



SAMSUNG

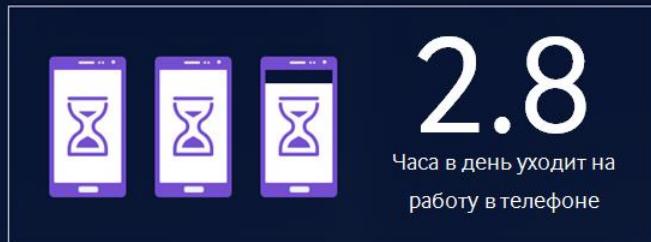
Мобильная Безопасность

Содержание

1. Корпоративная мобильность
2. Тенденции в сфере корпоративной мобильности
3. Почему необходимо инвестировать в Мобильную безопасность?
4. Мобильные устройства – самое слабое звено в ИТ безопасности
5. Принятие мобильности
6. Android представляет риск для предприятий
7. Тенденция BYOD
8. Платформа и решения Knox
9. Примеры внедрений. Применение в Бизнесе

Корпоративная мобильность

Увеличение мобильного использования в работе



*Source: visualcontenting.com



Тенденции в сфере корпоративной мобильности

Мобильные устройства широко используются на предприятиях

555M

Прогнозируемые продажи мобильных устройств в 2016¹

Рост использования корпоративных мобильных решений

324M

Число пользователей, использующих корпоративные мобильные решения в 2016²

Корпоративная мобильность преобразуется в «Интернет вещей» (IoT)

8.3B

Общее число конечных точек сети на предприятиях к 2020³

¹ Strategy Analytics : Sept. 2015

² Strategy Analytics: Oct. 2015

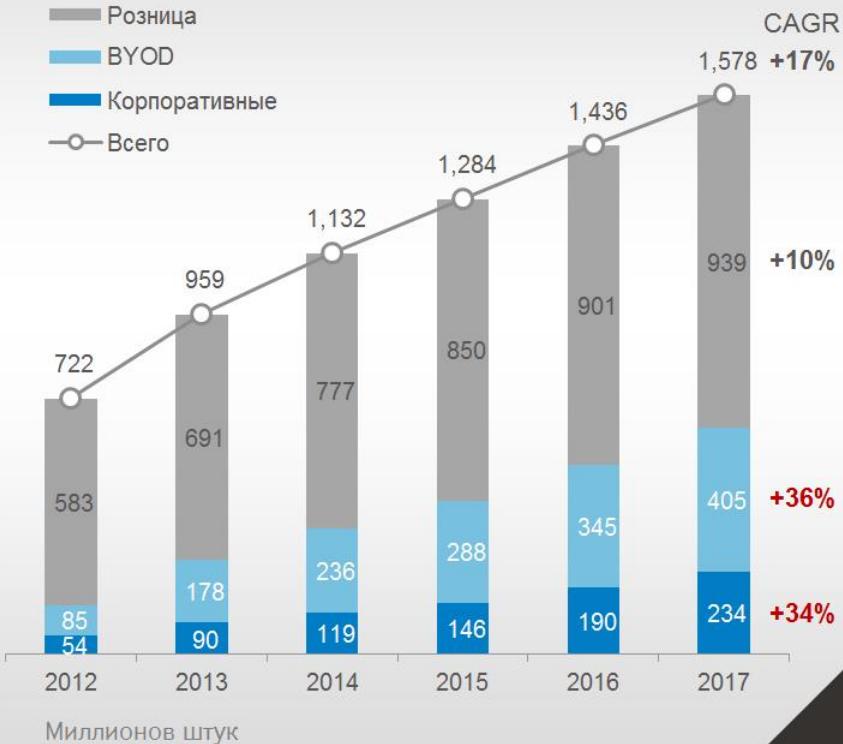
³ Gartner: July 2015

Тенденции в сфере корпоративной мобильности

41% ИСПОЛЬЗОВАНИЕ
ДЛЯ РАБОТЫ

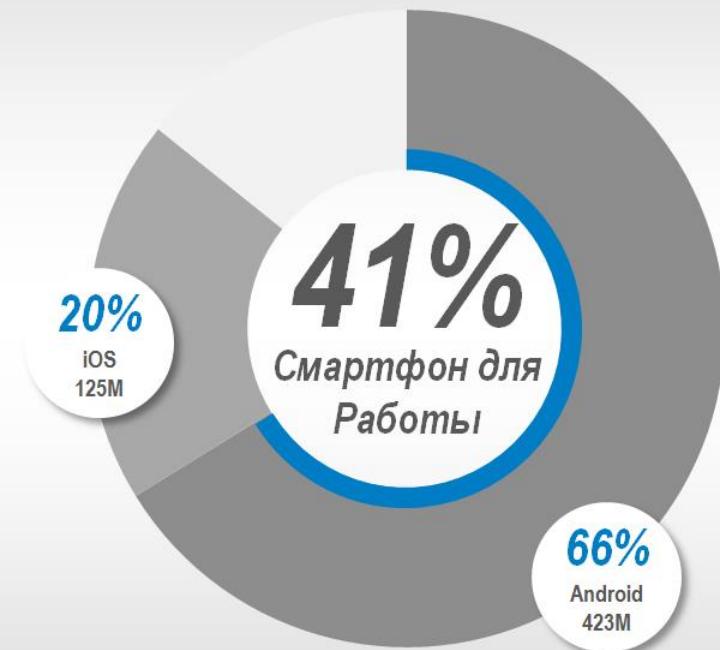


1 IDC #241599



Тенденции в сфере корпоративной мобильности

66% ДОЛЯ
ANDROID



Почему необходимо инвестировать в Мобильную безопасность?



Новые угрозы выявляются каждый день



4 ЧАСА -

Столько требуется хакеру, чтобы получить
несанкционированный **доступ к данным**



**90% Компаний считают, что не готовы к
кибер-атакам**

1 <https://www.kennasecurity.com/wp-content/uploads/data-breach-investigation-report-2016.pdf>

2 <http://www.pwc.pl/pl/publikacje/2015/w-obronie-cyfrowych-granic-gsiss-2016.html>

3 World Economic Forum „The Global Risks Report 2016, 11th edition

Почему необходимо инвестировать в Мобильную безопасность?



> \$250 000 – расходы на мобильные инциденты по
безопасности



Каждые 5 мин. – используются приложения
повышенного риска



Каждые 36 мин. конфиденциальные данные
высылаются за пределы компании

Мобильные устройства – самое слабое звено в ИТ безопасности

РИСК УТЕЧКИ ДАННЫХ



Интеллектуальная
собственность



Сетевые
полномочия/данные



Местонахождение
сотрудников



Звонки



Закрытые сведения

Мобильные устройства – самое слабое звено в ИТ безопасности

Опасность заключается в мобильности
самых устройств – легко **теряются** или
могут быть **украдены**, что поставит
под угрозу **данные**, которые
на них хранятся



Сотрудники часто **путешествуют** вне
сетевого периметра организации, где
подвергают **рискам** конфиденциальные
и персональные **данные** или могут
подвергнуться **нападению**
злоумышленников

Принятие мобильности

Топ 3 опасения для использования Android на предприятии

Отсутствие
безопасности
платформы

01

Отсутствие
информационной
безопасности

02

Отсутствие
политики контроля
и управления

03

Android представляет риск для предприятий

PC NEWS / OPINIONS / FEATURES / DEALS / HOW-TO / BUSINESS / SUBSCRIBE
ALL REVIEWS ▾ LAPTOPS / TABLETS / PHONES / APPS / SOFTWARE / SECURITY / PRINTERS / CAMERAS / HDTVs

Home ▾ Reviews ▾ Software ▾ Security ▾ You Need Mobile Security for Android, But Not Because of Malware

BY MAX EDDY JULY 16, 2013 5 COMMENTS

There are a lot of reasons you need mobile security for your Android, and all of them are bigger than malware, for the moment.

You Need Mobile Security for Android, But Not Because of Malware

1.6K SHARES



The deep, dark fear of security-minded people was that smartphones would surpass PCs as the prime target for malware. The good news is this hasn't happened...yet. Apple's strict control over its store has kept out nearly all the overtly malicious apps, and the Google Play store has seen remarkably little malware despite the freedoms it allows.

Malware is a threat for mobile users, but if you stick to Google Play it's highly unlikely you'll encounter it. There are, however, other, more pressing concerns. Scammers and aggressive ad networks want access to your personal information, and mobile device theft is a burgeoning problem. Thankfully, Android security suites are already guarding against these threats, and are ready to defend you, should the mobile malware threat ever really take off.

Mobile Malware Protection Today

App stores have largely cleaned up their act, so the real threat now is what was well established by the time Google got involved. That's where the bad guys have made the jump to mobile, and they've come up with some clever techniques.

“79% мобильных вредоносных программ нацелены на Andorid”

PC Magazine 8/28/2013

Data-Tech KEEPING AN EYE ON THREATS TO YOUR COMPUTER

Home Services Company Industries Resources Partner Program Support Contact Shop

Android security flaw uncovered

admin July 16, 2013



The security of devices used in the office should be a top priority for business owners and managers.

It is easy to think that a fully functioning device like a mobile phone is secure, and most of the time it is. The thing to be aware of however, is that there are always hackers looking for security flaws in these products. The latest flaw highlighted happens to be on the Android system.

In early July, mobile security company Bluebox announced that they had discovered a large security flaw in the Android system. The threat centers around a trojan application that can gain access to application data including email addresses, SMS messages, etc, and can get service and account passwords. In other words, it can take over your whole phone.

The way this so-called trojan infects mobile devices is through an app. Hackers have figured out how to tinker with the application's code, and implement the malware without changing the cryptographic features that are used by Google Play and other online stores to validate and identify apps.

“Раскрыты дефекты в безопасности Android”

Data-Tech 7/16/2013

PC NEWS / OPINIONS / FEATURES / DEALS / HOW-TO / BUSINESS / SUBSCRIBE
ALL REVIEWS ▾ LAPTOPS / TABLETS / PHONES / APPS / SOFTWARE / SECURITY / PRINTERS / CAMERAS / HDTVs

Home ▾ Reviews ▾ Software ▾ Security ▾ 79 Percent of Mobile Malware Targets Android

BY ANGELA MOSCARITO AUGUST 28, 2013 11:41AM EST 8 COMMENTS

An overwhelming 79 percent of all mobile malware threats target devices running Google's Android operating system, according to a joint unclassified memo from the U.S. Department of Homeland Security and Department of Justice.

114 SHARES



An overwhelming 79 percent of all mobile malware threats target devices running Google's Android operating system, according to a joint unclassified memo from the U.S. Department of Homeland Security and Department of Justice.

“Android is the world's most widely used mobile operating system and continues to be a primary target for malware due to its market share and open source architecture,” notes the July 23 memo [PDF], which was obtained and published online by the website Public Intelligence.

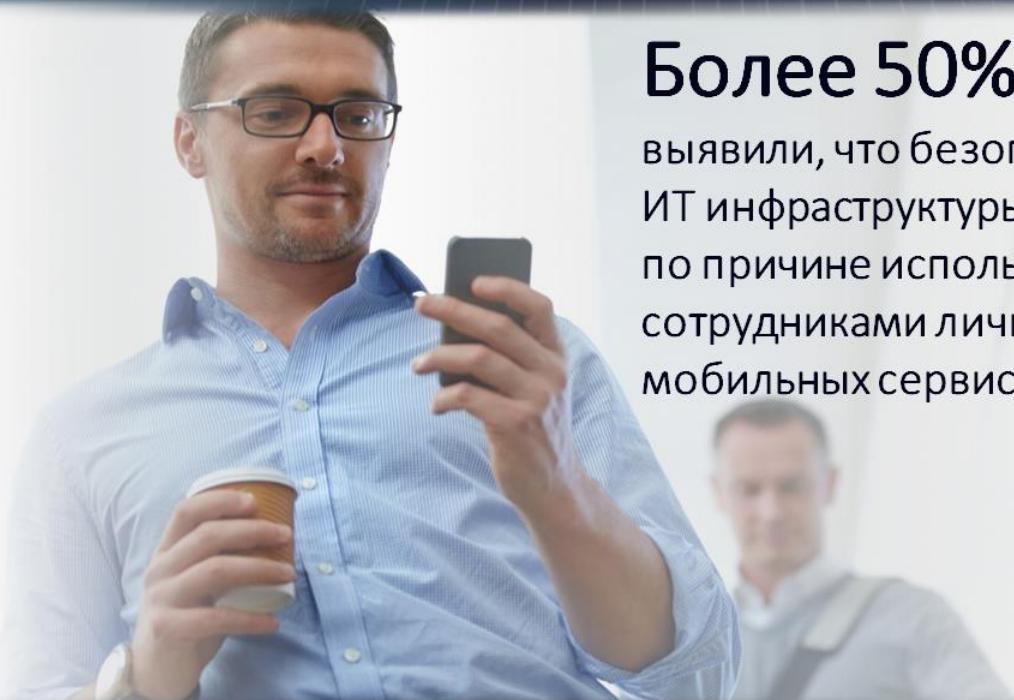
In comparison, just 0.7 percent of mobile malware is designed to take advantage of Apple's iOS, according to the document, which cites data from 2012. Apache, 19 percent targets Nokia's aging Symbian platform while 0.3 percent affects Windows Mobile and BlackBerry, and the remaining 0.7 percent targets a variety of other mobile operating systems.

A major part of the problem is that many companies still run old versions of their software, leaving them vulnerable to attacks. The memo also notes that the vast majority of mobile malware is spread via social media.

“Телефоны Android – «мины» карманного размера”

PC Magazine 7/8/2013

Развитие BYOD* позвод для беспокойства ИТ менеджеров



Более 50% ИТ Директоров*

выявили, что безопасность
ИТ инфраструктуры была нарушена
по причине использования
сотрудниками личных
мобильных сервисов

Противоречивые потребности в тенденции BYOD

Мне нравится
устройство с
высоким уровнем
безопасности.

Я хочу
контролировать
и управлять
мобильными
устройствами

Директор



Я хочу использовать
свое **личное мобильное**
устройство для работы

Я хочу **защитить свою**
частную жизнь на
мобильном устройстве

Сотрудник

Противоречивые потребности в тенденции BYOD

Мне нравится
устройство с
**высоким уровнем
безопасности**

Я хочу
контролировать
и управлять
мобильными
устройствами

Директор



Сотрудник

Я хочу использовать
**свое личное
мобильное устройство**
для работы

Я хочу **защитить свою
частную жизнь** на
мобильном устройстве



Корпоративная платформа мобильной безопасности
и пакет программных решений



Решения KNOX

Корпоративные мобильные решения, основанные на
встроенной платформе

KNOX Workspace

Полнофункциональный
рабочий контейнер
для предприятий

KNOX Premium

Облачное решение EMM с
рабочим контейнером

KNOX Enabled App

Невидимый безопасный
контейнер для
определенных приложений

KNOX Customization

Набор услуг и инструментов
по кастомизации

Платформа KNOX

Встроенная аппаратная платформа
безопасности и управления Samsung

Защита корпоративных данных от вредоносных атак



SAMSUNG Кнокс

- Усиленная безопасность от аппаратного уровня до уровня приложений
- Защита в режиме реального времени с момента включения

Samsung Knox

безопасность мирового класса



1ST

Награжден высшим баллом в
области мобильной безопасности
Gartner, Апр. 2016



Лучшее решение по обеспечению
безопасности или защиты от
мошенничества

Позволяет сотрудникам быть мобильными

- Современные средства корпоративных коммуникаций (Email, PIMS): улучшенные функции EAS;
- Установка корпоративных приложений в защищенную область;
- KNOX поддерживает работу разнообразных средств Samsung по повышению производительности. (такие как: многозадачность, сканер отпечатков пальцев, S-Pen, клавиатура в виде корпуса).

Introduction to Carbon Bonding

Chemistry fundamentals

Working with organic chemistry requires significant background in classical chemistry before getting started. Here we provide a brief review of valence shell theory, Lewis structures, and molecular geometry.

Electron configurations and valence bonding theory—the idea that all atoms either gain or lose electrons to achieve full outer shells.

Most of what we know about chemical bonding revolves around **valence shell theory**—the idea that all atoms either gain or lose electrons to achieve full outer shells.

Carbon is unique in this respect due to the four electrons in its outer shell. It can either

Contoso Electronics Sales Presentation

Opportunity

Sales alignment with Contoso gives Litware a strong opportunity to take a market leadership position and deliver quality, consistency, and innovation to its customers.

Contoso Monthly Report

Contoso Expenses

Category	2008	2009
Rent and Utilities	\$ 18,840	\$ 17,628
Equipment	\$ 18,000	\$ 3,972
Marketing	\$ 5,560	\$ 5,424
Freelancers	\$ 5,000	\$ 5,506
Travel	\$ 1,474	\$ 1,104
Taxes	\$ 2,460	\$ 2,774
Total	\$ 43,104	\$ 43,080

Contoso Monthly Report

Contoso Expenses

A hand holding a Samsung smartphone displays the Samsung Knox app interface. The screen shows various app icons such as Contacts, Email, Gallery, Internet, S Planner, Camera, and My Files. The background of the phone's home screen is blue with white text.

The Samsung Knox app interface is shown on the smartphone screen. It features a grid of app icons including Contacts, Email, Gallery, Internet, S Planner, Camera, and My Files. Below the icons is a "MEMO" icon. At the bottom of the screen, there is a numeric keypad for entering a passcode. The background is white with blue accents.

Friday 14/08/2015

Me	seceas001	oliver
8 AM		
9		
10		
11		
12		
1	1	2
2	4	5
3	6	7
4	8	9
5	10	11
6	12	13
7	1	2
8	3	4
9	5	6
10	7	8
11	9	10
12	11	12
1	13	14
2	14	15
3	15	16
4	16	17
5	17	18
6	18	19
7	19	20
8	20	21
9	21	22
10	22	23
11	23	24
12	24	25
13	25	26
14	26	27
15	27	28
16	28	29
17	29	30
18	30	31
19	31	32
20	32	33
21	33	34
22	34	35
23	35	36
24	36	37
25	37	38
26	38	39
27	39	40
28	40	41
29	41	42
30	42	43
31	43	44
32	44	45
33	45	46
34	46	47
35	47	48
36	48	49
37	49	50
38	50	51
39	51	52
40	52	53
41	53	54
42	54	55
43	55	56
44	56	57
45	57	58
46	58	59
47	59	60
48	60	61
49	61	62
50	62	63
51	63	64
52	64	65
53	65	66
54	66	67
55	67	68
56	68	69
57	69	70
58	70	71
59	71	72
60	72	73
61	73	74
62	74	75
63	75	76
64	76	77
65	77	78
66	78	79
67	79	80
68	80	81
69	81	82
70	82	83
71	83	84
72	84	85
73	85	86
74	86	87
75	87	88
76	88	89
77	89	90
78	90	91
79	91	92
80	92	93
81	93	94
82	94	95
83	95	96
84	96	97
85	97	98
86	98	99
87	99	100

From: oliver@mail1002.net

ATTACH SEND MORE

Good news gentleman

Permission

- Do Not Forward
- Do not Extract
- Do not Forward
- Do not Print
- Do not Reply
- Do not Reply All
- No restrictions

A screenshot of an email application showing a message from "oliver@mail1002.net". The message subject is "Good news gentleman". On the right, a "Permission" dialog box is open, listing several options for handling attachments. The option "Do not Reply All" is selected with a green checkmark.

KNOX Workspace

Полнофункциональный корпоративный контейнер

Зарекомендовавший себя на рынке:

Широко используется Банками и Гос.органами более чем в 20 странах.

Повышенная безопасность:

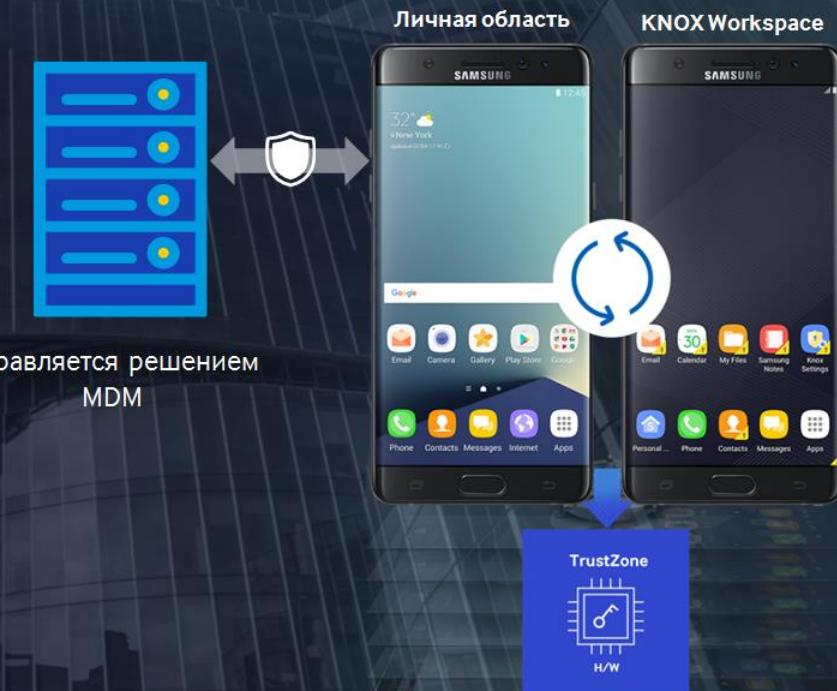
Защита от аппаратного уровня до уровня приложений.

Простая интеграция:

Совместимость с ведущими решениями MDM, любыми приложениями Андроид.

Усиленная безопасность приложений и данных:

- Ключ шифрования для KNOX Workspace хранится в полностью изолированной аппаратной области называемой TrustZone
- Если устройство находится под угрозой взлома, доступ к KNOX Workspace заблокируется окончательно



Управляется решением
MDM

KNOX Premium

ЕММ - Управление мобильным парком девайсов
Облачное решение с безопасным рабочим
контейнером

Экономически выгодное решение:

Дешевле большинства существующих MDM решений

Простое управление:

Простая конфигурация устройств
через веб-консоль.

Повышенная безопасность:

Защита от аппаратного уровня до
уровня приложений.



сервер



инженер



Конкурентный
лицензионный сбор
50%~70% дешевле, чем другие MDM



Нет необходимости в
специализированной
инфраструктуре

Экономичное ЕММ решение



Удалённая
блокировка и
сброс



Режим киоска



Управление
настройками и
приложениями



Отчет о
местоположении
устройства

KNOX Customization

Преобразование устройств Samsung
в специализированные устройства

Ребрендинг ПО:

Добавление клиентского логотипа на экране загрузки и обоев.



Индивидуальная настройка:

Режим киоска, переназначение кнопок, контроль
настроек связи.



Простая конфигурация:

Готовая стандартная конфигурация без ручной
работы, без MDM.



KNOX Customization

Примеры внедрения

Развлекательный контент



- ✓ Специализированное мультимедийное решение на планшете (контроль аудио/видео, управление контентом и др.)

Услуги цифровой библиотеки



- ✓ Профессиональный режим киоска (ограничения доступа к настройкам и другим действиям на устройстве)

Привлечение клиентов



- ✓ Онлайн-меню для комфорtnого привлечения клиентов

Использование в розничной сети



- ✓ Воспроизведение рекламы
- ✓ Электронное меню
- ✓ Дополнительный контент

«Решения для любых сфер
бизнеса»

KNOX Enabled App

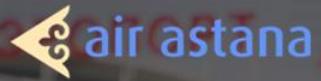
Дополнительная защита
пользовательских приложений

Защита на аппаратном уровне с
Samsung KNOX.

Идентичная пользовательская среда
в сравнении со стандартными приложениями.



Примеры внедрений



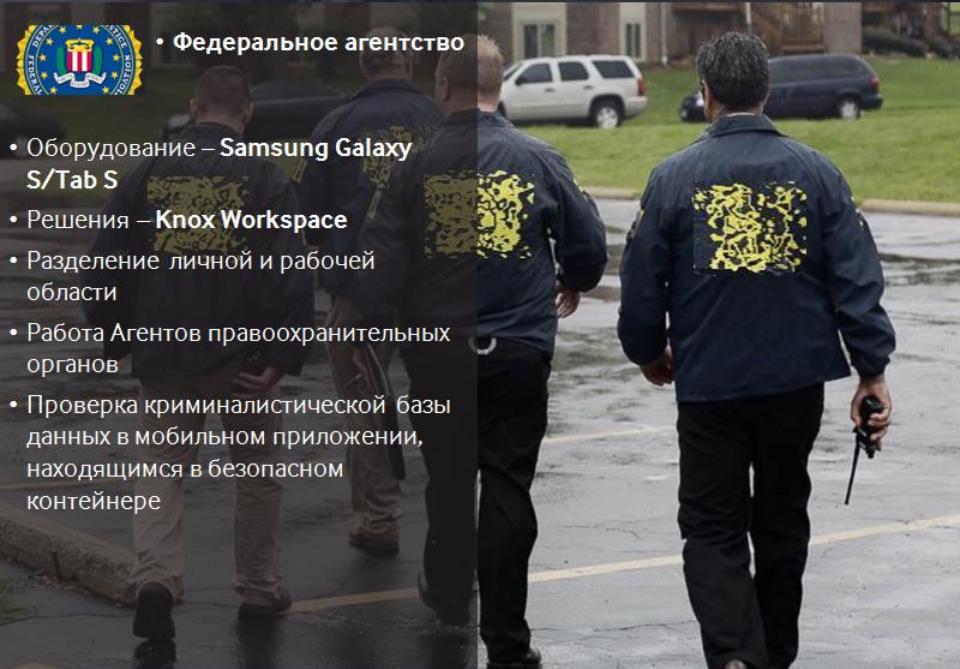
- Оборудование – **Tab Active**
Противоударный планшет с
защитой от воды и пыли (IP 67)
- Решения – **Knox Premium + Workspace**
- Корпоративные приложения
находятся в безопасной рабочей
области – Контейнере **Knox**.
- Настройка политик для устройств
(правила создания паролей,
удаленная установка и у
правление приложениями, VPN-
подключения, и т.д.).



Примеры внедрений



- Федеральное агентство
- Оборудование – **Samsung Galaxy S/Tab S**
- Решения – **Knox Workspace**
- Разделение личной и рабочей области
- Работа Агентов правоохранительных органов
- Проверка криминалистической базы данных в мобильном приложении, находящимся в безопасном контейнере



- Оборудование – **Samsung Galaxy Note**
- Решения – **Knox Workspace**
- Samsung предоставил комплексное решение, позволяющее защитить важные и конфиденциальные данные на мобильных устройствах
- Разделение личной и рабочей области



KNOX: Применение в бизнесе

Корпоративное
применение



Решения KNOX

Knox
Workspace

Knox
Premium

Knox
Enabled App

Knox
Customization



Спасибо!

SAMSUNG