Varianten standardisieren. Auf diese Weise kann der hohe Verwaltungsaufwand reduziert werden, der durch die starke Plattform-Fragmentierung entsteht – besonders bei Android, wo jeder Hersteller seine eigene angepasste Variante anbietet.

Worauf Sie bei der Wahl einer Container-Lösung für mobile Geräte achten sollten

Mitarbeiter nutzen Smartphones und Tablets, um flexibel und produktiv arbeiten zu können. Eine Mobile-Security-Lösung sollte sie dabei nicht beeinträchtigen. Achten Sie bei der Wahl einer Container-Lösung deshalb darauf, dass diese sich einfach bedienen und verwalten lässt.

Ermitteln Sie, wie viele unterschiedliche Betriebssysteme Sie derzeit unterstützen, und beachten Sie Folgendes:

- Ist es schwierig festzustellen, welche Betriebssytemsversion auf einem Gerät ausgeführt wird?
- Haben Sie mit Telekommunikationsunternehmen zu tun, die auf der aktuellen Betriebssystemsversion nicht die neuesten Sicherheitsfunktionen unterstützen?

Lautet Ihre Antwort auf eine dieser Fragen „Ja“, sollten Sie nach einer Container-Lösung suchen, die alle in Ihrem Unternehmen genutzten Betriebssysteme und Betriebssystemsversionen unterstützt. Nicht nur zwischen den drei führenden Betriebssystemen iOS, Windows und Android gibt es gravierende Unterschiede im Hinblick auf Funktionalität, Verwaltung und Sicherheit. Auch die Fragmentierung des Android-Markts macht IT-Organisationen zu schaffen. Denn die verschiedenen Betriebssystem-Varianten müssen einzeln konfiguriert werden. Die von Ihnen gewählte Container-Lösung sollte Datenzugriffskontrollen (z. B. für E-Mails) standardisieren, damit Sie Geräte nicht einzeln konfigurieren und kein Android-Experte werden müssen.

Neben E-Mail-Containern können Inhaltscontainer die unternehmensübergreifende Zusammenarbeit verbessern. Die meisten Unternehmen möchten einen sicheren Zugang zu E-Mails, Kalendern und Kontakten gewähren. Dies ist mit einem Personal Information Management (PIM) Container möglich.

ERMITTELN SIE ZUNÄCHST, WIE VIELE BETRIEBSSYSTEME SIE DERZEIT UNTERSTÜTZEN

ÜBERLEGEN SIE, WELCHE DATEITYPEN, DATEIEN UND DOKUMENTE SIE BENUTZERN ZUR VERFÜGUNG STELLEN MÖCHTEN

Sie können auch eine sichere Arbeitsumgebung bereitstellen, in der Benutzer Dokumente abrufen, gemeinsam bearbeiten und austauschen können. Diese Methode bietet sich an, wenn Mitarbeiter Zugriff auf bestimmte Geschäftanwendungen oder Daten-Repositorys auf Unternehmens-Websites benötigen.

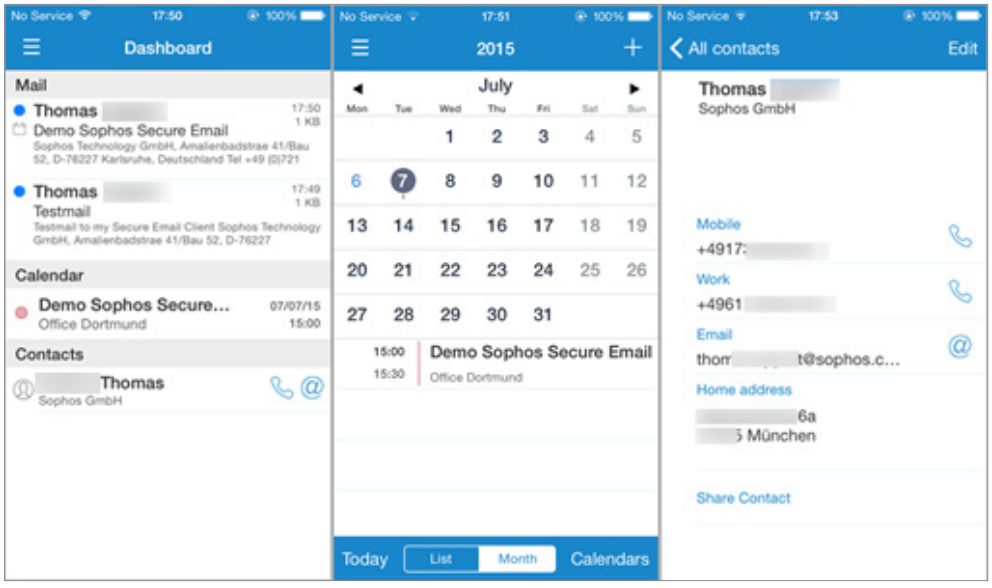
Sophos Mobile Control: Einfache Container, leistungsstarke Sicherheit

Sophos Mobile Control ist eine Enterprise Mobility Management (EMM) Lösung, die für verschiedene Bereitstellungsmodelle wie BYOD und CYOD geeignet ist. Sophos Mobile Control bietet einfache, sichere Container für mobile Geräte, die Unternehmensdaten schützen, ohne Benutzer bei der Arbeit zu behindern.

E-Mail-Container

Mit Sophos Secure Email können IT-Teams einfach sichere Unternehmens-E-Mails bereitstellen. Sophos Secure Email fungiert als sichere Container-Lösung für E-Mails, Kalender und Kontakte und trennt diese von anderen E-Mail-Anwendungen auf dem Gerät. E-Mails, Kontakte und Ereignisse werden über das Microsoft-Exchange-ActiveSync-Protokoll synchronisiert und alle Daten im Container zur Sicherheit verschlüsselt.

E-Mail-Container ermöglichen der IT, für verschiedenste iOS-, Android- und Windows-Mobile-Versionen einen gemeinsamen Standard-E-Mail-Zugang bereitzustellen und eine einfach verwaltbare Umgebung für Unternehmens-E-Mails einzurichten. Features und Einstellungen variieren zwischen den einzelnen Betriebssystemen leicht, um den jeweils unterschiedlichen Gerätefunktionen gerecht zu werden.



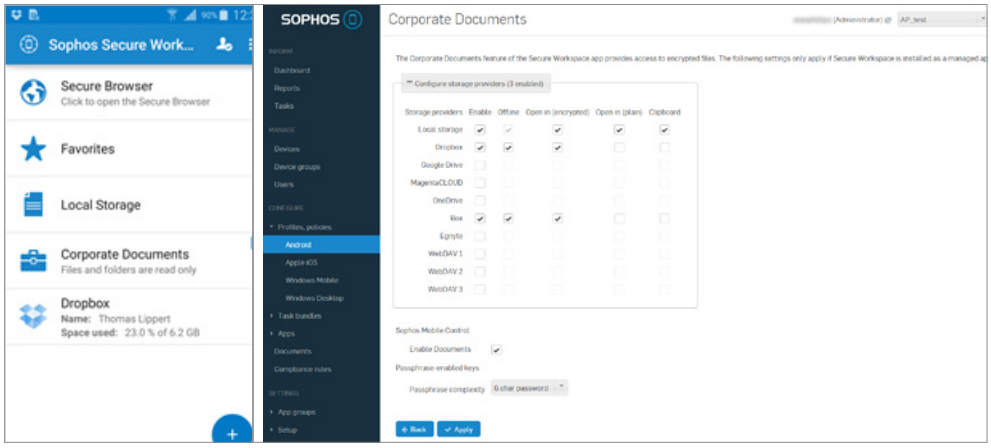
Benutzeroberfläche von Sophos Secure Email

Inhaltscontainer

Sophos Secure Workspace Sophos Secure Workspace ermöglicht Mitarbeitern, sicher und produktiv auf mobilen Geräten zu arbeiten. Sie können Dokumente sowohl intern als auch extern austauschen und gemeinsam bearbeiten. IT-Abteilungen können kontrollieren, wie Benutzer Dokumente ändern, austauschen und verteilen. Außerdem können sie vorgeben, welche Cloudspeicher-Anwendung genutzt werden darf.

Durch die Einbindung der Sophos SafeGuard Dateiverschlüsselung können verschlüsselte Dateien an den Inhaltscontainer gesendet und nur dann geöffnet werden, wenn das Gerät sich in einem sicheren Zustand befindet und der Benutzer seine Identität mit einem Passwort verifizieren kann. Die Verschlüsselung kann zudem überwacht und kontrolliert werden, sodass nur verschlüsselte Dateien auf Zusammenarbeits- und Speicher-Websites in der Cloud wie Box, Google Drive oder Unternehmens-WebDAV-Sites gespeichert werden dürfen.

EIN UNTERNEHMENS-BROWSER INNERHALB EINES INHALTSCONTAINERS GEWÄHRT EINEN SICHEREN BROWSING-ZUGRIFF OHNE ZUSÄTZLICHE PASSWÖRTER



Benutzer- und Administratoroberfläche von Sophos Secure Workspace

Unternehmensbrowser

Mit dem Sophos Corporate Browser kann die IT einen sicherer Browser-Zugriff auf häufig genutzte geschäftsrelevante Websites und interne Unternehmens-Websites bereitstellen. Der Browser vereinfacht den Single Sign-on für Intranet-Sites des Unternehmens. Der Browser wird als Teil des Containers behandelt und im Rahmen der Konfiguration kann die „save password"(sicheres Passwort)-Funktion auf Wunsch aktiviert oder deaktiviert werden, um das Risiko für wichtige Unternehmens-Websites zu minimieren. Auf diese Weise lässt sich auch die Datenmigration von einem internen Speicherort zu einer externen App verhindern (z. B. durch Unterbinden von Kopieren und Einfügen).

Einfache Bedienung

Sophos Mobile Control ist einfach zu bedienen – sowohl für die Mitarbeiter als auch die IT.

Für Mitarbeiter:

- Mitarbeiter können die E-Mail- und Inhaltscontainer einfach im App Store für ihr Betriebssystem herunterladen.
- Mit nur einem Anmeldevorgang erhalten die Benutzer Zugriff auf die Daten und Unternehmensressourcen in den Containern.

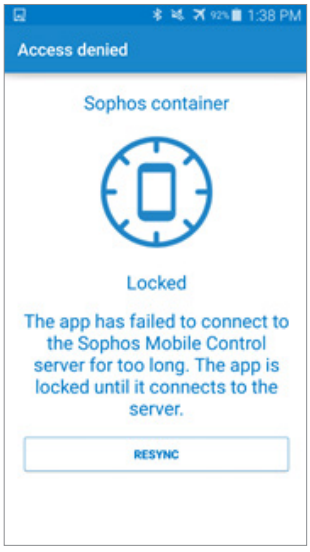
Für die IT:

- Über das einfache, intuitive Dashboard kann die IT die Container einfach bereitstellen und verwalten.
- Für Benutzer kann ein Self-Service-Portal eingerichtet werden, in dem einfache Helpdesk-Aufgaben wie die Registrierung und Außerbetriebsetzung von Geräten oder die Zurücksetzung von Passwörtern erledigt werden können.

Allumfassende Sicherheitskontrollen

Die Sophos-Container-Richtlinien geben dem Administrator die Kontrolle darüber, wie, wann und wo auf einen Container zugegriffen wird. Prüfungen beim Start stellen sicher, dass der Container kein kompromittiertes Gerät ist und sich in einem bestimmten geografischen Gebiet, Zeitfenster oder in einer bestimmten WLAN-Reichweite befindet. Auf diese Weise ist gewährleistet, dass nur ordnungsgemäß authentifizierte Benutzer, die innerhalb zulässiger Grenzen agieren, Zugriff auf sensible Unternehmensdaten erhalten.

Administrator-Oberfläche für allgemeine Sicherheitseinstellungen in Sophos Mobile Control



Beispiel der Benutzeroberfläche, wenn Sophos Mobile Control Sicherheitsanforderungen nicht erfüllt sind

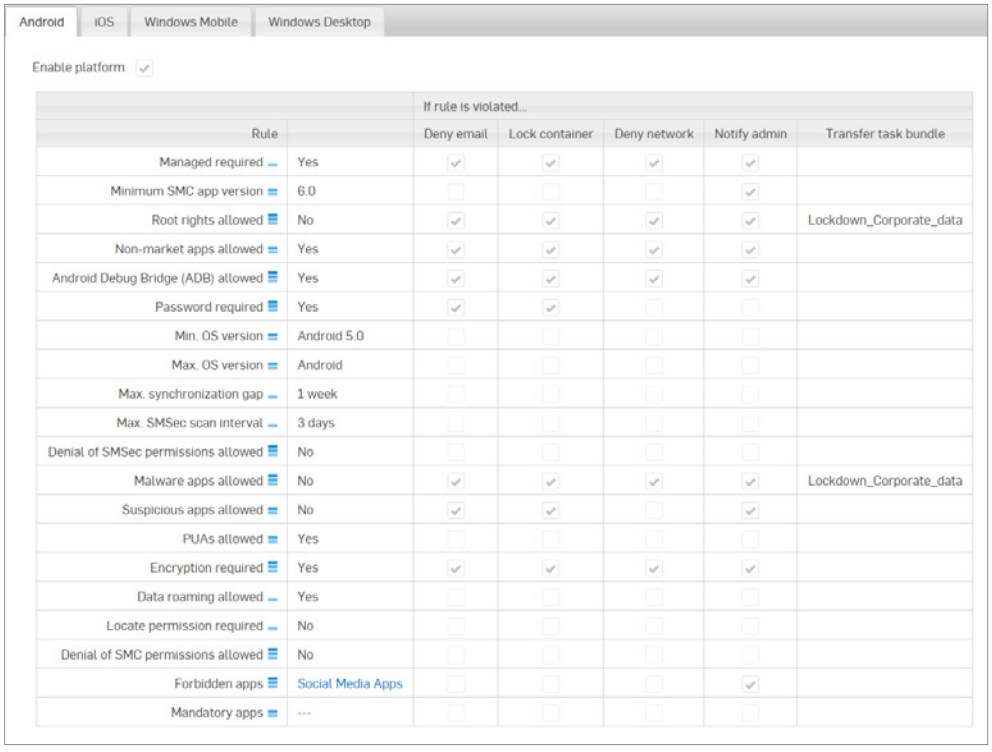
Container sind wichtig, aber kein Allheilmittel

Container sind nur ein Element innerhalb einer ganzheitlichen Mobile-Security-Strategie. Sie schützen Unternehmensdaten auf Geräten. Doch eine Reihe weiterer Kontrollen ist notwendig, um die Integrität des Geräts selbst zu wahren. Sophos Mobile Control ist eine umfassende Sicherheitslösung, die leistungsstarke EMM-Funktionen mit bewährter Sicherheitstechnologie kombiniert.

Compliance

Sophos Mobile Control setzt Compliance-Richtlinien der IT durch und stellt so sicher, dass jedes Gerät die Mindestsicherheitsstandards erfüllt, bevor es Zugang zum Container erhält. Die integrierte Netzwerkkontrolle beobachtet den Gerätestatus kontinuierlich und erkennt Jailbreaks, Anwendungen auf der Blacklist und unsichere Einstellungen.

Wird eine Sicherheitslücke erkannt, lässt sich Sophos Mobile Control so konfigurieren, dass automatisch die Administratoren benachrichtigt werden, das Gerät umkonfiguriert wird, der Zugriff auf die Container verweigert wird oder die Container komplett zurückgesetzt werden. Dadurch ist sichergestellt, dass Unternehmensdaten nicht aufgrund mangelnder Compliance kompromittiert werden.



Compliance-Einstellungen in Sophos Mobile Control

Malware-Schutz

Die marktbeherrschende Stellung von Android-Geräten und die Offenheit der Android-Plattform haben zu einem dramatischen Anstieg von Malware und potenziell unerwünschten Anwendungen (PUAs) geführt. Allein 2014 erkannten die SophosLabs über 1 Mio. neue Malware-Samples für mobile Geräte – Tendenz weiter steigend, weil Hacker sich zunehmend auf dieses „leichte Ziel" konzentrieren.

Sophos Mobile Control bietet prämierten Virenschutz für Android-Geräte, der auf der Sophos Antivirus Engine basiert und stetig mit minutenaktuellen Bedrohungsdaten aus den SophosLabs aktualisiert wird. Alle neu installierten Anwendungen auf Android-Geräten werden automatisch gescannt und infizierte Geräte in die Quarantäne verschoben.

Integration mit weiteren Sicherheitslösungen

Indem Sie dafür sorgen, dass Ihre IT-Sicherheit als System arbeitet, können Sie nicht nur Ihren Schutz erhöhen, sondern auch Ihre Produktivität steigern. Sophos Mobile Control lässt sich integrieren – sowohl in Sophos UTM, wo es Administratoren ermöglicht, den WLAN- und VPN-Zugriff für nicht richtlinienkonforme Geräte zu sperren, als auch in Sophos SafeGuard, wo es Benutzern ermöglicht, über ihre Mobiltelefone und Tablets auf verschlüsselte Daten zuzugreifen.

Fazit

Mit sicheren Containern für mobile Geräte erhalten IT-Organisationen die Kontrolle, die sie benötigen, um Unternehmensdaten auf Smartphones und Tablets zu schützen. Sophos Mobile Control ist eine leistungsstarke, benutzerfreundliche Lösung mit sicheren Containern für Unternehmens-E-Mails, -Kalender und -Kontakte, die eine sichere Zusammenarbeit auf mobilen Geräten ermöglicht. Zusammen mit unübertroffenen Schutzfunktionen und Sicherheitskontrollen erhalten Unternehmen umfassende Mobile Security, die sie effektiv bereitstellen und nutzen können.

Weitere Infos

und kostenlose Testversion unter
www.sophos.de/mobile

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

04.16/NP.wpde.simple

SOPHOS