ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія уніфікованого керування безпекою корпоративних мобільних пристроїв на базі Sophos Mobile»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Дмитро ШПОРТКО
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-62
ШПОРТКО Дмитро
(прізвище, ім'я)

Керівник к.військ.н., доцент ГАХОВ Сергій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
Систем та технологій
кібербезпеки
_____ Галина ГАЙДУР
"___" жовтня 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

ШПОРТКУ Дмитру Вікторович
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Технологія уніфікованого керування безпекою корпоративних мобільних пристроїв на базі Sophos Mobile»

керівник кваліфікаційної роботи Гахов Сергій Олександрович, к.військ.н., доц.
(прізвище, ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «15» жовтня 2024 року № 320.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 15.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
рішення Sophos Mobile;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження проблеми уніфікованого керування безпекою корпоративних мобільних пристроїв;

2. Аналіз методів та засобів уніфікованого керування безпекою корпоративних мобільних пристроїв на базі Sophos Mobile;

3. Розроблення варіанта технології уніфікованого керуввання безпекою корпоративних мобільних пристроїв на базі Sophos Mobile.

5. Перелік графічного матеріалу

Презентація PowerPoint.

6. Дата видачі завдання 01.10.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми уніфікованого керування безпекою корпоративних мобільних пристроїв.	01.10.2024 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	12.10.2024 р.	
3.	Аналіз методів та засобів уніфікованого керування безпекою корпоративних мобільних пристроїв на базі Sophos Mobile.	27.10.2024 р.	
4.	Розроблення варіанта технології уніфікованого керування безпекою корпоративних мобільних пристроїв на базі Sophos Mobile.	03.11.2024 р.	
5.	Розроблення рекомендацій щодо уніфікованого керування безпекою корпоративних мобільних пристроїв.	15.11.2024 р.	
6.	Оформлення результатів дослідження.	26.11.2024 р.	
7.	Підготовка доповіді до захисту.	15.12.2024 р.	

Здобувач вищої освіти _____ Дмитро ШПОРТКО
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Сергій ГАХОВ
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 74 сторінок, 25 рисунків, 13 джерел.

Об'єкт дослідження – керування безпекою корпоративних мобільних пристроїв.

Предмет дослідження – технологія уніфікованого керування безпекою корпоративних мобільних пристроїв на базі Sophos Mobile.

Мета роботи – розробити рекомендації щодо впровадження та використання технології уніфікованого керування безпекою корпоративних мобільних пристроїв на основі Sophos Mobile.

Методи дослідження – аналіз літератури, технічної документації, стандартів у сфері інформаційної безпеки, а також порівняльний аналіз функціональних можливостей сучасних систем керування мобільними пристроями.

Технологія уніфікованого керування безпекою корпоративних мобільних пристроїв на базі Sophos Mobile забезпечує комплексний підхід до захисту корпоративних даних на мобільних пристроях. Вона надає можливість централізованого управління конфігурацією пристроїв, контролю доступу до корпоративних ресурсів, захисту конфіденційної інформації та моніторингу безпеки.

У роботі було проведено аналіз актуальних викликів у сфері мобільної безпеки, визначено основні загрози, пов'язані з використанням мобільних пристроїв у корпоративному середовищі. Проаналізовано можливості Sophos Mobile, зокрема управління політиками безпеки, шифрування даних, захист від шкідливих програм, інтеграцію з іншими компонентами кібербезпеки та засоби реагування на інциденти.

На основі отриманих результатів розроблено рекомендації для впровадження Sophos Mobile у корпоративні інформаційні системи. Запропоновано поетапний підхід до налаштування системи, включаючи моніторинг, автоматизацію оновлень та управління доступом. Наведено практичні поради для фахівців з кібербезпеки щодо адаптації технології до специфічних потреб організацій.

Галузь використання: забезпечення безпеки мобільних пристроїв у корпоративному середовищі.

КЛЮЧОВІ СЛОВА: ЗАХИСТ КОРПОРАТИНВИХ МОБІЛЬНИХ ПРИСТРОЇВ, УНІФІКОВАНЕ КЕРУВАННЯ БЕЗПЕКОЮ КОРПОРАТИВНИХ МОБІЛЬНИХ ПРИСТРОЇВ, ТЕХНОЛОГІЯ УНІФІКОВАНОГО КЕРУВАННЯ БЕЗПЕКОЮ КОРПОРАТИВНИХ МОБІЛЬНИХ ПРИСТРОЇВ

ABSTRACT

Text part of the qualification work: 74 pages, 25 figures, 13 sources.

Object of the research – technology of unified security management of corporate mobile devices.

Subject of the research – system of unified security management of corporate mobile devices based on Sophos Mobile.

Aim of Reserch – develop recommendations for the implementation and use of the technology of unified security management of corporate mobile devices based on Sophos Mobile.

Research methods – analysis of the literature, technical documentation, standards in the field of information security, as well as a comparative analysis of the functional capabilities of modern

The work analyzed current challenges in the field of mobile security, identified the main threats associated with the use of mobile devices in a corporate environment. The capabilities of Sophos Mobile are analyzed, including security policy management, data encryption, malware protection, integration with other cybersecurity components, and incident response tools.

Based on the results, recommendations for implementing Sophos Mobile into corporate information systems are developed. mobile device management systems.

The technology of unified security management of corporate mobile devices based on Sophos Mobile provides a comprehensive approach to protecting corporate data on mobile devices. It provides the ability to centrally manage device configuration, control access to corporate resources, protect confidential information and monitor security.

A phased approach to configuration systems is proposed, including monitoring, update automation, and access control. Practical advice is provided for cybersecurity professionals to adapt technologies to the specific needs of organizations.

Application area: ensuring the security of mobile devices in a corporate environment.

CORPORATE MOBILE DEVICE PROTECTION, UNIFIED SECURITY MANAGEMENT OF CORPORATE MOBILE DEVICES, UNIFIED SECURITY MANAGEMENT TECHNOLOGY OF CORPORATE MOBILE DEVICES

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AI - Artificial Intelligence

BYOD - Bring Your Own Device

CVE - Common Vulnerabilities and Exposures

EMM - Enterprise Mobility Management

GDPR - General Data Protection Regulation

IAM - Identity and Access Management

IoT - Internet of Things

ISMS - Information Security Management System

LAN - Local Area Network

MAM - Mobile Applications Management

MCM - Mobile Content Management

MDM - Mobile Device Management

MFA - Multi-factor Authentication

MitM - Man-in-the-Middle

MTD - Mobile Threat Defense

NIST - National Institute of Standards and Technology

OT - Operational Technology

PUA - Potentially Unwanted Application

SSO - Single sign-on

UEM - Unified Endpoint Management

VPN - Virtual Private Network

ВСТУП

Технологія уніфікованого керування безпекою корпоративних мобільних пристроїв (MDM) стала надзвичайно актуальною у світлі стрімкого зростання використання мобільних технологій у бізнес-середовищі. У сучасному світі, де мобільність, гнучкість та швидкість є ключовими факторами успіху, організації все частіше впроваджують мобільні пристрої в свою щоденну діяльність. Це створює нові можливості, але водночас й виклики, особливо в контексті безпеки даних.

Однією з основних причин актуальності MDM є необхідність захисту конфіденційної інформації. Корпоративні мобільні пристрої, такі як смартфони та планшети, часто містять важливі дані про бізнес, клієнтів і стратегії. В умовах, коли зловмисники стають дедалі витонченішими у своїх підходах до крадіжки інформації, підприємства повинні забезпечити надійний захист від актуальних загроз. MDM дозволяє організаціям централізовано управляти безпекою мобільних пристроїв, впроваджуючи політики безпеки, шифрування даних та контроль доступу.

Крім того, важливим аспектом є відповідність нормативним вимогам, які пов'язані з захистом даних. У багатьох країнах існують законодавчі акти, що регулюють обробку та зберігання персональних даних (наприклад, GDPR у Європейському Союзі). MDM рішення допомагають компаніям відповідати цим вимогам, забезпечуючи контроль за тим, хто має доступ до даних і як вони використовуються.

Зростаюча популярність практики Bring Your Own Device (BYOD) також підкреслює важливість впровадження MDM. Співробітники часто користуються власними пристроями для роботи, що може привести до ризиків, адже ці гаджети можуть бути менш захищеними, ніж корпоративні. Уніфіковане керування дозволяє

інтегрувати особисті пристрої в корпоративну середу, захищаючи інформацію та забезпечуючи контроль над нею.

Інтеграція MDM з іншими системами безпеки є ще одним важливим компонентом. Сучасні рішення можуть забезпечувати взаємодію з іншими елементами безпекової інфраструктури, такими як системи управління доступом, засоби виявлення загроз, що дозволяє створити комплексний, багатоаспектний підхід до забезпечення безпеки. Це дозволяє організаціям швидко реагувати на інциденти, такі як втрата чи крадіжка пристроїв, а також зменшує ризик витоку даних.

Таким чином, технології уніфікованого керування безпекою корпоративних мобільних пристроїв стали невід'ємною складовою сучасного бізнесу, що прагне не лише досягти успіху, але й забезпечити захист своїх даних у складних умовах цифрового середовища. Їх застосування є критично важливим для управління ризиками, збереження конфіденційності та створення надійної інфраструктури безпеки.

Вищесказане визначає актуальність теми даної роботи, основний зміст якої становлять дослідження технології забезпечення уніфікованого керування безпекою корпоративних мобільних пристроїв на базі Sophos Mobile

Об’єкт дослідження – уніфіковане керування безпекою корпоративних мобільних пристроїв.

Предмет дослідження – технологія забезпечення уніфікованого керування безпекою корпоративних мобільних пристроїв на базі Sophos Mobile

Мета роботи – розробити рекомендації щодо забезпечення уніфікованого керування безпекою корпоративних мобільних пристроїв.

Наукові завдання:

дослідити сутність проблеми забезпечення уніфікованого керування безпекою корпоративних мобільних пристроїв;

проаналізувати підходи до забезпечення уніфікованого керування безпекою

корпоративних мобільних пристроїв;

проаналізувати існуючі рішення із забезпечення уніфікованого керування безпекою корпоративних мобільних пристроїв;

проаналізувати методи та засоби забезпечення уніфікованого керування безпекою корпоративних мобільних пристроїв на базі Sophos Mobile;

розкрити порядок реалізації технології забезпечення уніфікованого керування безпекою корпоративних мобільних пристроїв на базі Sophos Mobile.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: запропоновано порядок застосування технології забезпечення уніфікованого керування безпекою корпоративних мобільних пристроїв, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 25 жовтня 2024 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ УНІФІКОВАНОГО КЕРУВАННЯ БЕЗПЕКОЮ КОРПОРАТИВНИХ МОБІЛЬНИХ ПРИСТРОЇВ

1.1. Дослідження проблеми уніфікованого керування безпекою корпоративних мобільних пристроїв

Звіт Verizon Mobile Security Index за 2024 рік містить деякі знайомі теми, як-от збереження віддаленої та гібридної роботи, а також розкриває нові питання безпеки мобільних пристроїв, пов’язані з критично важливими секторами інфраструктури, зростанням розгортання Інтернету речей (IoT) і прогресом штучного інтелекту (AI). (як з точки зору нападу, так і з точки зору захисту). Також було виявлено цікаві відмінності між уявленнями респондентів і реальністю. Багато хто припускає, що у них є надійний мобільний захист і що виправлення інциденту буде швидким і легким. Але те, що ці респонденти насправді повідомляють про атаки та частоту порушень, разом із негативними наслідками порушень і занепокоєннями, говорить про інше. У нашому глибшому дослідженні сектору критичної інфраструктури ми виявили, що неадекватна безпека мобільних пристроїв у будь-якій із 16 визначених галузей критичної інфраструктури може мати значний вплив на організації в цих галузях і може мати низький вплив на громади та окремих осіб, які обслуговуються. З даних опитування можна зробити один головний висновок: зростання мобільних комп’ютерів та Інтернету речей експоненціально розширює поверхню атак, які потребують захисту, що, у свою чергу, вимагатиме відповідного фокусу на забезпеченні достатніх процесів мобільної безпеки, політик та інвестицій [1].

Навіть якщо деякі організації повертають працівників до офісу, парадигма віддаленої або гібридної роботи навряд чи найближчим часом повернеться до свого попереднього стану. Однією з причин є те, що працівники все ще надають перевагу гнучкості, щоб принаймні деякий час працювати віддалено, працювати в

нетрадиційний графік або проводити частину кожного робочого дня в офісі, а частину вдома [1].

Роботодавці в цілому все ще схиляються до дозволу співробітникам працювати віддалено. Незалежно від того, працюєте ви вдома, в аеропорту, готелі чи місцевій кав'ярні, 92% респондентів стверджують, що їхні організації підтримують певну форму віддаленого підключення. Це означає, що мобільні пристрої глибше впроваджені в критично важливі робочі процеси, ніж це було в минулому. 92% офісних працівників цінують можливість працювати за гнучким графіком. 89% організацій мають співробітників, які принаймні деякий час працюють вдома. 83% мають працівників, які дотримуються гібридної моделі роботи. 90% цінують можливість залишати роботу протягом дня з особистих причин. 80% мають працівників, які їздять на роботу. 80% респондентів погоджуються, що мобільні пристрої мають вирішальне значення для безперебійної роботи їхніх організацій. 55% організацій мають більше користувачів із більшою кількістю мобільних пристроїв, ніж 12 місяців тому. 46% респондентів погоджуються, що мобільні пристрої перетворилися з приємного в важливий бізнес-інструмент [1].

Підтримка роботодавцями гнучкої та віддаленої роботи означає, що все більше мобільних пристроїв різних типів регулярно підключаються до корпоративних мереж. Ці пристрої все частіше використовуються для доступу до конфіденційної інформації. 50% кажуть, що мобільні пристрої мають більший доступ до конфіденційної інформації, ніж рік тому. 86% що гнучкість у тому, де люди працюють і якими пристроями вони користуються, є ключовою частиною для залучення найкращих талантів. 86% погоджуються, що збільшення віддаленої роботи перемістило мобільну безпеку на перше місце в їхній програмі [1].

Оскільки мобільні пристрої зараз відіграють дедалі зростаючу роль у корпоративних обчислювальних середовищах, ці екосистеми є складнішими, різноманітнішими та динамічнішими, ніж будь-коли раніше. 62 % автентифікації в

корпоративних мережах надходять із мобільних і нетрадиційних операційних систем – новий рекорд [1].

Оскільки гібридна та віддалена робота стає наріжним каменем політики на робочому місці, а організації все більше залежать від різних типів пристроїв – у більшій кількості місць – стратегічні інвестиції в мобільну безпеку більше не є необов'язковими [1].

Датчики та пристрої IoT застосовуються у величезній кількості випадків використання, що постійно розширюється. Вони допомагають підтримувати заклади в безпеці, пацієнтів та комфорті у лікарнях належним чином спостерігаючи та доглядаючи за ними, а ланцюги поставок безперебійні. Роздрібні продавці використовують їх для відстеження запасів у магазинах, тоді як інші використовують IoT для моніторингу споживання енергії. Іншим популярним випадком використання є прогнозне технічне обслуговування, яке забезпечує більш надійну безвідмовну роботу під час виробничих операцій, наприклад у промисловому чи енергетичному секторах. Організації, які використовують пристрої IoT, використовують їх у середньому більш ніж трьома способами [1].

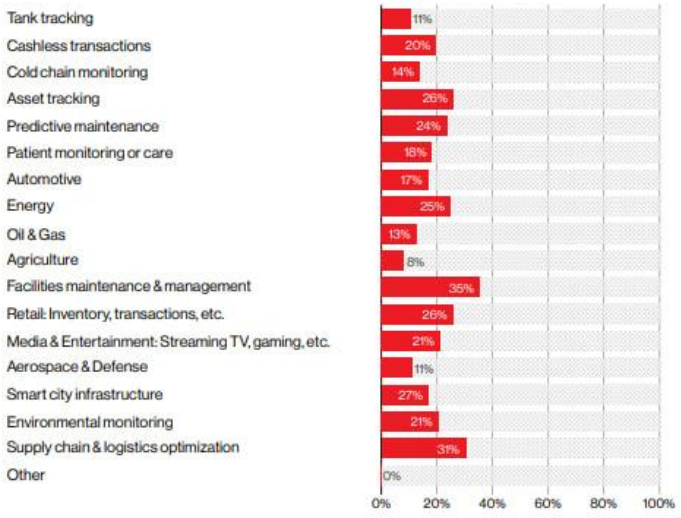


Рис 1.1. Використання датчиків або пристроїв IoT [2]

Національний інститут стандартів і технологій (NIST) описує галузі критичної інфраструктури як такі, що забезпечують «основу для економіки, безпеки

та охорони здоров'я суспільства». Таким чином, ці сектори часто є головною мішенню для суб'єктів загрози національних держав, особливо за NIST. Ті, які зосереджені на підриві національної та громадської безпеки, оскільки операції критичної інфраструктури вважаються важливими для національної безпеки. Сьогодні широке та зростаюче використання датчиків IoT та пристроїв, підключених до Інтернету, також може збільшити кіберризики [11].

Пристрої та датчики IoT сьогодні використовуються для моніторингу та контролю всіх типів активів, об'єктів і систем у широкому діапазоні критичних процесів, підвищуючи ефективність, безпеку та стійкість. Пристрої IoT забезпечують прогнозне технічне обслуговування в промислових середовищах і можуть виявляти збій обладнання на ранній стадії, перш ніж він призведе до простою. Вони також використовуються для підвищення безпеки працівників, одночасно зменшуючи потребу в ручному втручанні [2].

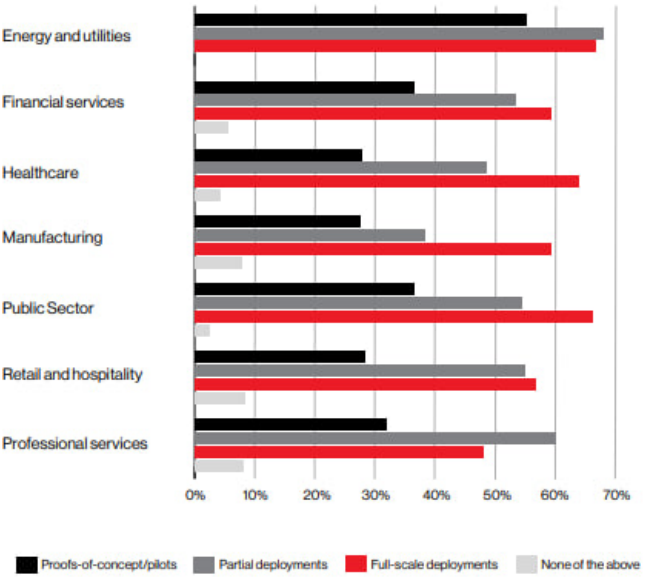


Рис 1.2. Залученість IoT у різноманітних сферах [2]

Пристрої IoT також використовуються для перетворення мереж електропостачання на розумні мережі, перетворюючи мегаполіси на розумні міста та роблячи багато типів громадських об'єктів безпечнішими та комфортнішими. І це лише верхівка айсберга використання IoT у критично важливих

інфраструктурних операціях. У результаті впровадження IoT стрімко поширюється майже в усіх секторах критичної інфраструктури [2].

Пристрої IoT часто мають слабкий захист і слабке підключення до мережі. Це робить їх існування розширенням поверхні атаки. Ця експозиція особливо занепокоєна для організацій критичної інфраструктури, які вже є привабливими цілями для деяких із найдосконаліших і найкраще забезпечених джерелами загроз у світі. Пристрої IoT все ще не підлягають управлінню активами або моніторингу безпеки в усіх організаціях. Пристрої IoT, як правило, відстежують застаріле обладнання в середовищах операційних технологій (OT), де можуть бути відсутні сучасні функції безпеки – це звичайна реальність у галузях критичної інфраструктури [2].

Багато вразливостей безпеки Інтернету речей існують з моменту виготовлення пристрою. Багато з них постачаються зі слабкими паролями за замовчуванням, і зміна їх часто не є інтуїтивно зрозумілою. Деякі пристрої мають облікові дані, вбудовані в мікропрограму, тому їх неможливо змінити. Інші можуть взагалі не використовувати автентифікацію. І оскільки пристрої IoT розроблені таким чином, щоб споживати невелику кількість електроенергії для зниження витрат і продовження терміну служби батареї, їх можливості обробки вкрай обмежені. Це обмеження означає, що вони не можуть запускати програми захисту від зловмисного програмного забезпечення або шифрувати дані, які передаються між корпоративними мережами. Підключення до мережі домінує у викликах безпеки IoT. Багато пристроїв розроблено для автоматичного підключення до найближчої Wi-Fi або локальної мережі (LAN), потенційно перетворюючи кожен пристрій на просту та привабливу точку входу для зловмисників, які шукають сходинку до більш широких мереж. У той же час може бути складно захистити зв’язок між пристроями IoT і хмарними програмами. Також часто буває важко доставити й інсталювати оновлення безпеки на пристрої в польових умовах. Відсутність загальногалузевих стандартів безпеки для пристроїв IoT та їхніх

протоколів зв’язку підвищує ризики безпеки, так само як і наявність багатьох пристроїв, встановлених у віддалених місцях, де вони можуть бути вразливими до фізичного втручання [2].

Впровадження IoT широко поширене в секторах критичної інфраструктури, де майже всі респонденти повідомляють, що вони використовують принаймні деякі пристрої IoT. Більше половини респондентів у секторах критичної інфраструктури повідомляють, що вони стикалися зі значними інцидентами безпеки, пов’язаними з мобільними пристроями або пристроями Інтернету речей. Під «значними інцидентами безпеки» ми маємо на увазі інциденти, що призводять до втрати даних або простою системи. Респонденти в організаціях критичної інфраструктури усвідомлюють серйозність ризиків, з якими вони стикаються. Більшість з них розуміють наслідки порушення безпеки, і вони бачать поширення мобільних пристроїв і пристроїв Інтернету речей як серйозну проблему безпеки. Тим не менш, швидке впровадження продовжується [2].

Організації з критично важливою інфраструктурою бачать велику користь від ефективності та видимості, які приносить IoT. В енергетичному секторі датчики допомагають працівникам виявляти відключення ліній електропередач і електростанцій. Використовуючи аналітику даних, постачальники електроенергії можуть краще спрямовувати електроенергію в мережу, щоб збалансувати попит і пропозицію, одночасно допомагаючи максимізувати інтеграцію відновлюваних джерел енергії. Інтелектуальні лічильники та термостати все частіше з’являються вдома та на підприємствах, надаючи дані, які комунальні компанії тепер використовують для покращення послуг. Не дивно, що впровадження IoT майже повсюдно в енергетичному та комунальному секторах. Але для цих організацій надзвичайно важливо розробити розумні стратегії управління ризиками, оскільки суб’єкти загрози дедалі частіше демонструють бажання атакувати їх. Щоб оцінити величезну геополітику, не дивіться далі, окрім атаки програми-вимагача Colonial Pipeline, удару безпілотника Saudi Aramco або диверсії на трубопроводах Nord

Stream [2].

Державний сектор також стикається зі значними ризиками безпеки, пов’язаними з мобільними пристроями та Інтернетом речей. Відповідно до Звіту про розслідування витоків даних за 2024 рік, державне управління є основною мішенню для організованої злочинності разом із пов’язаними з державою суб’єктами загрози (разом відповідальні за 96% порушень, спричинених зовнішніми суб’єктами, у яких тип суб’єкта був відомий, n=305). Тридцять відсотків порушень у цьому секторі (якщо відомо) були вмотивовані шпигунством [2].

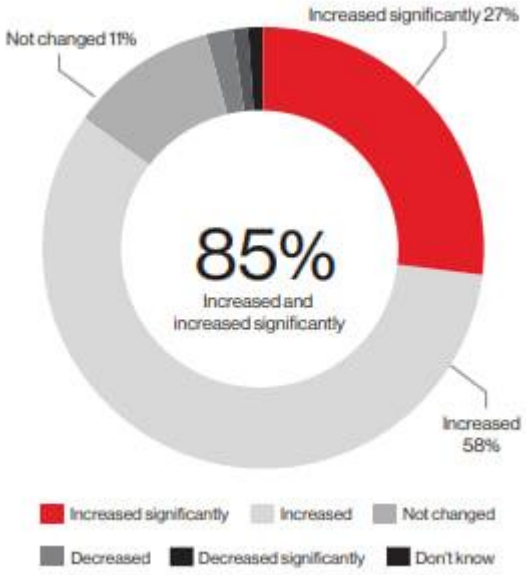


Рис. 1.3. Очікуваний ризик безпеки мобільного пристрою [2]

З тих пір, як було запущено звіт сім років тому, існувала тенденцію до постійного зростання відсотка компаній, які постраждали від зламу мобільних пристроїв, з менш ніж 30% у 2018 році до більш ніж половини (53%) сьогодні. Частково це збільшення пов’язане із розширенням поверхні атаки. Оскільки мобільні пристрої та пристрої Інтернету речей вбудовані в усі типи робочих процесів, величезна кількість пристроїв і додатків, на які підприємства покладаються (як і ризики), залежить від них [2].

У той же час, поряд з номерами пристроїв, також зросла обізнаність про

ризики безпеки мобільних пристроїв. Багато людей колись вважали, що мобільні пристрої за своєю суттю безпечніші, ніж настільні чи портативні комп'ютери. Більше ні. Переважна більшість респондентів (85%) зараз визнають, що загрози для мобільних пристроїв зростають, і більше половини опитаних стикалися з інцидентами безпеки безпосередньо [2].

Для бізнес-користувачів і споживачів 2023 рік став рекордним за кількістю мобільних загроз. В iOS було виявлено більше вразливостей нульового дня, ніж будь-коли раніше. Ризиковані політики збору даних, які використовували такі популярні додатки, як TikTok і PinDuoDuo, були оприлюднені, а 75% організацій стикалися зі спробами мобільного фішингу, націленими на своїх співробітників. 33% мобільних фішингових атак на співробітників технологічних компаній у 2023 році були успішними. 27% мобільних фішингових атак проти фінансового сектору вдалося. 21% мобільних фішингових атак, націлених на медіа та комунікаційні компанії, вдалося [2].

У 2023 році майже кожне оновлення iOS, яке користувачам було запропоновано встановити на своїх смартфонах, містило вразливість у безпеці. У 2023 році було опубліковано понад 260 поширених уразливостей і вразливостей iOS (CVE). Оскільки так багато операційних систем мобільних пристроїв не оновлюються, часто, як і повинно бути, дані та особиста інформація, що зберігаються на них або доступні через них, залишаються сприйнятливими до експлойтів протягом тривалих періодів часу. А кількість атак, які використовували вразливості як критичний шлях для ініціювання злому, зросла майже втричі (збільшення на 180%) у 2023 році порівняно з попереднім роком. Частково це зростання пояснюється надзвичайно успішними широко поширеними кампаніями, такими як програма-вимагач Cl0p [2].

Найпопулярніші вразливості Android у 2023 [2]:

CVE-2023-5217: уразливість у бібліотеці відеокодексів, яка використовується Chrome, Firefox і Firefox Focus для Android;

CVE-2023-6345: уразливість у механізмі 2D-графіки для Google Chrome, Chrome OS, Android і Microsoft Edge;

CVE-2023-3019: уразливість нульового дня в механізмі JavaScript V8 Chromium впливає на версії мобільних браузерів Google Chrome і Microsoft Edge;

CVE-2023-2033_2136: група вразливостей, деякі з яких впливають на пристрої Samsung, а інші – на всі пристрої Android;

CVE-2023-4863: уразливість у форматі зображення WebP Chrome для Android. Подібна вразливість обробки зображень, BlastPass, була використана для доставки шпигунського програмного забезпечення.

Наша постійна залежність від мобільних пристроїв і стрімке зростання використання Інтернету речей створюють можливості для зловмисників скористатися ключовими вразливими місцями, включаючи ще не виявлені атаки нульового дня. Переважна більшість респондентів (93%) висловлюють стурбованість ризиками мобільної кібербезпеки. Тим не менш, меншість (39%) визначили загальноорганізаційні стандарти IoT, і ще менше (37%) стверджують, що їхні організації централізовано координують проекти IoT. Визначення та дотримання міжорганізаційних стандартів має вирішальне значення для того, щоб пристрої та датчики Інтернету речей могли відповідати змінним вимогам безпеки та нормативним вимогам. Зважаючи на величезну різноманітність можливостей пристроїв, випадків використання та ризиків, важливо встановити технічні та нетехнічні стандарти для кожного проекту IoT у кожному бізнес-підрозділі [2].

Сьогодні дані є критично важливими для сучасних підприємств, і створення ефективної стратегії безпеки даних є необхідним для захисту та бізнесу. Раніше організації покладалися на приватні дата-центри з серверами та мережевим обладнанням, що вимагало постійних оновлень і було вразливим до атак. Зараз більшість корпоративних даних зберігається в хмарі, що зменшує проблеми з підтримкою, але збільшує ризики, пов'язані з неправильними налаштуваннями систем. З переходом до хмарних технологій традиційні атаки з використанням

шкідливого ПЗ втратили свою ефективність, і зловмисники почали використовувати соціальну інженерію, націлюючись на мобільні пристрої для викрадення облікових даних. Це дозволяє їм швидко отримувати доступ до критично важливої інфраструктури. Яскраві приклади - атаки на MGM Resorts, Caesars Entertainment і Twilio, де група Scattered Spider використовувала фішинг-кит Oktapus. Інша група використовувала CryptoChameleon для атак на FCC, Coinbase та інші. Успішний фішинговий напад призводить до швидкого доступу до хмарної інфраструктури, скорочуючи час атаки з місяців до хвилин. Це загрожує не лише організаціям, але й особам, які ризикують стати жертвами крадіжки особистих даних. Для захисту від таких швидких атак підприємствам необхідно забезпечити видимість та автоматизовані механізми реагування на мобільних пристроях і в хмарних додатках [2].

Незважаючи на зростаюче занепокоєння щодо будь-чого: від ризиків злому до атак із мобільних пристроїв і потенційних загроз штучного інтелекту, дані опитування змушують нас вважати, що ступінь занепокоєння, виявлений респондентами, часто не відповідає ризикам [2].

Респонденти повідомляють про високий рівень впевненості в своїх мобільних засобах захисту в ряді сфер. Наприклад, вони висловлюють велику віру в те, що поточні заходи безпеки мобільних пристроїв ефективні, причому 96% стверджують, що їхній захист принаймні певною мірою ефективний [2].

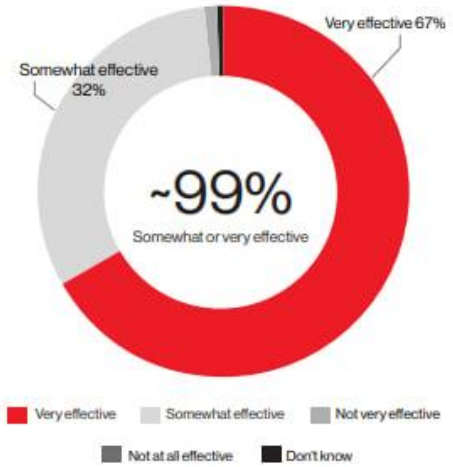


Рис. 1.4. Ефективність заходів безпеки мобільних пристроїв [2]

Незважаючи на висловлену впевненість у своїй здатності захищати від мобільних загроз і відновлюватися після інцидентів, респонденти водночас посилаються на постійні занепокоєння мобільною безпекою. Майже половина вважає, що кінцеві користувачі самовдоволено ставляться до конфіденційності та безпеки даних, не помічають небезпеки крадіжки облікових даних і, як правило, не дотримуються гігієни безпеки [2].

Частково проблема може полягати в тому, що респонденти просто не знають того, чого вони не знають. З поширенням тіньових IT, невеликим централізованим IT-наглядом за проектами Інтернету речей і багатьма співробітниками, які вибирають власний підхід до домашнього та загальнодоступного Wi-Fi-підключення, зацікавлені сторони безпеки стикаються з надскладною проблемою точної оцінки ризиків [2].

Хоча опитування висвітлює деякі тривожні тенденції, є й хороші новини, якими можна поділитися. Оскільки широкомасштабні атаки програм-вимагачів і витоки даних тепер регулярно стають заголовками газет, зацікавлені сторони звернули увагу на це. Витрати на безпеку мобільних пристроїв збільшуються протягом багатьох років, і темпи, ймовірно, збільшаться, оскільки більша обізнаність про ризики та вартість зломів спонукає організації централізувати засоби контролю, стандартизувати політику безпеки та розгортати ефективні рішення [2].

Інвестиції в захист мобільних пристроїв і пристроїв Інтернету речей зростають. Насправді понад чотири з п’яти організацій (84%) збільшили витрати на безпеку мобільних пристроїв за останній рік. Збільшення було зумовлено зростанням обсягу та більшою обізнаністю про загрози, а також збільшенням віддаленої роботи. Витрати, ймовірно, також збільшаться в бюджеті наступного року, що є обнадійливим знаком того, що все більше організацій приділяють більшу увагу безпеці мобільних пристроїв [2].

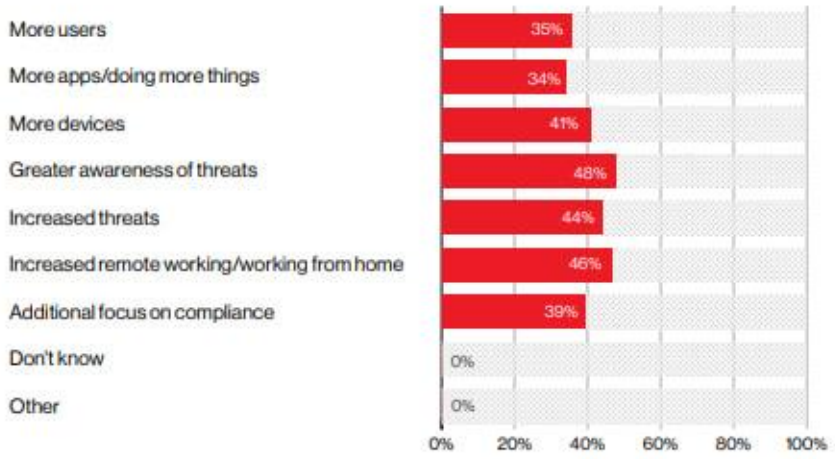


Рис. 1.5. Причини збільшення витрат на мобільну безпеку [2]

Також хороші новини: організації критичної інфраструктури збільшують свої витрати, щоб зрівнятися з іншими секторами або перевищити їх. 84% опитаних сказали, що витрати на мобільну безпеку зросли за останній рік. І ще більш імовірно, що вони планують інвестувати більше в наступному році. Оскільки зростаюча важливість штучного інтелекту для кіберзахисту широко визнана, деякі з цих інвестицій, ймовірно, будуть спрямовані на рішення на базі штучного інтелекту [2].

У MSI 2022 року 53% організацій, які відповіли, визначили стандарти безпеки IoT, які застосовуються до всіх проектів, а 48% організацій централізовано координували всі свої проекти IoT. Цього року лише 39% респондентів сказали, що вони визначили стандарти безпеки IoT які стосуються всіх проектів, і лише 47% мають централізовану координацію всіх проектів IoT. Ймовірно, це зменшення пов’язано з надзвичайно швидкими темпами впровадження IoT. Коли ви рухаєтеся швидко, охороні може бути важко встигати. Зниження також може бути свідченням тіньових IT-проектів, коли окремі напрямки бізнесу координують власні проекти без повного централізованого контролю. Незалежно від того, як ви це розрізаєте, значні прогалини в політиці безпеки залишаються, що призводить до більш високого рівня кіберризику [2].

У звіті також наголошується на важливості впровадження розширених

інфраструктур безпеки, таких як модель Zero Trust, і дотримання таких стандартів, як NIST Cybersecurity Framework і NIS2 Директива ЄС, щоб зменшити ці ризики. Крім того, розвиток Інтернету речей вимагає стратегічної еволюції в плануванні кібербезпеки, особливо тому, що компанії продовжують інтегрувати все більше датчиків і пристроїв у свої мережі [2].

У відповідь на ці виклики 84% опитаних організацій збільшили свої витрати на мобільну безпеку, а майже 90% учасників критичної інфраструктури планують інвестувати більше в найближчому майбутньому[2].

У цьому звіті підкреслюється нагальна потреба компаній адаптувати свої стратегії безпеки до загроз мобільних пристроїв та Інтернету речей, що постійно розвиваються[2].

1.2. Аналіз підходів до уніфікованого керування безпекою корпоративних мобільних пристроїв

Управління мобільними пристроями (MDM) – це перевірена методологія та набір інструментів, які надають робочій силі інструменти та програми для підвищення продуктивності мобільних пристроїв, зберігаючи корпоративні дані в безпеці. Завдяки зрілій платформі MDM відділи IT і безпеки можуть керувати всіма пристроями компанії, незалежно від їх операційної системи. Ефективна платформа MDM допомагає захищати всі пристрої, зберігаючи гнучкість і продуктивність робочої сили [3].

Останніми роками мобільні пристрої стали широко поширеними на підприємствах. Компанії та їхні працівники покладаються на мобільні пристрої, такі як смартфони, планшети та ноутбуки, для виконання широкого спектру завдань. І оскільки віддалена робота стала важливою, мобільні пристрої стали невід’ємною частиною більшості організацій, будучи життєво важливими інструментами продуктивності та ефективності. Але оскільки корпоративні

мобільні пристрої отримують доступ до критично важливих бізнес-даних, вони можуть загрожувати безпеці в разі злому, викрадення або втрати. Таким чином, важливість керування мобільними пристроями зросла так, що керівникам IT та безпеки тепер доручено надавати, керувати та захищати мобільні пристрої у відповідних корпоративних середовищах [3].

Поширене запитання в Інтернеті таке: «Чи є керування мобільними пристроями частиною програмного забезпечення?» Коротка відповідь: «так» і «ні». MDM – це рішення, яке використовує програмне забезпечення як компонент для надання мобільних пристроїв, одночасно захищаючи активи організації, наприклад дані. Організації практикують MDM, застосовуючи програмне забезпечення, процеси та політики безпеки на мобільних пристроях та їхньому використанні. Окрім керування інвентаризацією пристрою та наданням доступу, рішення MDM захищають програми, дані та вміст пристрою. У цьому сенсі MDM і мобільна безпека схожі. Однак MDM – це підхід, орієнтований на пристрій, тоді як мобільна безпека та уніфіковане керування кінцевими точками розвинулися до позиції, орієнтованої на користувача. У програмі MDM співробітники можуть отримати спеціальний робочий пристрій, як-от ноутбуки чи смартфони, або віддалено зареєструвати персональний пристрій. Персональні пристрої отримують рольовий доступ до корпоративних даних і електронної пошти, захищений VPN, GPS-відстеження, захищені паролем програми та інше програмне забезпечення MDM для оптимальної безпеки даних. Потім програмне забезпечення MDM може відстежувати поведінку та критично важливі для бізнесу дані на зареєстрованих пристроях. А з більш складними рішеннями MDM машинне навчання та ШІ можуть аналізувати ці дані. Ці інструменти захищають пристрої від шкідливих програм та інших кіберзагроз. Наприклад, фірма може призначити ноутбук або смартфон співробітнику або консультанту, у якому попередньо запрограмовано профіль даних, VPN та інше необхідне програмне забезпечення та програми. У цьому сценарії MDM пропонує найбільший контроль роботодавцю. За допомогою

інструментів MDM підприємства можуть відстежувати, контролювати, усувати неполадки та навіть видаляти дані пристрою у разі крадіжки, втрати чи виявлення злому. Отже, що таке політики керування мобільними пристроями? Політика MDM відповідає на питання про те, як організації керуватимуть мобільними пристроями та регулюватимуть їх використання. Щоб налаштувати та опублікувати свої політики та процеси, підприємства ставитимуть такі запитання, як: Чи потрібен пристрої захист паролем? Чи камери потрібно вимкнути за замовчуванням? Чи важливе підключення до Wi-Fi? Які можливості налаштування надасть пристрій? Чи потрібно огороджувати певні пристрої [3]?

Компоненти засобів керування мобільними пристроями [3]

Відстеження пристрою

Кожен пристрій, який підприємство реєструє або випускає, можна налаштувати для включення GPS-відстеження та інших програм. Програми дозволяють IT-фахівцям підприємства контролювати, оновлювати та усувати неполадки пристрою в режимі реального часу. Вони також можуть виявляти пристрої високого ризику або несумісні з ними та повідомляти про них, а також віддалено блокувати або стирати дані з пристрою, якщо він загублений чи вкрадений.

Мобільний менеджмент

IT-відділи закуповують, розгортають, керують і підтримують мобільні пристрої для своїх співробітників, включаючи усунення несправностей функціональних пристроїв. Ці відділи гарантують, що кожен пристрій постачається з необхідними операційними системами та програмами для своїх користувачів, включаючи програми для продуктивності, безпеки та захисту даних, резервного копіювання та відновлення.

Безпека програми

Безпека програми може включати упаковку програми, під час якої IT-адміністратор застосовує до програми функції безпеки або керування. Потім цю

програму повторно розгортають як контейнерну програму. Ці функції безпеки можуть визначити, чи потрібна автентифікація користувача для відкриття програми; чи можна копіювати, вставляти або зберігати дані з програми на пристрої; і чи може користувач ділитися файлом.

Управління ідентифікацією та доступом

(IAM) Безпечне керування мобільними пристроями вимагає надійного керування ідентифікацією та доступом (IAM). IAM дозволяє підприємству керувати ідентифікаторами користувачів, пов'язаними з пристроєм. Доступ кожного користувача в організації можна повністю регулювати за допомогою таких функцій, як єдиний вхід (SSO), багатофакторна автентифікація та рольовий доступ. Безпека кінцевих точок охоплює всі пристрої, які мають доступ до корпоративної мережі, включаючи переносні пристрої, датчики Інтернету речей (IoT) і нетрадиційні мобільні пристрої. Безпека кінцевої точки може включати стандартні інструменти безпеки мережі, такі як антивірусне програмне забезпечення та контроль доступу до мережі та реагування на інциденти, фільтрування URL-адрес і безпеку в хмарі.

Принесіть власний пристрій

Принесіть свій власний пристрій (BYOD) означає, що співробітники використовують для роботи свої особисті мобільні пристрої замість пристроїв, виданих компанією. Застосування корпоративної безпеки на персональному мобільному пристрої складніше, ніж просто надання таких пристроїв. Але BYOD популярний, особливо серед молодих працівників. Організації йдуть на такий компроміс, щоб підвищити задоволеність і продуктивність працівників. BYOD також може зробити мобільну робочу силу доступнішою, оскільки позбавляє від необхідності купувати додаткове обладнання.

Управління мобільністю підприємства

Управління мобільністю підприємства (EMM) (посилання знаходиться за межами ibm.com) описує ширшу форму керування мобільними пристроями. Виходячи за рамки самого пристрою, його користувача та даних, EMM охоплює

керування додатками та кінцевими точками, а також BYOD. Рішення EMM мають високу масштабованість, а завдяки новим функціям безпеки на основі штучного інтелекту ці рішення можуть пропонувати статистику в реальному часі та сповіщення про тисячі поведінки та дій, що надходять із кількох джерел одночасно.

Уніфіковане керування кінцевими точками

Уніфіковане керування кінцевими точками (UEM) являє собою інтеграцію та еволюцію MDM і EMM. Він вирішує більше проблем, пов'язаних із безпекою Інтернету речей, комп'ютерів чи інших мобільних пристроїв. Рішення UEM можуть допомогти підприємствам захистити та контролювати все IT-середовище та його кінцеві точки, такі як смартфони, планшети, ноутбуки та настільні ПК. Рішення UEM також можуть допомогти захистити особисті та корпоративні дані, програми та вміст користувачів. Завдяки гнучкій системі UEM підприємства можуть вибирати масштабовані рішення на основі потреб, незалежно від того, чи охоплюють ці підприємства одну операційну систему чи різні пристрої на різних платформах, наприклад Apple iOS iPhone, Android, Microsoft Windows, macOS і Chrome OS. Досконалі рішення UEM базуються на машинному навчанні та штучному інтелекті, що може допомогти IT-відділу підприємства швидко приймати рішення щодо безпеки на основі даних у реальному часі та аналітики.

Незалежно від того, чи це хмарна модель, чи локальна модель, рішення MDM повинні дозволяти організації бачити кінцеві точки, користувачів і все, що між ними. Гарне програмне забезпечення для керування мобільними пристроями: економте час, підвищення ефективності, збільшити виробництво, підвищення безпеки, простота загальної системи мобільного керування [3].

Ось три найкращі практики, які слід враховувати при виборі рішення MDM [3]:

Автоматичні звіти

Переконайтеся, що інструмент звітування та інвентаризації об'єднує всі зареєстровані пристрої та пов'язану інформацію у звіти, які легко використовувати.

Щоденні оновлення мають генеруватися автоматично без ручного введення.

Автоматичні оновлення

Крім переваг миттєвої доступності, яку надає хмарне MDM, не потрібно ані відповідних комісій, ані придбання, встановлення чи обслуговування обладнання. Платформа повинна автоматично оновлюватися новими функціями, які є в розпорядженні компанії.

Легкий пошук

Здатність шукати будь-що і будь-що є ключовою для хмарного рішення. Організація повинна мати легкий доступ до своїх пристроїв, інтеграцій, звітів, програм і захищених документів.

Управління безпекою мобільних корпоративних пристроїв є критично важливим для забезпечення захисту даних та запобігання кіберзагрозам. Деякі з ключових рішень для зміцнення безпеки включають наступні стратегії [3]:

Впровадження політики "Zero Trust"

Ця модель передбачає перевірку кожного користувача та пристрою перед наданням доступу до корпоративних ресурсів. Для мобільних пристроїв це означає обов'язкове підтвердження автентичності через багатофакторну автентифікацію (MFA), перевірку стану пристрою та моніторинг поведінки користувачів. Це знижує ризики несанкціонованого доступу.

Мобільне управління пристроями (MDM)

Системи управління мобільними пристроями дозволяють контролювати, оновлювати, блокувати або видаляти корпоративні дані з мобільних пристроїв дистанційно. MDM дозволяє адміністратору конфігурувати політики безпеки, шифрувати дані та слідкувати за активністю пристроїв. Це особливо корисно в умовах розширення роботи з дому.

Шифрування даних

Шифрування є ключовим методом захисту даних на мобільних пристроях. Воно гарантує, що навіть у разі втрати або крадіжки пристрою, дані залишаться

захищеними. Шифрування повинне застосовуватися як для зберігання даних на пристрої, так і для передавання даних в мережі.

Розмежування особистих і робочих даних (контейнери)

Використання спеціальних "контейнерів" на мобільних пристроях для ізоляції корпоративних даних від особистих дозволяє забезпечити більший контроль та безпеку робочої інформації. Ця методика полегшує управління пристроями та дозволяє компаніям не впливати на приватне життя співробітників.

Антивірусне програмне забезпечення та захист від загроз

На кожному корпоративному мобільному пристрої повинне бути встановлене антивірусне ПЗ, яке автоматично оновлюється. Важливо також використовувати рішення, які вміють виявляти нові типи загроз, такі як шкідливі програми для мобільних пристроїв або атаки через SMS (фішинг).

Навчання та підвищення обізнаності працівників

Безпека багато в чому залежить від обізнаності користувачів. Регулярні тренінги щодо кібербезпеки, навчання з виявлення фішингових атак, безпечного використання мобільних додатків та оновлення пристроїв є необхідними для мінімізації людського фактору.

Впровадження штучного інтелекту (AI) для виявлення загроз

AI може аналізувати поведінку користувачів, виявляти аномалії та автоматично реагувати на підозрілі дії. Такі технології корисні для захисту від складних атак, таких як підробка (deepfake) або атак через фальшиві SMS (фішинг).

Віддалене блокування та очищення даних

У разі втрати або крадіжки пристрою, компанія повинна мати можливість дистанційно заблокувати пристрій або повністю стерти всі корпоративні дані, щоб запобігти їх витоку.

Кожен із цих заходів дозволяє ефективно зменшити ризики, пов'язані з мобільною безпекою, і захистити компанію від сучасних кіберзагроз.

Технологія уніфікованого керування безпекою корпоративних мобільних

пристроїв охоплює стандарти, що спрямовані на управління мобільними пристроями, забезпечення конфіденційності, безпеки даних та відповідності нормативним вимогам. Основні стандарти, пов’язані з безпекою мобільних пристроїв і технологіями керування, включають:

NIST SP 800-124 Revision 2 (Guidelines for Managing the Security of Mobile Devices in the Enterprise)

Національний інститут стандартів і технологій США (NIST) надає рекомендації щодо управління безпекою мобільних пристроїв, зокрема впровадження політик для керування мобільними пристроями, шифрування даних, використання VPN, а також застосування антивірусного програмного забезпечення. Документ також охоплює важливі аспекти віддаленого керування і захисту даних
Стандарт NIST SP 800-124 Revision 2 стосується уніфікованого управління безпекою корпоративних мобільних пристроїв і надає рекомендації щодо забезпечення безпеки мобільних пристроїв у корпоративних середовищах. Основні аспекти цього стандарту включають наступне:

Розробка політик безпеки мобільних пристроїв

Стандарт підкреслює важливість створення чітких політик для мобільних пристроїв у компанії, які охоплюють використання особистих та корпоративних пристроїв, методи захисту даних і взаємодію з корпоративними системами. Це забезпечує контроль над тим, як мобільні пристрої підключаються до корпоративних мереж та отримують доступ до конфіденційної інформації.

Управління ризиками

Ключовою частиною стандарту є аналіз та управління ризиками. Це включає визначення можливих загроз для мобільних пристроїв (втрати, крадіжки, несанкціонований доступ) та їхнє вчасне виявлення. NIST рекомендує використовувати регулярний моніторинг пристроїв, оцінку їхнього стану безпеки та впровадження механізмів захисту від загроз.

Управління пристроями через Mobile Device Management (MDM)

NIST SP 800-124 рекомендує використовувати рішення Mobile Device Management (MDM), які забезпечують централізоване управління мобільними пристроями. Це дозволяє адміністраторам дистанційно керувати налаштуваннями пристроїв, застосовувати політики шифрування, блокувати пристрої в разі втрати або крадіжки, а також контролювати доступ до корпоративних додатків та інформації.

Захист даних

Стандарт наголошує на важливості шифрування даних, зокрема використання шифрування для зберігання інформації на пристрої та для захисту переданих даних. Використання VPN та інших засобів захисту мережевих з'єднань також рекомендується для забезпечення захисту від атак на комунікаційні канали.

Аутентифікація та контроль доступу

Мобільні пристрої повинні підтримувати багатофакторну автентифікацію (MFA) для доступу до корпоративних систем. Це забезпечує надійний контроль доступу до конфіденційних даних і знижує ризики несанкціонованого проникнення.

Моніторинг і виявлення загроз

Стандарт радить застосовувати рішення для постійного моніторингу активності мобільних пристроїв та використання аналітики для виявлення аномалій або можливих загроз. Використання засобів виявлення шкідливих програм та загроз також є важливим компонентом захисту мобільних пристроїв.

Віддалене блокування та видалення даних

Одним із ключових елементів безпеки є можливість віддалено блокувати пристрій або видаляти корпоративні дані у разі втрати чи крадіжки. Це мінімізує ризики витоку конфіденційної інформації.

Оновлення програмного забезпечення

Регулярне оновлення операційних систем і додатків мобільних пристроїв є критичним для запобігання вразливостям, які можуть бути використані хакерами для отримання доступу до корпоративних мереж.

Цей стандарт пропонує комплексний підхід до управління безпекою мобільних пристроїв, охоплюючи не лише технічні заходи, але й процеси та політики, які мають бути впроваджені для мінімізації ризиків.

ISO/IEC 27001

Міжнародний стандарт ISO/IEC 27001 задає вимоги до систем управління інформаційною безпекою (ISMS), які можуть застосовуватися до мобільних пристроїв. Він фокусується на управлінні ризиками, що виникають у мобільному середовищі, і надає рамки для впровадження політик безпеки мобільних пристроїв, включно з використанням VPN, шифруванням та контролем доступу

Стандарт ISO/IEC 27001 є міжнародним стандартом для систем управління інформаційною безпекою (ISMS), який може застосовуватися до корпоративних мобільних пристроїв. Основні аспекти ISO/IEC 27001 в контексті уніфікованого керування безпекою мобільних пристроїв охоплюють:

Політики безпеки інформації

ISO/IEC 27001 вимагає від організацій встановлення політик інформаційної безпеки, що охоплюють мобільні пристрої. Це включає визначення вимог щодо доступу до корпоративних даних, шифрування та моніторинг пристроїв для мінімізації ризиків витоку даних. Політики повинні враховувати як особисті, так і корпоративні пристрої, з огляду на зростання використання моделі Bring Your Own Device (BYOD)

Оцінка ризиків

Стандарт ISO/IEC 27001 ставить у центр уваги процес оцінки ризиків, що пов’язані з використанням мобільних пристроїв у корпоративній мережі. Організації повинні ідентифікувати потенційні загрози, пов'язані з втратами даних, вразливістю до атак або витоком інформації, та запровадити механізми для їх зниження.

Контроль доступу

ISO/IEC 27001 передбачає впровадження надійних механізмів контролю

доступу для мобільних пристроїв, таких як багатофакторна автентифікація (MFA). Це дозволяє гарантувати, що лише авторизовані користувачі можуть отримати доступ до конфіденційних даних компанії. У мобільних рішеннях також використовуються методи ідентифікації користувачів та пристроїв.

Управління активами

Організація повинна мати чіткий контроль над мобільними пристроями, які використовуються для доступу до корпоративної мережі. ISO/IEC 27001 наголошує на необхідності реєстрації всіх активів (мобільних пристроїв), що підключаються до корпоративної системи, а також їхньої перевірки на наявність засобів захисту. Важливо розмежовувати робочі та особисті дані на пристроях.

Шифрування та захист даних

Одна з ключових вимог ISO/IEC 27001 – це захист даних на мобільних пристроях через шифрування як під час зберігання, так і під час передачі. Використання VPN і захищених каналів зв'язку також є важливим елементом для безпечного доступу до корпоративних даних через мобільні пристрої.

Управління інцидентами

Організації повинні мати чіткі процедури реагування на інциденти безпеки, пов'язані з мобільними пристроями. Це включає моніторинг, виявлення та усунення потенційних загроз. Важливим аспектом є наявність плану дій у разі втрати пристрою або компрометації даних, включно з віддаленим блокуванням пристроїв і видаленням даних.

Моніторинг та аудит

Стандарт ISO/IEC 27001 вимагає постійного моніторингу безпеки мобільних пристроїв і регулярного проведення аудиту, щоб переконатися в дотриманні політик безпеки. Це передбачає активне використання систем моніторингу та виявлення загроз, щоб мінімізувати ризики вразливостей у мобільному середовищі.

Навчання працівників

ISO/IEC 27001 рекомендує постійне навчання працівників, що використовують

мобільні пристрої, з питань кібербезпеки. Співробітники мають бути обізнані щодо ризиків, пов’язаних з фішингом, шкідливим ПЗ та використанням незахищених мереж.

Відповідність нормативним вимогам

ISO/IEC 27001 забезпечує відповідність нормативним вимогам щодо захисту даних (наприклад, GDPR для ЄС), що важливо для організацій, які працюють з мобільними пристроями, підключеними до корпоративних мереж.

Переваги впровадження ISO/IEC 27001:

- Стандарт забезпечує комплексний підхід до управління інформаційною безпекою, що включає захист мобільних пристроїв, а також відповідність нормативним вимогам;

- покращена здатність компаній швидко реагувати на кіберзагрози та захищати конфіденційну інформацію, яка може зберігатися або передаватися через мобільні пристрої.

European Union NIS2 Directive

Директива ЄС NIS2 визначає правила для покращення кібербезпеки в європейських організаціях, зокрема впровадження безпечного управління мобільними пристроями. Вона зобов’язує організації впроваджувати кращі практики безпеки для мобільних пристроїв, такі як шифрування, контроль доступу, багатофакторну автентифікацію та управління загрозами.

Директива NIS2 Європейського Союзу (Network and Information Security Directive 2) є оновленням попередньої NIS-директиви і спрямована на підвищення рівня кібербезпеки в Європейському Союзі. Вона впроваджує суворіші вимоги щодо безпеки критичних інформаційних систем та мереж, включаючи мобільні пристрої в корпоративному середовищі. Ось як основні аспекти NIS2 можуть бути застосовані до технології уніфікованого керування безпекою мобільних пристроїв:

Розширення суб'єктів дії директиви

NIS2 розширює список суб'єктів, які підпадають під дію директиви,

охоплюючи більшу кількість галузей та організацій. Це стосується підприємств, що використовують мобільні пристрої для обробки критичних даних або надання ключових послуг. Організації, які підпадають під NIS2, повинні дотримуватися суворих вимог до безпеки своїх мобільних систем.

Управління ризиками та безпекою

Як і ISO/IEC 27001, NIS2 приділяє велику увагу управлінню ризиками. Організації повинні проводити регулярну оцінку ризиків, включаючи ті, що виникають внаслідок використання мобільних пристроїв. Це включає загрози, пов’язані з мобільними пристроями, такими як зломи, несанкціонований доступ або витік даних.

Інцидент-менеджмент

NIS2 вимагає від організацій ефективної системи реагування на інциденти кібербезпеки, включаючи інциденти, що стосуються мобільних пристроїв. Це означає, що підприємства повинні мати механізми для виявлення, управління та усунення інцидентів, які можуть загрожувати мобільним пристроям, зокрема віддалене видалення даних та блокування пристроїв у разі компрометації.

Безпека ланцюгів постачання

Одним з ключових аспектів NIS2 є акцент на безпеці ланцюгів постачання. Організації повинні гарантувати, що мобільні пристрої та мобільне програмне забезпечення, які вони використовують, відповідають найвищим стандартам безпеки. Це включає перевірку постачальників програмного забезпечення для мобільних пристроїв і обладнання на відповідність вимогам безпеки.

Шифрування та захист конфіденційності

NIS2 наголошує на необхідності захисту конфіденційних даних через шифрування, особливо під час їх обробки та передачі на мобільних пристроях. Це дозволяє гарантувати, що навіть у разі втрати або крадіжки пристрою, дані залишатимуться недоступними для зловмисників.

Звітування про інциденти

Відповідно до вимог NIS2, організації повинні звітувати про серйозні інциденти кібербезпеки до відповідних національних органів протягом визначеного терміну. Це стосується будь-яких інцидентів, що виникли через мобільні пристрої або їх використання в корпоративній мережі.

Моніторинг і аудит

NIS2 вимагає від організацій регулярного моніторингу своїх систем безпеки, включно з мобільними пристроями, а також проведення внутрішніх і зовнішніх аудитів для перевірки дотримання безпекових вимог. Це включає моніторинг активності мобільних пристроїв і виявлення потенційних загроз або вразливостей у реальному часі.

Навчання персоналу

Відповідно до вимог NIS2, організації повинні проводити навчання свого персоналу щодо безпеки мобільних пристроїв. Це включає навчання з кібербезпеки, виявлення фішингових атак, безпечного використання додатків і дотримання корпоративних політик.

Координація з національними органами

NIS2 передбачає посилену координацію між приватними компаніями та національними кібербезпековими агентствами. Організації, що використовують мобільні пристрої, повинні регулярно звітувати перед державними органами про стан своєї безпеки та виконання вимог директиви.

Переваги впровадження NIS2:

- Підвищення рівня кібербезпеки у критичних секторах та серед ключових постачальників послуг;

- Забезпечення безпечного використання мобільних пристроїв і мінімізація ризиків, пов'язаних із витоком даних або зловживанням корпоративними ресурсами через мобільні платформи;

- Покращена координація з національними регуляторами кібербезпеки і швидке реагування на загрози.

NIS2 встановлює суворі вимоги до безпеки мобільних пристроїв у корпоративних середовищах, фокусуючись на управлінні ризиками, реагуванні на інциденти, моніторингу та звітуванні про загрози. Це критично важливо для організацій, які покладаються на мобільні пристрої для обробки конфіденційних даних та управління операціями.

1.3 Аналіз існуючих рішень щодо уніфікованого керування безпекою корпоративних мобільних пристроїв

Gartner Magic Quadrant є одним із найавторитетніших джерел аналізу технологій. Його мета - допомогти організаціям оцінити постачальників рішень [7].

Рис. 1.6. Магічний квадрант Гартнера за 2022 рік для платформ з технолгоіями уніфікованого керування безпекою корпоративних мобільних пристроїв [7]

VMware

Вендор пропонує рішення для управління безпекою корпоративних мобільних пристроїв через свій продукт VMware Workspace ONE. Це комплексна платформа для управління мобільними пристроями (MDM) та забезпечення корпоративної безпеки, яка об'єднує різні технології для управління та захисту мобільних пристроїв, додатків і корпоративних даних.

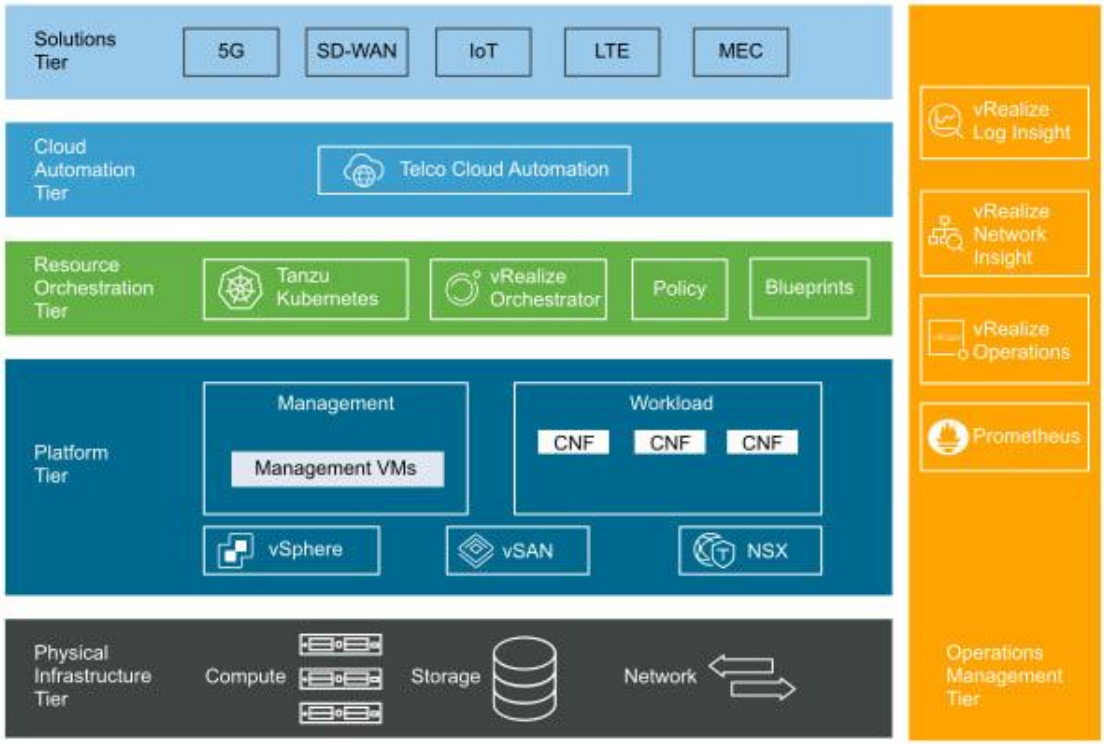


Рис. 1.7. Архітектура рішення VMware [8]

Ось основні компоненти рішення VMware щодо безпеки мобільних пристроїв:

Unified Endpoint Management (UEM)

VMware Workspace ONE забезпечує централізоване управління мобільними пристроями, ноутбуками, настільними комп'ютерами та іншими кінцевими точками за допомогою єдиної платформи. Це дозволяє адміністраторам керувати всіма пристроями з однієї консолі, що спрощує управління безпекою та конфігурацією.

Mobile Device Management (MDM)

Workspace ONE включає потужні засоби управління мобільними пристроями, які дозволяють адміністраторам налаштовувати пристрої, застосовувати політики безпеки, керувати доступом до корпоративних ресурсів і дистанційно блокувати або видаляти дані на пристроях у разі втрати або крадіжки.

Identity and Access Management (IAM)

Рішення VMware Workspace ONE використовує інтегровані інструменти для управління ідентифікацією користувачів і контролем доступу, включаючи багатофакторну автентифікацію (MFA). Це гарантує, що лише авторизовані користувачі можуть отримати доступ до корпоративних даних з мобільних пристроїв.

Conditional Access

Workspace ONE забезпечує умовний доступ, який дозволяє надавати або обмежувати доступ до корпоративних додатків на основі відповідності пристроїв політикам безпеки. Наприклад, пристрій повинен мати встановлені певні оновлення або захист від шкідливого програмного забезпечення для отримання доступу до критичних ресурсів.

Data Encryption

Рішення VMware підтримує шифрування даних як на пристрої, так і під час передачі. Це гарантує, що конфіденційна корпоративна інформація буде захищена в разі втрати або крадіжки мобільного пристрою.

Secure Content Locker

Workspace ONE дозволяє безпечно зберігати та обмінюватися корпоративними файлами через мобільні пристрої, забезпечуючи контроль доступу і можливість видалення файлів з віддалених пристроїв у разі потреби.

Compliance Monitoring

Платформа включає інструменти для моніторингу відповідності мобільних пристроїв політикам безпеки в реальному часі. Адміністратори можуть

налаштовувати правила для автоматичної блокади пристроїв або обмеження доступу в разі невідповідності вимогам безпеки.

Application Management

VMware Workspace ONE дозволяє управляти корпоративними додатками на мобільних пристроях, включно з установкою, оновленням та видаленням додатків. Це забезпечує безпеку додатків і контроль за тим, які програми використовуються на корпоративних пристроях.

Zero Trust Security Model

VMware Workspace ONE підтримує концепцію Zero Trust, де кожен доступ до ресурсів перевіряється незалежно від того, чи знаходиться пристрій у корпоративній мережі. Це підвищує рівень безпеки, особливо при використанні мобільних пристроїв у віддаленому доступі.

Переваги рішення VMware Workspace ONE:

- Єдине рішення для всіх пристроїв: одна консоль для управління всіма кінцевими точками, включно з мобільними пристроями;

- Посилена безпека: шифрування, багатофакторна автентифікація та умовний доступ підвищують захист корпоративних даних ;

- Віддалене управління: можливість керувати пристроями дистанційно, включно з блокуванням та видаленням даних у разі інцидентів.

VMware Workspace ONE є універсальним інструментом для корпоративного управління мобільними пристроями, який поєднує безпеку, зручність управління і розширені можливості для підприємств різних масштабів.

Mobileron (Ivanti)

MobileIron, яка тепер є частиною Ivanti, пропонує рішення для управління безпекою корпоративних мобільних пристроїв через платформу Ivanti Neurons for MDM (MobileIron). Це рішення поєднує управління мобільними пристроями (MDM), управління мобільними додатками (MAM) та управління мобільним

контентом (MCM) в єдиній платформі, орієнтованій на забезпечення корпоративної безпеки.

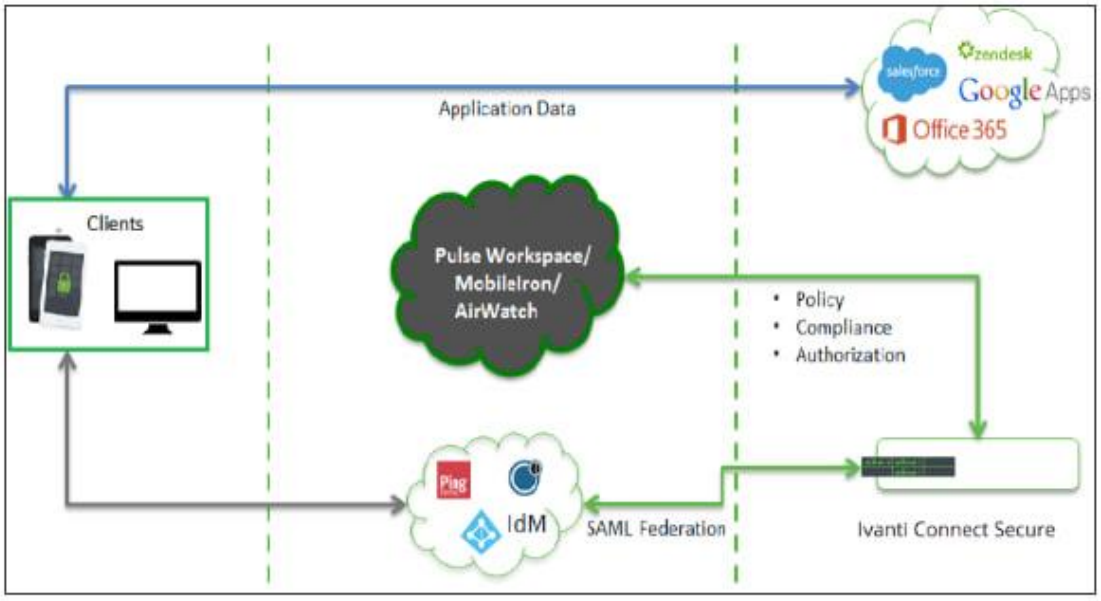


Рис. 1.8. Архітектура рішення Mobileron (Ivanti)[9]

Ось ключові компоненти рішення MobileIron щодо безпеки корпоративних мобільних пристроїв:

Unified Endpoint Management (UEM)

MobileIron пропонує рішення для єдиного управління кінцевими точками (UEM), яке об'єднує управління різними пристроями, такими як мобільні телефони, планшети та ноутбуки. Це забезпечує централізоване управління пристроями в корпоративній мережі, дозволяючи впроваджувати політики безпеки на всіх пристроях і моніторити їх у реальному часі.

Mobile Device Management (MDM)

MobileIron дозволяє адміністраторам повністю контролювати мобільні пристрої, на яких використовується корпоративний контент. Серед можливостей:

- Реєстрація пристроїв: автоматичне налаштування нових пристроїв із застосуванням корпоративних політик;

- Контроль доступу: контроль за тим, які пристрої мають доступ до корпоративних даних і мереж;

- Дистанційне керування: можливість віддаленого блокування пристроїв або видалення корпоративних даних у разі втрати або крадіжки.

Mobile Application Management (MAM)

MobileIron дозволяє адміністраторам контролювати мобільні додатки, включаючи можливості:

- Управління додатками: централізоване встановлення та видалення додатків на мобільних пристроях;

- Розподіл додатків: надання доступу до корпоративних додатків через власний магазин додатків (enterprise app store);

- Контроль за додатками: обмеження використання певних додатків, які не відповідають вимогам безпеки.

Контейнеризація додатків

Рішення MobileIron дозволяє використовувати технологію контейнеризації, яка ізолює корпоративні дані від особистих даних на мобільних пристроях. Це дозволяє уникнути витоків даних через особисті програми користувачів.

Zero Trust Model

MobileIron використовує підхід Zero Trust, де кожен пристрій і кожен користувач підлягає ретельній перевірці перед отриманням доступу до корпоративних ресурсів. У цьому випадку використовуються механізми багатофакторної автентифікації (MFA), перевірка відповідності пристроїв вимогам безпеки та контроль доступу в реальному часі.

Conditional Access

MobileIron дозволяє впроваджувати умовний доступ, що дозволяє компаніям налаштовувати правила доступу до корпоративних ресурсів на основі стану пристрою, місця розташування користувача або рівня безпеки мережі. Якщо

пристрій не відповідає вимогам безпеки, доступ до ресурсів автоматично обмежується.

Шифрування і захист даних

MobileIron забезпечує шифрування даних як під час їх зберігання на пристрої, так і під час передачі через корпоративні мережі. Це захищає конфіденційну інформацію від несанкціонованого доступу навіть у разі втрати або крадіжки пристрою.

Mobile Threat Defense (MTD)

MobileIron пропонує можливості для захисту від мобільних загроз, такі як захист від шкідливого ПЗ, фішингу та вразливостей в мобільних додатках. Це рішення інтегрується з іншими системами захисту для забезпечення повної безпеки мобільного середовища.

Compliance Monitoring

Система MobileIron дозволяє в режимі реального часу моніторити відповідність мобільних пристроїв корпоративним політикам безпеки. Якщо пристрій виходить за межі політики безпеки, доступ до корпоративних ресурсів автоматично припиняється, або на пристрій застосовуються санкції.

Переваги рішення MobileIron:

- Гнучкість і масштабованість: рішення підходить як для малих, так і для великих організацій і може масштабуватися відповідно до потреб бізнесу;

- Безперервний контроль доступу: завдяки Zero Trust та умовному доступу пристрої постійно проходять перевірку на відповідність вимогам безпеки;

- Реальний захист від загроз: можливості для виявлення та захисту від мобільних загроз забезпечують безпечне використання мобільних пристроїв в корпоративних середовищах.

Рішення MobileIron дозволяє організаціям контролювати свої мобільні середовища, забезпечуючи захист даних і управління доступом до корпоративних ресурсів у мобільній інфраструктурі.

Blackberry

BlackBerry, відома колись як провідний виробник смартфонів, сьогодні спеціалізується на корпоративних рішеннях кібербезпеки та управління мобільними пристроями. Її рішення для управління безпекою корпоративних мобільних пристроїв представлені через BlackBerry UEM (Unified Endpoint Management), що забезпечує надійне управління кінцевими точками, захист мобільних пристроїв, і захист даних на різних платформах

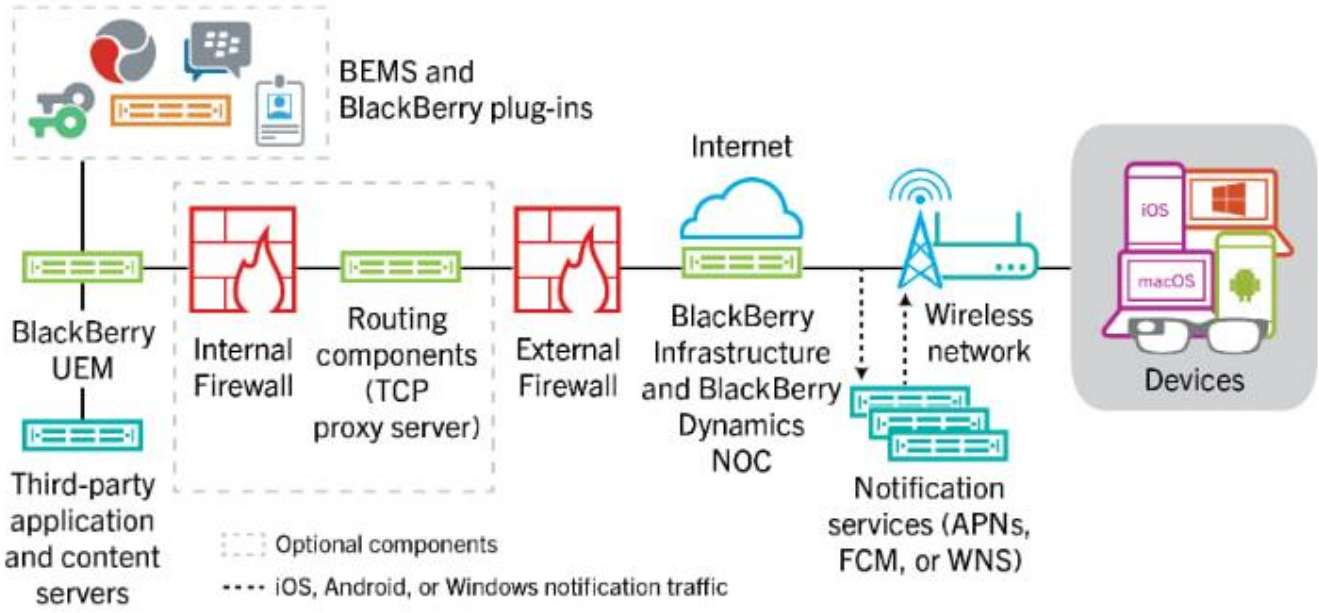


Рис. 1.9. Архітектура рішення Blackberry [10]

Ось основні компоненти рішення BlackBerry для управління безпекою мобільних пристроїв:

Unified Endpoint Management (UEM)

BlackBerry UEM є основою платформи управління мобільними пристроями, що дозволяє організаціям контролювати смартфони, планшети, ноутбуки та інші

кінцеві точки через єдину платформу. Це рішення забезпечує централізоване управління пристроями з різними операційними системами, включаючи iOS, Android, Windows, macOS і BlackBerry.

Mobile Device Management (MDM)

BlackBerry UEM дозволяє контролювати всі аспекти корпоративних мобільних пристроїв, включаючи:

- Реєстрація та налаштування пристроїв: дозволяє централізовано реєструвати нові пристрої і застосовувати політики безпеки;

- Контроль доступу до мережі та даних: забезпечує контроль доступу до корпоративних ресурсів, таких як електронна пошта, календар, файли та інші додатки;

- Віддалене управління пристроями: у разі втрати або крадіжки пристроїв, адміністратори можуть віддалено блокувати пристрої або видаляти з них корпоративні дані.

Mobile Application Management (MAM)

BlackBerry UEM підтримує централізоване управління додатками, надаючи інструменти для:

- Розповсюдження додатків: адміністратори можуть централізовано встановлювати, оновлювати і видаляти корпоративні додатки на мобільних пристроях;

- Контроль доступу до додатків: це включає використання контейнерів для додатків, що забезпечує захист корпоративних даних навіть у разі компрометації пристрою.

Containerization (Контейнеризація)

BlackBerry використовує технологію контейнеризації, яка ізолює корпоративні дані від особистих даних на пристрої. Це означає, що користувачі можуть використовувати свої пристрої як для роботи, так і для особистих цілей, а корпоративні дані будуть надійно захищені.

Багатофакторна автентифікація (MFA) та Zero Trust

BlackBerry UEM підтримує концепцію Zero Trust і впроваджує багатофакторну автентифікацію (MFA), щоб забезпечити безпечний доступ до корпоративних ресурсів. Це дозволяє переконатися, що лише авторизовані користувачі з перевіреними пристроями можуть отримати доступ до корпоративної інформації.

Secure Connectivity (Безпечне з'єднання)

BlackBerry UEM підтримує шифрування даних як у стані спокою, так і під час передачі. Це гарантує, що корпоративні дані залишаються захищеними навіть у разі використання загальнодоступних або незахищених мереж.

Compliance Monitoring (Моніторинг відповідності)

BlackBerry UEM надає інструменти для моніторингу відповідності пристроїв корпоративним політикам безпеки в реальному часі. Якщо пристрій не відповідає політикам (наприклад, через відсутність оновлень або встановлених антивірусних програм), доступ до корпоративних ресурсів може бути обмежений.

Mobile Threat Defense (MTD)

BlackBerry інтегрує можливості захисту від мобільних загроз, які включають:

- Виявлення загроз: захист від шкідливого ПЗ, фішингових атак, програмних вразливостей;

- Аналіз поведінки: платформа аналізує поведінкові патерни пристроїв для виявлення потенційних загроз.

Детальне керування політиками безпеки

BlackBerry UEM дозволяє налаштовувати гнучкі політики безпеки, що можуть застосовуватися до різних типів пристроїв, користувачів і мережевих умов. Наприклад, пристрої можуть бути заблоковані або мати обмежений доступ до корпоративних ресурсів, якщо не виконані певні вимоги (встановлені оновлення, налаштована багатофакторна автентифікація тощо).

Переваги рішення BlackBerry UEM:

- Підтримка різних платформ: єдина платформа для управління пристроями на Android, iOS, Windows, macOS і BlackBerry;

- Надійний захист даних: шифрування, контейнеризація та Zero Trust забезпечують високий рівень захисту корпоративної інформації;

- Гнучке масштабування: рішення підходить для організацій будь-якого розміру, від малих підприємств до великих корпорацій.

BlackBerry UEM забезпечує комплексне рішення для управління мобільними пристроями, що поєднує захист даних, контроль доступу, багатофакторну автентифікацію і захист від мобільних загроз.

Ці компанії стали лідерами галузі завдяки своїм новаторським рішенням у сфері керування безпекою корпоративних мобільних пристроїв. Їх успіх зумовлений не лише високою ефективністю поточних технологій, але й постійним вдосконаленням своїх платформ, щоб відповідати динамічним викликам сучасної кібербезпеки. Завдяки безперервному впровадженню інновацій, вони здатні передбачати нові типи загроз і вчасно адаптувати свої стратегії, що дозволяє їм зберігати конкурентну перевагу та відповідати потребам найвимогливіших клієнтів.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УНІФІКОВАНОГО КЕРУВАННЯ БЕЗПЕКОЮ КОРПОРАТИВНИХ МОБІЛЬНИХ ПРИСТРОЇВ НА БАЗІ SOPHOS MOBILE

2.1. Призначення та основні функції рішення Sophos Mobile

Дане рішення призначене для управління мобільними пристроями (MDM, Mobile Device Management), яке дозволяє організаціям безпечно управляти мобільними пристроями, використовувати їх для корпоративних цілей та забезпечувати належний рівень захисту даних. Призначення рішення полягає в централізованому управлінні мобільними пристроями, забезпеченні їх безпеки, контролі за використанням мобільних додатків, а також у підтримці відповідності вимогам безпеки та нормативним актам. Це рішення дає можливість централізовано управляти мобільними пристроями співробітників на платформі Android та iOS, що важливо для організацій, що використовують політику BYOD (Bring Your Own Device) або корпоративні мобільні пристрої.

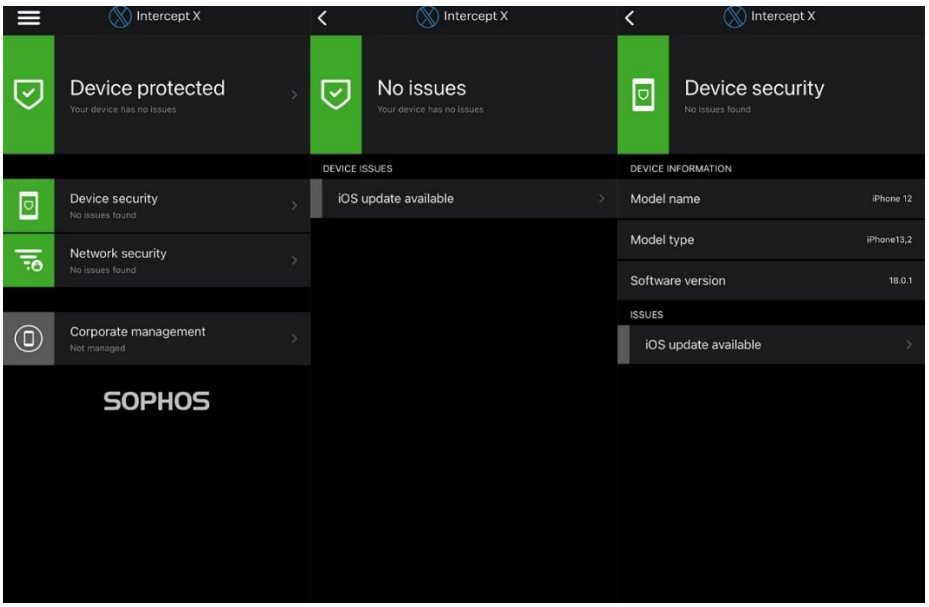


Рис. 2.1. Основний функціонал Sophos Mobile на телефоні

Основними функціями SOPHOS Mobile є: управління пристроями (MDM), що включає реєстрацію мобільних пристроїв, централізоване налаштування конфігурацій пристроїв (Wi-Fi, VPN, параметри безпеки) та віддалене блокування або стирання даних на пристрої у разі втрати чи крадіжки; управління мобільними додатками (MAM), яке дозволяє встановлювати, оновлювати та видаляти додатки, обмежувати доступ до певних додатків або категорій, а також моніторити політики безпеки для корпоративних додатків; забезпечення безпеки даних через шифрування, захист від витоків даних і реалізацію політик безпеки для паролів, що включають вимоги до складності паролів; управління політиками безпеки, що дозволяє налаштовувати та застосовувати політики безпеки для мобільних пристроїв і додатків, а також визначати рівні доступу до корпоративних ресурсів залежно від стану пристрою; антивірусний захист та управління шкідливими програмами, яке включає інтеграцію з антивірусними рішеннями та виявлення шкідливих програм, що можуть загрожувати безпеці даних; моніторинг та звітність, що дозволяє отримувати звіти про стан пристроїв, їх використання та відповідність політикам безпеки, а також виявляти порушення та ризики;

Управління конфіденційністю та доступом через налаштування політик доступу до ресурсів і інтеграцію з корпоративними обліковими записами для контролю доступу та аутентифікації. SOPHOS Mobile є потужним інструментом для забезпечення безпеки мобільних пристроїв в корпоративному середовищі, дозволяючи організаціям здійснювати централізоване управління та моніторинг, мінімізуючи ризики для безпеки даних та ефективно управляючи мобільними пристроями [11].

Сторінка перегляду завдань надає огляд усіх завдань, які були створені та початі, і відображає їхній поточний стан. Є можливість контролювати всі завдання та втручатися у разі виникнення проблем. Наприклад, є можливість видалити завдання, яке неможливо виконати, але блокує пристрій. Щоб видалити завдання, натисніть значок «Видалити» поруч із ним. Також можна фільтрувати завдання

відповідно до їх типу та стану та сортувати їх за назвою пристрою, назвою пакета, автором і запланованою датою.

У розділі меню налаштування налаштовуєтюся загальна поведінка Sophos Mobile, взаємодія з пристроями та взаємодія із зовнішніми компонентами, такими як портали Google або Apple.

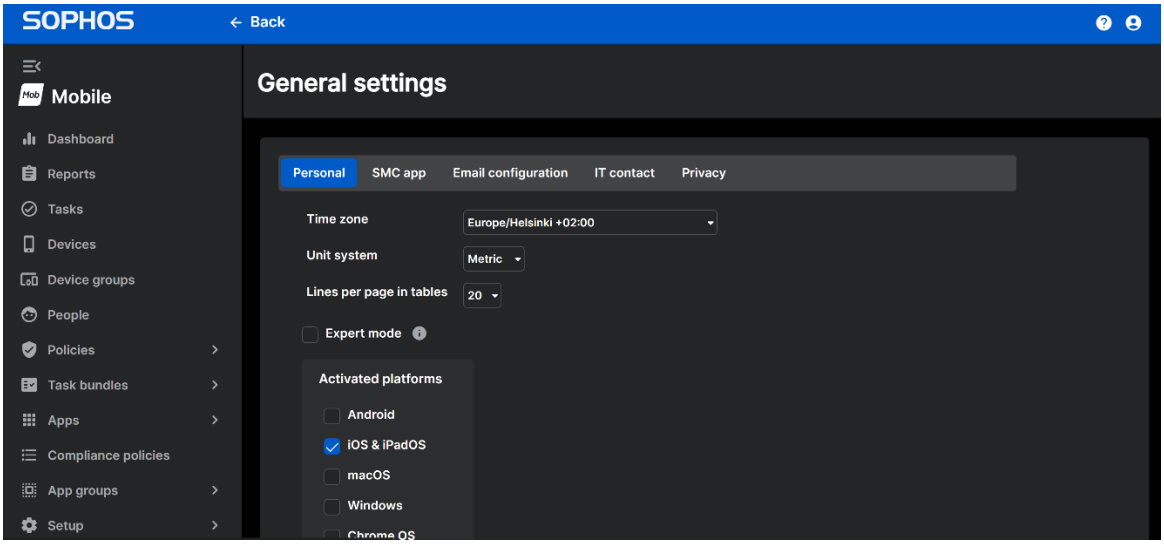


Рис. 2.2. Розділ меню налаштувань

Групи пристроїв використовуються для класифікації пристроїв. Вони допомагають ефективно керувати пристроями, оскільки можуть виконуватись завдання на групі, а не на окремих пристроях. Пристрій завжди належить до однієї групи пристроїв. Користувач призначає пристрій до групи пристроїв, коли додає його до Sophos Mobile [11].

На сторінці «Люди» є можливість керувати обліковими записами користувачів Sophos Mobile. За допомогою груп користувачів надається доступом до центрального порталу самообслуговування Sophos і доступними варіантами реєстрації. Щоб створити конфігурацію порталу самообслуговування лише для певних користувачів, додайте їх до групи користувачів і призначте цю групу конфігурації порталу самообслуговування. Керування групами користувачів відбувається на сторінці «Люди» в Sophos Central Admin [11].

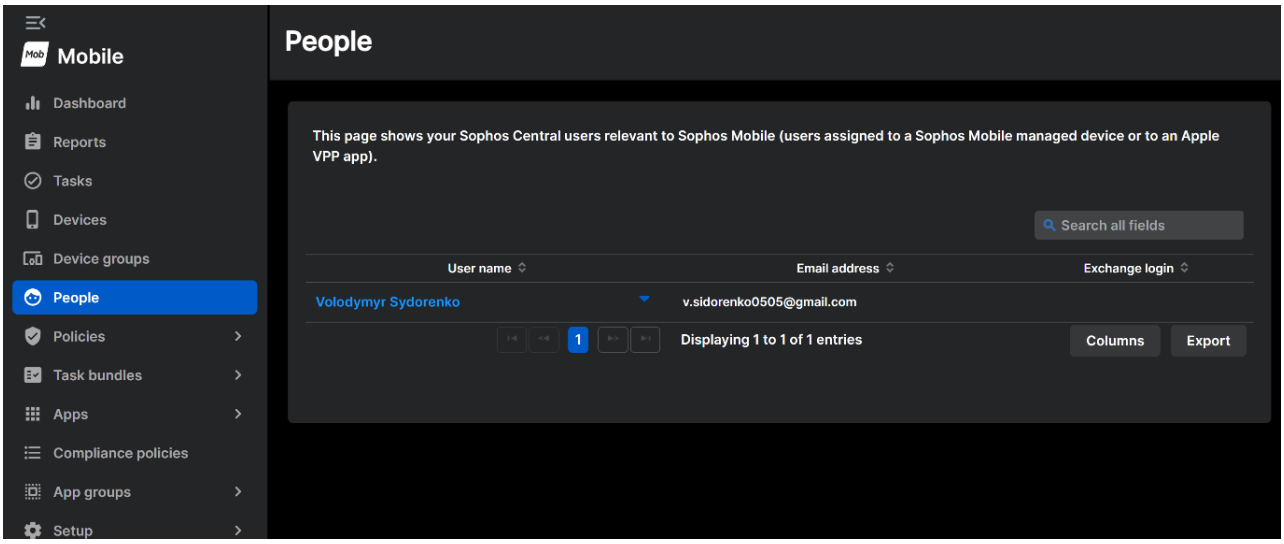


Рис. 2.3. Сторінка «Люди»

Політика містить параметри, які можна застосувати до пристрою чи групи пристроїв. Політики набувають чинності негайно, коли вони призначаються пристрою. Вони синхронізуються кожного разу, коли пристрій підключається до Sophos Mobile. Коли змінюється політика, не потрібно оновлювати її на пристрої. Щоб видалити параметри, застосовані політикою, потрібно оновити політику або призначити іншу.

Завдяки політикам відповідності можна: дозволяти, забороняти або застосовувати певні функції пристрою; визначте дії, які виконуються, коли порушується правило відповідності. Також можна створювати різні політики відповідності та призначати їх групам пристроїв. Це дозволяє застосовувати різні рівні безпеки до керованих пристроїв.

За допомогою групи завдань можна об’єднати кілька завдань в одну транзакцію. Наприклад, можна об’єднати всі завдання для реєстрації та налаштування пристрою.

Sophos Intercept X for Mobile – це рішення Mobile Threat Defense (MTD) для пристрою Android, iPhone або iPad. Керуючи Sophos Intercept X for Mobile за допомогою Sophos Mobile, можна виконувати такі завдання: призначати на

пристрій політику Mobile Threat Defense , щоб налаштувати Sophos Intercept X for Mobile; призначте політику відповідності пристрою, щоб відстежувати його стан відповідності. На пристроях Android є функція сканування зловмисного програмного забезпечення.

Користувач може налаштувати Sophos Mobile як постачальника Mobile Threat Defense для Microsoft Intune. Intune – це служба Microsoft для керування мобільними пристроями та програмами. За допомогою Mobile Threat Defense підключається Sophos Mobile до свого облікового запису Intune і використовується статус безпеки, який повідомляє Sophos Intercept X for Mobile, щоб контролювати доступ до робочих ресурсів.

2.2 Архітектура рішення Sophos Mobile, призначення та основні функції компонентів

Архітектура рішення Sophos Mobile включає кілька основних компонентів:

Сервер Sophos Mobile:

Сервер є основою системи, яка забезпечує зв’язок між пристроями, адміністративною консоллю та агентами на мобільних пристроях. Він відповідає за зберігання та обробку інформації, що стосується політик безпеки, конфігурацій і стану пристроїв. Сервер обробляє команди, надсилані адміністраторами, і відправляє їх на пристрої. Також він може зберігати журнали подій, інформацію про відповідність політикам і статус безпеки кожного пристрою. Сервер може бути розгорнутий як у хмарному середовищі Sophos, що знижує витрати на інфраструктуру, так і локально, що дозволяє підприємствам з високими вимогами до приватності та контролю використовувати його в своїй мережі.

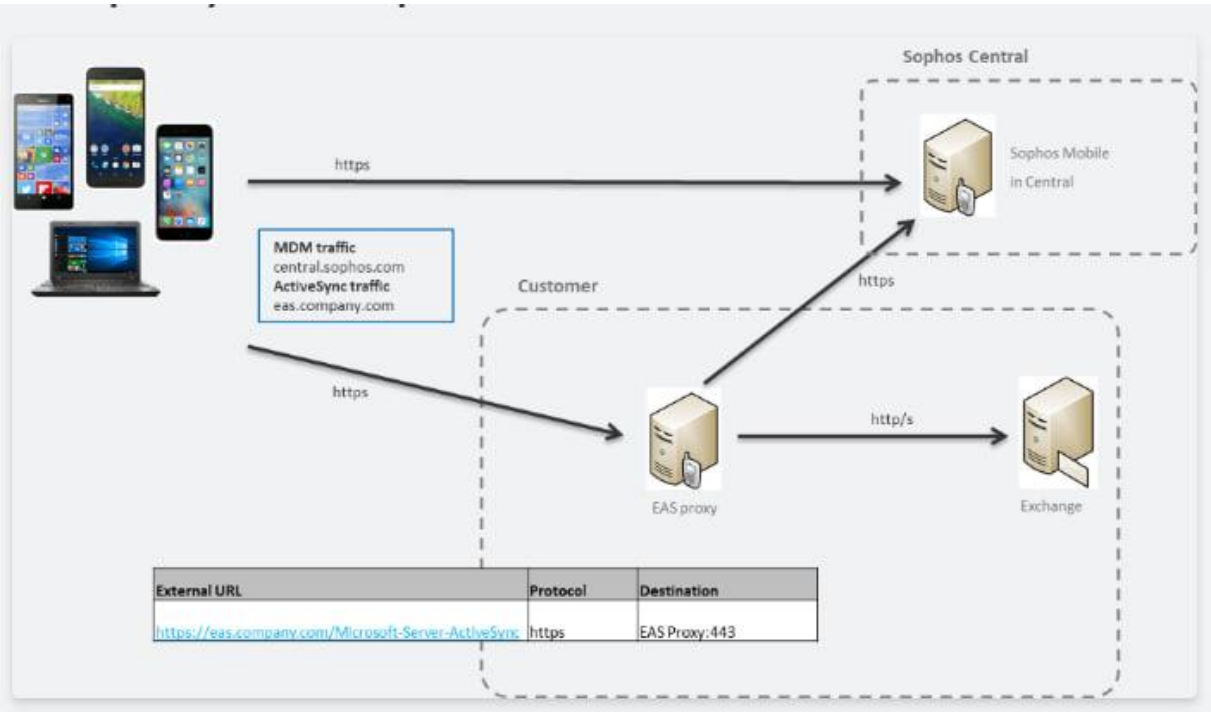


Рис. 2.4. Проксі EAS із Sophos Mobile [4]

Консоль адміністратора (Sophos Mobile Admin Console):

Консоль є веб-інтерфейсом для адміністраторів, який надає всі необхідні інструменти для управління мобільними пристроями та політиками безпеки. Через консоль адміністратори можуть виконувати різні операції, такі як налаштування облікових записів користувачів, встановлення та зміна політик безпеки, контроль за встановленням додатків і шифруванням даних на пристроях. Консоль дозволяє здійснювати моніторинг пристроїв у режимі реального часу, перевіряти відповідність політикам і налаштовувати автоматичні сповіщення про порушення або загрози. Це зручний інструмент для централізованого управління всіма мобільними пристроями в організації, що дозволяє швидко реагувати на інциденти та забезпечувати дотримання політик.

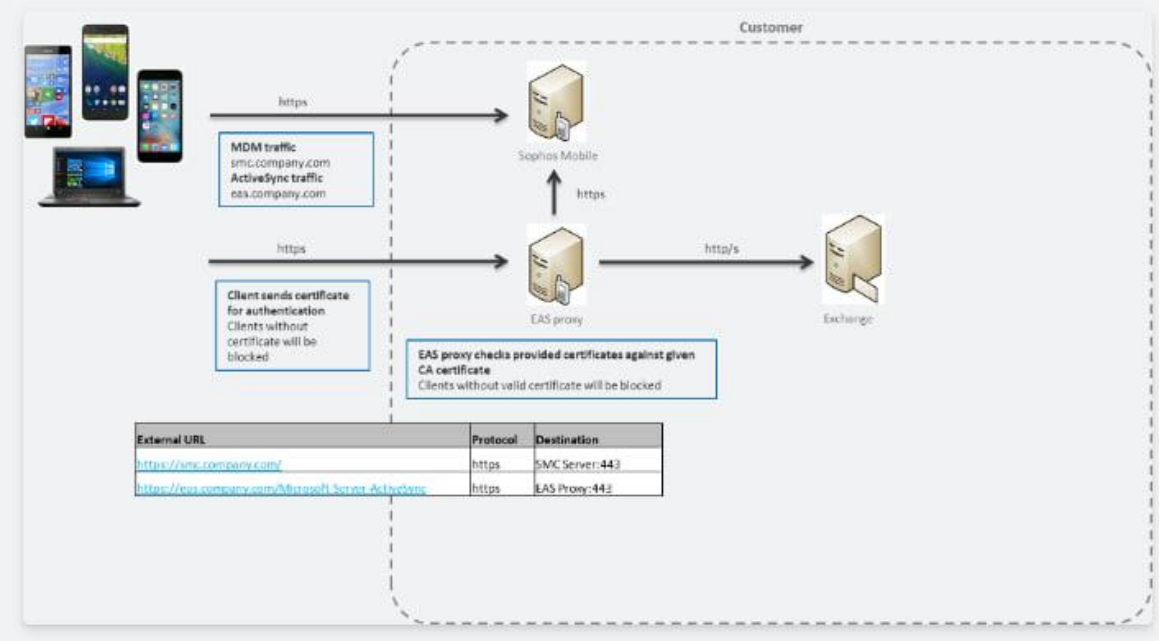


Рис. 2.5. Авторизація сертифіката клієнта [4]

Прикладний агент (Sophos Mobile Agent):

Це застосунок, що встановлюється на кожен пристрій, який є частиною корпоративної інфраструктури безпеки. Агент забезпечує зв'язок між мобільним пристроєм та сервером Sophos Mobile, застосовуючи політики безпеки, відправляючи дані про стан пристрою, а також забезпечуючи зворотній зв'язок для адміністраторів. Агент також може виконувати дії, такі як блокування пристрою в разі його втрати, очищення даних (часткове або повне) у разі крадіжки, контроль за доступом до певних додатків і функцій. Цей компонент є основним інструментом безпеки на пристрої, який дозволяє організації здійснювати контроль на віддаленому рівні, забезпечуючи дотримання політик.

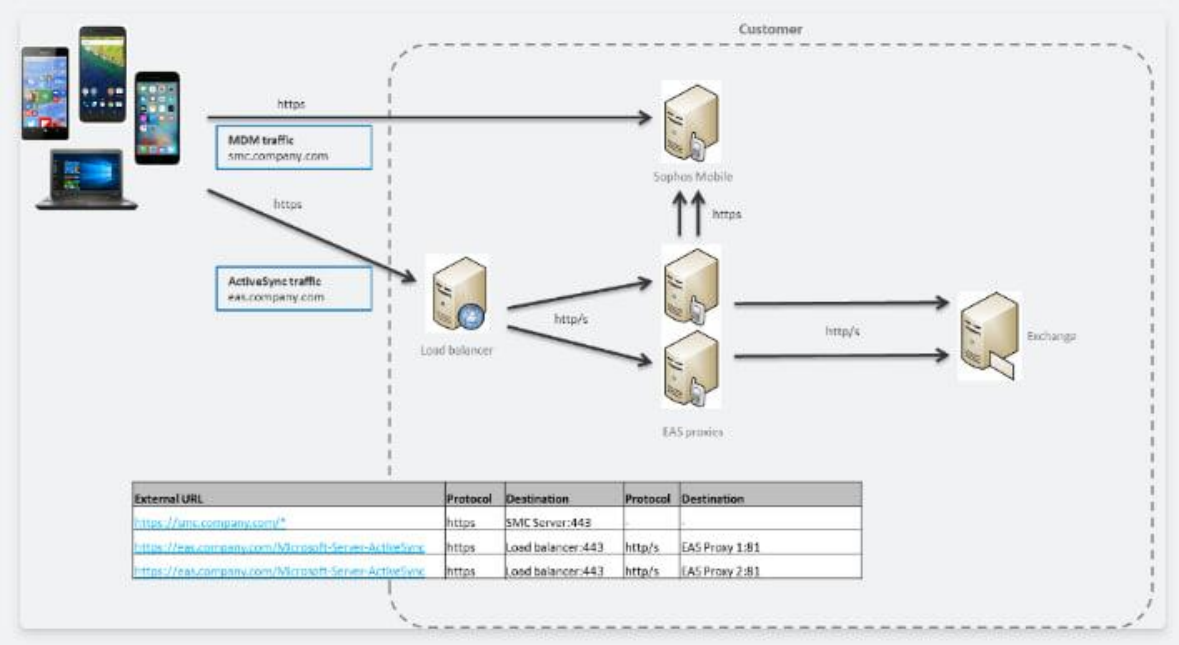


Рис. 2.6. EAS-проксі за балансувальником навантаження [4]

Портал самообслуговування (Self-Service Portal):

Портал самообслуговування надає користувачам можливість самостійно керувати своїми пристроями, зменшуючи навантаження на IT-відділ. Користувачі можуть самостійно додавати нові пристрої, блокувати їх у разі втрати, відновлювати з доступом або запускати діагностику. Наприклад, у випадку втрати пристрою користувач може самостійно його заблокувати, що скорочує час реакції на інцидент. Доступ до порталу самообслуговування регулюється політиками безпеки, і користувачі можуть виконувати лише ті дії, які дозволені адміністратором. Це знижує кількість запитів на підтримку, одночасно підвищуючи зручність для користувачів.

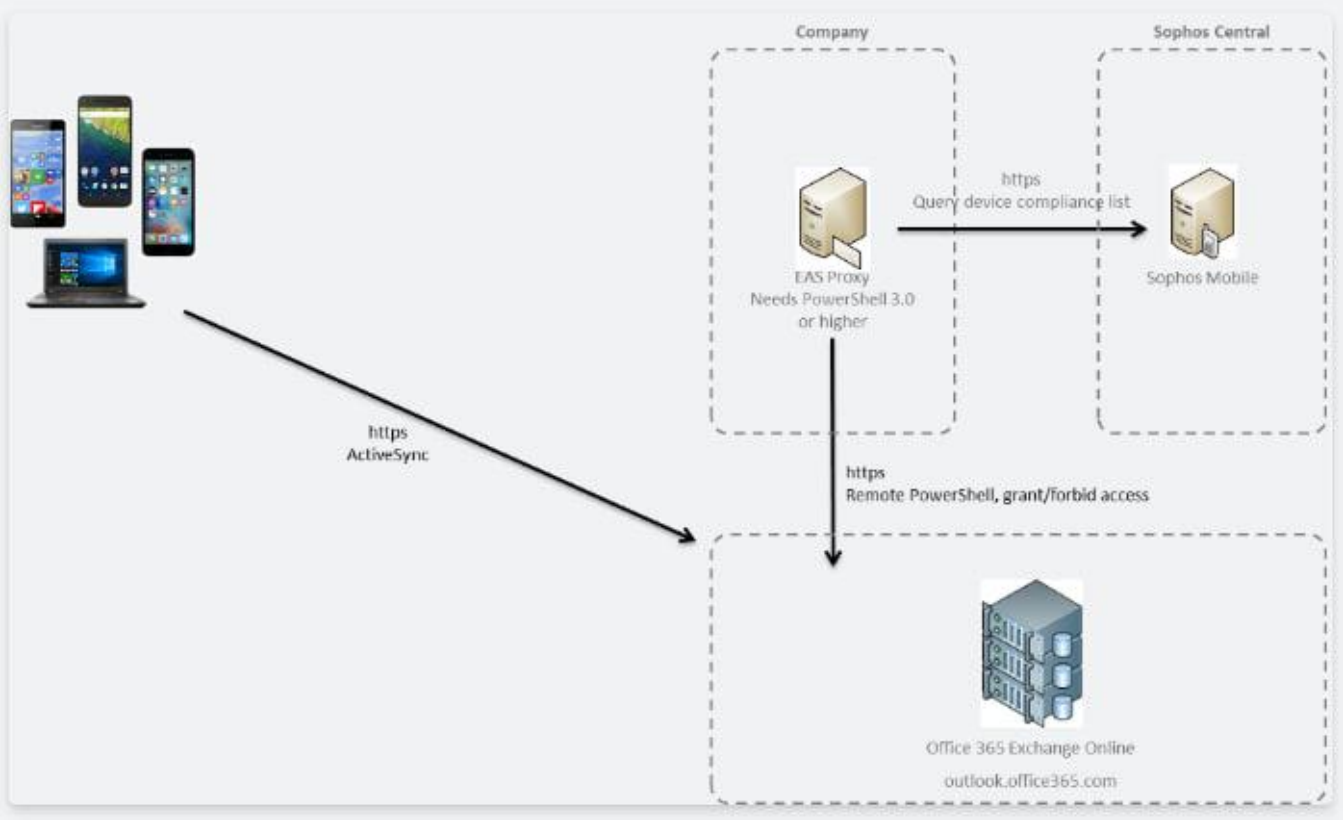


Рис. 2.7. Режим PowerShell [4]

Проксі-сервер Sophos Mobile EAS підключається до поштового сервера через PowerShell, щоб контролювати доступ до пошти для ваших пристроїв.

Режим PowerShell має такі переваги перед режимом проксі:

- Пристрої взаємодіють безпосередньо з поштовим сервером Exchange;

- Оскільки жодному поштовому трафіку не потрібно проходити через проксі Sophos Mobile EAS, вам не потрібно відкривати порт для вхідної пошти у вашому брандмауері;

- Ви можете заблокувати доступ до пошти для некерованих пристроїв;

- Режим PowerShell підтримує Exchange Online і Exchange Server, тоді як режим проксі підтримує лише Exchange Server.

Компонент управління додатками (Application Management):

Цей компонент забезпечує централізоване управління додатками, що встановлені на мобільних пристроях. Адміністратори можуть налаштовувати

дозволені та заборонені додатки, контролювати їх встановлення та оновлення, а також блокувати використання додатків, що не відповідають вимогам безпеки. Управління додатками дає можливість обмежувати доступ до небезпечних програм і гарантувати, що всі корпоративні додатки завжди актуальні та безпечні. Компонент дозволяє створювати список дозволених додатків, блокувати інсталяцію додатків з неперевірених джерел і забезпечувати контрольоване оновлення критичних додатків.

Шифрування та захист даних (Data Protection):

Sophos Mobile використовує механізми шифрування для захисту даних, що зберігаються на пристроях. Шифрування може бути налаштоване на рівні всього пристрою або лише для певних додатків або даних. Наприклад, компанія може застосувати шифрування лише до корпоративних даних, залишаючи особисті дані користувача незмінними. Захист даних є важливим для забезпечення конфіденційності інформації у випадку втрати або крадіжки пристрою. Окрім шифрування, цей компонент включає механізми контролю за передачею даних, щоб запобігти несанкціонованому копіюванню або відправці конфіденційної інформації.

Sophos Mobile легко інтегрується з іншими продуктами Sophos, такими як Sophos Central, що забезпечує комплексне управління безпекою для всієї IT-інфраструктури підприємства. Завдяки інтеграції з такими рішеннями, як Sophos Intercept X, організації можуть поєднувати захист від шкідливого ПЗ, управління мобільними пристроями та моніторинг загроз в єдину екосистему. Це дозволяє централізовано отримувати інформацію про загрози та інциденти, керувати політиками безпеки для різних типів пристроїв і підвищувати загальну ефективність захисту від загроз.

2.3. Можливості рішення Sophos Mobile щодо уніфікованого керування безпекою корпоративних мобільних пристроїв

Sophos Mobile Security забезпечує надійний захист пристрою без негативного впливу на його продуктивність чи тривалість роботи батареї. Завдяки реальному часу синхронізації з SophosLabs мобільний пристрій постійно захищений від останніх загроз у вигляді шкідливих програм та інтернет-атак.

Технологія Sophos Anti-Malware забезпечує найвищий рівень захисту від шкідливого ПЗ, виявлення потенційно небезпечних додатків, веб-захист та фільтрацію небажаного контенту. Постійний моніторинг стану безпеки пристрою інформує кристувача про потенційні загрози та автоматично обмежує доступ до корпоративних ресурсів у випадку компрометації.

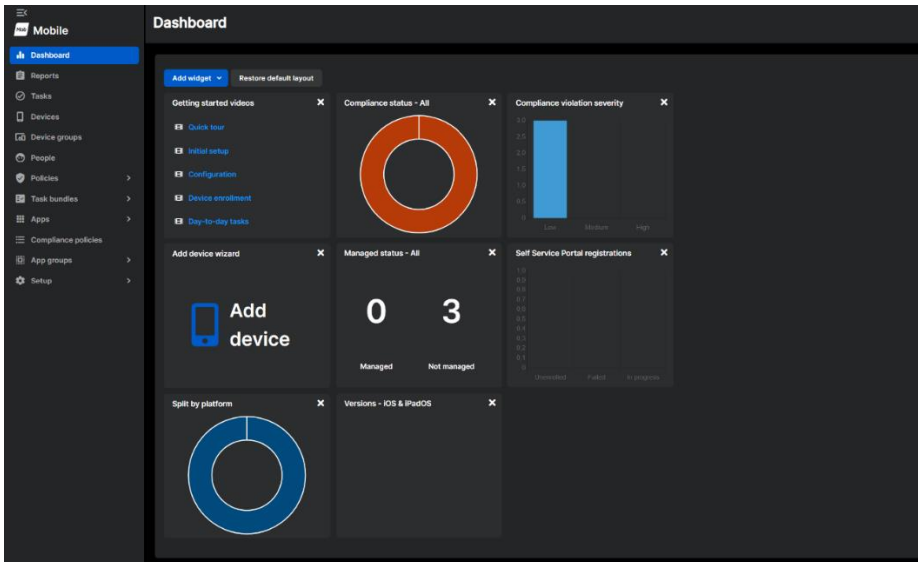


Рис. 2.8. Можливість рішення моніторингу загроз та звітності

Розроблена спеціально для мобільних пристроїв, Sophos Mobile Security розпізнає шкідливі або небажані додатки, що можуть спричинити витік даних, втрати інформації чи надмірні витрати на використання мережі. У разі втрати чи

крадіжки пристрою функція віддаленого блокування і видалення даних (включаючи кеш, паролі тощо) захистить особисту інформацію від сторонніх.

Sophos Intercept X для мобільних пристроїв постійно відстежує стан пристрою та сповіщає користувача, якщо пристрій зламано, щоб можна було вжити заходів щодо виправлення чи автоматично скасувати доступ до корпоративних ресурсів. Консультанти з безпеки пристрою виявляють вторгнення і можуть інформувати користувача та адміністратора про необхідні оновлення операційної системи [5].

Мережеві з’єднання перевіряються в режимі реального часу на наявність підозрілих характеристик, які можуть ідентифікувати атаку. Це допомагає знизити ризик атак типу " Man-in-the-Middle" (MitM) [5].

Рис. 2.9. Інтерфейс стану поточного стану девайсу Sophos Intercept X

Веб-фільтрація та перевірка URL-адрес припиняють доступ до завідомо шкідливих сайтів на мобільних пристроях, а функція виявлення фішингу SMS виявляє шкідливі URL-адреси [5].

Безпека програм Sophos Intercept X для мобільних пристроїв виявляє шкідливі та потенційно небажані програми, встановлені на пристроях Android, використовуючи технологію глибокого навчання Intercept X разом із розвідкою глобальної дослідницької групи SophosLabs. Користувачі та адміністратори отримують сповіщення про зміну статусу загрози пристрою [5].

Інтеграція з Microsoft Intune дозволяє адміністраторам створювати політики умовного доступу, обмежуючи доступ до програм і даних у разі виявлення загрози.

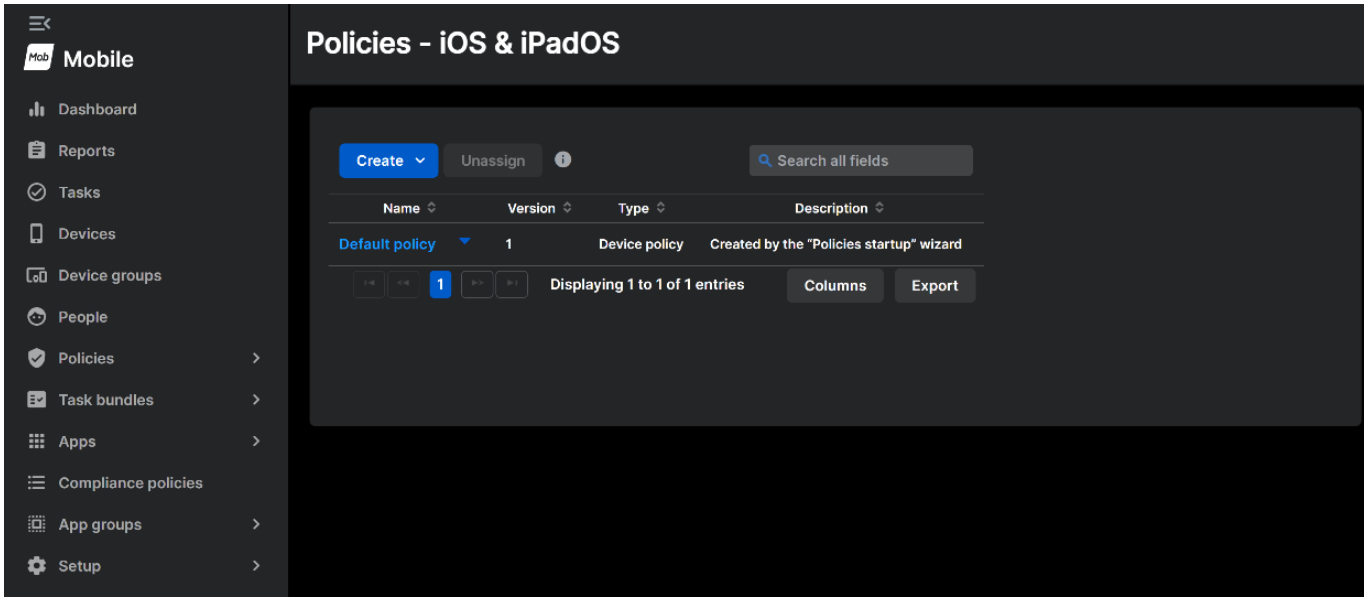


Рис. 2.10. Політики

Централізоване розгортання, налаштування та звітування Sophos Intercept X для мобільних пристроїв можна централізовано налаштувати з Sophos Central, де розміщено платформу Unified Endpoint Management (UEM). Розгортання може відбуватися через існуючі магазини додатків із реєстрацією користувача або програму можна надсилати за допомогою існуючих UEM, таких як Sophos Mobile, або сторонніх інструментів Enterprise Mobility Management (EMM) [5].

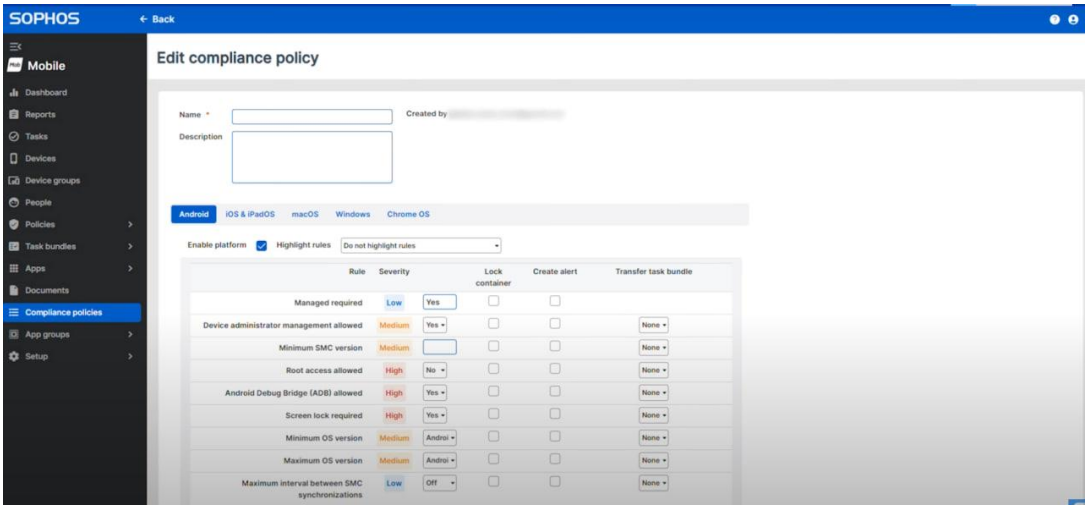


Рис. 2.11. Можливості рішення щодо налаштувань пріоритетності політик безпеки мобільних пристроїв користувачів

Синхронізована безпека дозволяє оборонним засобам працювати разом як система, яка є більш скоординованою, ніж зловмисники. Інформацію про статус загрози можна надати точкам доступу Sophos Wireless, щоб забезпечити повне усунення всіх загроз на пристроях, перш ніж буде надано доступ до конфіденційних мереж [5].

Sophos Mobile поєднує в собі Unified Endpoint Management (UEM) і Mobile Threat Defense (MTD) – це єдине рішення для зменшення зусиль, необхідних для керування та захисту мобільних кінцевих точок у мережі BYOD з пристроями Android та iOS. Уніфіковані політики забезпечують узгодженість для захисту бізнес-даних і їх користувачів на будь-якій мобільній платформі. Надалі захищаючи особисту інформацію, Sophos забезпечує керування лише контейнером, щоб запобігти вторгненню електронної пошти та документів, що містять корпоративні дані [6].

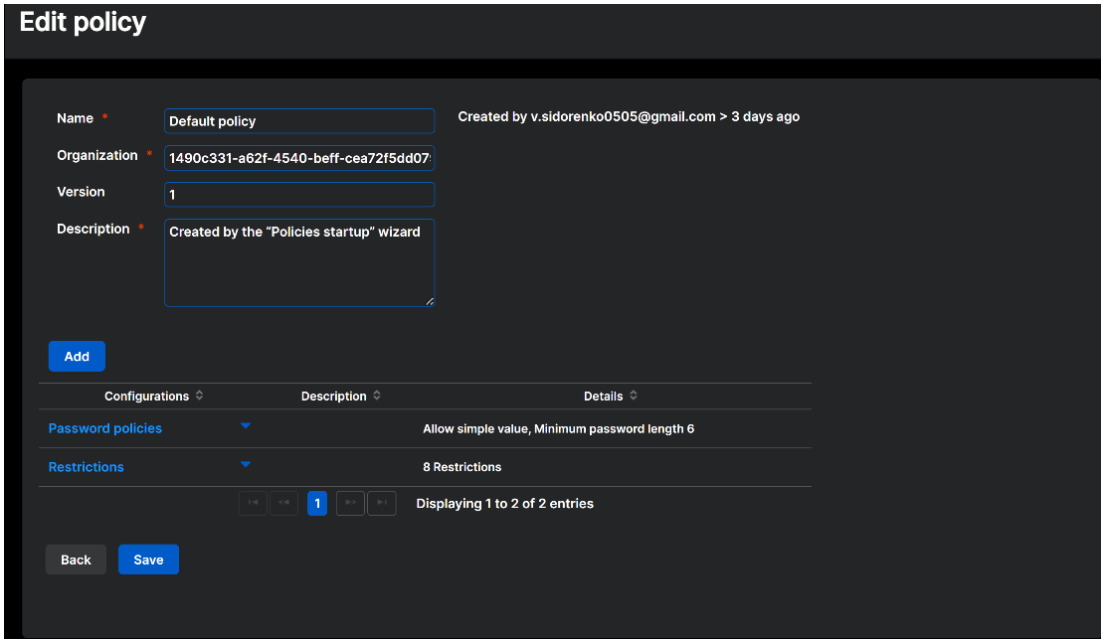


Рис. 2.12. Можливості рішення щодо встановлення та редагування політик

Віддалене керування може встановлювати, видаляти або переглядати програми для контролю, білого та чорного списку та налаштування. Його захист від зловмисного програмного забезпечення глибокого навчання, PUA, фішинговий і веб-захист, а також фільтрування URL-адрес можна застосувати та переглядати у звітах, щоб спростити видимість на мобільних пристроях [6].

Ключові сильні сторони [6]:

- 90% запобігання зловмисному програмному забезпеченню;

- 100% виявлення зловмисного програмного забезпечення нульового дня, хибних спрацьовувань і завантаженого шкідливого програмного забезпечення;

- 80% запобігання від стійких зловмисних програм;

- 100% виявлення доступу до конфіденційної файлової системи, незахищеного мережевого трафіку та хмарних служб;

- 100% запобігання викраданню даних;

- 100% виявлення відомих і фішингових сайтів нульового дня, шкідливих URL-адрес ;

- 100% високоякісна фільтрація веб-перегляду на основі вмісту.

Підтримує виправлення на основі інтеграції керування мобільними пристроями (MDM). Sophos Mobile має високу ефективність безпеки та отримав показник QoE у 87 відсотків, що на 12 відсотків вище, ніж інші оцінені продукти. Ця оцінка відображає його здатність виявляти зловмисне програмне забезпечення, мережеві загрози та вразливі місця пристроїв, водночас забезпечуючи відповідні та прості у використанні інтерфейси для негайного перегляду, контролю та виправлення. Враховуючи, що це одне з найдоступніших рішень для продуктів MTD, Sophos забезпечує вражаючий захист, який захистить корпоративні мережі BYOD [6].

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ УНІФІКОВАНОГО КЕРУВАННЯ БЕЗПЕКОЮ КОРПОРАТИВНИХ МОБІЛЬНИХ ПРИСТРОЇВ НА БАЗІ SOPHOS MOBILE

3.1 Розроблення варіанта технології уніфікованого керування безпекою корпоративних мобільних пристроїв на базі Sophos Mobile

Sophos Mobile Security виділяється серед рішень для уніфікованого керування безпекою корпоративних мобільних пристроїв (UEM) завдяки комплексному підходу до захисту пристроїв, легкості управління та інтеграції з іншими продуктами Sophos. Завдяки інтеграції з єдиною екосистемою Sophos Central, зокрема з Intercept X, програма дозволяє IT-відділам контролювати безпеку всіх пристроїв - мобільних, комп'ютерів і серверів – з єдиної консолі, що спрощує управління безпекою і дає змогу оперативно реагувати на інциденти. Перевагою Sophos Mobile Security є комплексний захист у реальному часі: інтеграція з лабораторіями SophosLabs забезпечує захист пристроїв від новітніх загроз, включаючи шкідливі програми, фішинг та інтернет-атаки, а також постійне оновлення баз загроз, що гарантує захист від останніх кіберзагроз. Додатково, Sophos Mobile Security дозволяє автоматично відкликати доступ до корпоративних даних і додатків, якщо пристрій виявлений як скомпрометований, знижуючи ризик витоку конфіденційних даних навіть при втраті або крадіжці пристрою.

Програма також забезпечує розширені функції керування додатками та пристроями, підтримуючи гнучкі налаштування політик щодо встановлення додатків, доступу до мереж, захисту даних і дозволів на використання. Це дозволяє IT-відділам обмежувати використання небезпечних додатків і забезпечувати відповідність усіх пристроїв політикам безпеки компанії. У сфері захисту даних і конфіденційності Sophos Mobile Security надає функції шифрування, виявлення

небезпечних додатків і захисту конфіденційної інформації; у разі втрати чи крадіжки пристрою можна швидко видалити всі корпоративні дані або заблокувати доступ. Крім того, програма підтримує автоматизацію задач із налаштування політик безпеки, оновлень і відповіді на загрози, що допомагає знизити навантаження на IT-відділ, а звіти про стан безпеки пристроїв дозволяють компаніям контролювати відповідність стандартам безпеки та вимогам регуляторів.

Sophos Mobile забезпечує різноманітні функції керування, які залежать від типу пристроїв, політик безпеки та потреб організації. Основні етапи керування пристроями через Sophos Mobile включають: налаштування політик відповідності для пристроїв; створення груп пристроїв, що дозволяє ефективно їх класифікувати і керувати ними, виконуючи завдання на групах, а не на окремих пристроях. Реєстрація та активація пристроїв може здійснюватися як адміністраторами в Sophos Mobile Admin, так і самими користувачами через Sophos Central Self Service Portal.

Також рішення дозволяє налаштувати політики для пристроїв, створити пакети завдань, налаштувати доступні функції у порталі самообслуговування і застосувати нові або оновлені політики до зареєстрованих пристроїв.

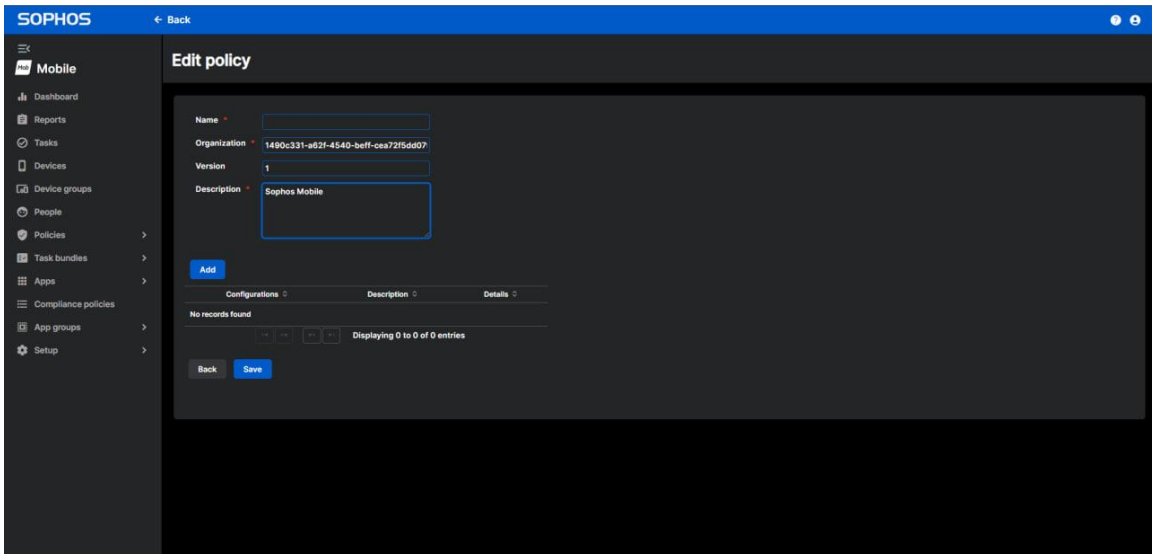


Рис. 3.1. Процес створення та налаштування політики

Налаштовуючи портал самообслуговування, користувач визначає типи пристроїв, які інші можуть зареєструвати, параметри реєстрації та доступні їм дії з пристроєм у Sophos Central Self Service Portal. Для різних користувачів можна встановити різні конфігурації, додаючи їх до груп і пов’язуючи ці групи з відповідною конфігурацією. Якщо користувач належить до кількох груп, пов'язаних із різними конфігураціями, застосовується конфігурація з найвищим пріоритетом.

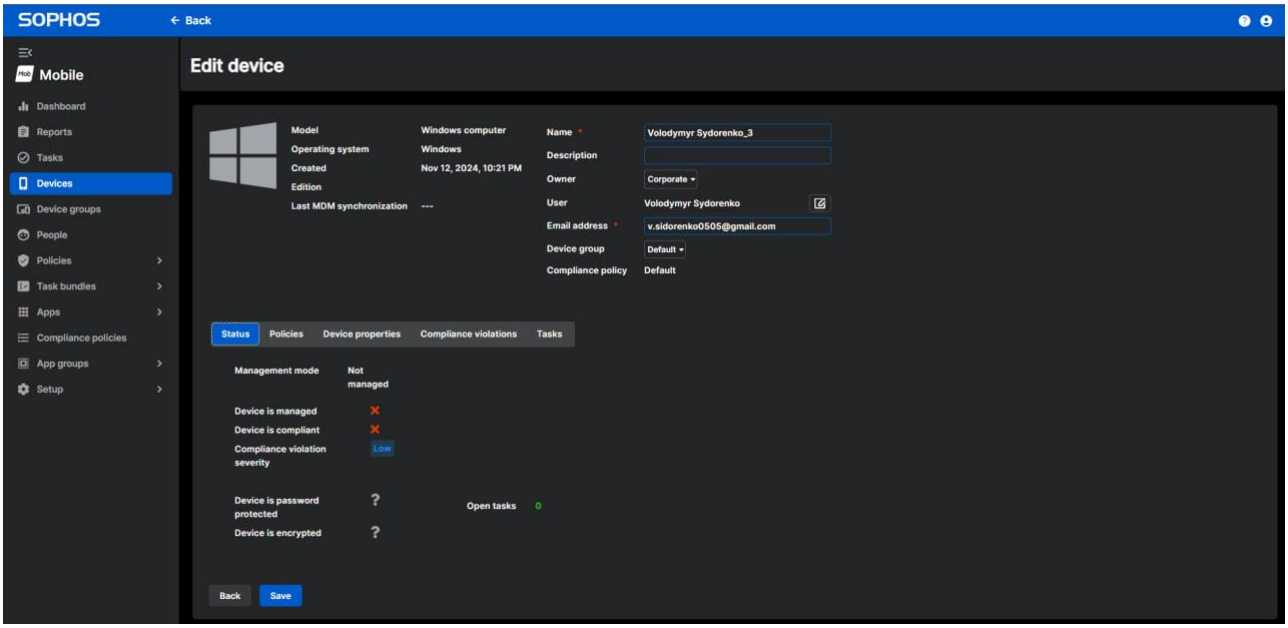


Рис. 3.2. Можливості налаштувань одного з пристроїв користувача

За потреби можна створити додаткові конфігурації порталу самообслуговування для інших груп користувачів. На сторінці налаштувань порталу самообслуговування можна змінювати пріоритет конфігурацій за допомогою стрілок біля кожної з них. Якщо користувач підпадає під дію кількох конфігурацій (оскільки є членом різних груп), діятиме конфігурація з найвищим пріоритетом. Завжди є конфігурація за замовчуванням, яка має найнижчий пріоритет і застосовується лише у випадку відсутності інших відповідних конфігурацій.

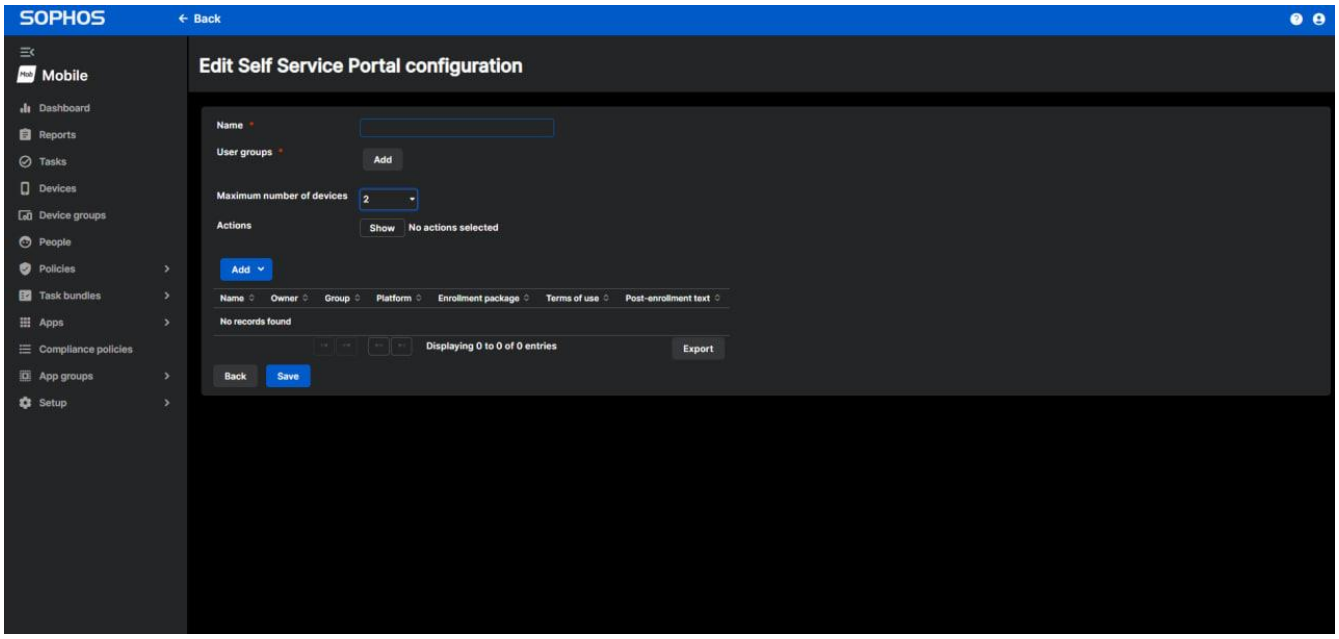


Рис. 3.3. Процес створення додаткових конфігурацій порталу самообслуговування

Для реєстрації пристрою Android Enterprise користувачеві необхідно мати керований обліковий запис Google, який прив’язаний до домену, зареєстрованого вами в Google. Облікові записи мають форму адреси електронної пошти. Під час реєстрації пристрою через портал Sophos Central Self Service Portal, Sophos Mobile перевіряє, чи існує для користувача керований обліковий запис Google на сервері Google. Для цього об'єднується ліва частина електронної адреси користувача в Sophos Mobile з керованим доменом Google. Якщо обліковий запис з такою назвою відсутній, Sophos Mobile створює його.

Окрім створення керованого облікового запису Google під час реєстрації, Sophos Mobile не керує його життєвим циклом. Якщо видалити обліковий запис користувача в Sophos Mobile, керований обліковий запис Google залишиться активним. Управління обліковими записами в керованому домені Google доступне через консоль адміністратора Google. При необхідності облікові записи можна створювати з каталогу LDAP за допомогою Google Cloud Directory Sync.

Для налаштування параметрів пристрої створюються політики. Якщо необхідно керувати різними типами пристроїв, створюється кілька політик. Політика складається з конфігурацій, які визначають області, що керуються Sophos Mobile на пристрої. За бажанням, можна вказати інтервал поновлення SCEP, якщо додано конфігурацію сертифіката пристрою SCEP або Duo. Після цього пристрій автоматично оновлюватиме сертифікат через обраний інтервал.

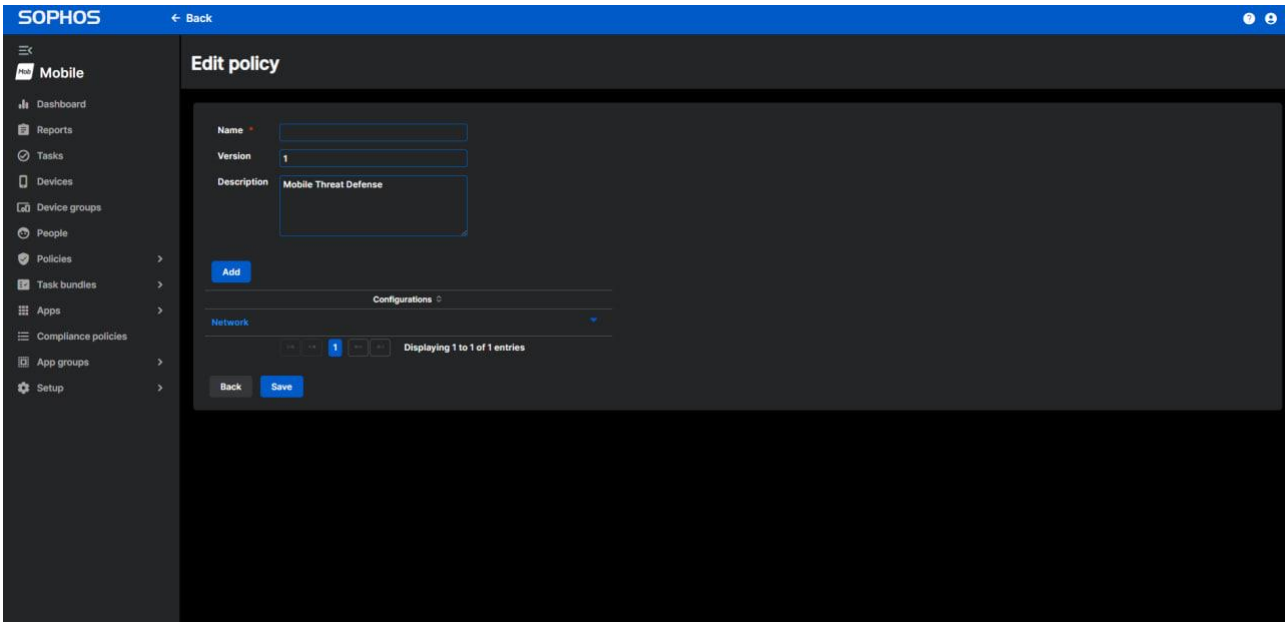


Рис. 3.4. Процес створення політики

3.2 Технологія застосування рішення Sophos Mobile

Після реєстрації пристрою в Sophos Mobile, залежно від налаштувань профілю конфігурації, можна очікувати наступне: можуть з’явитися нові програми, які організація рекомендує для встановлення. Деякі програми, як-от Камера, YouTube чи App Store, можуть бути недоступні на пристрої. Програма електронної пошти може бути налаштована для доступу до корпоративного поштового сервера. Якщо пристрій стає невідповідним політикам безпеки (наприклад, через заборонену програму), користувач отримає сповіщення від Sophos Mobile і зможе переглянути

всі порушення в додатку Sophos Mobile Control або на порталі Sophos Central Self Service Portal.

Якщо організація ввела захист для певних програм на пристрої, при першому відкритті захищеної програми потрібно буде створити пароль, який надалі буде вимагатися при кожному доступі до захищеної програми або після блокування пристрою. У Sophos Mobile Control можна переглядати захищені програми та блокувати їх всі одночасно. Програма також може запросити пароль електронної пошти. На Android-пристроях з підтримкою Samsung Knox може знадобитися прийняття ліцензійної угоди Samsung Knox для активації функцій MDM (ліцензія Samsung Knox є безкоштовною, Knox Premium не потрібен). Якщо під час реєстрації було створено робочий профіль на Android, Sophos Mobile можна буде керувати лише ним, без доступу до особистих даних та програм.

На порталі Sophos Central Self Service Portal можна вручну синхронізувати свій пристрій із сервером Sophos Mobile організації. Це може бути корисно в таких випадках: якщо пристрій був вимкнений тривалий час і не синхронізувався із сервером, він стає несумісним, що може призвести до обмеження в доступі, наприклад, до електронної пошти. Для відновлення сумісності пристрою слід виконати синхронізацію з сервером Sophos Mobile. Також синхронізація необхідна, якщо пристрій не відповідає вимогам через інші причини (наприклад, через встановлені заборонені програми). Після вирішення проблеми синхронізація оновить статус відповідності пристрою.

Після реєстрації пристрою в Sophos Mobile можна виконувати завдання, описані в розділах програми Sophos Mobile Control. Для більшості завдань потрібне інтернет-з'єднання.

Якщо організація налаштувала програми для пристрою, можна встановити їх через Sophos Mobile Control. Якщо організація налаштувала захист для певних програм, при першому відкритті захищеної програми потрібно створити пароль, який знадобиться при кожному доступі до неї або після блокування пристрою.

У Sophos Mobile Control можна переглянути всі захищені програми та заблокувати їх одночасно, що зручно, наприклад, коли передається пристрій іншій особі.

Рішення надає можливість налаштування як постачальника Mobile Threat Defense для Microsoft Intune. Intune – це служба Microsoft для керування мобільними пристроями та програмами. За допомогою Mobile Threat Defense користувавач підключає Sophos Mobile до свого облікового запису Intune і використовує статус безпеки, який повідомляє Sophos Intercept X for Mobile, щоб контролювати доступ до робочих ресурсів.

Також є можливість підключити Sophos Mobile до програмного забезпечення автентифікації Duo Security. Це дозволяє Duo Security ідентифікувати надійні пристрої за їхнім статусом керування Sophos Mobile. Ця функція доступна лише для iPhone та iPad, але не для пристроїв із реєстрацією користувачів.

Є можливість налаштувати проксі-сервер Sophos Mobile EAS для контролю доступу керованих пристроїв до сервера електронної пошти. Електронний трафік керованих пристроїв направляється через цей проксі-сервер. Можна заблокувати доступ до електронної пошти для пристроїв, наприклад для пристрою, який порушує правило відповідності.

Пристрої мають бути налаштовані на використання проксі-сервера EAS як сервера електронної пошти для вхідних і вихідних електронних листів. Проксі-сервер EAS пересилатиме трафік на фактичний сервер електронної пошти, лише якщо пристрій відомий Sophos Mobile і відповідає необхідним політикам. Це гарантує вищий рівень безпеки, оскільки сервер електронної пошти не повинен бути доступним з Інтернету, і лише авторизовані пристрої (правильно налаштовані, наприклад, із вказівками щодо пароля) можуть отримати доступ до нього.

3.3 Рекомендації щодо технологій уніфікованого керування безпекою корпоративних мобільних пристроїв

Спираючись на вищезазначене, хотілось би сформувати рекомендації щодо технологій уніфікованого керування безпекою корпоративних мобільних пристроїв.

Для ефективного керування мобільними пристроями рекомендується обирати системи, що підтримують різні операційні системи, зокрема iOS, Android і Windows. Це забезпечить можливість централізованого контролю над усіма пристроями в компанії. Сучасні MDM-рішення повинні надавати функції дистанційного блокування пристрою, стирання даних у разі втрати чи крадіжки, а також гнучке налаштування політик для різних категорій пристроїв.

Для забезпечення безпеки мобільних пристроїв необхідно використовувати рішення для захисту від мобільних загроз (Mobile Threat Defense, MTD), наприклад, Sophos Mobile чи Check Point Harmony Mobile. Ці системи допомагають виявляти й запобігати шкідливим програмам, фішинговим атакам і підозрілим діям. Інтеграція з антивірусними сервісами, що автоматично оновлюються, є обов’язковою вимогою для зменшення ризиків.

Контроль встановлення додатків на мобільних пристроях має бути частиною політики безпеки. Це включає обмеження встановлення небажаних додатків і доступ до корпоративних програм через спеціально створений каталог. Також важливо впроваджувати захист даних у додатках, зокрема їх шифрування, щоб уникнути компрометації інформації у разі втрати пристрою [12].

Для забезпечення безпеки пристроїв варто налаштувати політики відповідності, що визначатимуть вимоги до пристроїв, зокрема актуальність оновлень, наявність шифрування й активного антивірусу. Пристрої, які не відповідають цим вимогам, повинні автоматично втрачати доступ до

корпоративних ресурсів. Крім того, слід проводити регулярний аудит пристроїв і контролювати їхній статус [12].

Шифрування даних, як під час їх передачі, так і на пристроях, має бути стандартом для всіх мобільних пристроїв. Впровадження багатофакторної аутентифікації (MFA) допоможе додатково захистити доступ до корпоративних ресурсів. Особливо важливим є розмежування особистих і корпоративних даних, що сприяє дотриманню конфіденційності [12].

MDM-рішення повинні бути інтегровані з іншими інструментами безпеки, такими як SIEM-системи (системи управління інформацією про безпеку), VPN-сервіси для захищеного доступу до корпоративної мережі та системи захисту веб-доступу. Це створить комплексну інфраструктуру для моніторингу та реагування на кіберзагрози.

Запровадження порталу самообслуговування дозволить користувачам самостійно налаштовувати свої пристрої, синхронізувати їх із корпоративними системами й отримувати доступ до дозволених додатків. Це зменшить навантаження на IT-відділ і прискорить вирішення потенційних проблем.

Для забезпечення актуальності програмного забезпечення та захисту від нових загроз необхідно регулярно оновлювати MDM-системи й операційні системи мобільних пристроїв. Рекомендується впроваджувати автоматичне розгортання оновлень, а перед цим тестувати їхню сумісність із існуючою інфраструктурою.

Виконання цих рекомендацій допоможе створити потужну й надійну систему уніфікованого керування мобільною безпекою в організації, що дозволить захистити корпоративні дані та ефективно управляти доступом до ресурсів.

ВИСНОВОК

У роботі проведено дослідження проблеми уніфікованого керування безпекою корпоративних мобільних пристроїв, визначено її мету та завдання.

Проведено аналіз існуючих технологій уніфікованого керування мобільними пристроями, які спрямовані на захист даних і забезпечення безпеки мобільних пристроїв у корпоративному середовищі. Технологія Unified Endpoint Management (UEM), реалізована на базі Sophos Mobile, забезпечує централізоване управління всіма пристроями, що використовуються в організації, включаючи смартфони, планшети та ноутбуки.

Досліджено функціональні можливості Sophos Mobile, які включають: управління пристроями через профілі та політики безпеки; забезпечення шифрування даних і управління доступом; інтеграцію з системами автентифікації (SSO, MFA); виявлення та реагування на загрози за допомогою технологій штучного інтелекту.

Sophos Mobile пропонує такі інструменти, як керування застосунками, шифрування даних, захист від шкідливого ПЗ та функції віддаленого блокування або стирання пристрою у разі компрометації.

На основі проведених досліджень запропоновано порядок впровадження Sophos Mobile у корпоративну інфраструктуру, включаючи налаштування політик безпеки, інтеграцію з іншими засобами управління інформаційною безпекою, а також моніторинг та аналітику.

Розроблено рекомендації для фахівців з кібербезпеки щодо використання Sophos Mobile з метою підвищення загального рівня захисту корпоративних даних, особливо в умовах використання моделі BYOD (Bring Your Own Device).

Таким чином, правильна реалізація технології уніфікованого керування безпекою корпоративних мобільних пристроїв сприяє мінімізації ризиків втрати чи

витоку інформації, забезпечує відповідність нормативним вимогам та підвищує ефективність захисту інформаційних ресурсів організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Шпортко Д.В. Технологія уніфікованого керування безпекою корпоративних мобільних пристроїв на базі Sophos Mobile. Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». Державний університет інформаційно-комунікаційних технологій. 25 жовтня 2024. Тези доповідей. С. 247-251. URL: https://duikt.edu.ua/uploads/p_2661_48963150.pdf (дата звернення: 01.11.2024).

2. 2024 Mobile Security Index. URL : https://www.verizon.com/business/resources/reports/mobile-security-index/ (дата звернення: 01.11.2024).

3. What is mobile device management (MDM). URL: https://www.ibm.com/topics/mobile-device-management (дата звернення: 05.11.2024).

4. EAS proxy architecture examples. Technical guide. URL: https://docs.sophos.com/central/Mobile/help/en-us/TechnicalGuide/EASProxyArchitecture/index.html#eas-proxy-with-sophos-mobile (дата звернення: 15.11.2024).

5. Sophos Mobile. Mobile Threat Defense for Android, iOS, and Chrome OS. URL: https://www.sophos.com/en-us/products/mobile-control/intercept-x (дата звернення: 17.11.2024).

6. Sophos Mobile: MTD Industry Assessment Product Profile. URL: https://miercom.com/sophos-mobile-mtd-industry-assessment-product-profile/ (дата звернення: 18.11.2024).

7. Kamil Glowinski, Christian Gossmann, Dominik Strümpf. Gartner. Magic Quadrant for Mobile Device Management. 9 July 2022 – ID G0055759. URL: https://www.gartner.com/en (дата звернення: 18.11.2024).

8. Telco Cloud Platform - 5G Edition Reference Architecture Guide 2.7. VMware docs. 2 March 2023. URL: https://docs.vmware.com/en/VMware-Telco-Cloud-Platform/2.7/telco-cloud-platform-5G-edition-reference-architecture-guide-27/GUID-B035B0EC-A7CB-41ED-9D06-3B3051D9C7A1.html (дата звернення: 18.11.2024).

9. Ivanti Cloud Secure PingOne Integration Configuration Guide. Architecture. URL: https://help.ivanti.com/ps/help/en_US/ICS/vNow/cloud-INT-pingone/architecture.htm (дата звернення: 18.11.2024).

10. BlackBerry Docs. BlackBerry UEM architecture and data flows. URL: https://docs.blackberry.com/en/endpoint-management/blackberry-uem/12_17/planning-architecture/architecture/ake1452094272560 (дата звернення: 18.11.2024).

11. SOPHOS NEWS. 26 November 2024. URL: https://news.sophos.com/en-us/ (дата звернення: 18.11.2024).

12. National Institute of Standards and Technology. NIST SP 800-124 Revision. URL: https://www.nist.gov/ (дата звернення: 18.11.2024).

13. Support Sophos. URL: https://support.sophos.com/support/s/?language=en_US#t=AllTab&sort=relevancy (дата звернення: 18.11.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-
КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Кваліфікаційна робота
на тему:

«Технологія уніфікованого керування безпекою корпоративних мобільних пристроїв на базі Sophos Mobile»

Виконав: ШПОРТКО Дмитро Вікторович, БСДМ – 62

Керівник: ГАХОВ Сергій Олександрович, к. військ. н., доцент

Об’єкт дослідження – технології уніфікованого керування безпекою корпоративних мобільних пристроїв.

Предмет дослідження – система уніфікованого керування безпекою корпоративних мобільних пристроїв на базі Sophos Mobile.

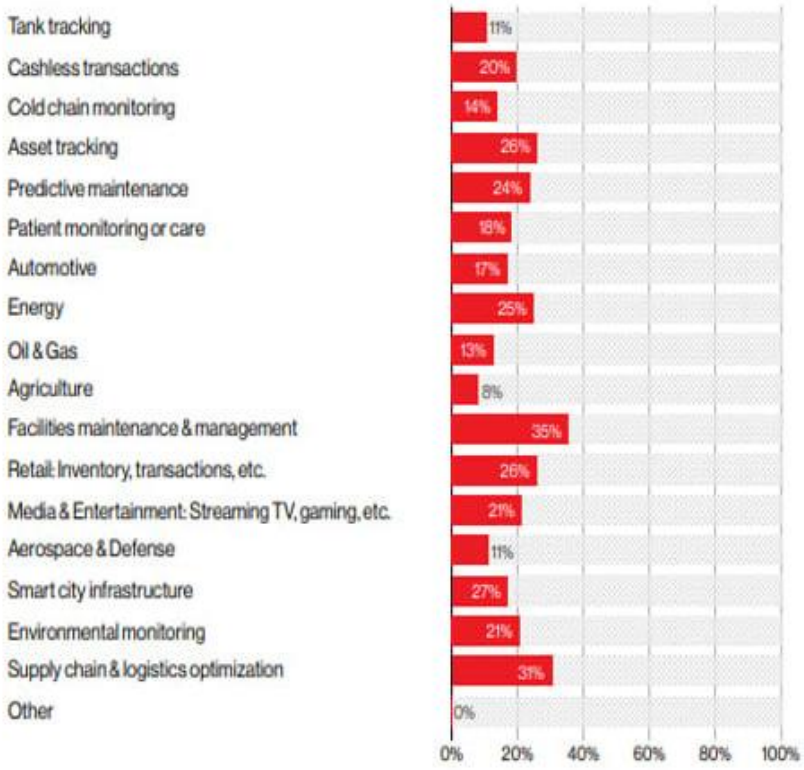
Мета роботи – розробити рекомендації щодо впровадження та використання технології уніфікованого керування безпекою корпоративних мобільних пристроїв на основі Sophos Mobile.

Наукові завдання:

- Дослідити сутність проблеми забезпечення уніфікованого керування безпекою корпоративних мобільних пристроїв;
- проаналізувати підходи до забезпечення уніфікованого керування безпекою корпоративних мобільних пристроїв;
- проаналізувати існуючі рішення із забезпечення уніфікованого керування безпекою корпоративних мобільних пристроїв;
- проаналізувати методи та засоби забезпечення уніфікованого керування безпекою корпоративних мобільних пристроїв на базі Sophos Mobile;
- розкрити порядок реалізації технології забезпечення уніфікованого керування безпекою корпоративних мобільних пристроїв на базі Sophos Mobile.

ДОСЛІДЖЕННЯ ПРОБЛЕМИ УНІФІКОВАНОГО КЕРУВАННЯ БЕЗПЕКОЮ КОРПОРАТИВНИХ МОБІЛЬНИХ ПРИСТРОЇВ

Технологія уніфікованого керування безпекою корпоративних мобільних пристроїв (MDM) стала надзвичайно актуальною у світлі стрімкого зростання використання мобільних технологій у бізнес-середовищі. У сучасному світі, де мобільність, гнучкість та швидкість є ключовими факторами успіху, організації все частіше впроваджують мобільні пристрої в свою щоденну діяльність. Це створює нові можливості, але водночас й виклики, особливо в контексті безпеки даних.

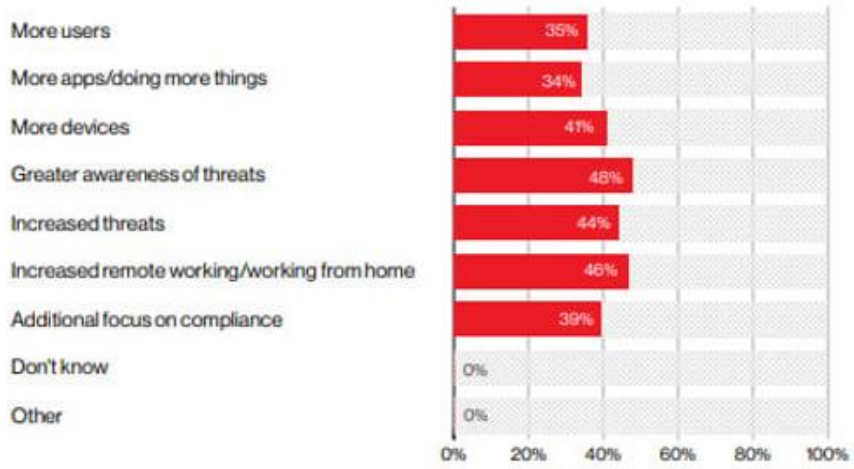


Розповсюдженість використання корпоративних мобільних пристроїв у критичних інфраструктурах

Аналіз підходів до уніфікованого керування безпекою корпоративних мобільних пристроїв

За останнє десятиліття кількість мобільних пристроїв і платформ у корпоративних середовищах значно зросла, а вимоги до їхньої безпеки стали більш складними. Це спричинено поширенням моделей BYOD (Bring Your Own Device) та необхідністю інтеграції з хмарними сервісами. Така ситуація підвищила потребу в централізованих рішеннях, які об'єднують захист, управління доступом, контроль даних і реагування на інциденти в єдиній платформі. Уніфіковане керування безпекою корпоративних мобільних пристроїв дозволяє компаніям створити інтегрований підхід до захисту даних та пристроїв, забезпечуючи одночасно зручність для користувачів і відповідність сучасним стандартам безпеки.

Причини збільшення витрат на мобільну безпеку

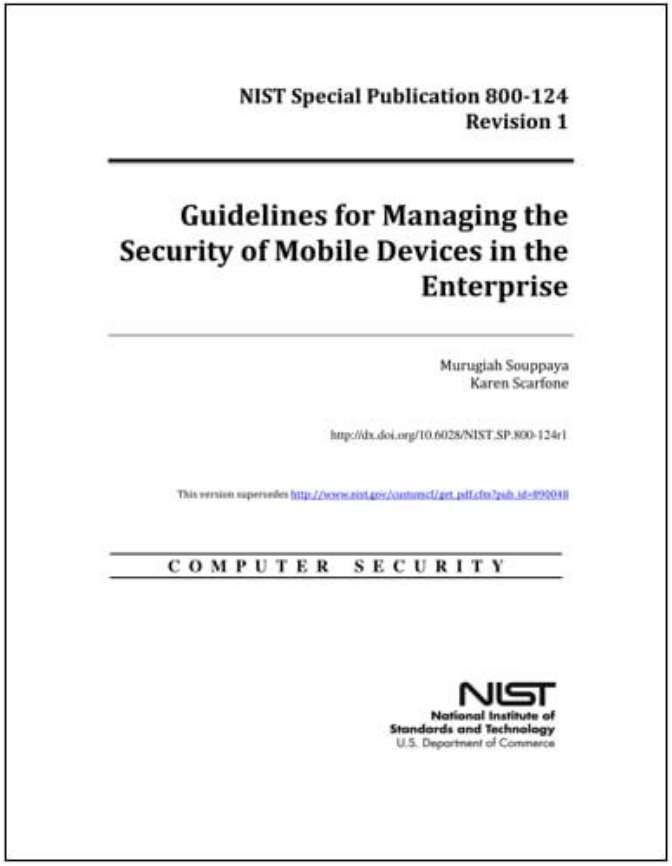


Зі зростанням кількості мобільних пристроїв у корпоративному середовищі, а також розмаїттям платформ та операційних систем, фахівцям з кібербезпеки стало важче забезпечувати централізований контроль і моніторинг безпеки цих пристроїв. Виникнення нових загроз, таких як шкідливе ПЗ, витік корпоративних даних через ненадійні додатки або незахищені мережі, ускладнює управління безпекою кожного пристрою окремо. У цьому контексті головну роль відіграють системи уніфікованого керування кінцевими точками (Unified Endpoint Management, UEM).

Стандарт NIST SP 800-124 Revision 2 надає рекомендації щодо управління безпекою мобільних пристроїв а також стосується уніфікованого управління безпекою корпоративних мобільних пристроїв і надає рекомендації щодо забезпечення безпеки мобільних пристроїв у корпоративних середовищах. Основні аспекти цього стандарту включають наступне: Розробка політик безпеки мобільних пристроїв, Управління ризиками, Управління пристроями через Mobile Device Management (MDM), Захист даних, Аутентифікація та контроль доступу, Моніторинг і виявлення загроз, Віддалене блокування та видалення даних, Оновлення програмного забезпечення

Цей стандарт пропонує комплексний підхід до управління безпекою мобільних пристроїв, охоплюючи не лише технічні заходи, але й процеси та політики, які мають бути впроваджені для мінімізації ризиків.

NIST SP 800-124 Revision



NIST Special Publication 800-124
Revision 1

Guidelines for Managing the Security of Mobile Devices in the Enterprise

Murugiah Souppaya
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-124r1

This version supersedes http://www.nist.gov/customcf/get_pdf.cfm?pub_id=890048

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

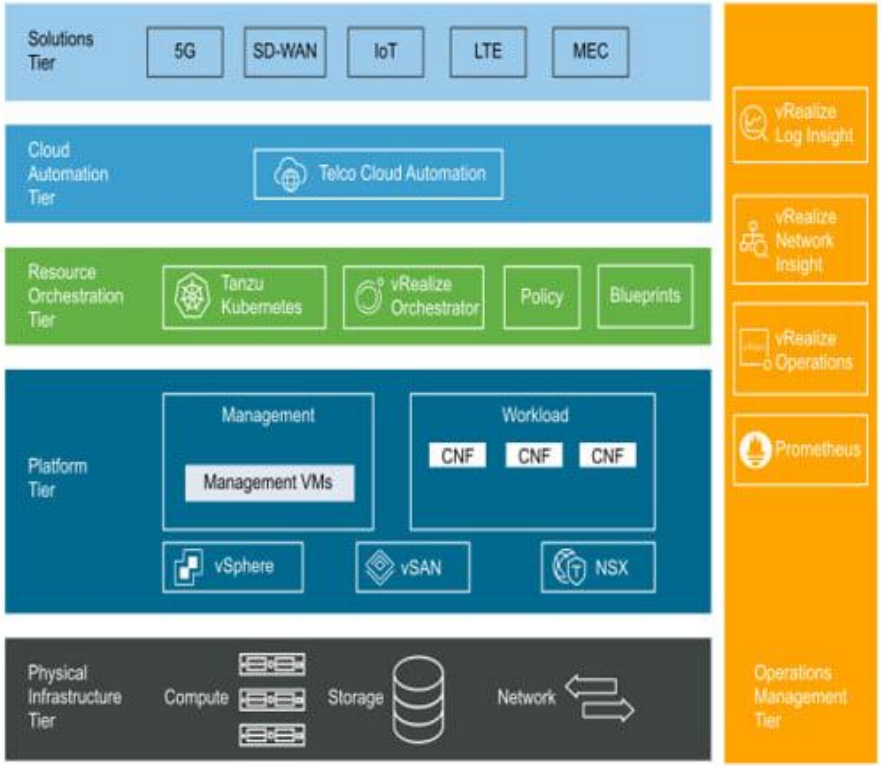
Gartner Magic Quadrant є одним із найавторитетніших джерел аналізу технологій. Його мета - допомогти організаціям оцінити постачальників рішень. Gartner надає короткий огляд функціональних можливостей для кожного обговорюваного рішення та розміщує їх у Quadrant для загальної візуалізації, класифікуючи їх за чотирма категоріями: «лідери», «претенденти», «провидці» та «нішеві гравці».

Магічний квадрант Гартнера за 2022 рік для платформ з технолгоіями уніфікованого керування безпекою корпоративних мобільних пристроїв

Аналіз існуючих рішень щодо уніфікованого керування безпекою корпоративних мобільних пристроїв

VMware

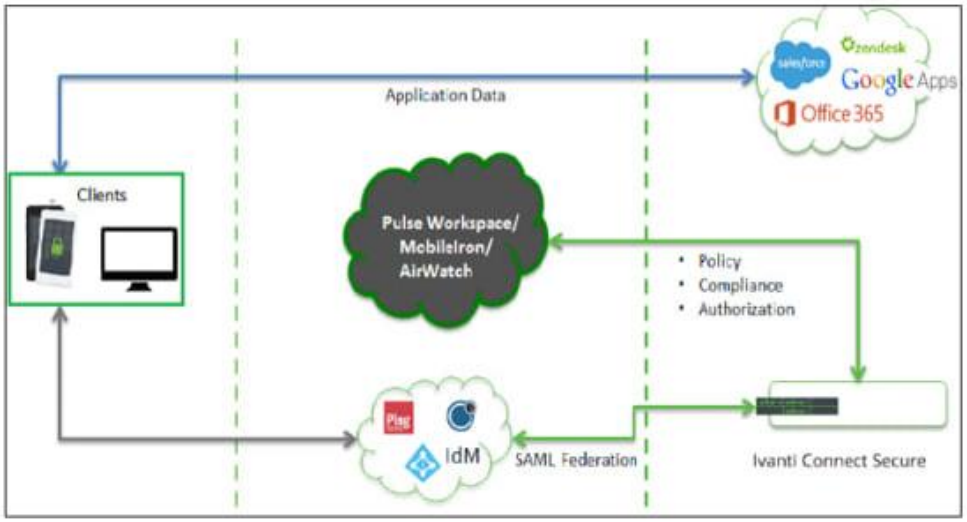
Вендор пропонує рішення для управління безпекою корпоративних мобільних пристроїв через свій продукт VMware Workspace ONE. Це комплексна платформа для управління мобільними пристроями (MDM) та забезпечення корпоративної безпеки, яка об'єднує різні технології для управління та захисту мобільних пристроїв, додатків і корпоративних даних.



Аналіз існуючих рішень щодо уніфікованого керування безпекою корпоративних мобільних пристроїв

Mobileron (Ivanti)

MobileIron, яка тепер є частиною Ivanti, пропонує рішення для управління безпекою корпоративних мобільних пристроїв через платформу Ivanti Neurons for MDM (MobileIron).

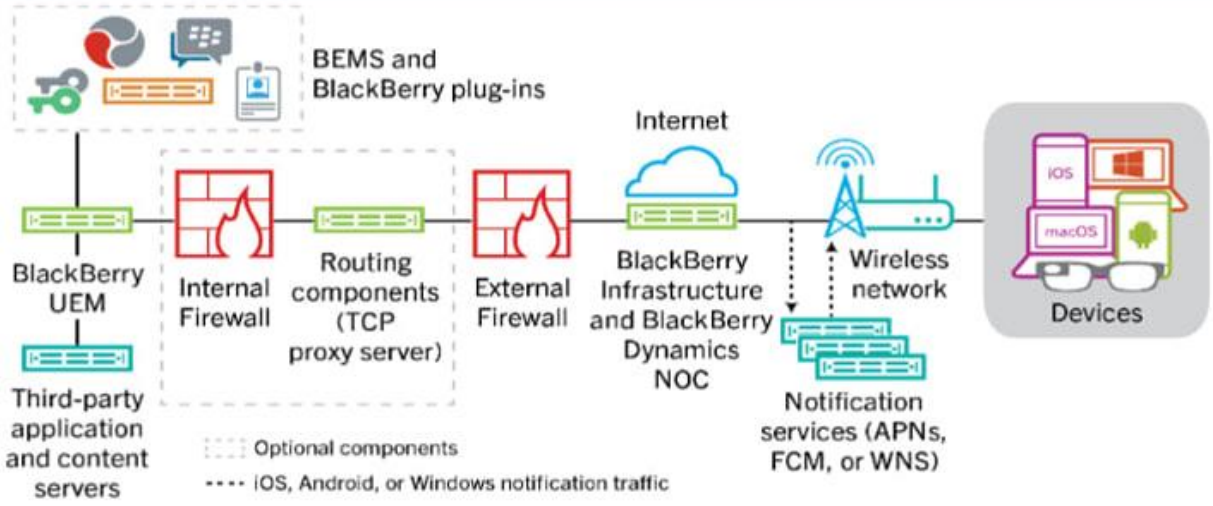


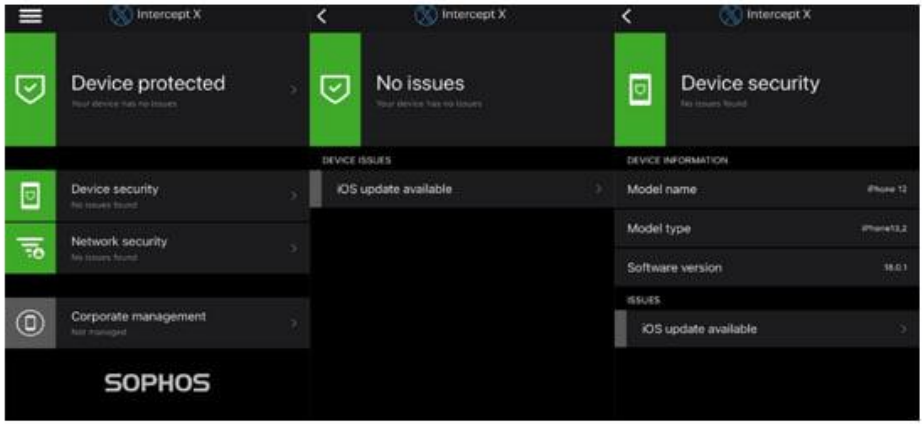
Це рішення поєднує управління мобільними пристроями (MDM), управління мобільними додатками (MAM) та управління мобільним контентом (MCM) в єдиній платформі, орієнтованій на забезпечення корпоративної безпеки.

Аналіз існуючих рішень щодо уніфікованого керування безпекою корпоративних мобільних пристроїв

Blackberry

BlackBerry, відома колись як провідний виробник смартфонів, сьогодні спеціалізується на корпоративних рішеннях кібербезпеки та управління мобільними пристроями. Її рішення для управління безпекою корпоративних мобільних пристроїв представлені через BlackBerry UEM (Unified Endpoint Management), що забезпечує надійне управління кінцевими точками, захист мобільних пристроїв, і захист даних на різних платформах

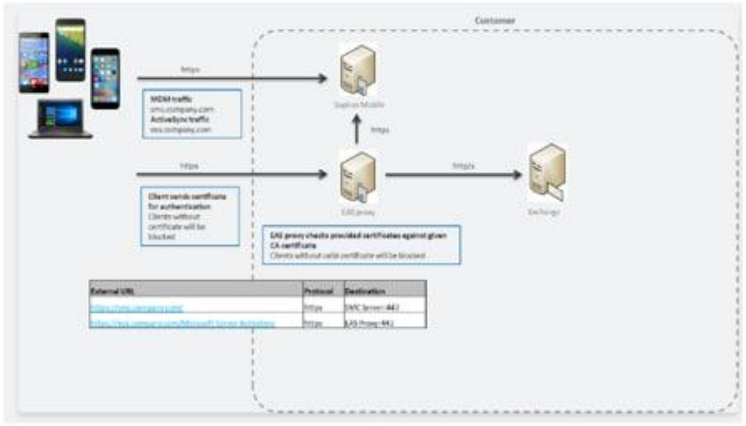


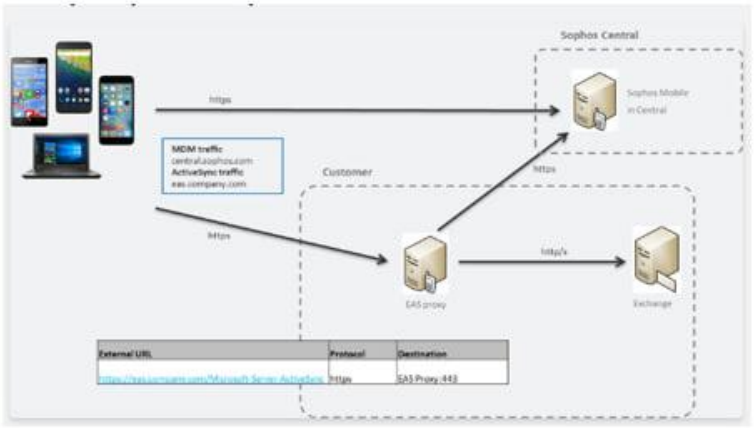


Призначення та основні функції рішення Sophos Mobile

Дане рішення призначене для управління мобільними пристроями (MDM, Mobile Device Management), яке дозволяє організаціям безпечно управляти мобільними пристроями, використовувати їх для корпоративних цілей та забезпечувати належний рівень захисту даних. Призначення рішення полягає в централізованому управлінні мобільними пристроями, забезпеченні їх безпеки, контролі за використанням мобільних додатків, а також у підтримці відповідності вимогам безпеки та нормативним актам. Це рішення дає можливість централізовано управляти мобільними пристроями співробітників на платформі Android та iOS, що важливо для організацій, що використовують політику BYOD (Bring Your Own Device) або корпоративні мобільні пристрої.

Архітектура рішення Sophos Mobile, призначення та основні функції компонентів



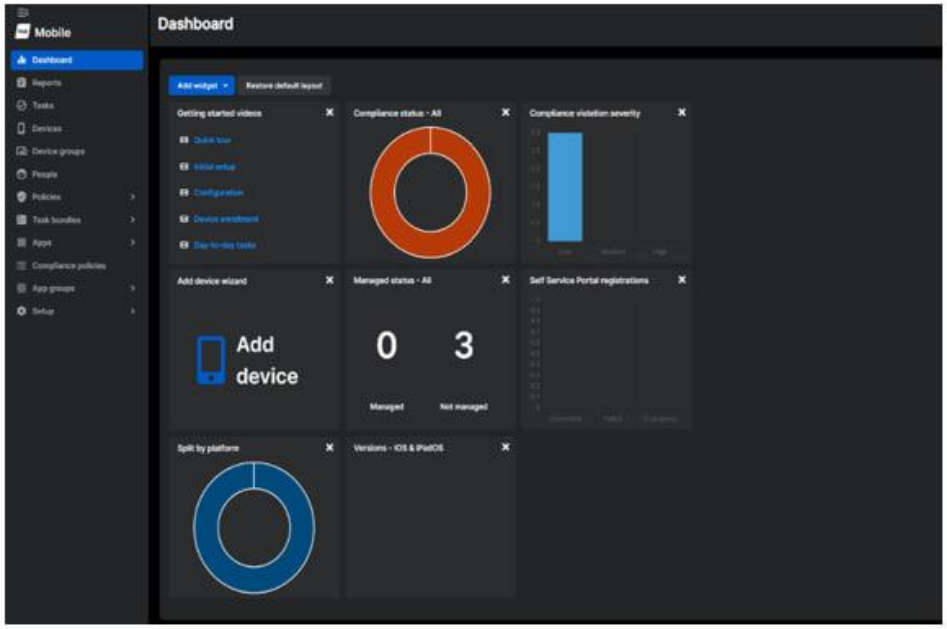


Сервер Sophos Mobile: є основою системи, яка забезпечує зв'язок між пристроями, адміністративною консоллю та агентами на мобільних пристроях. Він відповідає за зберігання та обробку інформації, що стосується політик безпеки, конфігурацій і стану пристроїв.

Консоль адміністратора: є веб-інтерфейсом для адміністраторів, який надає всі необхідні інструменти для управління мобільними пристроями та політиками безпеки.

Прикладний агент (Sophos Mobile Agent): це застосунок, що встановлюється на кожен пристрій, який є частиною корпоративної інфраструктури безпеки.

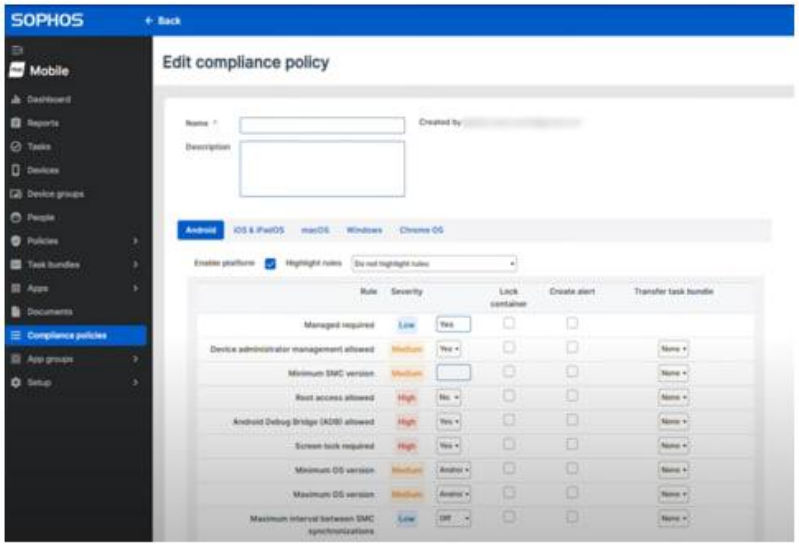
Технологія Sophos Anti-Malware забезпечує найвищий рівень захисту від шкідливого ПЗ, виявлення потенційно небезпечних додатків, веб-захист та фільтрацію небажаного контенту. Постійний моніторинг стану безпеки пристрою інформує кристувача про потенційні загрози та автоматично обмежує доступ до корпоративних ресурсів у випадку компрометації.

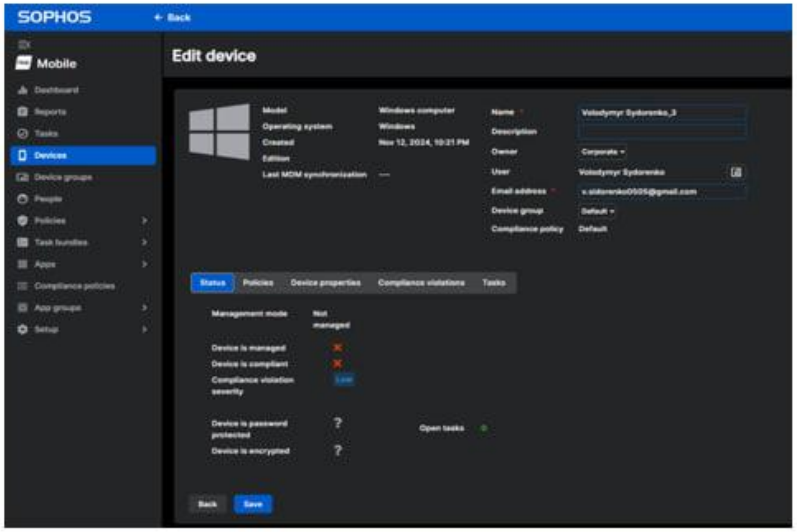


Можливості рішення Sophos Mobile щодо уніфікованого керування безпекою корпоративних мобільних пристроїв

Розроблена спеціально для мобільних пристроїв, Sophos Mobile Security розпізнає шкідливі або небажані додатки, що можуть спричинити витік даних, втрати інформації чи надмірні витрати на використання мережі. У разі втрати чи крадіжки пристрою функція віддаленого блокування і видалення даних (включаючи кеш, паролі тощо) захистить особисту інформацію від сторонніх.

Sophos Mobile Security виділяється серед рішень UEM завдяки комплексному підходу до захисту пристроїв, легкості управління та інтеграції з іншими продуктами Sophos. Завдяки інтеграції з єдиною екосистемою Sophos Central, зокрема з Intercept X, програма дозволяє IT-відділам контролювати безпеку всіх пристроїв - мобільних, комп'ютерів і серверів - з єдиної консолі, що спрощує управління безпекою і дає змогу оперативно реагувати на інциденти. Перевагою Sophos Mobile Security є комплексний захист у реальному часі: інтеграція з лабораторіями SophosLabs забезпечує захист пристроїв від новітніх загроз, включаючи шкідливі програми, фішинг та інтернет-атаки, а також постійне оновлення баз загроз, що гарантує захист від останніх кіберзагроз. Додатково, Sophos Mobile Security дозволяє автоматично відкликати доступ до корпоративних даних і додатків, якщо пристрій виявлений як скомпрометований, знижуючи ризик витоку конфіденційних даних навіть при втраті або крадіжці пристрою.





Рекомендації щодо застосування методів та засобів управління кіберінцидентами в інформаційній системі організації

Рекомендується обирати системи, що підтримують різні операційні системи, зокрема. Це забезпечить можливість централізованого контролю над усіма пристроями в компанії. Сучасні MDM-рішення повинні надавати функції дистанційного блокування пристрою, стирання даних, гнучке налаштування політик для різних категорій пристроїв.

Необхідно використовувати рішення для захисту від мобільних загроз. Ці системи допомагають виявляти й запобігати шкідливим програмам. Інтеграція з антивірусними сервісами, що автоматично оновлюються, є обов'язковою вимогою для зменшення ризиків.

Варто налаштувати політики відповідності, що визначатимуть вимоги до пристроїв, зокрема актуальність оновлень, наявність шифрування й активного антивірусу. Пристрої, які не відповідають цим вимогам, повинні автоматично втрачати доступ до корпоративних ресурсів.

Шифрування даних, як під час їх передачі, так і на пристроях, має бути стандартом для всіх мобільних пристроїв. Впровадження багатофакторної аутентифікації (MFA) допоможе додатково захистити доступ до корпоративних ресурсів.

MDM-рішення повинні бути інтегровані з іншими інструментами безпеки, такими як SIEM-системи, VPN-сервіси для захищеного доступу до корпоративної мережі та системи захисту веб-доступу.

Необхідно регулярно оновлювати MDM-системи й операційні системи мобільних пристроїв. Рекомендується впроваджувати автоматичне розгортання оновлень, а перед цим тестувати їхню сумісність.

ВИСНОВОК

У роботі проведено дослідження проблеми уніфікованого керування безпекою корпоративних мобільних пристроїв, визначено її мету та завдання.

Проведено аналіз існуючих технологій уніфікованого керування мобільними пристроями, які спрямовані на захист даних і забезпечення безпеки мобільних пристроїв у корпоративному середовищі.

Досліджено функціональні можливості Sophos Mobile, які включають: управління пристроями через профілі та політики безпеки; забезпечення шифрування даних і управління доступом; інтеграцію з системами автентифікації (SSO, MFA); виявлення та реагування на загрози за допомогою технологій штучного інтелекту.

На основі проведених досліджень запропоновано порядок впровадження Sophos Mobile у корпоративну інфраструктуру, включаючи налаштування політик безпеки, інтеграцію з іншими засобами управління інформаційною безпекою, а також моніторинг та аналітику.

Розроблено рекомендації для фахівців з кібербезпеки щодо використання Sophos Mobile з метою підвищення загального рівня захисту корпоративних даних, особливо в умовах використання моделі BYOD (Bring Your Own Device).

Дякую за увагу!