SAMSUNG

Wie Unternehmen von Samsung Knox profitieren

Die Angriffsfläche wächst: Kriminelle Betriebsspione, Saboteure oder Cybererpresser nutzen die gewachsene Mobilität in der IT für ihre Ziele aus. Samsung Knox hält mit Sicherheit und Effizienz bei viel Freiheit dagegen.

Inhaltsverzeichnis

Wie Unternehmen von Samsung Knox profitieren

IT findet sich ebenso an Bord eines 40-Tonners wie in der Kitteltasche einer Pflegekraft, im Kampfanzug eines Soldaten oder in den Händen von Lageristen. In mobilen und heterogenen IT-Infrastrukturen fällt es Cyberkriminellen leicht, Schwachstellen zu finden. Doch nicht nur von diesen gehen Risiken aus: Entwickler von Schadprogrammen verbreiten diese oft ungezielt, was die Schäden ihrer Zufallsopfer vergrößert. Und selbst wenn keinerlei böse Absicht im Spiel ist, führen menschliche Fehler mitunter zu Datenverlusten oder zur Preisgabe vertraulicher Informationen.

Andererseits hat die mobile Revolution zu einem gewaltigen Zuwachs an Produktivität und Effizienz geführt. Es grenzt an Selbstsabotage, den Mitarbeitern die Smartphones wegzunehmen. Die einzige sinnvolle Lösung: Mit der Angriffsfläche müssen Unternehmen auch ihre Verteidigungsfähigkeit vergrößern.

Wie Samsung Knox die Sicherheit von innen schützt

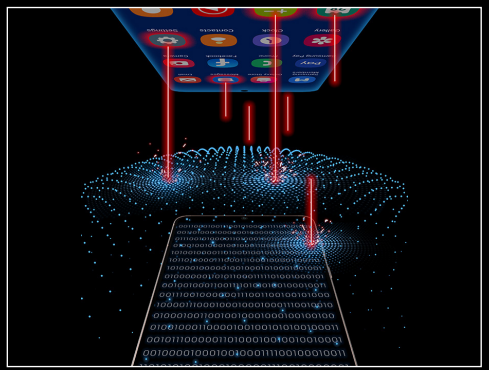
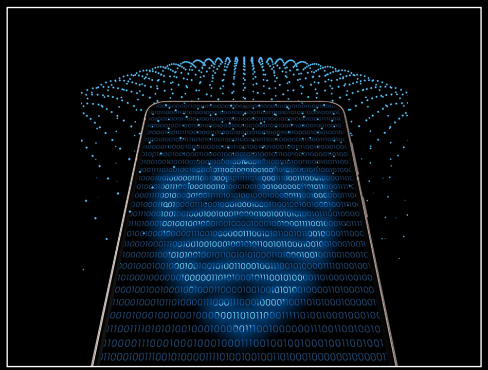
Mit der Security-Plattform Samsung Knox schützen Unternehmen die mobilen Endpunkte ihrer IT wirksam auf allen Ebenen. Auch in heterogenen Umgebungen kann die Sicherheit steigen. Um allerdings einen Schutz auf allen Ebenen (auch in puncto Hardware) zu ermöglichen, können die entsprechend ausgestatteten Galaxy Smartphones und Tablets eine entscheidende Rolle spielen. Die darin hard- und software-

seitig verbauten Sicherheitssysteme reichen bis hin zur faktischen Unbenutzbarkeit sensibler Daten, wenn das Gerät den Versuch einer physischen Manipulation entdeckt. Konkret setzt Samsung das dadurch um, dass beim Versuch einer physischen Manipulation ein eFUSE-Chip durchbrennt. Das Gerät bleibt danach benutzbar, aber sobald der eFUSE-Chip durchgebrannt ist, können die mit einer 256-Bit-AES-Verschlüsselung gesicherten Daten im KNOX-Modus nicht mehr erreicht werden. Die Entschlüsselung über das Gerät ist nicht mehr möglich. Auch wenn es Industriespionen gelingen sollte, ein so geschütztes Gerät zu stehlen, bleiben die Daten sicher.

Ein wichtiges Feature beim Einsatz der Hardware ist, dass nahezu die komplette Lieferkette aus einer Hand stammt – der Hersteller hat die Komponenten aufeinander abgestimmt. Da sich fast der gesamte Produktionslebenszyklus in den Händen von Samsung befindet, kann das Unternehmen die Kontrolle über die Prozesse behalten. Gut angesichts der Tatsache, dass Angriffe aus der Lieferkette seit Jahren zu den häufigsten und erfolgreichsten Cyberattacken gehören.

Worum es sich bei Samsung Knox genau handelt

Die Sicherheitslösung richtet sich in erster Linie an Firmen und Organisationen, die ihre Mobilgeräte in sicherheitskritischen Umgebungen einsetzen, wovon letztendlich aber jeder Galaxy Nutzer profitiert, denn die Samsung-Knox-Plattform ist bei allen Galaxy Smartphones und Tablets ab Werk integriert. Sie bietet IT-Administratoren und Geschäftskunden granulare Schnittstellen für die Verwaltung und Sicherheit von mobilen Endgeräten, die über Android Enterprise hinausgehen. Die Sicherheitslösung kann sensible Daten schützen und ermöglicht die Einhaltung von unternehmensinternen Datenschutzrichtlinien. Bei Samsung Knox handelt es sich nicht um ein einzelnes Produkt oder Leistungsmerkmal, sondern um ein Portfolio an Lösungen, das die Verwaltung und Absicherung mobiler Geräte vereinfachen soll. Das Paket kann unter anderem sicherstellen, dass Angestellten ein sicherer Fernzugriff auf Anwendungen und Dokumente gelingt.

Ein oft übersehenes, aber hoch einzuschätzendes Leistungsmerkmal von Samsung Knox ist die einfache Handhabung. Zwar sind Administratoren daran gewöhnt, mit komplexen Systemen zu arbeiten, dennoch stellt jeder unnötige Konfigurationsaufwand eine Fehlerquelle dar. Samsung Knox reduziert den Aufwand für administrative Arbeiten und kann allein dadurch die Sicherheit erhöhen. Eine der Hauptfunktionen ist der sichere Speicherbereich, in dem sensible Informationen (Passwörter, Kreditkartendaten und persönliche Dateien) sicher lagern. Dieser Bereich ist durch eine starke Verschlüsselung geschützt.

Darüber hinaus bietet die Lösung Funktionen zur Überwachung und Verwaltung von Geräten. Administratoren können darüber die Sicherheitseinstellungen der Geräte ihrer Mitarbeiter und Mitarbeiterinnen zentral verwalten. So stellen sie sicher, dass sie auf dem aktuellen Stand sind und der Unternehmens-Policy entsprechen.

Wie der Schutz entsteht

Samsungs „Root Of Trust" bildet das Fundament des Sicherheitsprotokolls. Dabei handelt es sich um eine Reihe strenger Kontrollmechanismen, die auf der Hardware- und nicht auf der Software-Ebene ansetzen. Das kann die Sicherheit der Geräte erhöhen, da sich Hardware nicht so leicht verändern lässt wie Software – und somit schwieriger anzugreifen ist:

Die Sicherheit der Knox-Plattform beginnt bereits beim Herstellungsprozess, noch bevor die Benutzer ihr Gerät einschalten. Dabei wird für ein Gerät ein einzigartiger Hardware-Schlüssel (DUHK) mithilfe des Hardware-Zufallszahlengenerators generiert.

Anschließend erzeugt und verschlüsselt der DUHK den Geräte-Root-Schlüssel (DRK) und Samsungs Attestation-Schlüssel (SAK).

Beim Start des Geräts kommt der Samsung-Secure-Boot-Schlüssel (SSBK) zum Einsatz, um alle Software-Komponenten zu überprüfen. Eine dieser Komponenten ist die TrustZone, ein für sichere Codes und Daten reservierter Bereich. Nur privilegierte Software-Module, die innerhalb der TrustZone ausgeführt werden, dürfen auf diese Schlüssel zugreifen.

Die Software überprüft die Knox-Plattform-Features vor der Ausführung. Da diese Kette von Sicherheitsprüfungen mit der allerersten Hardware-Prüfung beginnt, genießen die Features durch die auf Hardware basierende „Root of Trust" Schutz. Egal auf welches Glied in der Kette ein Angreifer zielt: Eine der Sicherheitsprüfungen kann den Angriff erkennen.

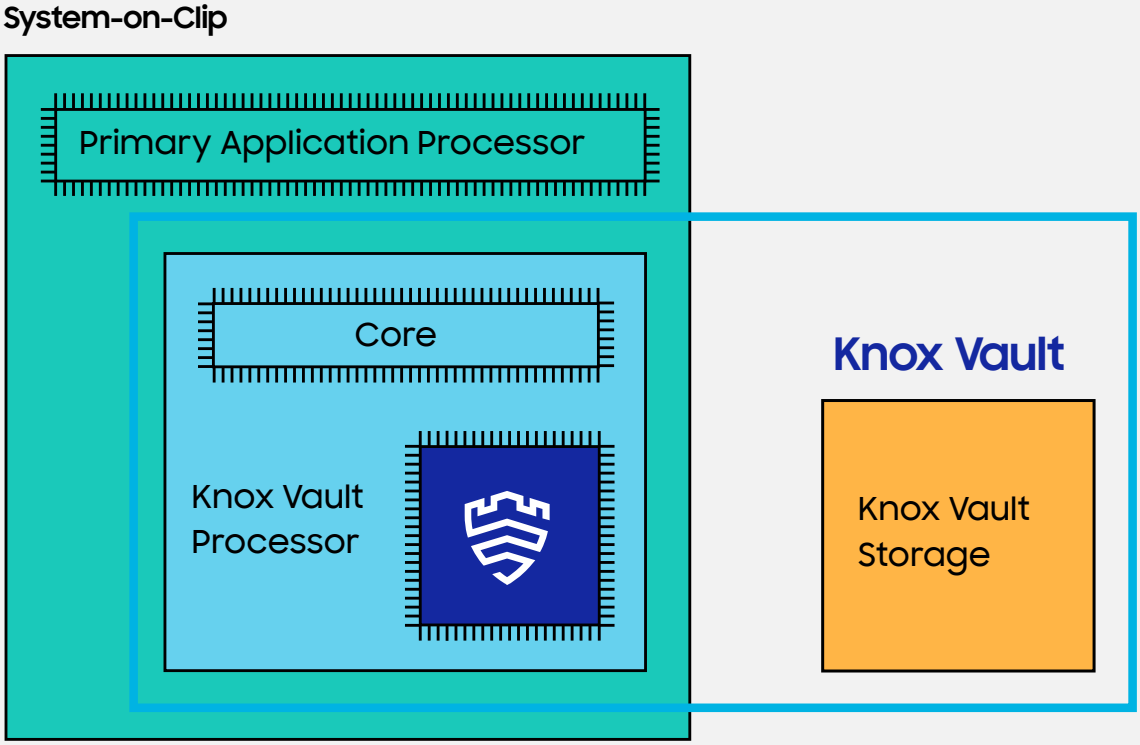
Was Knox Vault und Real-time Kernel Protection bringen

Knox Vault erweitert den Schutz, den die TrustZone bietet. Während die TrustZone ein anderes Betriebssystem neben Android auf dem Hauptanwendungsprozessor ausführt, arbeitet Knox Vault unabhängig vom Hauptprozessor, auf dem das Android-Betriebssystem läuft.

Als Kernkomponente der Knox-Sicherheitsplattform bildet Knox Vault ein isoliertes, nahezu manipulationssicheres, nicht kompromittierbares Subsystem mit eigenem Prozessor und Speicher sowie eine Schnittstelle zu einem dedizierten, nicht flüchtigen und sicheren Speicher. Knox Vault kann:

- sensible Daten wie hardwaregesicherte Android-Keystore-Schlüssel, den Samsung-Attestation-Schlüssel (SAK), biometrische Daten und Blockchain-Zugangsdaten speichern.

- einen sicherheitskritischen Code ausführen, der Benutzer mit zunehmenden Zeitabständen zwischen Fehlern authentifiziert und den Zugriff auf Schlüssel steuert - je nach Authentifizierung.



Quelle: Knox Vault, https://docs.samsungknox.com/admin/whitepaper/kpe/knox-vault.htm

Ein weiteres Sicherheitsmerkmal der Knox-Plattform ist die Real-time Kernel Protection (RKP). Um den Kernel zu schützen, überwacht Samsung Knox diesen in einer isolierten Ausführungsumgebung. Je nach Gerätemodell kümmert sich entweder

ein dedizierter Hypervisor oder die hardwaregestützte Secure World um die isolierte Ausführungsumgebung, die durch TrustZone-Technologie bereitgestellt wird.

Die Schutzmaßnahmen der Real-time Kernel Protection bestehen aus drei Bereichen:

- Kernel-Code – RKP kann die Modifikation von Kernel-Code und -Logik verhindern.
- Kernel-Daten – RKP wendet die Modifikation kritischer Kernel-Datenstrukturen ab.
- Kernel-Kontrollfluss – RKP torpediert Return-Oriented-Programming- und Jump-Oriented-Programming-Angriffe.

Für Unternehmen bedeuten diese Sicherheitsmerkmale zweierlei:

1. Ist ein Gerät auf irgendeinem Weg kompromittiert worden, fällt es augenblicklich für geschäftskritische Anwendungen aus. Dritte können die sensiblen, auf dem Gerät gespeicherten Daten nicht mehr verwenden, sie sind also vor unbefugtem Zugriff sicher.

2. Bei einem komplett nutzbaren Gerät befinden sich Kernel, Bootloader und Systemdateien in einem guten Zustand. Die Daten können ebenfalls sicher bleiben.

Welche Freiheiten die Beschäftigten haben können

Unternehmen, die ihren Mitarbeitenden Smartphones zur Verfügung stellen, stehen vor einer schwierigen Entscheidung: Sie können die Installation von Apps zur privaten Nutzung untersagen, eine eingeschränkte Auswahl privater Apps zulassen oder ihren Beschäftigten freie Hand lassen. Samsung Knox bietet Möglichkeiten für alle drei Szenarien.

Auch im großzügigen Fall gefährdet die Anwesenheit privat genutzter Apps nicht die Sicherheit der Firmendaten, da Samsung Knox Androids „Work Profile" nutzt, um die privaten und geschäftlichen Apps samt der zugehörigen Daten in getrennten Containern aufzubewahren. Das kann zudem sicherstellen, dass das Unternehmen keinen Zugriff auf die persönlichen Daten der Beschäftigten erhält.

Wie Samsungs Knox-Ökosystem funktioniert: sichern, bereitstellen, verwalten, analysieren

Wie eingangs erwähnt, umfasst das Knox-Ökosystem mehr als die ab Werk auf Sicherheit optimierten Mobilgeräte. Mit dem System lassen sich auch unterschiedliche Prozesse beim Einsatz von Mobilgeräten im Unternehmensumfeld abdecken – von der automatisierten Ersteinrichtung über die Durchsetzung geltender Sicherheitsrichtlinien bis hin zum Update-Management. Die breit aufgestellte Lösung bietet eine einfache Lizenzverwaltung und nahtlose Nutzung über eine einheitliche, intuitiv bedienbare Konsole. Eine separate Anmeldung entfällt dabei.

In der Knox-Suite bündelt Samsung mehrere Einzellösungen. Dazu gehören:

Bereitstellen

Knox Mobile Enrollment:

Knox Mobile Enrollment ermöglicht die einfache und automatisierte Registrierung von mobilen Geräten in Firmennetzwerken. Geschäftskunden profitieren von effizienter Geräteverwaltung, reduziertem Zeitaufwand bei der Einrichtung und sicherem Zugriff auf Unternehmensressourcen.

Verwalten

Knox Manage:

Knox Manage ist eine Lösung für die Betreuung von mobilen Geräten in Firmen. Unternehmen verwalten damit die Sicherheit, Konfiguration und Anwendungen ihrer Geräte zentral. Dadurch können sie von hoher Effizienz, Datensicherheit und starkem Schutz vor Bedrohungen profitieren. Über Knox Manage können Firmen das Equipment mit unterschiedlichen Betriebssystemen per Fernzugriff verwalten. Dazu gehören sämtliche Android-Geräte (ab Android 4.4) sowie andere Smartphones und Tablets mit den Betriebssystemen Windows (ab Win 10), iOS (ab iOS 8) sowie Chrome OS und Wear OS.

Knox E-FOTA One:

Bei Knox E-FOTA One handelt es sich um eine Firmware-Over-the-Air-Lösung für Unternehmen, mit der sie die Kontrolle über Geräte-Updates behalten können. Geschäftskunden planen, testen und verwalten damit Firmware-Updates zentral, was Kompatibilitätsprobleme vermeidet und die Geräteleistung anpasst. Die Folge: wenig Unterbrechungen, gute Geräteverwaltung und hohe Sicherheit.

Sichern

Knox Platform for Enterprise:

Knox Platform for Enterprise ist eine ganzheitliche Lösung für die sichere Verwaltung und den Schutz von Firmengeräten. Geschäftskunden erhalten Sicherheitsfunktionen wie Datenverschlüsselung, sicheren Zugriff auf Unternehmensressourcen und Richtlinienverwaltung. Knox Platform for Enterprise lässt sich in viele Enterprise-Mobility-Management-Produkte (EMM) direkt integrieren. Zu den kompatiblen Lösungen zählen VMware AirWatch, Blackberry, MobileIron, IBM, Citrix, SOTI und Knox Manage.

Analysieren

Knox Asset Intelligence:

Knox Asset Intelligence unterstützt Firmen dabei, den Zustand, die Nutzung und das Management ihrer IT-Geräte anzupassen. Durch die Erfassung und Analyse von Gerätedaten erhalten die Verantwortlichen wertvolle Einblicke, auf deren Basis sie fundierte Entscheidungen bei der Ressourcenverwaltung, Gerätewartung und Produktivitätssteigerung treffen können.

Unterstützen

Knox Remote Support:

Knox Remote Support ist eine Funktion von Samsung Knox, die es IT-Administratoren ermöglicht, mobilen Geräten aus der Ferne technischen Support anzubieten. So gelingt es, ohne physischen Zugriff Probleme zu lösen oder Updates direkt auf den Geräten zu installieren·

Samsung bündelt all diese Lösungen in einer Lizenz. Allerdings können Geschäftskunden auch gezielt einzelne Leistungen dieser Lösungen auswählen, je nach Bedarf.

Darüber hinaus gehören zum Knox-Ökosystem eine Reihe von Lösungen, die nur einzeln zu lizenzieren sind, zum Beispiel:

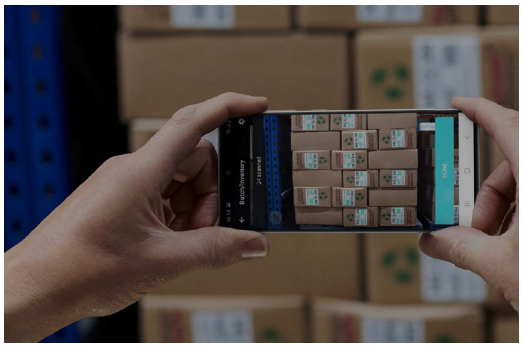
Knox Configure:

Bei Knox Configure handelt es sich um eine Software-Plattform, die Unternehmen bei der effizienten Verwaltung ihrer mobilen Geräte hilft. Mit Knox Configure können Geschäftskunden ihre Samsung-Geräte in großem Maßstab konfigurieren, personalisieren und sichern. Die Plattform ermöglicht eine einfache Gerätebereitstellung und -registrierung, die zentrale Verwaltung von Einstellungen, Anwendungen und Inhalten sowie die Durchsetzung von Sicherheitsrichtlinien. Anwender, die ein mit Knox Configure vorbereitetes Ersatzgerät erstmals einschalten, erleben eine positive Überraschung: Viele Apps, Inhalte und Widgets befinden sich bereits dort, wo sie es von ihrem vorherigen Gerät gewohnt sind. Und um den mitunter sperrigen Einrichtungsassistenten von Android müssen sie sich ebenfalls nicht kümmern.

Außerdem ermöglicht Knox Configure ein vielseitiges Branding der Geräte: Wenn Ihre Mitarbeiter und Mitarbeiterinnen Kunden und Kundinnen oder andere Kontakte besuchen, repräsentieren auch deren Geräte dann beeindruckend Ihr Unternehmen. Knox Configure macht die Anpassung des Start- und Sperrbildschirms mit eigenen Bildern möglich, auch das Ersetzen der Standardanimationen beim Ein- und Ausschalten des Geräts funktioniert. Die Corporate Identity von Unternehmen beschränkt sich damit nicht auf die Gestaltung des Briefpapiers.

Knox Capture:

Mit Knox Capture gelingt es, Scans in hoher Qualität direkt über das kompatible Smartphone durchzuführen, ohne Abstriche bei der Leistung und Stabilität des Geräts machen zu müssen. Mithilfe der Datenerfassungs-Engine von Scandit verwandeln sich im Rahmen von Knox Capture kompatible Smartphones in leistungsstarke Barcode-Scanner. Mithilfe von Knox Capture lassen sich kompatible Smartphones und Tablets im Kundendienst als Scanner einsetzen. Dank intuitiver Funktionen wie der „Push to Scan"-Taste lässt sich nahtlos zwischen Smartphone- und Scanner-Nutzung wechseln. So können User zum Beispiel Formularfelder im Handumdrehen durch Scannen ausfüllen, statt die Daten per Hand einzutippen.



Was einen maßgeschneiderten Service ausmacht

Zum Knox-Ökosystem gehören neben den oben erwähnten Lösungen auch folgende Dienstleistungen:

Der Enterprise Tech Support von Samsung hilft Unternehmen bei der Aufrechterhaltung ihrer Geschäftskontinuität. Wenn Mobilgeräte für die Arbeitsabläufe in einer Firma eine wichtige Rolle spielen, führen Ausfallzeiten und ineffiziente Prozesse zu Produktivitätsverlusten. Der Enterprise Tech Support baut einen direkten Draht zu den Mobilitätsexperten von Samsung auf und erweitert das interne IT-Team um externe Fachkräfte. Sie bieten Third-Level-Support für Probleme im Zusammenhang mit Samsung-Hardware und -Software. Darüber hinaus helfen sie beispielsweise auch bei der Vorbereitung des nächsten Betriebssystem-Releases.

Darüber hinaus zählt auch Software Customization zum Leistungsspektrum: Samsung bietet Software-Anpassungen als Teil der Business-Services an, um individuellen Bedürfnissen gerecht zu werden. Mit der Custom-Binary-Funktion gelingt es, Mobilgeräte an spezifische Einsatzszenarien anzupassen. Auf Systemebene sind dabei tiefgreifende Eingriffe möglich, etwa die Belegung von Hardware-Tasten mit speziellen Funktionen oder die Anpassung von Netzwerkparametern. Auch die Integration von Spezialzubehör klappt. Auf der Software-Ebene können User steuern, welche Apps vorinstalliert oder entfernt werden und wann die Geräte Sicherheits-Updates erhalten. Samsung stellt die Geräte mit kundenspezifischer Software her, sodass der Kunde die Kontrolle über die Software-Version haben kann.

Zu den Diensten, die die Nutzung der Samsung-Hardware noch sicherer machen, gehört auch eine Versicherung: Samsung Care+ for Business ADH wird von Servify angeboten, einer globalen Plattform für das Management des Produktlebenszyklus. Die

Versicherung beinhaltet im Versicherungsfall entweder Hardware-Reparaturen mit Originalteilen durch geschulte Techniker und Technikerinnen oder den Austausch des versicherten Gerätes. Samsung Care+ for Business ADH kommt unter anderem zum Einsatz, wenn physikalische Schäden an den Geräten entstehen, beispielsweise durch ein Herabstürzen des Smartphones oder einen Wasserschaden.

Diese Ansprüche können Kunden und Kundinnen von Samsung Care+ for Business ADH einfach geltend machen. Dazu können die IT-Verantwortlichen einen Servicefall über ihr Samsung-Knox-Portal eröffnen oder die gebührenfreie Nummer anrufen und einen Anspruch beim Service-Center einreichen. Dieses ermittelt dann den Versicherungsschutz und startet den Schadenbearbeitungsprozess.

Fazit: Härten Sie die mobile Front

Mit den Lösungen des Knox-Ökosystems können Sie die Verteidigungsfähigkeit beim Einsatz mobiler Technologien erhöhen. Damit können Sie das Potenzial der mobilen Revolution ausschöpfen und Ihr Unternehmen gleichzeitig schützen. Erfahren Sie mehr über die einzelnen Lösungen des Knox-Ökosystems und nehmen Sie Ihre Sicherheit selbst in die Hand.

Kontaktieren Sie uns noch heute für weitere Informationen. Finden Sie heraus, wie die Knox-Lösungen Ihrem Unternehmen dabei helfen, eine kontinuierlich gewachsene Angriffsfläche wirksam zu verteidigen.

Sie haben Fragen oder möchten mehr über Samsung Knox erfahren? Wir beraten Sie gerne!

Holger Dohrmann
Product & Solution Manager B2B
E-Mail h.dohrmann@samsung.com

Samsung Electronics GmbH
Am Kronberger Hang 6
65824 Schwalbach/Ts.
Geschäftsführer: Man Young Kim

Technische Service-Hotline: 06196 77 555 77*
* Kosten laut Konditionen des Vertragspartners für Festnetzanschlüsse oder Mobilfunkanschlüsse

Mehr Informationen finden Sie unter: samsungknox.com/de

Bleiben Sie auf dem Laufenden:

Über Samsung Electronics Co. Ltd.
Als Unternehmen mit zunächst starkem Fokus auf die Consumer-Technologie hat sich Samsung Electronics mit seinem Partnernetzwerk auch im B2B-Bereich breit aufgestellt. Mit ganzheitlichen technologischen Lösungen für eine sichere, mobile Businesskommunikation unterstützt Samsung Unternehmen verschiedenster Branchen, von der Digitalisierung zu profitieren und langfristig wettbewerbsfähig zu bleiben.

Entdecken Sie die neuesten Nachrichten, Hintergrundinformationen und Pressematerialien auf www.samsung.de/business/ und im Samsung-Newsroom unter news.samsung.com.