
AirIT
AirITSystems

mediaTest
digital

Sichere Apps auf mobilen Firmengeräten

# Trusted App Directory (Whitelist/Blacklist)

# für Smartphones und Tablets

## Inhalt



**Für weitere Informationen sprechen Sie uns an:**

Markus Fischer

Tel.: 0511 977 4055
m.fischer@airitsystems.de

AirITSystems GmbH,
Benkendorffstraße 6
30855 Langenhagen

www.airitsystems.de

# Whiteplist/Blacklist: Trusted App Directory

## Die Herausforderung:

Schaffung einer sicheren App-Umgebung auf Ihren mobilen Geräten (Smartphones und Tablets) um sensible Unternehmens- und Personendaten zu schützen.

## Das Problem:

Apple und Google können und wollen keine ausreichenden Sicherheitskontrollen gewährleisten, bevor Sie eine App zum Download bereitstellen. Knapp die Hälfte aller Apps bestehen die von mediaTest digital durchgeführten Sicherheits-Audits nicht.

## Die Risiken unsicherer Apps:

- Unerlaubte Zugriffe auf sensible Firmen-, Zahlungs-, Kalender-, und Kontaktdaten
- Diebstahl und Missbrauch sensibler Korrespondenz
- Erstellung von Bewegungsprofilen
- Zugriff auf Daten aus WLAN-Netzen

## Die Lösung:

Das Trusted App Directory (White- und Blacklist) stellt die nötigen Informationen zur Verfügung, um mobile Geräte frei von unsicheren Apps zu halten:

- Sofortiger Zugriff auf detaillierte Sicherheitsinformationen von 300 Apps - 150 iOS & 150 Android Anwendungen (siehe FAQ für Details)
- Stetig wachsende Datenbank
- Rollierende Aktualisierung der Sicherheitsinformationen (siehe FAQ für Details)
- Einfaches Hinzufügen von Wunsch-Apps

- Optional: Einbindung der Datenbank in ein bestehendes Mobile Device Management System (siehe FAQ für Details)

- Optional: vorheriger Abgleich des bestehenden App-Inventars mit der mTd-Datenbank

## Ihre Vorteile:

- Optimierung des internen App-Auditings und Schonung interner Ressourcen
- Sofortige Absicherung aller Smartphones (auch Bring Your Own Device!)
- Schutz vor
  - unerlaubtem Zugriff auf sensible Firmen-, Zahlungs-, Kalender-, und Kontaktdaten
  - Zugriff auf sämtliche Daten aus W-LAN-Netzen
  - Diebstahl und Missbrauch sensibler Korrespondenz und Daten
- Eindämmung des App-Wildwuchses
- Sensibilisierung der Belegschaft und Minimierung des Haftungsrisikos für Mitarbeiter und IT

# Whiteplist/Blacklist: Trusted App Directory

## Frequently Asked Questions:

### 1. Warum wird ein Trusted App Directory (TAD) benötigt?

Apple und Google stellen zusammen etwa 1.600.000 Apps zum Download bereit. Eine Vielzahl der Anwendungen weisen Sicherheitslücken auf oder spionieren Daten aus. Die Sicherheitsaudits von mediaTest digital zeigen: Apple und Google können und wollen keine ausreichenden Sicherheitskontrollen gewährleisten. Etwa 50% der Apps bestehen die Audits von mediaTest digital (mTd) nicht weil Sie zum Beispiel Daten unverschlüsselt versenden, Nutzerdaten an nicht bestätigte Empfänger übertragen, oder Gerätenummern und Standorte übertragen. Die Nutzung von Apps birgt damit ein erhebliches Risiko, sensible Daten zu verlieren.

### 2. Welche Apps sind im Trusted App Directory enthalten?

mediaTest digital wählt für seine Datenbank die populärsten und relevantesten Apps aus den Bereichen Business und Freizeit. Die Datenbank deckt erfahrungsgemäß mehr als 80% der in Unternehmen am häufigsten verwendeten Apps ab. Standardmäßig beinhaltet das Trusted App Directory etwa 80% Business- und 20% Freizeit-Apps. Natürlich können Sie auch Apps zur Aufnahme in die Datenbank bei mTd einreichen. Gegenstand des Testings und damit Teil der Datenbank sind zum Beispiel folgende (sichere und unsichere) Apps aus den Kategorien:

- Reise- und Reiseplanung:
  DB-Navigator, Expedia , Sixt Mietwagen, stau mobil, Google Maps, u.v.m
- Nachrichten:
  Spiegel Online, wetter.de, Sportschau, CNN, heise, Bild, u.v.m ;
- Kommunikation:
  What's App, Skype, Facebook, Xing, u.v.m.;
- Dokumente:
  Dropbox, DocumentsToGo, Microsoft OneNote, Office Plus, u.v.m;
- Banking:
  Deutsche Bank, Visa, S-Banking, PayPal, u.v.m;
- Freizeit/Unterhaltung:
  YouTube, ZDF Mediathek, Skyscanner, Spotify, u.v.m;
- Produktivität:
  AnyList, iTranslate, barcoo, web.de, u.v.m.

### 3. Was passiert, wenn ein Update einer App erscheint?

mediaTest digital erhält automatisch eine Meldung aus den App-Stores, sobald eine neue Version einer App verfügbar ist. Dieses Ereignis stößt den Re-Test-Prozess einer App an, der dazu führt, dass eine App spätestens einmal pro Quartal neu geprüft wird. Ändert sich der Sicherheitsstatus einer App, wird das TAD aktualisiert und der verantwortliche Mitarbeiter in Ihrem Unternehmen per Email darüber informiert.

### 4. Wie kann ich das TAD in ein bestehendes Mobile Device Management System integrieren?

Die Datenbank kann über eine Schnittstelle, die durch mTd bereitgestellt wird, mit dem MDM-System gekoppelt werden. So fließen die aktuellsten Sicherheitsinformationen automatisch in das MDM-System ein.

# Whiteplist/Blacklist: Trusted App Directory

## Frequently Asked Questions:

### 5. Wie kann das Trusted App Directory genutzt werden, wenn die mobilen Geräte noch nicht systematisch und IT gestützt verwaltet werden?

Über das mTd-Webinterface kann sofort auf die Informationen in der Datenbank zugegriffen werden. Diese Informationen können allen Benutzern von Smartphones und Tablets an die Hand gegeben werden, um den Mitarbeitern, der IT und der Geschäftsführung von Beginn an zu mehr Sicherheit und Sensibilität im Umgang mit Apps zu verhelfen.

### 6. Welche Kriterien liegen einer sicheren App zugrunde?

- Gesetzliche Datenschutz- und Datensicherheitsrichtlinien
- BDSG-konforme Datenverarbeitung
- Verschlüsselte Übermittlung sensibler und vom Nutzer zuvor bestätigter Daten
- Sichere Datenspeicher auf dem Device
- Authentifizierte Empfänger der übermittelten Daten

### 7. Wie läuft ein App-Audit von mTd ab?

a. Überprüfung der verfügbaren App-Versionen und deren Aktualisierungen
b. Wenn vorhanden: Analyse des Quellcodes, ansonsten Dekompilation und Analyse
c. Protokollierung der angegebenen Zugriffsberechtigungen
d. Starten der Man-in-the-Middle-Umgebung zum Aufbrechen einer vorhandenen SSLVerschlüsselung
e. App-Test (virtualisiert oder auf physikalisch vorhandenem Testgerät):
   i. Überprüfung der AGB
   ii. Anwahl aller Menüpunkte der App
   iii. Anlegen von User-Accounts
   iv. Artikelkauf
   v. Senden von Dateien aus der App heraus
   vi. Empfangen und Speichern von Inhalten
   vii. Überprüfung der Zugriffsrechte während des Tests
f. Auswertung:
   i. Abgleich der entstandenen Zugriffsrechte mit den Angegebenen
   ii. Überprüfung der gesendeten Daten (was, wohin, wie)?
   iii. Überprüfung der übermittelten Daten innerhalb des Quellcodes
   iv. Ist der Versand oder die Erhebung der Daten notwendig für die Funktionalität der App? Wurde die Kommunikation verschlüsselt?
   v. Protokollierung der entstandenen Verbindungen (IP, Unternehmen, whois)
   vi. Auswertung der entstanden Verbindungen (an wen, was, berechtigt)?

### 8. Wie lange dauert es, bis auf die Datenbank zugegriffen werden kann?

Die Lieferung der Leistungen erfolgt innerhalb von maximal drei Werktagen.

### 9. Kann das Trusted App Directory individualisiert werden?

Sollten gewünschte Apps nicht in der Datenbank vorhanden sein, können diese jederzeit bei mTd zum Testen eingereicht werden. Dafür steht ein entsprechendes Formular im Webinterface bereit.

# Whiteplist/Blacklist: Trusted App Directory

## Frequently Asked Questions:

### 10. Ändert sich der Umfang des Trusted App Directory?

Ja, das TAD wächst kontinuierlich an und wird aus unterschiedlichen Kanälen bespeist:

a. Mit Apps, die mTd aus eigener Initiative testet
b. Mit Apps, die bei mTd zum Testen eingereicht werden
c. Mit Apps, die mTd mit dem Trusted App Siegel auszeichnet

### 11. Wozu brauche ich die mediaTest digital Produkte, wenn ich doch bereits ein MDM im Einsatz habe?

MDM-Systeme bieten in der Regel Container in denen White- und Blacklists verwaltet werden können, oder hauseigene Apps aufbewahrt werden können. Ein systematisches App-Auditing inklusive der Versions-Updates in den Stores findet nicht statt, weil der Aufwand selbst bei kleinsten App-Volumina extrem hoch ist; genau hier liegt die Spezialisierung und Expertise von mediaTest digital.

### 12. Welche Plattformen und Systeme unterstützt denn mediaTest digital?

Das App-Auditing ist für die Systeme iOS, Android, Windows Phone und Blackberry konzipiert. Derzeit liegt der Fokus im rollierenden Testing auf iOS und Android. Es werden alle gängigen MDM-Systeme unterstützt. Konkrete Kooperationen, bei denen bereits eine Implementierung vorhanden ist, zeigt Ihnen das Team von mTd gern auf.

### 13. Was ist mediaTest digital?

mediaTest digital ist spezialisiert auf Sicherheits- und Qualitätsaudits von Anwendungen (Apps) für mobile Geräte. mTd unterstützt Entwickler und Anbieter von Apps bei der Optimierung Ihrer Produkte und bietet Unternehmen Sicherheitslösungen für den Schutz von sensiblen Unternehmens- und Personendaten. Das Trusted App Directory (White- und Blacklist) stellt die nötigen Informationen zur Verfügung, um mobile Geräte frei von unsicheren Apps zu halten.