ENDPOINT PROTECTOR | by CoSoSys

bako tech®

Data Loss Prevention

Ochrona przed wyciekiem danych dla dowolnej sieci i każdej branży.

DLP dla Windows, macOS i Linux

ENDPOINT PROTECTOR

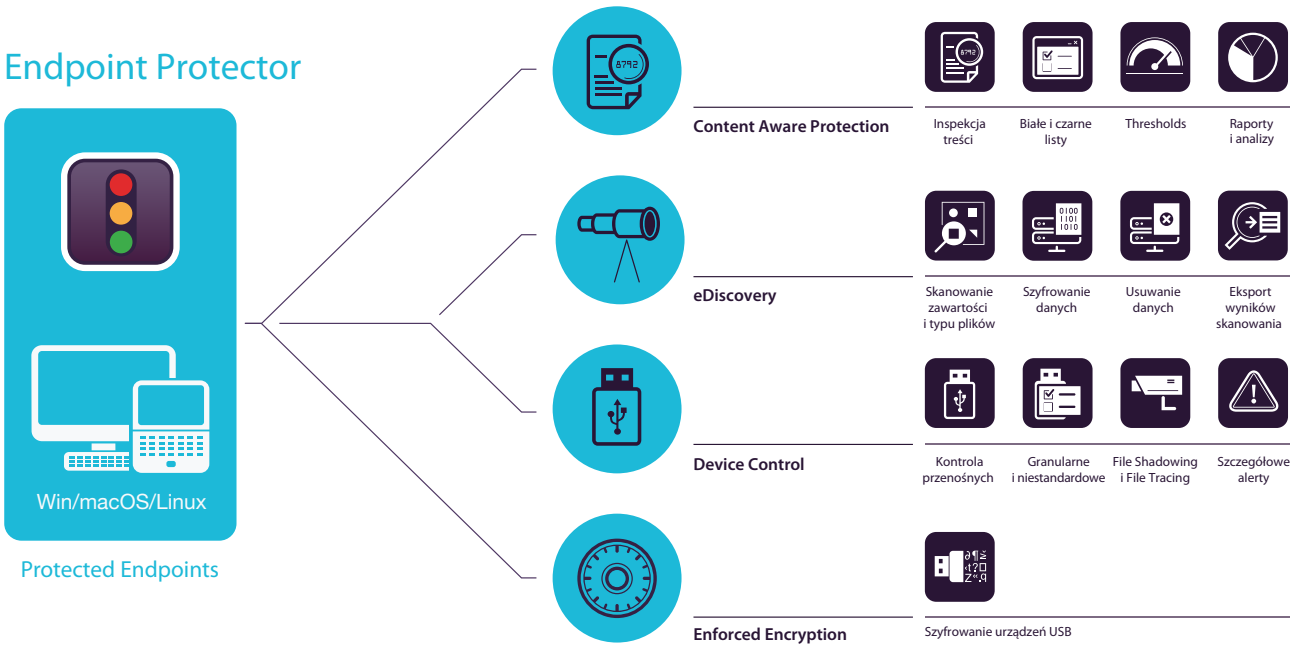
by CoSoSys

Rozwiązanie typu Out-of-the-Box zapewnia ochronę wrażliwych danych przed wyciekiem poprzez urządzenia przenośne, aplikacje oraz usługi w chmurze.

W świecie, w którym urządzenia przenośne, styl życia i chmura zmieniają sposób, w jaki pracujemy i żyjemy, Endpoint Protector ma na celu ochronę poufnych danych przed zagrożeniami z wewnątrz, przy jednoczesnym utrzymaniu wydajności i uczynieniu pracy bardziej wygodną i bezpieczną.

Podejście oparte na czarnych i białych listach zapewnia elastyczność w tworzeniu polityk bezpieczeństwa. Organizacje mogą zabronić używania określonych urządzeń wymiennych i transferów danych w aplikacjach do udostępniania plików w chmurze i innych usługach online, a także skanować określone informacje PII, umożliwiając transfery do określonych adresów URL i nazw domen określonym komputerom / użytkownikom / grupom, bez wpływu na wydajność pracy.

Implementacja Endpoint Protector dostępnego jako sprzęt lub urządzenie wirtualne trwa zaledwie kilka minut. Co więcej, intuicyjna konsola webowa umożliwia zarządzanie politykami i sprawdzanie raportów z dowolnego urządzenia, od komputera do tabletu. Endpoint Protector radykalnie zmniejsza ryzyko stwarzane przez wewnętrzne zagrożenia, które mogą prowadzić do wycieku danych lub ich kradzieży, a także zapewnia zgodność z przepisami i regulacjami.



Content Aware Protection
dla Windows, macOS i Linux

Monitoruj i kontroluj dane w ruchu, decydując które poufne pliki mogą lub nie mogą opuścić organizację poprzez rózne kanały komunikacji. Filtrowanie typów plików, aplikacji, predefinowanej i niestandardowej zawartości, wyrażeń regularnych, etc.

eDiscovery
dla Windows, macOS i Linux

Skanuj dane przechowywane na stacjach końcowych i zastosuj działania naprawcze, takie jak szyfrowanie lub usuwanie w przypadku zidentyfikowania poufnych danych na nieautoryzowanych komputerach.

Device Control
dla Windows, macOS i Linux

Monitoruj i kontroluj USB i porty peryferyjne. Ustaw prawa dla urządzenia, użytkownika, komputera, grupy lub globalnie.

Enforced Encryption
dla Windows i macOS

Automatycznie zabezpiecz dane skopiowane na urządzenia pamięci masowej USB szyfrowaniem AES 256. Wieloplatformowe, oparte na hasłach, łatwe w użyciu i bardzo wydajne.

Content Aware Protection

dla Windows, macOS i Linux

- Email Clients: Outlook / Thunderbird / Lotus Notes
- Web Browsers: Internet Explorer / Firefox / Chrome / Safari
- Instant Messaging: Skype / Microsoft Communicator / Yahoo Messenger
- Cloud Services & File Sharing: Dropbox / iCloud / Sky Drive / Bit Torrent / Kazaa
- Other Applications: iTunes / Samsung Kies / Windows DVD Maker / Total Commander / Team Viewer

Filtrowanie predefiniowanej zawartości

Filtry można tworzyć na podstawie wstępnie zdefiniowanych treści, takich jak numery kart kredytowych, numery ubezpieczenia społecznego i wiele innych.

Filtrowanie zawartości niestandardowej

Filtry można również tworzyć na podstawie niestandardowych tresci, takich jak słowa kluczowe i wyrażenia.

Filtrowanie wyrażeń regularnych

Twórz zaawansowane filtry niestandardowe, wyszukując powtarzalne regexy w przesyłanych plikach.

Filtrowanie typu plików

Filtry typu plików mogą być używane do blokowania określonych dokumentów w oparciu o ich rozszerzenie, nawet jeśli zostaną ręcznie zmodyfikowane przez użytkowników.

Białe listy plików

Można utworzyć białe listy plików, które nie będą blokowane, aby uniknąć obciążenia systemu i zwiększyć wydajność.

Białe listy domen i URL

Egzekwuj politykę firmy, ale pozwól pracownikom na elastyczność, której potrzebują do wykonywania pracy. Dodaj portale firmowe lub adresy e-mail do białej listy.

DLP dla drukarek

Polityki dla drukarek lokalnych i sieciowych blokują drukowanie poufnych dokumentów oraz zapobiegają utracie i kradzieży danych.

DLP dla Cienkich Klientów

Chroń dane na serwerach terminalowych i zapobiegaj utracie danych w środowiskach zwirtualizowanych.

Wyłącz Print Screen

Wyłącz funkcję przechwytywania ekranu, zabezpieczając poufne dane przed wyciekiem.

Alerty E-mail

Predefiniowane i niestandardowe powiadomienia e-mail można skonfigurować w celu dostarczania informacji o najważniejszych wydarzeniach związanych z poufnymi transferami plików.

Active Directory

Łatwe wdrożenie dzięki integracji z AD lub podobnymi narzędziami. Importuj i synchronizuj wszystkie grupy i jednostki.

Monitoring schowka

Wyeliminuj wycieki poufnych treści za pomocą narzędzi kopiuj/wklej oraz wytnij/wklej.

Raporty i analizy

Monitoruj aktywność zwiazaną z przesyłaniem plików dzięki zaawansowanemu narzędziu do raportowania i analizy. Dzienniki i raporty można również eksportować do rozwiązań SIEM.

Globalne i regularne progi dla filtrów

Określ, do jakiej liczby naruszeń dozwolony jest transfer plików. Dotyczy to każdego rodzaju treści lub sumy wszystkich naruszeń.

File Tracing

Nagrywaj wszystkie transfery plików lub próby transferów do róznych aplikacji internetowych i usług w chmurze, zapewniając jasny obraz działan użytkowników.

File Shadowing

Zachowaj kopię plików, które zostały przesłane do kontrolowanych urządzeń lub przez e-maile, serwisy cloudowe lub inne aplikacje.

Offline Temporary Password

Tymczasowo zezwalaj na przesyłanie plików do komputerów odłączonych od sieci.

Dashboard

Dostęp do grafik i wykresów, dla szybkiego wizualnego przeglądu najważniejszych wydarzeń i statystyk.

eDiscovery

dla Windows, macOS i Linux

- File type: Graphic Files / Office Files / Archive Files / Programming Files / Media Files / etc.
- Predefined content: Credit Cards / Personally Identifiable Information / Address / SSN / ID / Passport / Phone Number / Tax ID / Health Insurance Number / etc.
- Custom Content / File Name / Regular Expression / HIPAA

Skanowanie zawartości i typu plików

Stwórz polityki eDiscovery definiując jaka zawartość jest wrażliwa dla Twojej organizacji w oparciu o typ plików, predefiniowaną, domyślną czy niestandardową zawartość, nazwę pliku, wyrażenia regularne. Rozpocznij skanowanie wrażliwych danych na podstawie wybranej zawartości.

Szyfruj odnalezione dane

Po odnalezieniu poufnych danych, możesz je zaszyfrować za pomocą AES 256, aby zapobiec nieautoryzowanemu dostępowi nieupoważnionych pracowników i zapobiec wyciekowi danych.

Usuń odnalezione dane

Zabezpiecz dane i zapewnij zgodność z przepisami kasując wrażliwe dane natychmiast po zidentyfikowaniu.

Eksportuj wyniki skanowania

Wyniki skanowania można wyeksportować do plików Excel, PDF lub CSV, przez co mogą być wykorzystane jako raporty na kadry zarządzającej lub do audytu.

Czarna lista typu plików

Czarna lista typu plików może być użyta do wykrycia specyficznych dokumentów przechowywanych na stacjach roboczych: plików graficznych, office, archiwów, plików programistycznych, media, etc.

Czarna lista predefiniowanej zawartości

Dodaj do czarnej listy predefiniowanej treści informacje tj. numery kart kredytowych, numery ubezpieczenia społecznego, wrażliwe dane osobowe, etc. Odkryj gdzie są przechowywane i czy narusza to politykę firmy.

Czarna lista niestandardowej zawartości

Stwórz czarną listę niestandardowej zawartości bazując na słowach i wyrażeniach kluczowych. Słowniki mogą być tworzone poprzez kopiuj/wklej, wpisanie lub import.

Czarna lista nazw pliku

Szukaj specyficznych plików bazując na ich nazwie. Rezultaty są wyświetlane w wynikach wyszukiwania eDiscovery z możliwością usunięcia lub zaszyfrowania.

Czarna lista wyrażeń regularnych

Twórz czarne listy w celu odnalezienia określonych regexów wsród danych przechowywanych na stacjach końcowych.

Thresholds

Unikaj zbędnego skanowania korzystając z opcji treshold. Sprecyzuj globalną sumę naruszeń lub minimalny rozmiar skanowanych plików.

Biała lista typu plików MIME

Wyklucz typy plików MIME od skanowania, dodając je do białej listy, aby uniknąć obciążenia i zwiększyć wydajność.

Biała lista dozwolonych plików

Ustaw białe listy plików jako wyjątki od polityk skanowania zdefiniowanych w eDiscovery. Bez względu czy polityka jest oparta o typ pliku, predefiniowana lub niestandardowa zawartość, pliki z białej listy będą wyłączone ze skanowania.

Device Control

dla Windows, macOS i Linux

USB Drivers / Printers / Bluetooth Devices / MP3 Players / External HDDs / Teensy Board / Digital Cameras / Webcams / Thunderbolt / PDAs / Network Share / FireWire / iPhones / iPads / iPods ZIP Drivers / Serial Port / PCMCIA Storage Devices / Biometric Devices / Inne

Ustaw prawa globalne
Domyślnie prawa urządzeń mają zastosowanie globalne.

Ustaw prawa dla grup
Uprawnienia do urządzeń mogą być konfigurowane w sposób granularny w oparciu o grupy, umożliwiając różne prawa dostępu dla różnych działów.

Ustaw prawa dla komputera
Uprawnienia do urządzeń można konfigurować dla każdego komputera.

Ustaw prawa dla komputera
Na podstawie ról i zadań każdy użytkownik może otrzymać różne prawa dostępu do urządzenia zgodnie z zasadami firmy.

Ustaw prawa dla urządzenia
Granularność praw może być zniesiona do poziomu urządzenia na podstawie identyfikatora dostawcy, identyfikatora produktu i numeru seryjnego.

Niestandardowe klasy
Prawa można tworzyć na podstawie klas urządzeń ułatwiających zarządzanie produktami od tego samego dostawcy.

Zaufane urządzenia (TD)
W przypadku zaszyfrowanych urządzeń, różne prawa dostępu mogą być konfigurowane w oparciu o poziom szyfrowania (oprogramowanie, sprzęt, etc.).

File Tracing
Nagrywaj wszystkie transfery lub próby transferu plików na różne urządzenia USB, zapewniając widoczność działań użytkowników.

File Shadowing
Zapisz kopię plików, które zostały przesłane do kontrolowanych urządzeń, w celach audytowych.

Offline Temporary Password
Tymczasowo zezwalaj na przesyłanie plików do komputerów odłączonych od sieci. Zapewnij bezpieczeństwo i wydajność.

Alerty E-mail
Predefiniowane i niestandardowe powiadomienia e-mail o najważniejszych wydarzeniach związanych z użytkowaniem urządzenia.

Raporty i analizy
Monitoruj całą aktywność związaną z korzystaniem z urządzenia dzięki zaawansowanemu narzędziu do raportowania i analizy. Dzienniki i raporty można również eksportować.

Enforced Encryption

dla Windows i macOS

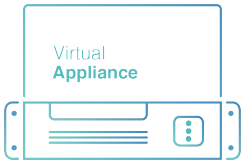
USB Enforced Encrypyion
Autoryzuj tylko zaszyfrowane urządzenia USB, upewnij się, że wszystkie dane skopiowane na wymienne urządzenia magazynujące są automatycznie zabezpieczane.

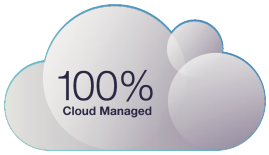
Master Password
Utworzenie hasła głównego zapewni ciągłość działania w różnych sytuacjach, np. reset hasła użytkownika.

Silne mechanizmy bezpieczeństwa
Zatwierdzone przez rząd 256-bitowe szyfrowanie AES, ochrona hasłem i zapobieganie nieuprawnionym działaniom w celu zapewnienia integralności aplikacji.

Elastyczne wdrożenie

Cososys nadaje się do każdego rodzaju sieci i może być używany przez klientów korporacyjnych, ale także małe i średnie przedsiębiorstwa. Endpoint Protector działa na zasadzie klient - serwer i jest centralnie zarządzany z poziomu interfejsu webowego.
Dostępny jest w opcji urządzenia wirtualnego (virtual appliance), można go wdrożyć za pomocą dostawców usług w chmurze (jak Amazon Web Services, Microsoft Azure lub Google Cloud) lub skorzystać z modelu SaaS poprzez wdrożenie z chmury producenta.





Endpoint Protector

Moduły EPP, takie jak **Content Aware Protection**, **Device Control** oraz **eDiscovery** są dostępne dla różnych dystrybucji i wersji wszystkich systemów operacyjnych: Windows, moc OS i Linux (lista poniżej).

Moduły

	Chronione urządzenia końcowe					
Windows	Windows XP / Windows Vista	(32/64 bit)	●	●	●	●
	Windows 7 / 8 / 10	(32/64 bit)	●	●	●	●
	Windows Server 2003 - 2019	(32/64 bit)	●	●	●	●
macOS	macOS X 10.7	Lion	●	●	●	●
	OS X 10.8	Mountain Lion	●	●	●	●
	OS X 10.9	Mavericks	●	●	●	●
	OS X 10.10	Yosemite	●	●	●	●
	OS X 10.11	ElCapitan	●	●	●	●
	macOS 10.12	Sierra	●	●	●	●
	macOS 10.13	High Sierra	●	●	●	●
	macOS 10.14	Mojave	●	●	●	●
	macOS 10.15	Catalina	●	●	●	●
Linux	Debian		●	●	●	n/a
	Ubuntu		●	●	●	n/a
	LinuxMint		●	●	●	n/a
	RHEL		●	●	●	n/a
	CentOS		●	●	●	n/a
	Fedora		●	●	●	n/a
	OpenSUSE		●	●	●	n/a
	SUSE Enterprise		●	●	●	n/a

CoSoSys | www.**endpointprotector**.com

Official Partner:

Bakotech Sp. z o.o.

Strona: www.bakotech.pl

E-mail: kontakt@bakotech.com

Telefon: +48 12 376 95 08

Adres: Ul. Drukarska 18/5
30-348 Kraków

bako tech®