JAK NIE DAĆ SIĘ RANSOMWARE

Ransomware zostaną z nami na dłużej,
więc **naucz się przed nimi bronić**!

Ransomware to dziś jedno z największych zagrożeń, jakie czyhają na użytkowników. A ponieważ dane stanowią siłę napędową biznesu, to właśnie firmy są szczególnie narażone na skutki cyber-ataków. Gdy już do niego dojdzie, nawet przedsiębiorstwa o ugruntowanej pozycji na rynku zaliczają duże straty.

Chyba, że z zawczasu odpowiednio się zabezpieczą.

O malwarze, klasyfikowanym obecnie jako ransomware (od angielskiej zbitki słów ransom i software – okup i oprogramowanie), głośno zrobiło się już kilka lat temu. W 2013 roku najgłośniejszy wirus należący do tej kategorii – CryptoLocker – pozwolił swoim twórcom (tylko podczas pierwszego ataku) „zarobić" aż 27 milionów dolarów. Jak szacuje McAfee Labs na jednej kampanii rozsyłania CryptoLockera przestępcy są w stanie uzyskać nawet 325 mln dolarów. Ataku nie ustrzegło się nawet FBI.

Czym zatem jest ransomware? Bardzo dobrze wyjaśnia to już sama jego nazwa. Ten rodzaj złośliwego oprogramowania ma na celu wyłudzić pieniądze od swojej ofiary. Atak wirusa polega na zablokowaniu dostępu do plików, dokumentów lub nawet na przejęciu całego komputera, bądź firmowego serwera. Wszystkie dane, do których ten rodzaj malware'u blokuje dostęp są zazwyczaj szyfrowane, a na ekranie pojawia się komunikat, co musi zrobić właściciel plików, aby je odzyskać. Zwykle cyberprzestępcy domagają się przelania pieniędzy na ich konto i w zamian obiecują wysłanie ofierze klucza oraz instrukcji jak odszyfrować dane. Coraz częściej, do pozyskiwania okupu wykorzystuje się platformę cyfrowej waluty Bitcoin. Pozwala to cyberprzestępcom ominąć oficjalny obieg pieniądza. Jest to dla nich bezpieczniejsze i często uniemożliwia policji wykrycie, kto fizycznie stoi za przeprowadzonym atakiem.

RODZAJE RANSOMWARE

Obecnie znane są trzy różne rodzaje złośliwego oprogramowania typu ransomware. Pierwszy z nich to tzw. screen-locker. Malware ten blokuje użytkownikowi dostęp do urządzenia poprzez zablokowanie ekranu. Jest to dość irytujące, ale można się go pozbyć samodzielnie przy podstawowej wiedzy technicznej lub za pomocą dobrego antywirusa.

Ponieważ ten rodzaj ransomware'u okazał się mało skuteczny w wyłudzaniu pieniędzy, cyberprzestępcy zaczęli stosować malware typu crypto-ransomware. Szyfruje on wybrane typy plików, np. zdjęcia i dokumenty Word, na lokalnym dysku ofiary. Coraz częściej zakodowuje on również pliki w innych lokalizacjach, do których ma dostęp – w tym pliki znajdujące się na

Bo do tanga trzeba dwojga

PHISHING+NIEWIEDZA=☠

Jaki jest najczęstrzy powód infekcji ransomware? Statystyki pokazują, że niechlubny prym wiodą rozsyłne przez przestępców maile typu phishing oraz ... niewyedukowani użytkownicy

serwerach oraz w chmurze. Następnie oferowany jest klucz do odszyfrowania danych, który przekazywany jest przez cyberprzestępców ofierze po uiszczeniu odpowiedniej opłaty. Przeważnie wartość żądanego okupu oscyluje w przedziale od 150 do 900 dolarów.

Niestety, crypto-ransomware wykorzystuje ten sam typ szyfrowania co oprogramowanie chroniące transakcje bankowe lub wojskową komunikacje. Pliki szyfrowane są przy użyciu algorytmów AES 256 dlatego realnie dane są nie do odzyskania (chyba, że jest się gotowym na atak, ale o tym później). Szacuje się, że oprogramowanie crypto-ransomware jest odpowiedzialne za wyłudzenie od ofiar ponad miliarda dolarów rocznie. Trzeci rodzaj ransomware to tzw. disk-encryptor. W odróżnieniu od crypto-ransomware oprogramowanie typu disk-encryptor zaszyfrowuje cały dysk ofiary i w ten sposób blokuje dostęp do całego komputera, nie pozwalając na uruchomienie się systemu operacyjnego.

W tym miejscu należy wspomnieć o wirusie Spora, który pojawił się pod koniec zeszłego roku. Działa on nietypowo. Malware typu ransomware niemal zawsze korzysta z serwerów CnC (Command-and-Control). Serwer taki odpowiedzialny jest za wygenerowanie klucza prywatnego i publicznego. Zainstalowany na komputerze ransomware pobiera klucz publiczny i szyfruje za jego pomocą dane, klucz prywatny, służący do odszyfrowania informacji przechowywany jest cały czas przez serwer CnC i udostępniany dopiero w momencie, gdy ofiara zapłaci okup.

Pliki są szyfruje w trybie offline. Spora korzysta przy tym z publicznego klucza RSA, zaszytego w programie, ale nie używa go do szyfrowania plików przechowywanych na komputerze ofiary, lecz do zaszyfrowania unikalnego klucza AES, który jest generowany lokalnie na zainfekowanym komputerze. Chcąc zapłacić okup, ofiara musi wysłać zaszyfrowany klucz AES do witryny wskazanej przez cyberprzestępców. Ci wykorzystują wówczas prywatny klucz RSA do odszyfrowania klucza AES i odsyłają go z powrotem do ofiary, która może już przy jego pomocy odszyfrować swoje pliki.

NIEBEZPIECZEŃSTWO CZAI SIĘ WSZĘDZIE

Najczęściej oprogramowanie ransomware dostaje się na nasz komputer po otworzeniu załącznika z maila lub kliknięciu w odnośnik, kierujący do specjalnie spreparowanej strony. Oszuści mają różne psychologiczne metody, aby zachęcić nas do otworzenia załącznika lub kliknięcia na link. Może to być np. informacja o przesyłce kurierskiej lub o zaległościach podatkowych, bądź też śmieszny filmik z kotkiem czy link do nagich zdjęć celebrytki. W ten sposób namawiają nas do otworzenia załącznika z niebezpiecznym oprogramowaniem, lub kliknięcia w link prowadzący do instalatora wirusa. Według firmy Trend Micro, 60 proc. ransomware ukrywa się w normalnych plikach multimedialnych. Co gorsza, programy antywirusowe, nie zawsze są w stanie wychwycić taki atak.

Ransomware przenosi się też przez złośliwe reklamy wyskakujące w przeglądarkach internetowych, poprzez strony WWW, najczęściej z treściami pornograficznymi i nielegalnym oprogramowaniem, bądź wykorzystywane są do tego zewnętrzne nośniki danych, takie jak klucze USB. W ostatnim wypadku, bardzo często atak jest profilowany pod konkretną ofiarę – osobę lub firmę. Twórcy ransomware dołączają też swoje złośliwe oprogramowania do pirackiego kontentu, który użytkownicy komputerów chętnie pobierają

Dwa największe dotąd ataki miały miejsce w MAJU I CZERWCU 2017

WannaCry

Cryptolocker odpowiedzialny za falę ataków w maju 2017. Program zdołał zarazić ponad 300 tys. komputerów w 150 krajach. W ataku ucierpiało wiele firm m.in. hiszpańska Telefónica, część brytyjskiej narodowej służby zdrowia (NHS), Fedex oraz Deutsche Bahn.

ExPetr/Petya/NotPetya

Seria ataków z 28 czerwca 2017, która rozpoczęła się na Ukrainie. Malware szybko rozprzestrzenił się na inne kraje europejskie, a także USA, Indie i Australię. Analiza firmy Kaspersky pokazują, że autorzy ataku nie przewidywali odszyfrowania plików swoich ofiar. Generowany przez program klucz szyfrujący był losowy. Oznacza to więc, że przestępcy go nie znali. Warto zaznaczyć to po raz kolejny – NIE WARTO PŁACIĆ PRZESTĘPCOM.

Podstawą ochrony jest dobry program antywirusowy, przezorność i oczywiście REGULARNIE WYKONYWANY BACKUP.

z torrentów lub stron internetowych z nielegalnym contentem. O tym, że nie można czuć się bezpiecznym, nawet jeśli w ogóle nie odwiedza się podejrzanych stron, świadczy fakt, że ransomware trafiał również na bardzo popularne serwisy informacyjne. Wśród stron WWW, które zostały zaatakowane wymienić można m.in. msn.com, nytimes.com, bbc.com, theweathernetwork.com czy newsweek.com.

ŻYCIE PO RANSOMWARE... LEPIEJ BYĆ GOTOWYM ZANIM MALWARE UDERZY

Jak widać, motywacją cyberprzestępców są pieniądze, a zagrożeni, bez wyjątku, są wszyscy użytkownicy. Jeżeli zaatakuje nas wirus typu ransomware, w pierwszej kolejności należy wyłączyć komputer. Część złośliwego oprogramowania, najpierw wyświetla komunikat o infekcji, a później szyfruje nasze pliki. W takiej sytuacji możemy zapobiec zaszyfrowaniu przynajmniej części danych. Pliki należy wówczas odzyskiwać podłączając dysk do innego komputera, który nie jest podpięty do sieci, tak aby wyeliminować możliwość połączenia się wirusa z serwerem CnC. Bez tego nie jest on w stanie szyfrować plików.

Podstawą ochrony jest jednak dobry program antywirusowy, przezorność i backup. Nie klikajmy w każdy odnośnik i nie otwierajmy wszystkich załączników w wiadomościach e-mail, na portalach społecznościowych oraz w komunikatorach. Należy też unikać logowania się na konto z uprawnieniami administratora. Na co dzień powinniśmy pracować na koncie użytkownika, a konto administracyjne powinno być wykorzystywane wyłącznie wtedy, kiedy jest to niezbędne – na przykład przy instalacji oprogramowania.

W firmach istotne jest też prawidłowe przydzielanie uprawnień do zasobów w firmowej sieci i wykorzystywanej przez użytkowników firmowej chmurze. Bardzo częstym błędem jest przydzielanie dostępu do wszystkich firmowych zasobów kierownictwu firmy. Osoby te są najczęściej narażone na spersonalizowane ataki cyberprzestępców, a niejednokrotnie zdarzało przy atakach ransomware, że z laptopa prezesa były szyfrowane wszystkie pliki z dokumentami na wszystkich firmowych serwerach i we wszystkich lokalizacjach, paraliżując w ten sposób działalność całej firmy na kilka dni, do chwili zapłacenia okupu.

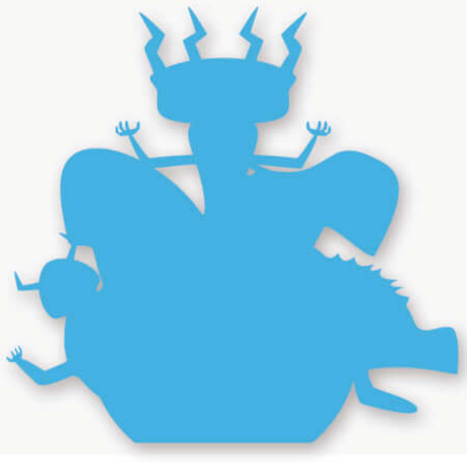
Uważaj nim będzie ZA PÓŹNO

Ransomware rozpowszechnia się zazwyczaj poprzez phishingowe maile, kryjąc się w załącznikach, takich jak pliki .zip, .pdf, .doc, .exe, .js i wiele innych. Po ich otwarciu rozprzestrzenia się już samodzielnie i bardzo szybko.

Ransomware typu locker wykorzystuje szyfrowanie asymetryczne lub inne nawet bardziej zaawansowane metody, których złamanie może okazać się niezwykle trudne lub wręcz niemożliwe.

Rynek rośnie wraz z popytem i z miesiąca na miesiąc uaktywnia się coraz więcej złośliwych malwarów. Tradycyjne programy antywirusowe zwykle nie są w stanie wykryć ukrytego ransomware najnowszej generacji.

Ofiary są zazwyczaj zmuszane do opłacenia okupu w bitcoinach, co uniemożliwia prześledzenie operacji finansowej.



BACKUP – NAJWAŻNIEJSZA LINIA OBRONY

Najlepszym sposobem zabezpieczenia firmy przed atakiem ransomware jest backup. W razie infekcji często dużo łatwiej jest bowiem sformatować cały dysk twardy i wczytać dane z kopii bezpieczeństwa, niż męczyć się z usuwaniem wirusa lub zapłacić cyberprzestępcom okup (CO ZDECYDOWANIE ODRADZAMY). Backup pozwala sprawnie i bez kłopotu cofnąć się do chwili sprzed ataku.

Dodatkowo w takich rozwiązaniach jak Xopero QNAP Appliance, która współpracuje z serwerami NAS firmy QNAP, możliwe jest uruchomienie obrazu odzyskiwanego komputera w środowisku wirtualnym z klucza USB. Obraz pobrany z serwera NAS uruchamiany jest wówczas w bezpiecznym środowisku wirtualnym, w którym możemy bez problemu sprawdzić, czy odzyskiwane dane nie są zarażone. Software ransomware często, przed zaszyfrowaniem danych, przez kilka dni ukrywa swoją obecność na komputerze ofiary.

Dobrym rozwiązaniem jest prowadzenie automatycznego backupu w chmurze. Warto pamiętać, że w chwili ataku szyfrowane są dane we wszystkich dostępnych z poziomu systemu operacyjnego lokalizacjach – w tym na zewnętrznych i sieciowych nośnikach, w tym przenośnych dyskach twardych czy serwerach NAS (w przypadku QNAP NAS bardzo przydatna jest wtedy funkcja odzyskiwania systemu/danych z wcześniej wykonanej migawki). Backup wykonywany w chmurze nie jest dostępny w prosty sposób z poziomu użytkownika. Ransomware nie ma więc do zbackupowanych danych bezpośredniego dostępu.

Do wykonywania backupu w chmurze warto korzystać z automatycznych narzędzi, wykonujących tą operację za nas. Nie musimy wówczas pamiętać o fizycznym zrobieniu backupu, gdyż ten wykona się w tle bez naszego udziału zawsze o wyznaczonej porze lub w chwili, gdy komputer bądź sieć nie są obciążone. Tego typu mechanizmami dysponują m.in. systemy backupu w chmurze Xopero Cloud i Xopero Cloud Personal.

Warto pamiętać, że technologia backupu może bez problemu zabezpieczać przed atakiem ransomware nie tylko komputery i laptopy poszczególnych użytkowników, ale również serwery – fizyczne i wirtualne. W ten sposób zyskujemy pewność, że w razie kłopotów szybko sobie z nimi poradzimy, nie płacąc przy tym cyberprzestępcom ani jednej złotówki.

Kilka słów o nas samych
XOPERO SOFTWARE S.A.

Jesteśmy jednym z największych producentów rozwiązań backupowych w Europie, dostarczającym profesjonalne narzędzia do kompleksowego zabezpieczenia firmowych danych. W naszej ofercie znajdują się rozwiązania do backupu lokalnego, backupu do chmury, appliance backup oraz disaster recovery i business continuity.

Rozumiemy, jak ważne dla naszych klientów jest bezpieczeństwo danych i zachowanie ciągłości biznesu. Ciągle rozwijamy produkty, tak by jeszcze lepiej pozwalały ograniczać ryzyko utraty danych oraz zagrożenie przestoju w firmie.

Wśród naszych klientów znajdują się firmy z segmentu MSP, administracja publiczna, finanse i bankowość, edukacja, medycyna, telekomunikacja oraz IT.

RODZINA PRODUKTÓW
XOPERO

XOPERO CLOUD
BACKUP DLA WYMAGAJĄCEGO BIZNESU

Xopero Cloud to zaawansowane rozwiązanie do backupu online, które pozwala na nielimitowane zabezpieczenie komputerów, baz danych oraz serwerów fizycznych i wirtualnych.

Xopero oferuje maksymalne zabezpieczenie danych. Jeszcze przed wysyłką do data center są one szyfrowane za pomocą algorytmu AES 256. Dodatkowo aby uniknąć jakiegokolwiej przestoju w firmie, są przechowywane w dwóch niezależnych lokalizacjach. Jeśli dojdzie do awarii jednego z centrów danych, można je zawsze odzyskać z drugiej lokalizacji.

XOPERO CLOUD PERSONAL
BACKUP I PLATFORMA SYNC & SHARE

Xopero Cloud Personal to prosty program do tworzenia kopii zapasowych, dzięki któremu wygodnie i szybko zaczniesz zabezpieczać dane na swoim komputerze.

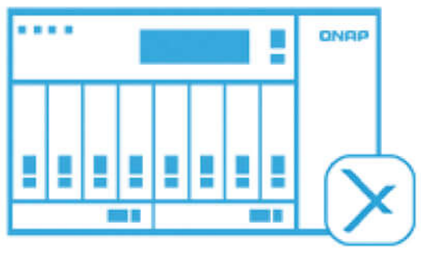
To ty decydujesz, które zasoby mają być chronione: pliki i foldery, skrzynkę pocztową, kolekcje muzyki, filmów oraz zdjęć z ostatnich wakacji. Backupy wykonują się automatycznie, a sama aplikacja działa w tle i nie wpływa w żaden sposób na pracę komputera. Dodatkowo masz do dyspozycji bezpieczne narzędzie do synchronizacji, współdzielenia i udostępniania szyfrowanych danych.

XOPERO QNAP APPLIANCE
BUSINESS CONTINUITY DLA QNAP NAS

Najlepsze rozwiązanie klasy enterprise dostępne dla MŚP, stworzone z myślą o użytkownikach serwerów QNAP NAS. Twój backup appliance QNAP to niezawodny storage, który umożliwia bezpieczne przechowywanie danych.

W połączeniu z Xopero staje się profesjonalnym backup appliance, dzięki któremu zabezpieczysz wszystkie biznesowe dane.

Jeśli dojdzie do awarii odtworzysz całe środowisko IT, w zaledwie kilka minut.

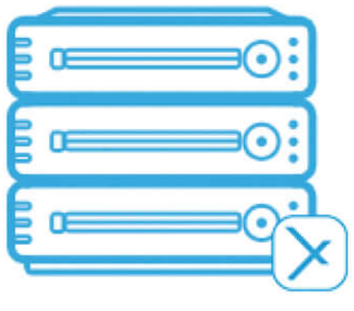


XOPERO BACKUP & RESTORE
BACKUP STWORZONY Z MYŚLĄ O TWOIM BIZNESIE

Zastąp dotychczasowy backup nowoczesnym i zaawansowanym rozwiązaniem do zabezpieczania danych. Utrata danych oznacza dla biznesu przestój i straty finansowe.

Xopero Backup & Restore to kompleksowe rozwiązanie softwarowe do backupu i odzyskiwania danych, które instalujesz na swojej infrastrukturze IT.

Decydując się na Xopero nie ponosisz dodatkowych kosztów, ponieważ wszystkie potrzebne komponenty już masz.



Produkt	**Xopero QNAP Appliance**	**Xopero Backup & Restore**	**Xopero Cloud**	**Xopero Cloud Personal**
Typ	Onsite / lokalnie	Onsite / lokalnie	Cloud / do chmury	Cloud / do chmury
Opis	**Profesjonalny backup dla QNAP NAS** Business continuity dla QNAP NAS Najlepsze rozwiązanie klasy enterprise dostępne dla MSP, stworzone z myślą o użytkownikach serwerów QNAP NAS. Twój backup appliance QNAP to niezawodny storage, który umożliwia bezpieczne przechowywanie danych. W połączeniu z Xopero staje się profesjonalnym backup appliance, dzięki któremu zabezpieczysz wszystkie biznesowe dane. Jeśli dojdzie do awarii odtworzysz całe środowisko IT, w zaledwie kilka minut.	**Backup na dowolnej infrastrukturze IT** Zastąp dotychczasowy backup nowoczesnym i zaawansowanym rozwiązaniem do zabezpieczania danych. Utrata danych oznacza dla biznesu przestój i straty finansowe. Xopero Backup & Restore to kompleksowe rozwiązanie softwarowe do backupu i odzyskiwania danych, które instalujesz na swojej infrastrukturze IT. Decydując się na Xopero nie ponosisz, dodatkowych kosztów, ponieważ wszystkie potrzebne komponenty już masz.	**Backup dla wymagającego biznesu** Xopero Cloud to zaawansowane rozwiązanie do backupu online, które pozwala na nielimitowane zabezpieczenie komputerów, baz danych oraz serwerów fizycznych i wirtualnych. Xopero oferuje maksymalne zabezpieczenie danych. Jeszcze przed wysyłką do data center są one szyfrowane za pomocą algorytmu AES 256. Dodatkowo aby uniknąć przestoju w firmie, są przechowywane w dwóch niezależnych lokalizacjach. Jeśli dojdzie do awarii jednego z centrów danych, można je zawsze odzyskać z drugiej lokalizacji.	**Backup i platforma sync & share** Xopero Cloud Personal to prosty program do tworzenia kopii zapasowych, dzięki któremu wygodnie i szybko zaczniesz zabezpieczać dane na swoim komputerze. To ty decydujesz, które zasoby mają być chronione: pliki i foldery, skrzynkę pocztową, kolekcje muzyki, filmów oraz zdjęć z ostatnich wakacji. Backupy wykonują się automatycznie, a sama aplikacja działa w tle i nie wpływa w żaden sposób na pracę komputera. Dodatkowo masz do dyspozycji bezpieczne narzędzie do synchronizacji, współdzielenia i udostępniania szyfrowanych danych.
Backup	- backup endpointów, - backup skrzynek pocztowych, - backup MS Exchange, - backup serwera, - backup baz danych: MS SQL, MySQL, PostgreSQL i Firebird - backup środowisk wirtualnych: Hyper-V i VMware, - image backup	- backup endpointów, - backup skrzynek pocztowych, - backup MS Exchange, - backup serwera, - backup baz danych: MS SQL, MySQL, PostgreSQL i Firebird - backup środowisk wirtualnych: Hyper-V i VMware, - image backup	- backup endpointów, - backup urządzeń mobilnych (IOS + Android), - backup skrzynek pocztowych, - backup MS Exchange, - backup serwera, - backup baz danych: MS SQL, MySQL, PostgreSQL i Firebird - backup środowisk wirtualnych: Hyper-V i VMware, - VHD image backup	- backup endpointów, - backup urządzeń mobilnych (IOS + Android), - backup skrzynek pocztowych , - VHD image backup
Odzyskiwanie	- odzyskiwanie danych z backupu plikowego, - odzyskiwanie / migracja danych za pomocą HDD image backup, - replikacja, kopia serwera na drugim serwerze QNAP, - technologia Smart Recovery, odpalanie zwirtualizowanych danych bezpośrednio z appliance'a, - technologia Smart Virtualization Stick, odpalanie zwirtualizowanych danych bezpośrednio z pendrive'a	- odzyskiwanie danych z backupu plikowego, - odzyskiwanie / migracja danych za pomocą HDD image backup, - technologia Smart Virtualization Stick, odpalanie zwirtualizowanych danych bezpośrednio z pendrive'a	- proste i szybkie odzyskiwanie danych, od pojedynczych plików i folderów na całej infrastrukturze IT kończąc, - łatwa i bezpieczna migracja danych	- proste i szybkie odzyskiwanie danych z backupu plikowego lub VHD image backup
Zarządzanie	- centralne zarządzanie, - zdalne zarządzanie, - zarządzanie użytkownikami, - zarządzanie przestrzenią storagu, - zarządzanie politykami backupu, - panel kontrolny, - dostęp do danych online, - dostęp do logów, - cicha instalacja	- centralne zarządzanie, - zdalne zarządzanie, - zarządzanie użytkownikami, - zarządzanie przestrzenią storagu, - zarządzanie politykami backupu, - panel kontrolny, - dostęp do danych online, - dostęp do logów, - cicha instalacja	- centralne zarządzanie, - zdalne zarządzanie, - zarządzanie użytkownikami, - zarządzanie przestrzenią storagu, - zarządzanie politykami backupu, - panel kontrolny, - dostęp do danych online, - dostęp do logów, - cicha instalacja	- dostęp do danych online
Bezpieczeństwo	- szyfrowanie algorytmem AES 256, - domyślny klucz szyfrujący, - klucz użytkownika, - podział pliku na chunk'i przed wysyłką, - logi aplikacji - szyfrowana Aktówka, Synchronizacja+	- szyfrowanie algorytmem AES 256, - domyślny klucz szyfrujący, - klucz użytkownika, - podział pliku na chunk'i przed wysyłką, - logi aplikacji - szyfrowana Aktówka, Synchronizacja+	- szyfrowanie algorytmem AES 256, - domyślny klucz szyfrujący, - klucz użytkownika, - podział pliku na chunk'i przed wysyłką, - logi aplikacji - szyfrowana Aktówka, Synchronizacja+ - redundantne centrum danych	- szyfrowanie algorytmem AES 256, - domyślny klucz szyfrujący, - klucz użytkownika, - podział pliku na chunk'i przed wysyłką, - logi aplikacji - szyfrowana Aktówka, Synchronizacja+ - redundantne centrum danych
Trial	30 dni	30 dni	14 dni	14 dni
Licencje + ceny	**Endpoint Agent** - 149 zł urządzenie **Server Agent Basic** - 999 zł urządzenie **Server Agent Pro** - 1499 zł urządzenie **Virtual Agent** (Vmware i Hyper-V) - 1499 zł za host'a	**Endpoint Agent** - 149 zł urządzenie **Server Agent Basic** - 999 zł urządzenie **Server Agent Pro** - 1499 zł urządzenie **Virtual Agent** (Vmware i Hyper-V) - 1499 zł za host'a	**Endpoint Protection** Starter 100GB – 289 zł / rok **Endpoint and Server Protection** Starter 100GB – 589 zł / rok	**Personal 1** – 119,99 zł / rok 1 user | 1 host | 1 TB **Personal 2** – 199,99 zł / rok 1 user | 3 hosts | 1,5 TB **Personal 3** – 359,99 zł / rok 1 user | 5 hosts | 2 TB
Reseller	Szkolenia: - regularne webinary - webinary specjalistyczne, - dokumenty techniczne i whitepapers - demo Support: - wsparcie techniczne, - wsparcie marketingowo-sprzedażowe	Szkolenia: - regularne webinary - webinary specjalistyczne, - dokumenty techniczne i whitepapers - demo Support: - wsparcie techniczne, - wsparcie marketingowo-sprzedażowe	**Łatwe zarządzanie sprzedażą, produktami oraz użytkownikami z poziomu panelu resellera.** Szkolenia: - regularne webinary - webinary specjalistyczne, - dokumenty techniczne i whitepapers - demo Support: - wsparcie techniczne, - wsparcie marketingowo-sprzedażowe	**Łatwe zarządzanie sprzedażą, produktami oraz użytkownikami z poziomu panelu resellera.** Szkolenia: - regularne webinary - webinary specjalistyczne, - dokumenty techniczne i whitepapers - demo Support: - wsparcie techniczne, - wsparcie marketingowo-sprzedażowe