



# ЗАХИСТ ВАШОГО ОФІСУ

**Canon**



**McAfee**  
PROTECTED

Canon uniFLOW Online  
Outstanding Cloud Output-Management Solution

New to the Line



# НАСКІЛЬКИ ЗАХИЩЕНА ІНФОРМАЦІЯ У ВАШОМУ ОФІСІ?

Сьогодні для роботи компаній дуже важливою є інформація, через що виникають складні мережі пов'язаних технологій, процесів, людей та організацій, які перетинають національні кордони. Виникають нові гнучкі робочі методиками, повністю змінюючи робочий простір та процеси створення, спільного використання та споживання інформації. Захист даних у такому непростому середовищі – більш складне завдання, ніж будь-коли раніше, і більшість компаній інвестують в передові технології, такі як надійні брандмауери, сучасні засоби антивірусного захисту, захисне програмне забезпечення тощо. Проте вони часто не розуміють, що захист необхідно поширювати й на офісні принтери, через що залишаються більш вразливими, ніж їм здається.



## ПОДУМАЙТЕ ПРО ВАШІ ПРИНТЕРИ

Сучасні багатофункціональні принтери (multifunctional printers, MFP) перетворилися на потужні інструменти, які, аналогічно комп'ютерам і серверам, мають операційну систему та величезний жорсткий диск, підключені до мережі та Інтернету і спільно використовуються багатьма робітниками для оброблення великої кількості найважливіших документів щодня.



## ЯКІ РИЗИКИ?

- Доступ сторонніх користувачів до важливої інформації на незахищених MFP-пристроях
- Можливість ураження вашої інфраструктури друку через помилки в роботі
- Отримання зловмисниками з-за меж організації доступу до вашої мережі через принтер для його подальшого використання з метою атак
- Розкриття важливих документів, що залишилися у вивідному лотку після друку
- Змішування надрукованих документів, що належать різним користувачам
- Надсилання документів факсом або електронною поштою не тому отримувачу через помилку під час введення адреси
- Перехоплення зловмисниками даних, що передаються під час друку або сканування
- Втрата даних через недбалу утилізацію принтерів після завершення їхньої експлуатації

«Прийняття стандартів інформаційної безпеки – дуже розумний вчинок в офісі, де ви можете працювати з величезними об'ємами даних. Принтер сьогодні – це не просто німа машина, а справжній сервер, який також може друкувати».

(CISO, Publicis Groupe)

# РІШЕННЯ ДЛЯ ЗАХИЩЕНОГО ДРУКУ ДЛЯ ВАШОГО БІЗНЕСУ

## Вбудовані безпека та конфіденційність

Коли ми розробляємо або вибираємо технології, продукти чи послуги для наших клієнтів, ми оцінюємо їхній потенційний вплив з точки зору безпеки на клієнтське середовище. Саме тому наші офісні багатофункціональні принтери обладнані цілою низкою засобів безпеки, як стандартних, так і опціональних, що дозволяють компанії будь-якого розміру досягти бажаного рівня захисту всіх компонентів:



ПРИСТРОЇВ



МЕРЕЖ



ДОКУМЕНТІВ



УСЬОГО  
ПІДПРИЄМСТВА



**МІЖНАРОДНІ  
СТАНДАРТИ ТА  
СЕРТИФІКАЦІЇ**

Наші багатофункціональні принтери imageRUNNER ADVANCE проходять обов'язкову оцінку та сертифікацію з використанням методики загальних критеріїв (Common Criteria) та відповідно до вимог стандартів IEEE2600, що регламентують питання безпеки друкувальних пристроїв.



**АНАЛІЗ РІВНЯ  
БЕЗПЕКИ**

У компанії Canon – один з найсуворіших режимів тестування на безпеку в галузі офісного обладнання. Технології, що використовуються в наших виробках, проходять перевірку відповідно до саме таких високих стандартів, які ми застосовуємо і в нашому власному бізнесі.

Canon як галузевий лідер в області розроблення інноваційних рішень для керування друком та інформацією для офісу та бізнесу допомагає клієнтам запровадити інклюзивний підхід до інформаційної безпеки, що враховуватиме наслідки з точки зору безпеки від наших офісних технологій в контексті всієї інформаційної екосистеми клієнта.



# ЗАХИСТ ВАШОГО ПРИСТРОЮ

## Комплексний захист фізичних активів



### РІШЕННЯ ДЛЯ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

Щоб захистити пристрій від несанкціонованого використання, слід запровадити засоби керування доступом користувачів через автентифікацію. Додатковою перевагою цього є прискорення доступу користувачів до їхніх налаштувань та завдань друку на фоні підвищення контрольованості й рівня керування. Наші принтери для організацій обладнані гнучким рішенням для входу Universal Login Manager, яке дозволяє реалізувати автентифікацію користувачів на основі бази даних облікових записів, створеної на пристрої, а також автентифікацію в домені через сервер Active Directory або uniFLOW. Це надає компаніям змогу контролювати доступ до пристроїв, забезпечуючи при цьому оптимальний баланс між зручністю та безпекою.



### ЗАХИСТ ДАНИХ НА ЖОРСТКОМУ ДИСКУ

У будь-який момент часу багатофункціональний принтер містить значні об'єми даних, які потребують захисту – від завдань друку, що очікують виконання, до отриманих факсів, відсканованих даних, адресних книжок, журналів активності та історії завдань. Пристрої Canon обладнані цілою низкою заходів для захисту даних на кожному етапі життєвого циклу та забезпечують конфіденційність, цілісність та доступність інформації.



### СИСТЕМА КЕРУВАННЯ ДОСТУПОМ

Ця функція забезпечує тонкий контроль над доступом до функцій пристрою. Адміністратори можуть використовувати стандартні або створювати власні ролі з бажаним рівнем прав доступу. Наприклад, певним користувачам можна заборонити копіювати документи або користатися функцією надсилання.



### НАЛАШТУВАННЯ ПОЛІТИКИ БЕЗПЕКИ

Найновіші пристрої imageRUNNER ADVANCE також підтримують налаштування політик безпеки, що забезпечує адміністратору доступ до всіх пов'язаних з безпекою параметрів через єдине меню та можливість відредагувати їх, перш ніж застосовувати на комп'ютері. Після застосування робота з пристроєм та всі зміни параметрів мають відповідати встановленій політиці. Політику безпеки можна захистити окремим паролем, щоб обмежити доступ до відповідних розділів, надаючи його лише відповідальним IT-спеціалістам з безпеки, що є додатковим рівнем контролю й захисту.



### АДМІНІСТРАТИВНЕ КЕРУВАННЯ ПРИСТРОЯМИ

Конфігурація пристроїв, така як налаштування мережі та інші параметри керування, доступна лише користувачам з правами адміністратора, що запобігає її навмисному або випадковому змінненню.



### ПРЕВЕНТИВНА БЕЗПЕКА

Продукти imageRUNNER ADVANCE мають певні налаштування безпеки, які дозволяють захистити принтери від атак. Функція перевірки системи під час захисту забезпечує цілісність даних на пристрої після його завантаження, а програмне забезпечення McAfee Embedded Control Software захищає пристрій протягом усього періоду його експлуатації, не дозволяючи модифікувати програми або запускати неавторизоване програмне забезпечення. Крім того, журнал системних даних у реальному часі надає інформацію про стан захисту пристрою, а також допомагає контролювати його (дані можуть бути зчитані відповідною сторонньою системою SIEM).



## НАСКІЛЬКИ ЗАХИЩЕНІ ВАШІ ПРИСТРОЇ?

**1**

Чи використовуються ваші пристрої в спільному режимі, і чи розташовані вони в загальнодоступних місцях?

**2**

Чи можуть користувачі отримати несанкціонований доступ до пристроїв?

**3**

Чи запроваджені у вас заходи захисту інформації на жорстких дисках пристроїв?

**4**

Чи можуть сторонні користувачі змінювати налаштування пристроїв?

**5**

Чи розглядали ви життєвий цикл свого пристрою та питання його безпечної утилізації?

### ШИФРУВАННЯ ЖОРСТКОГО ДИСКА

Наші пристрої imageRUNNER ADVANCE шифрують всі дані на жорсткому диску, підвищуючи їхню безпеку. Мікросхема безпеки, відповідальна за шифрування даних, відповідає стандарту безпеки FIPS 140-2 рівня 2, встановленому урядом США, та сертифіковано відповідно до Програми перевірки криптографічного модуля (CMVP), створеної США і Канадою, а також Програма перевірки криптографічного модуля Японії (JCMVP).

### ОЧИЩЕННЯ ЖОРСТКОГО ДИСКА

Певна інформація, така як дані скопійованих або відсканованих зображень чи документів, які надсилаються на друк з комп'ютера, зберігається на жорсткому диску лише тимчасово і видаляється, щойно операція буде завершено. Щоб гарантувати видалення всіх залишків інформацію, наші пристрої, обладнані жорсткими дисками, дозволяють у стандартному режимі видаляти такі дані в рамках виконання відповідного завдання.

### ІНІЦІАЛІЗАЦІЯ ВСІХ ДАНИХ І НАЛАШТУВАНЬ

Щоб запобігти втраті даних під час заміни чи утилізації жорсткого диска, ви можете перезаписати на ньому всі документи та інформацію, а також відновити значення за замовчуванням для всіх параметрів.

### ДЗЕРКАЛЬНЕ ВІДОБРАЖЕННЯ ЖОРСТКОГО ДИСКА \*

Компанії можуть створювати резервні копії даних із жорстких дисків своїх пристроїв на додаткових дисках. Під час дзеркального відображення дані на обох дисках повністю шифруються.

\*Не обов'язкова, для окремих моделей тільки. За докладною інформацією про доступність компонентів та функцій у рішеннях для офісного друку звертайтеся до свого представника Canon.



# ЗАХИСТІТЬ СВОЮ МЕРЕЖУ



## ЧИ МОЖЕ ПРИНТЕР ПІДАТИ ВАШУ МЕРЕЖУ РИЗИКУ?

- Чи залишаєте ви порти мережі відкритими для атаки?
- Чи можуть ваші гості друкувати й сканувати документи, не піддаючи вашу мережу ризикам?
- Чи безпечна та реалізовна політика використання власних пристроїв на роботі у вашій організації?
- Чи шифруються потоки даних для друку з комп'ютерів на вивідні пристрої?
- Чи захищені дані друку та сканування під час передавання?

# Canon пропонує низку рішень в області безпеки, які захистять вашу мережу та інформацію від внутрішніх та зовнішніх атак.

## ФІЛЬТРУВАННЯ IP- ТА MAC-АДРЕС

Захистіть свою мережу від несанкціонованого доступу з боку третіх осіб, дозволивши обмін даними – як на вхід, так і на вихід – лише з пристроями з певними IP- чи MAC-адресами.

## КОНФІГУРАЦІЯ ПРОКСІ-СЕРВЕРА

Налаштуйте проксі-сервер, який буде відповідати за обмін даними замість вашого комп'ютера, і використовуйте його для з'єднання з пристроями за межами вашої мережі.

## АВТЕНТИФІКАЦІЯ IEEE 802.1X

Несанкціонований доступ до мережі буде заблоковано LAN-комутатором, який надаватиме права доступу лише клієнтським пристроям, що авторизувалися на сервері автентифікації.

## КАНАЛ IPSEC

Канал IPSec для обміну даними запобігає перехопленню або несанкціонованому зміні IP-пакетів, що передаються через IP-мережу.

Ви можете користатися зашифрованим за допомогою TLS каналом для боротьби з прослуховуванням, спуфінгом або підробленням даних, якими обладнання обмінюється з іншими пристроями, такими як комп'ютери.

## КОНТРОЛЬ ЗА ПОРТАМИ

Налаштуйте порти в рамках своєї політики безпеки.

## АВТОМАТИЧНА РЕЄСТРАЦІЯ СЕРТИФІКАТІВ

Ця функція позбавляє вас від основної частини клопоту, пов'язаного з обслуговуванням сертифікатів безпеки. Використовуючи визнану в галузі технологію, системний адміністратор може автоматично оновлювати та випускати сертифікати, гарантуючи постійне дотримання політик безпеки.

## МОНІТОРИНГ ЖУРНАЛІВ

Різні журнали дозволяють відстежувати операції з вашим пристроєм, включаючи заблоковані запити на обмін даними.

## WI-FI DIRECT

Ви можете дозволити безпосередній обмін даними для друку з мобільних пристроїв, не надаючи їм доступ до вашої мережі.

## ШИФРУВАННЯ ДАНИХ ПІД ЧАС ПЕРЕДАВАННЯ НА ПРИСТРІЙ ТА З НЬОГО

Ця функція шифрує завдання друку, які передаються з користувацьких комп'ютерів на багатофункціональний принтер. Набір універсальних функцій безпеки також може шифрувати відскановані дані у форматі PDF.

## ГОСТЬОВИЙ ДРУК З МОБІЛЬНИХ ПРИСТРОЇВ

Наше програмне забезпечення для керування безпечним друком і скануванням у мережі позбавляє вас від поширених ризиків, пов'язаних із друком з мобільних пристроїв та гостьовим друком, завдяки можливості надсилати завдання через зовнішні канали – електронну пошту, Інтернет чи мобільний додаток. Це скорочує кількість векторів атаки, прив'язуючи багатофункціональний пристрій до захищеного джерела.

## ПІДТРИМКА ДВОХ МЕРЕЖ

До числа технологічних вдосконалень додано підтримку двох мереж: основне мережеве підключення має завжди бути дротовим, а додаткове тепер може бути дротовим або бездротовим, що дозволяє надійніше ізолювати мережеві середовища.



# ЗАХИСТ ВАШИХ ДОКУМЕНТІВ

Усім компаніям доводиться працювати з важливими документами, такими як контрактні угоди, інформація про заробітну платню персоналу, клієнтські дані, плани досліджень і розробок тощо. Якщо такі документи опиняться не в тих руках, це може призвести до різних наслідків – від репутаційних збитків до великих штрафів або навіть юридичних позовів.

**Canon пропонує цілу низку рішень в галузі безпеки для захисту ваших важливих документів на всіх етапах їхнього життєвого циклу.**



## КОНФІДЕНЦІЙНІСТЬ НАДРУКОВАНИХ ДОКУМЕНТІВ

### Захищений друк

Користувач може встановити PIN-код для друку, який потрібно буде ввести на пристрої, перш ніж можна буде роздрукувати документ. Це дозволяє робітникам захищати документи, які вони вважають конфіденційними.

### Припинення всіх завдань друку

Адміністратор може ініціювати на пристрої imageRUNNER ADVANCE припинення всіх завдань друку, після чого користувачі матимуть виконати вхід, перш ніж вони зможуть виконати завдання друку, що дозволяє захистити конфіденційність усіх друківаних документів.

### Поштові скриньки

Завдання друку або відскановані документи можна зберігати в поштовій скриньці для доступу пізніше. Поштові скриньки можуть бути захищені PIN-кодом, завдяки чому доступ до їхнього вмісту матиме лише призначений власник. У цьому захищеному просторі на комп'ютері можна зберігати документи, які часто друкуються (наприклад, форми), але потребують обережного ставлення.

### Захищений друк uniFLOW \*

Із функцією захищеного друку uniFLOW MyPrintAnywhere користувачі надсилають завдання на друк через універсальний драйвер на будь-який принтер в мережі.



## УСКЛАДНЕННЯ ЧИ УНИКНЕННЯ ДУБЛЮВАННЯ ДОКУМЕНТІВ

### Друк з помітними водяними знаками

Драйвери підтримують можливість накладання на сторінку помітних позначок зверху або під вмістом документа. Це запобігає копіюванню таких документів, тож користувач бачить, що він є конфіденційним.

### Друк та копіювання з невидимими водяними знаками

За допомогою цієї функції документи можна друкувати або копіювати з прихованим на фоні текстом, який стає видно на документі після його копіювання.

### Запобігання втраті даних на корпоративному рівні

Перейдіть на рішення iW SAM Express в поєднанні з uniFLOW, що розширяють ваші можливості із запобігання втраті даних. Це серверне рішення дозволяє реєструвати та архівувати документи, що надсилаються на принтер та з нього, аналізувати та інтерпретувати їх на основі тексту чи інших атрибутів з метою запобігти можливим небезпекам.

### Відстеження походження документів \*

На основі доданого в документ коду можна відстежити його походження до самого джерела.



## НАСКІЛЬКИ ЗАХИЩЕНІ ВАШІ ДОКУМЕНТИ?

1

Чи заблокований доступ до важливих документів у принтері для сторонніх користувачів?

2

Чи можна гарантувати конфіденційність усіх користувацьких документів, що проходять через спільний пристрій?

3

Чи можна відстежити походження надрукованих документів?

4

Чи може хтось просто забрати важливі документи з принтера?

5

Чи забезпечуєте ви захист від поширених помилок під час надсилання документів з пристроєм?



## КОНТРОЛЬ ЗА НАДСИЛАННЯМ ДОКУМЕНТІВ ПОШТОЮ І ФАКСОМ

### Обмеження кола потенційних отримувачів

Щоб зменшити ризик витоку інформації, адміністратори можуть обмежити коло потенційних одержувачів, дозволивши надсилати документи лише контактам з адресної книжки на LDAP-сервері чи адресного списку користувача, який увійшов до системи, або отримувачам з певних доменів.

### Вимкнення автоматичного заповнення адрес

Щоб запобігти надсиланню документів на невірні адреси, ви можете увімкнути автоматичне підставлення електронних адрес.

### Захист адресної книжки

Щоб захистити адресну книжку пристроєм від несанкціонованого змінення іншими користувачами, встановіть PIN-код.

### Підтвердження номерів факсів

Щоб запобігти надсиланню документів помилковим одержувачам, вимагайте від користувачів подвійного введення номера факсу для його підтвердження.

### Конфіденційність документів, отриманих через факс

Налаштуйте пристрій таким чином, щоб документи зберігалися в пам'яті без друку. Щоб захистити конфіденційність документів, отриманих через факс, також можна налаштувати умови їхнього збереження в конфіденційній поштовій скриньці або встановити PIN-коди.



## ПЕРЕВІРКА ПОХОДЖЕННЯ ТА АВТЕНТИЧНОСТІ ДОКУМЕНТІВ ЗА ДОПОМОГОЮ ЕЛЕКТРОННИХ ПІДПИСІВ

### Підпис пристроєм

До відсканованих документів у форматах PDF та XPS можна застосовувати підписи пристроїв на базі механізму ключа та сертифіката, завдяки чому отримувачі зможуть перевіряти походження та автентичність документів.

### Підпис користувача \*

Із цією функцією користувачі можуть надсилати PDF- та XPS-файли зі своїми унікальними підписами, які вони отримуватимуть від центра сертифікації. Завдяки цьому отримувач завжди зможе перевірити, який саме користувач підписав документ.



## ЗАСТОСУВАННЯ ПОЛІТИК З ІНТЕГРАЦІЄЮ З ADOBE LIFECYCLE MANAGEMENT ES

Користувачі можуть захищати PDF-файли та встановлювати постійні чи динамічні політики контролю доступу та користувацьких прав з метою захисту цінної інформації від випадкового чи навмисного розкриття. Політики безпеки

налаштовуються на серверному рівні, тому права доступу можна змінити навіть після розповсюдження файлу. Пристрої серії imageRUNNER ADVANCE можна налаштувати для інтеграції з Adobe® ES.

\* Додатковий компонент. За докладною інформацією про доступність компонентів та функцій у рішеннях для офісного друку звертайтеся до свого представника Canon.



# БЕЗПЕКА КОРПОРАТИВНОЇ ІНФОРМАЦІЇ

Canon може зробити свій внесок до загальної справи захисту інформації у вашій організації.

## ПОВНИЙ КОНТРОЛЬ ЗА ВСІМ СПЕКТРОМ ОПЕРАЦІЙ З ОТРИМАННЯ ТА ВИВЕДЕННЯ ДОКУМЕНТІВ

Наше модульне програмне забезпечення для керування виведенням допомагає компаніям забезпечити захист мережевих пристроїв, що використовуються в спільному режимі, дозволяючи надсилати документи для друку на будь-який принтер, під'єднаний до сервера керування. Користувачі мобільних пристроїв працюють через службу із централізованим контролем, де як внутрішні, так і гостьові користувачі мають захищений доступ до функцій друку з мобільних пристроїв. Для сканування документів на підприємствах окремий програмний модуль відповідає за отримання, стиснення, перетворення файлів та їхнього розповсюдження з багатофункціонального пристрою по різних отримувачах, включаючи хмарні системи. Завдання друку також можна безпечно перенаправляти на відповідні принтери, оптимізуючи вартість друку кожного документа. Наше рішення зміцнює захист документів на вашому підприємстві, а повний набір функцій для обліку документів забезпечує абсолютний контроль за всіма операціями кожного користувача, пристрою чи відділу.

## ЦЕНТРАЛІЗОВАНЕ КЕРУВАННЯ ПАРКОМ

Наше програмне забезпечення для керування пристроями IW MC підтримує налаштування пристроїв, політик безпеки, паролів та сертифікатів, а також оновлення вбудованого програмного забезпечення та його надсилання на весь парк пристроїв Canon у вашій мережі, що зберігає вашому IT-відділу цінний час та допомагає вам тримати систему захисту вашої інфраструктури друку в оновленому стані.

## КОМПЛЕКСНИЙ АУДИТ ДОКУМЕНТІВ

Нашу архітектуру служб для офісної документації можна розширити за допомогою доступних на замовлення компонентів, які дозволяють вести повний облік (тобто відскановані копії плюс метадані завдання) всіх документів, що проходять через пристрої imageRUNNER ADVANCE.

## MANAGED PRINT SERVICES

Керовані служби друку Canon MPS поєднують в собі інноваційні технології і програмне забезпечення з відповідними послугами, що надають вам доступ до всього спектра функцій друку та оброблення документів без додаткового навантаження на IT-відділ. Завдяки проактивному керуванню та постійній оптимізації вашої інфраструктури друку та процесів роботи з документами ми допоможемо вам досягти цілей з точки зору безпеки, оптимізуючи при цьому кошти та підвищуючи продуктивність праці на всьому підприємстві.

## ІНДИВІДУАЛЬНА РОЗРОБКА

Наша власна команда розробників готова запропонувати й розробити для вас індивідуальне рішення, яке відповідає вашій ситуації чи унікальним потребам.

## НАСКІЛЬКИ ІНКЛЮЗИВНИЙ ВАШ ПІДХІД ДО БЕЗПЕКИ НА ПІДПРИЄМСТВІ?

- Чи охоплює ваша політика безпеки також ваш парк багатофункціональних пристроїв?
- Як ви забезпечуєте оновлення вашої інфраструктури друку, а також вчасне та ефективне розгортання всіх покращень та виправлень помилок?
- Чи можуть ваші гості друкувати й сканувати документи, не піддаючи вашу мережу ризикам?
- Чи безпечна та реалізовна політика використання власних пристроїв на роботі у вашому парку друкувального обладнання?
- Чи достатньо у вашого ІТ-відділу часу на розслідування інцидентів з безпекою?
- Чи оптимальний у вас баланс між безпекою та зручністю для користувачів?



# ЧОМУ CANON?



## ДОСВІД

Завдяки інтеграції обладнання з програмним забезпеченням зменшується потенціал для порушень у системі.



## ПАРТНЕРСТВО

Ми допомагаємо клієнтам покращити їхні бізнес-процеси через наші **проактивні заходи з вирішення будь-яких проблем з безпекою даних.**



## ОБСЛУГОВУВАННЯ

За обслуговування клієнтів відповідає **та ж сама команда спеціалістів з безпеки**, що й за нашу власну внутрішню IT-безпеку.

Ми враховуємо всі потенційні загрози як в межах корпоративного брандмауера, так і за ними.



## ІННОВАЦІЇ

У наших продуктах і послугах **втілені ефективніші засоби** мінімізації ризиків для інформаційної безпеки.

**SCAwards**  
2017  
EUROPE



### Highly commended

(«Наполегливо рекомендуємо») – наша нагорода в категорії найкращих служб безпеки на конференції **2017 SCA Awards Europe**, яка відзначає досвід в галузі кібербезпеки.

Компанія Canon U.S.A. отримала дві нагороди **BLI PaceSetter Awards 2017** (безпека служб візуалізації документів та мобільний друк).

#### Canon Inc.

Canon.com

#### Canon Europe

canon-europe.com

Ukrainian edition

© Canon Europa N.V., 2019

#### ТОВ «Кенон Україна»

01601, Київ, ул. Мечникова, 2А

Україна

Телефон: +38 044 490 2595

Факс: +38 044 490 2598

www.canon.ua

**Canon**

**McAfee**  
PROTECTED