

# App Directory | Whitelist/Blacklist

## Trusted Enterprise Appstore

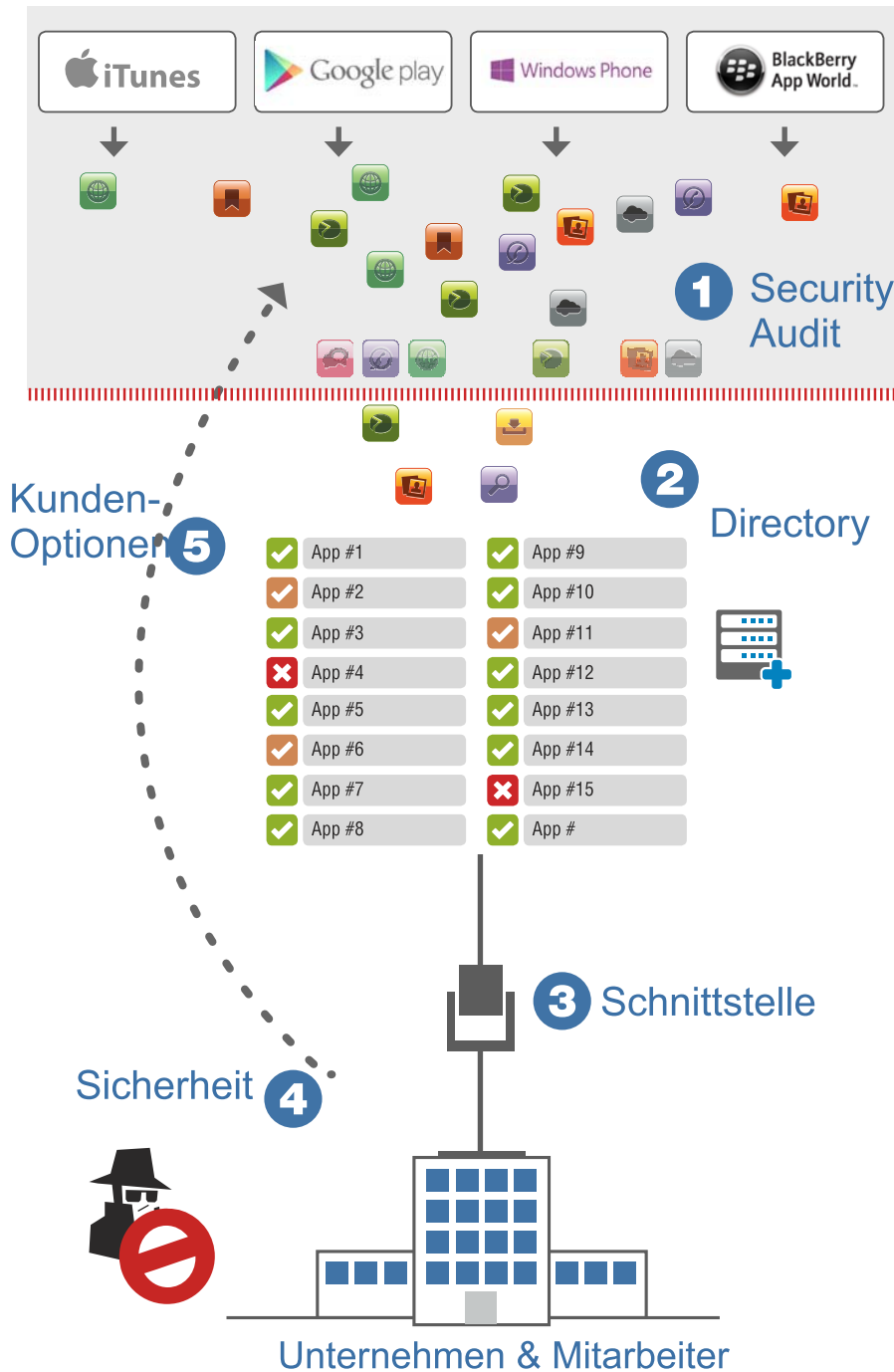
**1** Standardisierter und teilautomatisierter Qualitäts- und Sicherheits-Audit. Kriterien: Datenschutz- und Datensicherheitsrichtlinien, rechtliche Prüfung der BDSG-Konformität (Haftung!), Verschlüsselte Übermittlung sensibler Daten, Sichere Datenspeicherung auf dem Device, Authentifizierte Empfänger von übermittelten Daten. Updates werden regelmäßig neu überprüft und automatisch in das Trusted App Directory eingepflegt oder ggf. als sicherheitskritisch an Sie eskaliert.

**2** Sie greifen hier auf eine stetig wachsende Whitelist mit sicheren Applikationen zurück; derzeit ca. 300 ausgewählte und geprüfte Apps für den Unternehmensgebrauch.

**3** Auf Wunsch mehr (siehe 5.) Individuell angepasste Schnittstelle  
 A) Entweder als rollierender Export in Ihr Mobile Device Management (bspw. CSV-Format), B) zur automatischen Zustellung in Ihre IT-/Sicherheitsabteilung oder C) für den manuellen Zugriff per Login auf unsere Datenbank.

**4** Sichert Ihr Unternehmen und die Mitarbeiter u.a. vor unerlaubtem Zugriff auf sensible Firmen-, Zahlungs-, Kalender- und Kontaktdaten, sichert Sie vor möglicher Ortung bzw. Auswertung von standortbezogenen Daten, vor Zugriff auf sämtliche Daten aus WLAN-Netzen oder vor Diebstahl und Missbrauch von sensibler Korrespondenz.

**5** Sie verfügen auf Wunsch über individuelle Filterfunktionen, d.h. Sie selbst können bestimmen, welche Sicherheitskriterien auf die getesteten Apps angewandt werden. Standardmäßig sind hier maximale Sicherheitsbarrieren voreingestellt. Sie verfügen außerdem über ein App-Anfrage-System, bei dem unser Auditierungs-Team über weitere, zu testende Applikationen informiert wird, die nach dem Test sofort in die White-/Blacklist eingepflegt werden.



Für weitere Informationen sprechen Sie uns an: **Markus Fischer**  
 Tel.: 0511 977 -4055, [m.fischer@airitsystems.de](mailto:m.fischer@airitsystems.de)  
[www.airitsystems.de](http://www.airitsystems.de)