

Managed Document Services



Bezpieczeństwo dokumentów w sektorze sektorze finansowym i ubezpieczeniowym ubezpieczeniowym

Pełna kontrola nad środowiskiem wydruku w walce z ryzykiem operacyjnym



docu**soft**

arcus **si**

geotik



Trendy rynku systemów zarządzania wydrukiem

Cyfrowa transformacja

Rynek oprogramowania do zarządzania wydrukiem wzrósł do 2,38 mld USD w 2024 roku z prognozą wzrostu do 4,39 mld USD do 2032 roku (CAGR 8,1%)

Źródło: Fortune Business Insights 2024

Bezpieczeństwo danych

Tylko 16% firm jest pewnych bezpieczeństwa swojej infrastruktury druku (spadek o 3% w 2024), koszty cyberprzestępczości osiągną 15,6 bln USD do 2029 roku

Źródło: Quocirca Print Security Report 2024

Praca hybrydowa

Rynek druku w chmurze wzrósł do 1,65 mld USD w 2024 roku z prognozą wzrostu o 11,6% rocznie do 2030 roku, 55% nowych instalacji w 2023 to rozwiązania chmurowe

Źródło: Grand View Research 2024

Znaczenie Systemów Zarządzania Drukiem

Efektywne zarządzanie drukiem to kluczowy element optymalizacji operacji zarówno w sektorze biznesowym, jak i publicznym. Pozwala na znaczne obniżenie kosztów, zwiększenie bezpieczeństwa danych oraz redukcję śladu ekologicznego.



Redukcja Kosztów

Średnie oszczędności dzięki systemom zarządzania drukiem według najnowszych badań



Organizacji Doświadczyło Naruszeń

Odsetek firm, które odnotowały incydenty bezpieczeństwa związane z drukowaniem w 2024 roku

Źródła danych:

Redukcja kosztów: "Managed Print Services Market Analysis 2024", Grand View Research
Oszczędność papieru: "Print Management Sustainability Report 2024", Consegic Business Intelligence
Bezpieczeństwo danych: "Print Security Landscape 2024", Quocirca



Obecne trendy w bezpieczeństwie systemów wydruku



Ewolucja zagrożeń

W sektorze finansowym i ubezpieczeniowym, gdzie dokumenty zawierają dane wrażliwe i poufne, bezpieczeństwo wydruku stało się krytycznym elementem architektury bezpieczeństwa. Tradycyjne podejście, oparte na fizycznej kontroli dostępu do drukarek, nie wystarcza w erze cyfrowej transformacji.

Nowoczesne drukarki (MFP) są zawsze podłączone do sieci korporacyjnej, co czyni je potencjalnym wejściem dla ataków zewnętrznych. Badania pokazują, że ponad 60% incydentów bezpieczeństwa w sektorze finansowym zaczyna się od kompromitacji (endpoint compromise) urządzeń końcowych, w tym drukarek.

Nowe rozwiązania

Systemy zarządzania wydrukiem, takie jak MyQ, PaperCut integrują zaawansowane mechanizmy szyfrowania, uwierzytelniania wielofazowego i kontroli dostępu, tworząc warstwę ochrony od punktu inicjacji zadania drukowania po fizyczne wydrukowanie dokumentu.

W sektorze finansowym, gdzie zgodność z regulacjami takimi jak RODO, NIS2, DORA, PSD2 czy PCI DSS jest obowiązkowa, kompleksowe rozwiązania także w zakresie zarządzania wydrukiem zapewniają nie tylko bezpieczeństwo, ale również audytowalność i śledzenie wszystkich operacji związanych z dokumentami.

Trzy filary bezpieczeństwa wydruku

Strategia kompleksowego zabezpieczenia środowiska wydruku musi uwzględniać trzy wzajemnie uzupełniające się obszary ochrony, każdy z perspektywy urządzenia, użytkownika i administratora.



Zgodność formalna i regulacje prawne

Spełnienie wymagań RODO, NIS 2, DORA, ISO 27001 oraz branżowych standardów bezpieczeństwa w finansach



Ochrona przed ingerencją zewnętrzną

Zabezpieczenie sieci, szyfrowanie komunikacji i kontrola dostępu do urządzeń i serwerów



Monitorowanie środowiska wewnętrznego

Kontrola urządzeń, uprawnienia użytkowników, audyt działań użytkowników i śledzenie wszystkich zadań drukowania, kopiowania i skanowania

FILAR 1: Zgodność formalna i regulacje prawne

Wymagania prawne i zgodności



RODO i ochrona danych

Automatyczne usuwanie danych z pamięci urządzenia, szyfrowanie danych w spoczynku, tryb prywatności, dostęp jedynie do własnych danych

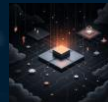
- Automatyczne czyszczenie pamięci
- Szyfrowanie danych
- Prawo do zapomnienia



NIS2 – cyberodporność

Zarządzanie prawami użytkowników, rejestrowanie i raportowanie incydentów, bezpieczne uwierzytelnianie wieloskładnikowe

- Zarządzanie dostępem
- Dzienniki audytu
- Dzienniki w czasie rzeczywistym



DORA – bezpieczeństwo cyfrowe

Testowanie odporności systemów, zarządzanie ryzykiem cybernetycznym, ciągłość operacyjna, plany ciągłości biznesu

- Testowanie odporności
- Zarządzanie ryzykiem
- Ciągłość biznesu



ISO 27001

Spełnienie przez producenta systemu standardów zarządzania bezpieczeństwem informacji

- Kontrola bezpieczeństwa
- Proces ciągłego doskonalenia
- Zarządzanie ryzykiem

Kompleksowa zgodność regulacyjna

Cztery filary regulacyjne - RODO, NIS2, DORA, ISO 27001 - tworzą fundament bezpieczeństwa dokumentów w sektorze finansowym i ubezpieczeniowym, zapewniając ochronę na poziomie urządzenia, użytkownika i administratora.

FILAR 2: Ochrona przed ingerencją zewnętrzną

Zabezpieczenie sieci i urządzeń

Bezpieczeństwo sieciowe

Urządzenie: Szyfrowanie komunikacji HTTPS/SSL/TLS między drukarką a serwerem, wyłączenie niebezpiecznych protokołów, autoryzacja urządzeń w sieci

Użytkownik: Bezpieczne połączenie z serwerem wydruku, ochrona danych podczas transmisji

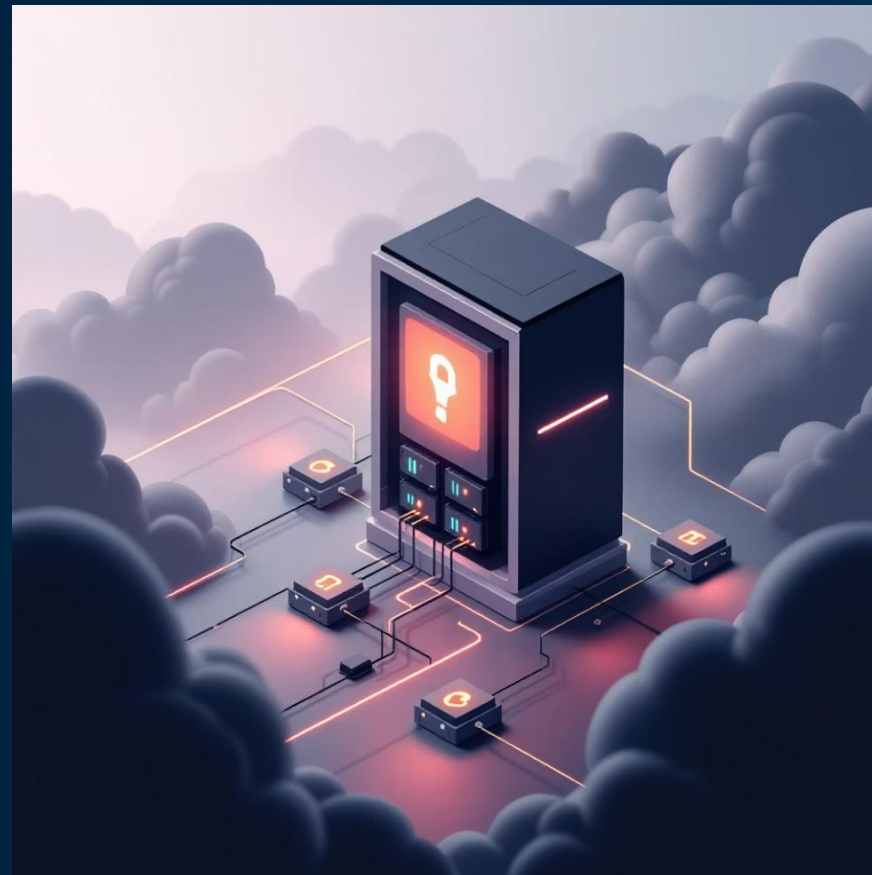
Administrator: Konfiguracja firewalli, implementacja protokołów HTTPS, LDAPS, SMTPS, IPPS, zarządzanie certyfikatami CA, kopia zapasowa, konserwacja, monitorowanie kondycji systemu

Kontrola dostępu

Urządzenie: Blokada dostępu nieautoryzowanym użytkownikom, automatyczne wylogowanie po określonym czasie bezczynności

Użytkownik: Wielofazowe uwierzytelnianie (karta + PIN), lub zaawansowana technologia RFID

Administrator: Definiowanie ról i uprawnień, kompleksowe logowanie prób dostępu, blokowanie kont dla osób nieuprawnionych



Szyfrowanie danych

Całkowite szyfrowanie bazy danych, logów i zadań drukowania i skanowania w spoczynku i podczas transmisji

Bezpieczne protokoły

HTTPS, LDAPS, SMTPS, IPPS - wyłączenie niebezpiecznych protokołów i szyfrów

Uwierzytelnianie

Wielofazowe uwierzytelnianie, certyfikaty, kontrola dostępu na podstawie ról i grup

FILAR 3: Monitorowanie środowiska wewnętrznego

Kontrola urządzeń i audyt działań

1 Kontrola urządzeń drukujących

Urządzenie: Śledzenie stanu drukarki, automatyczne czyszczenie pamięci, kontrola dostępu do funkcji kopiowania i skanowania

Użytkownik: Logowanie i wylogowanie z urządzenia, kontrola fizyczna nad dokumentami wyjściowymi

Administrator: Zarządzanie konfiguracją urządzeń, aktualizacje oprogramowania, monitorowanie stanu i zużycia, zarządzanie zmianą

3 Analiza i raportowanie

Urządzenie: Generowanie metadanych zadań, śledzenie parametrów wydruku

Użytkownik: Dostęp do własnych raportów użycia, śledzenie kosztów projektowych

Administrator: Kompleksowe raportowanie, analiza trendów, identyfikacja anomalii, audyt zgodności

2 Śledzenie zadań drukowania, kopiowania i skanowania

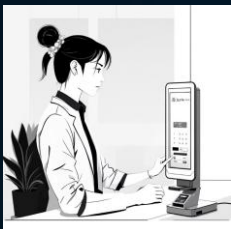
Urządzenie: Rejestracja wszystkich zadań, kontrola dostępu do kolejki drukowania, automatyczne usuwanie zadań po wydrukowaniu, dotyczy także przerwanej pracy

Użytkownik: Przegląd własnych zadań, możliwość anulowania zadania przed wydrukiem, prywatne kolejki

Administrator: Archiwizacja wszystkich zadań, audyt pełnego cyklu życia dokumentu, generowanie raportów użycia



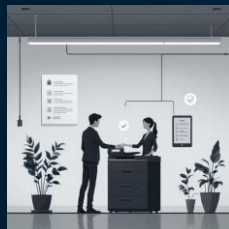
Bezpieczeństwo na poziomie użytkownika



Uwierzytelnianie i sesje

Bezpieczne logowanie z wieloma opcjami: karta RFID, PIN, nazwa i hasło, uwierzytelnianie dwuetapowe, logowanie offline w przypadku braku połączenia z serwerem, automatyczne wylogowanie po określonym czasie bezczynności, możliwość kontynuacji przetwarzania prac lub przerwanie przetwarzania po wylogowaniu.

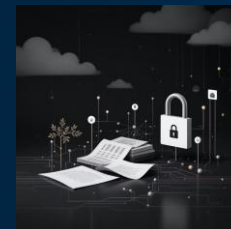
- Karta + PIN
- Uwierzytelnianie dwuetapowe
- Automatyczne wylogowanie
- Logowanie offline



Bezpieczne drukowanie

Zadanie drukowania wydrukowane tylko po uwierzytelnieniu użytkownika przy drukarce. Zapobiega nieautoryzowanemu odbiorowi dokumentów poufnych i pozostawianiu ich bez nadzoru, oznaczenie dokumentu znakiem wodnym, uniemożliwienie dokończenia przerwanej wydruku przez innego użytkownika po usunięciu usterki.

- Uwierzytelnianie przy drukarce
- Brak pozostawionych dokumentów
- Usuwanie pracy z drukarki w związku z usterką
- Znakowanie dokumentów



Tryb prywatności

Tryb prywatności ukrywa nazwy zadań innych użytkowników, pokazując tylko własne zadania. Prywatne kolejki natychmiast usuwają zadania po wydrukowaniu, zapobiegając dostępowi do dokumentów poufnych.

- Anonimizacja zadań
- Prywatne kolejki
- Automatyczne usuwanie

Pełna kontrola dla użytkownika

Kombinacja uwierzytelniania, bezpiecznego wydruku i trybu prywatności zapewnia pracownikom pełną kontrolę nad swoimi dokumentami przy jednoczesnej ochronie danych poufnych organizacji

Bezpieczeństwo na poziomie administratora

Kompleksowa kontrola i audyt środowiska

Zarządzanie uprawnieniami

Definiowanie ról i uprawnień użytkowników, kontrola dostępu do funkcji systemu, hierarchia administratorów z różnymi poziomami dostępu

Logowanie i audyt

Kompleksowe logowanie wszystkich zmian konfiguracji, śledzenie kto, kiedy i co zmienił, audit log dla celów audytowych i zgodności

Zarządzanie dostępnością (HA)

Wirtualizacja, Microsoft Failover Cluster, logowanie offline, buforowanie lokalne na stacji roboczej, fallback printing – zapasowe urządzenie drukujące (wydruk pomimo utraty połączenia z serwerem)

Archiwizacja zadań

Przechowywanie metadanych i informacji o użytkowniku, raportowanie pełnego cyklu życia dokumentu

Kontrola konfiguracji

- Centralna konfiguracja wszystkich urządzeń
- Wersjonowanie ustawień systemu
- Kontrola zmian przez audit log
- Automatyczne backupy konfiguracji

Bezpieczeństwo serwera

- Szyfrowanie bazy danych i logów
- Kontrola dostępu do interfejsu webowego
- Wielopoziomowe hasła i PIN-y
- Integracja z AD/ Entra ID



Bezpieczeństwo na poziomie urządzenia

Ochrona fizyczna i logiczna drukarek

Dostęp fizyczny

Kontrola lokalizacji drukarek, ochrona przed nieautoryzowanym dostępem fizycznym, blokada panelu sterowania

Pamięć urządzenia

Automatyczne czyszczenie pamięci po zadaniu, szyfrowanie danych w spoczynku, kontrola dostępu do pamięci

Oprogramowanie

Aktualizacje zabezpieczeń, kontrola wersji firmware, certyfikaty, automatyczne instalacje poprawek

Komunikacja

Szyfrowanie HTTPS/SSL, kontrola protokołów, blokada niebezpiecznych połączeń

Funkcje zabezpieczeń

- Szyfrowanie danych
- Automatyczne usuwanie danych po zakończeniu zadania
- Kontrola dostępu do funkcji kopiowania i skanowania
- Blokada panelu sterowania po określonym czasie
- Śledzenie stanu i zużycia materiałów
- Automatyczne zamawianie tonerów i części

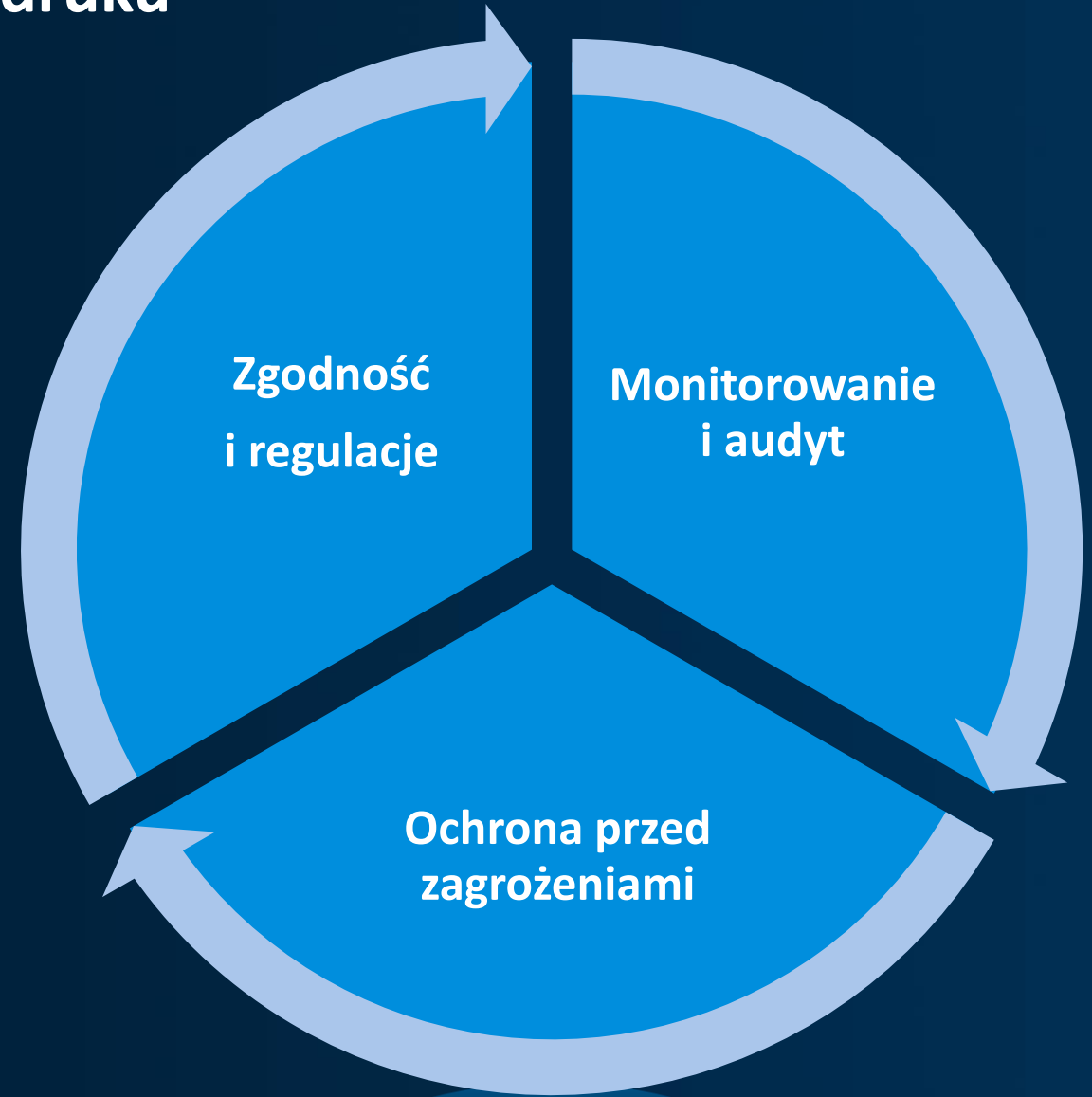
Kontrola sieciowa

- Autoryzacja urządzenia w sieci (802.1X)
- Kontrola dostępu na podstawie MAC/IP
- Monitorowanie nieprawidłowych prób dostępu
- Współpraca z systemami NAC

Pełna kontrola nad bezpieczeństwem wydruku

W sektorze finansowym i ubezpieczeniowym, bezpieczeństwo wydruku nie może być traktowane jako opcjonalne. Kompleksowe rozwiązanie musi uwzględniać wszystkie trzy filary: zgodność z regulacjami, ochronę przed zagrożeniami zewnętrznymi oraz monitorowanie środowiska wewnętrznego.

Strategia wielowarstwowa, obejmująca urządzenie, użytkownika i administratora, zapewnia pełną kontrolę nad dokumentami i minimalizuje ryzyko operacyjne.





docu**soft**

arcus **si**

geotik

Dziękuję za uwagę 😊

#ARCUSTEAM
Managed Document Services