

Samsung **Knox**

a potrzeby
działu IT



Do 2015 roku liczba pracowników aktywnie korzystających ze smartfonów, tabletów i komputerów przenośnych wzrośnie na świecie do 1,3 mld – szacuje IDC. Zwiększy się jednocześnie niebezpieczeństwo utraty danych firmowych przetwarzanych przez te urządzenia. Samsung Knox odpowiada na ten problem.

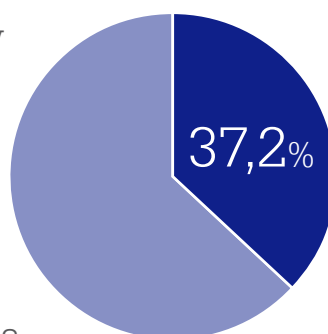
Do 2015 roku liczba pracowników mobilnych wzrośnie do

1,3 mld,

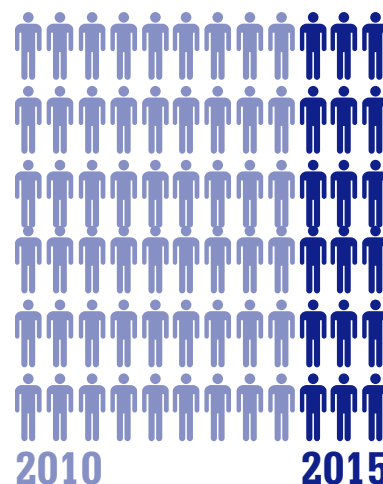
co będzie stanowiło 37,2% wszystkich zatrudnionych.

W porównaniu do 2010 roku liczba pracowników mobilnych zwiększyła się

o **300 milionów**

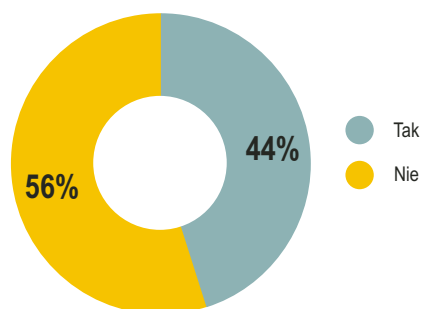


+30%

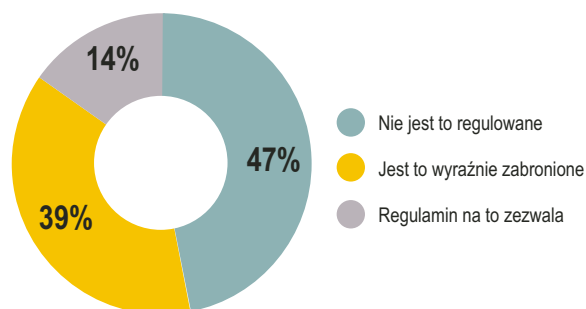


BADANIA SZEFOW IT

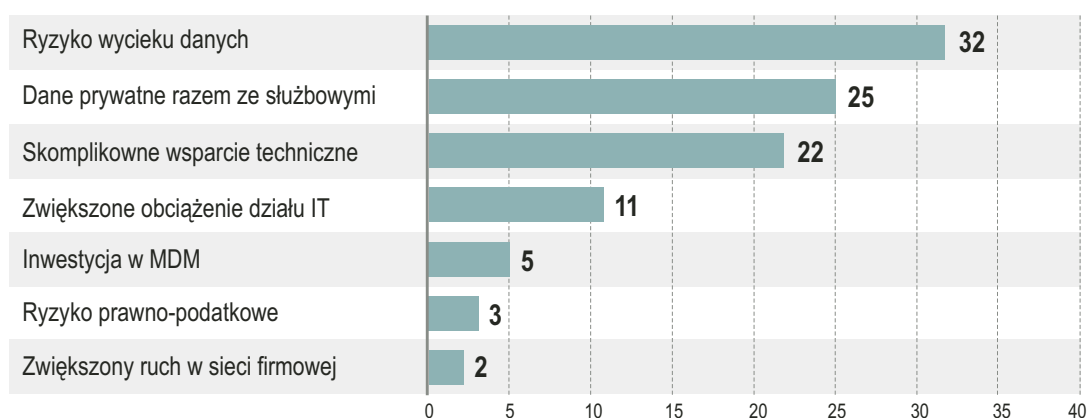
Czy w Twojej firmie pracownicy korzystają z prywatnych urządzeń do celów służbowych?



Czy Twoja firma dopuszcza wykorzystanie prywatnego sprzętu do celów służbowych?

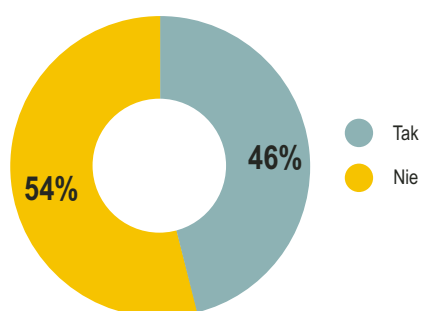


Czego boją się oddziały IT?

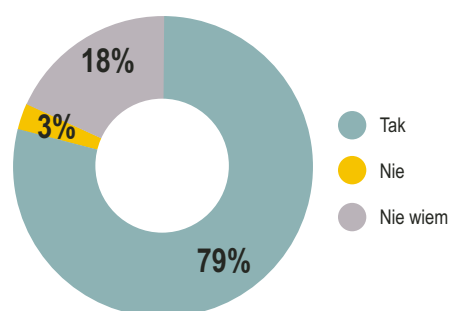


BADANIA PRACOWNIKÓW

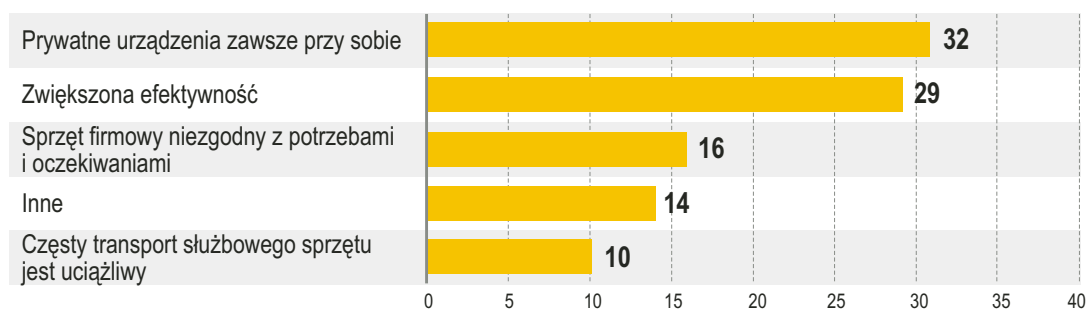
Czy wykorzystujesz prywatny sprzęt do celów służbowych?



Czy Twój pracodawca zezwala na używanie prywatnego sprzętu do celów służbowych?



Sprzęt prywatny na etacie – dlaczego?



- Dla pracowników działów IT popularność systemu Android wiąże się z koniecznością zwrócenia szczególnej uwagi na kwestie związane z bezpieczeństwem sieciowym i ochroną cennych danych firmowych. Korporacje patrzyły dotychczas dość niechętnie na urządzenia mobilne bazujące na tej platformie, głównie ze względu na bardzo niski poziom zabezpieczeń i ograniczone możliwości zarządzania.
- Dziś wiadomo już, że konfrontacja firmowych polityk bezpieczeństwa z powszechnie dostępnym systemem Android jest nieunikniona. Rosnącym problemem staje się również używanie prywatnych urządzeń do łączenia się z siecią korporacyjną. Zjawisko BYOD (ang. Bring Your Own Device) znacząco wpływa na zwiększenie się liczby incydentów sieciowych, coraz częściej łączących się z wymiernymi stratami finansowymi.
- Pracownicy przechowują na prywatnych smartfonach czy tabletach niezliczoną ilość firmowych danych. Te z kolei nie powinny znaleźć się w niepowołanych rękach. Najczęściej są to informacje gromadzone w służbowej poczcie elektronicznej, kalendarzach spotkań, opisach kontaktów biznesowych i cennych zbiorach danych o klientach kluczowych dla firmy. Szacuje się, że w dużych przedsiębiorstwach straty związane z wyciekiem danych, nadprogramowym zaangażowaniem działów IT, a nierzadko z konsultacjami prawnymi mogą sięgać setek tysięcy dolarów rocznie. Żadna firma nie może pozwolić sobie na to, by przynajmniej nie próbować zminimalizować ryzyka narażania się na takie koszty.

Samsung Knox – odpowiedź na potrzeby działów IT

- Jednym z podstawowych sposobów zwiększenia kontroli nad wykorzystaniem urządzeń mobilnych w firmie jest wdrożenie platformy MDM (ang. Mobile Device Management). Idealne rozwiązanie tego typu powinno zapewniać wsparcie dla wielu systemów operacyjnych, wymuszać polityki bezpieczeństwa zdefiniowane przez działy IT, na bieżąco inwentaryzować i korygować stan floty urządzeń mobilnych. Do ważnych zalet MDM należy również dystrybucja oprogramowania dla poszczególnych pracowników (najlepiej w modelu OTA, z ang. Over The Air), zdalny monitoring i administrowanie zawartością smartfonu lub tabletu (ze szczególnym uwzględnieniem takich opcji, jak kasowanie danych, blokowanie dostępu).

Czynniki o krytycznym lub bardzo ważnym znaczeniu dla oceny dostawców rozwiązań mobilnych

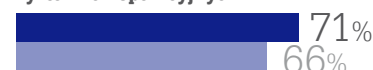
Zapewnienie bezpieczeństwa urządzeń



Łatwość integracji z istniejącą strukturą IT



Możliwość korzystania z produktów i usług na wielu platformach/systemach operacyjnych



Udział w zarządzaniu rosnącą liczbą urządzeń



Doradztwo i informacje nt. najlepszych praktyk w sprawach związanych z zarządzaniem



■ **Ponad 1000 pracowników**
■ **Poniżej 1000 pracowników**

- Problemem, z jakim często borykają się pracownicy działów IT jest wybór optymalnego rozwiązania MDM dla firmy. Poszczególne systemy różnią się dostępnymi funkcjami, co prowadzi do nadmiernego skomplikowania procesu wdrożenia i późniejszej eksploatacji.
- W 2013 roku Samsung wyszedł naprzeciw oczekiwaniom administratorów i zaprezentował nową platformę KNOX, stanowiącą kompleksowy system zabezpieczeń dla urządzeń mobilnych. Samsung KNOX jest rozwiązaniem kompletnym, zawierającym w sobie ponad 500 reguł MDM, zapewniającym bezpieczny dostęp do obszarów pracy służbowej i prywatnej (tzw. kontenery w jednym urządzeniu). Platforma KNOX oferuje usługi zarządzania smartfonami, tabletami za pośrednictwem chmury obliczeniowej (cloud computing), a dodatkowe funkcje można dokupić w formule SaaS (Software as a Service).

Do najważniejszych zalet KNOX należy zaliczyć nowe, wielowarstwowe systemy zabezpieczeń, które właściwie wykluczają możliwość utraty danych. Mechanizm Trusted Boot nie pozwoli, by na urządzeniu uruchomione zostały aplikacje, które nie były wcześniej sprawdzone i autoryzowane przez działy IT. Architektura TIMA (TrustZone-based Integrity Measurement Architecture) nadzoruje i monitoruje integralność systemu Linux (na którym bazuje Android). Jeśli nastąpi próba unieruchomienia TIMA lub zostanie wykryta próba włamania się do jądra systemu, to urządzenie przestanie działać. Kolejnym elementem zwiększającym bezpieczeństwo jest Security Enhancements for Android (SE for Android). Jest to specjalnie zaprojektowana technologia, zapewniająca wsparcie dla kontenerów dostarczanych przez innych producentów, co dodatkowo uelastycznia nadzorowanie floty urządzeń mobilnych przez działy IT.

- Samsung KNOX podnosi bezpieczeństwo również w warstwie sprzętowej. Dzięki rozwiązaniu SmartCard

- Framework smartfon może służyć jako dodatkowy czynnik uwierzytelniający dla czytników kart działających w standardzie Bluetooth.
- W platformie Samsung KNOX znacznie ułatwiono obsługę kontenerów, co dla wielu pracowników będzie wiązało się z łatwiejszym instalowaniem aplikacji i większym zadowoleniem z obsługi urządzenia. Obszar wyodrębniony na potrzeby oprogramowania korporacyjnego i danych firmowych będzie na stałe oddzielony od prywatnej przestrzeni użytkownika smartfonu. KNOX ma wbudowane skanery złośliwego oprogramowania, więc pracownik zyska dodatkową ochronę w swoim kontenerze. Możliwość instalowania w nim różnych aplikacji (np. pochodzących z Google Play) może być definiowana przez firmowe działy IT.
- Użytkownicy przyzwyczajeni do korzystania z własnych urządzeń przenośnych (BYOD) również mają ułatwioną możliwość rejestrowania i aktywowania swoich smartfonów (zgodnie z wewnętrzną polityką bezpieczeństwa). Wystarczy, że zainstalują na swoim urządzeniu aplikację Universal MDM Client (UMC), która połączy się z działającym w chmurze serwerem Samsung Enterprise Gateway (SEG).
- Na podkreślenie zasługuje fakt kompatybilności platformy KNOX z coraz popularniejszymi rozwiązaniami mobilnymi, działającymi w chmurach obliczeniowych. Samsung KNOX jest dostosowany do pracy z Microsoft Workplace Join, Windows Intune i Windows Azure.
- Samsung KNOX bezpośrednio odpowiada na zapotrzebowanie zgłaszane przez menedżerów działów IT. Do najważniejszych czynników branych pod uwagę przy wyborze platformy do zarządzania urządzeniami mobilnymi zaliczyli oni: zapewnienie bezpieczeństwa sieciowego, łatwość integracji z istniejącą infrastrukturą IT oraz możliwość elastycznego korzystania z produktów i usług pochodzących od różnych dostawców.

NAZWA POTRZEBY	GRUPY REGUŁ MDM W ŚRODOWISKU KNOX		
Zdalne zarządzanie	Zarządzanie aplikacjami	Zarządzanie kontami e-mail	Przeglądarka
	Hasło	Zarządzanie certyfikatami	Zarządzanie licencjami
Zapobieganie wyciekowi danych	Tryb widoku podwójnego [Dual Persona]	Firewall dla kontenera aplikacji	SE for Android**
	Ograniczenie funkcjonalności aparatu	Zarządzanie integralnością systemu	Kontrola przesyłanych wiadomości e-mail
	Zarządzanie kontenerami aplikacji	Zarządzanie aplikacjami/izolacja danych	
Kontrola i limity	Uprawnienia dla aplikacji	Ograniczenia dostępu dla kontenerów	Geofencing
Monitorowanie	Monitorowanie integralności systemu	Audytowanie	
Bezpieczny dostęp do zasobów przedsiębiorstwa	Sieci VPN oparte na IPSec, zgodne ze standardem FIPS	VPN dla każdej aplikacji	Szyfrowanie zgodne ze standardem FIPS
	Kontrola aplikacji	Konto Exchange	Szyfrowanie na urządzeniu
Wsparcie w czasie rzeczywistym dla użytkownika mobilnego	Zdalna kontrola		
Integracja z istniejącą strukturą IT	Pojedyncze logowanie w chmurze	Active Directory	Obsługa kart chipowych
	Wsparcie dla wielu bram VPN		

Więcej informacji

Szczegółowe informacje na temat Samsung Knox można znaleźć na oficjalnym polskojęzycznym portalu:
<http://www.samsung.com/pl/business/solutions-services/mobile-solutions/security/samsung-knox>