ORGANIZATOR

arcus

PARTNERZY TECHNOLOGICZNI

KYOCERA Lenovo FUJIFILM PaperCut

PATRONAT MERYTORYCZNY

PRACODAWCY RP



Jak zarząd odzyskuje kontrolę nad niewidzialnym obszarem ryzyka: środowisko druku

Radosław Gaworski

Partner & Product Development Manager
iTS: Info Technology Supply Ltd.

Drukowanie i skanowanie jako ryzyko biznesowe



- Kary regulacyjne i koszty incydentów
- Przestoje procesów biznesowych
- Utrata zaufania klientów i partnerów
- Rosnące wymagania audytowe
- Zmiany technologiczne
- Zapewnienie bezpieczeństwa

Bezpieczeństwo wydruku – wydruk bezpieczny i podążający



Cel biznesowy:
• Ograniczenie ryzyka wycieku informacji
• Zwiększenie odpowiedzialności użytkowników
• Zgodność z wymaganiami audytowymi

Przykład: Dokument odbierany dopiero po identyfikacji przy urządzeniu.

Bezpieczeństwo skanowania – skan bezpieczny i kontrolowany

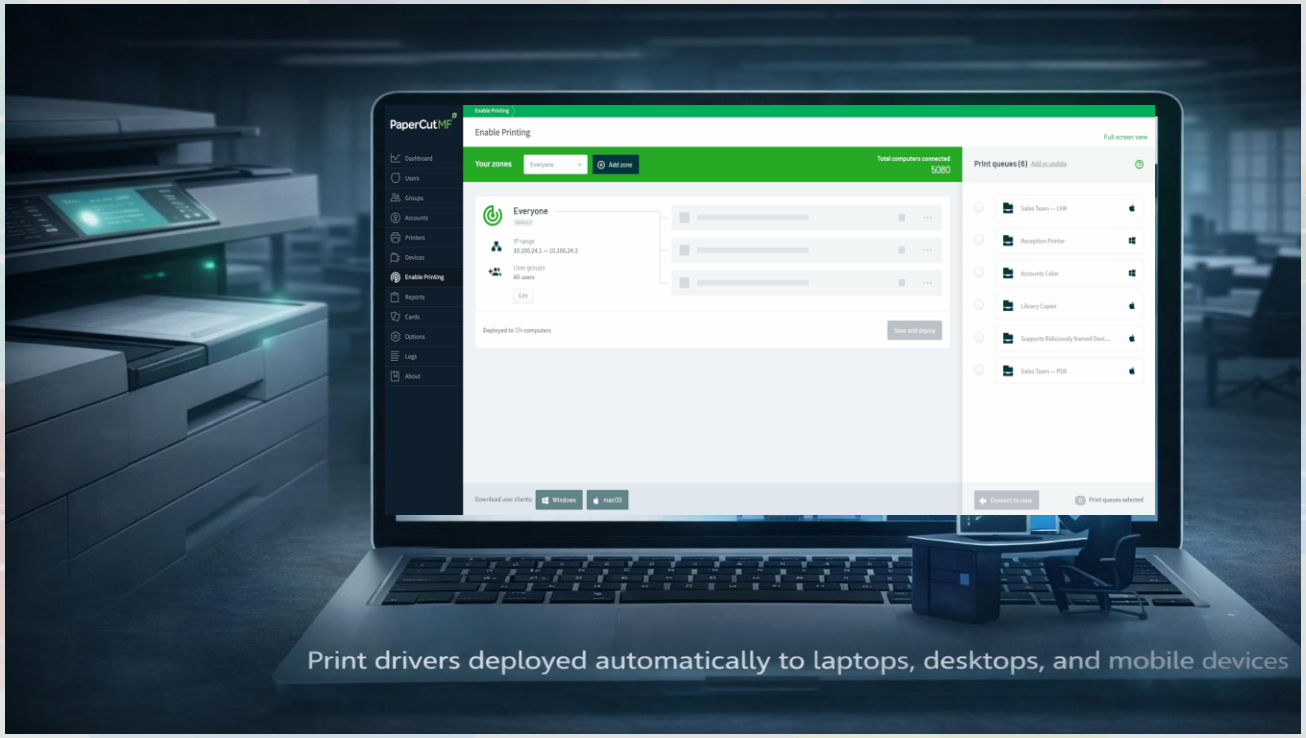


Cel biznesowy:

- Ograniczenie ryzyka wycieku informacji
- Personalizacja procesów skanowania
- Zamiana procesów papierowych na elektroniczne
- Możliwość audytowania procesów
- Bezpieczeństwo procesów skanowania

Przykład: Dokument może zostać zeskanowany wyłącznie przez uwierzytelnionego użytkownika

Dystrybucja kolejek druku

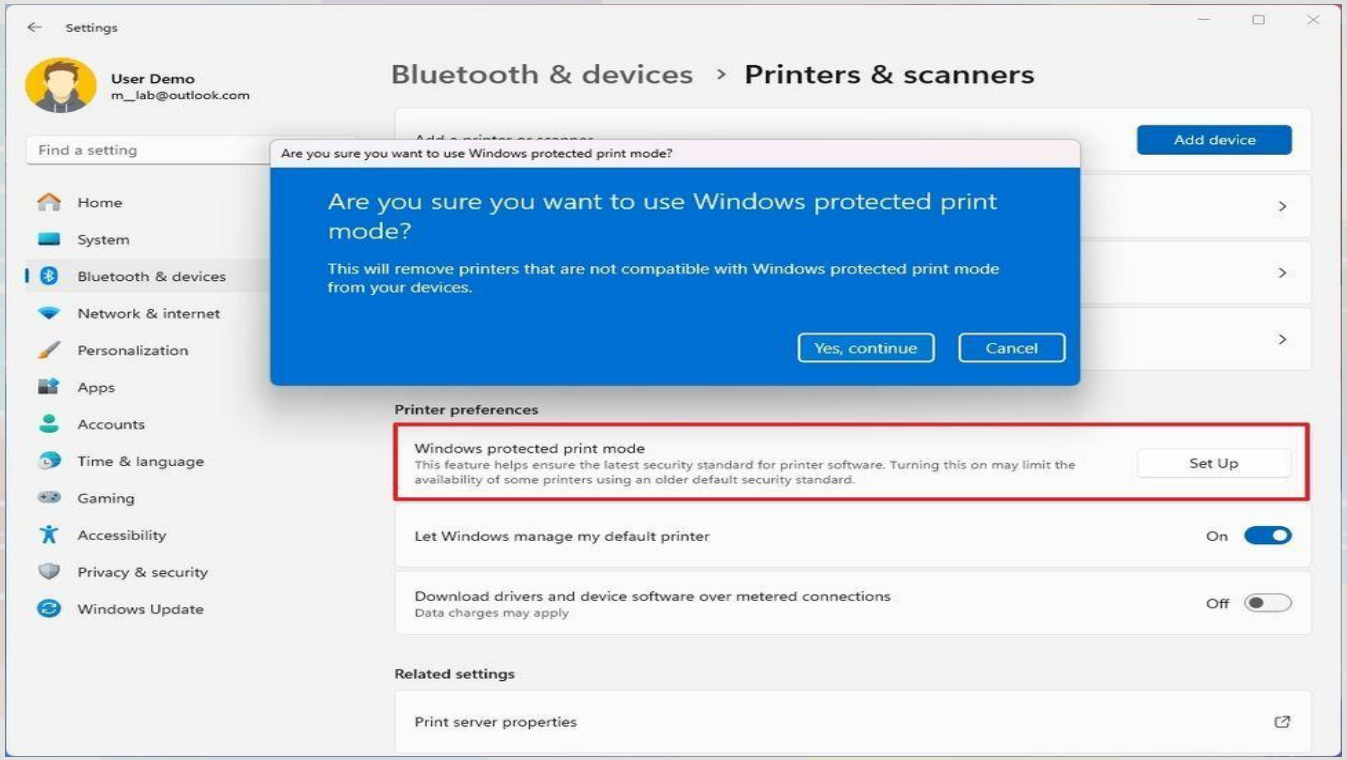


Cel biznesowy:

- ograniczenie ryzyka przestojów użytkowników i procesów biznesowych,
- zmniejszenie kosztów wsparcia IT, zapewnienie ciągłości działania podczas zmian organizacyjnych i technologicznych,
- standaryzacja środowiska drukowania.

Przykład: Pracownik zmienia lokalizację lub otrzymuje nowy komputer. Brak odpowiednich kolejek drukowania uniemożliwia realizację codziennych obowiązków, generując zgłoszenia do Service Desk i opóźnienia procesów.

Windows Protected Print



Microsoft zmienia model drukowania.

Wyzwania dla organizacji:
- konieczność weryfikacji zgodności środowiska
- wpływ na procesy i urządzenia
- ryzyko zakłócenia działania krytycznych procesów biznesowych

Przykład: Po włączeniu WPP brak możliwości drukowania w organizacji

Audyt druku i skanu



Cel biznesowy:

- zapewnienie pełnej identyfikowalności działań użytkowników,
- ograniczenie ryzyka nadużyć i nieuprawnionego dostępu do informacji,
- wsparcie procesów audytowych i zgodności regulacyjnej, skrócenie czasu analizy incydentów bezpieczeństwa.

Przykład: Organizacja przetwarza ściśle tajne informacje, możliwość blokowania ich drukowania lub skanowania.

Rekomendacje dla organizacji



- Ocena ryzyk związanych z drukiem i skanowaniem
- Analiza wpływu NIS2, DORA i RODO
- Przygotowanie do Windows Protected Print Mode
- Wdrożenie bezpiecznego wydruku, skanu i pełnego audytu
- Traktowanie druku i skanu jako elementu cyberbezpieczeństwa