

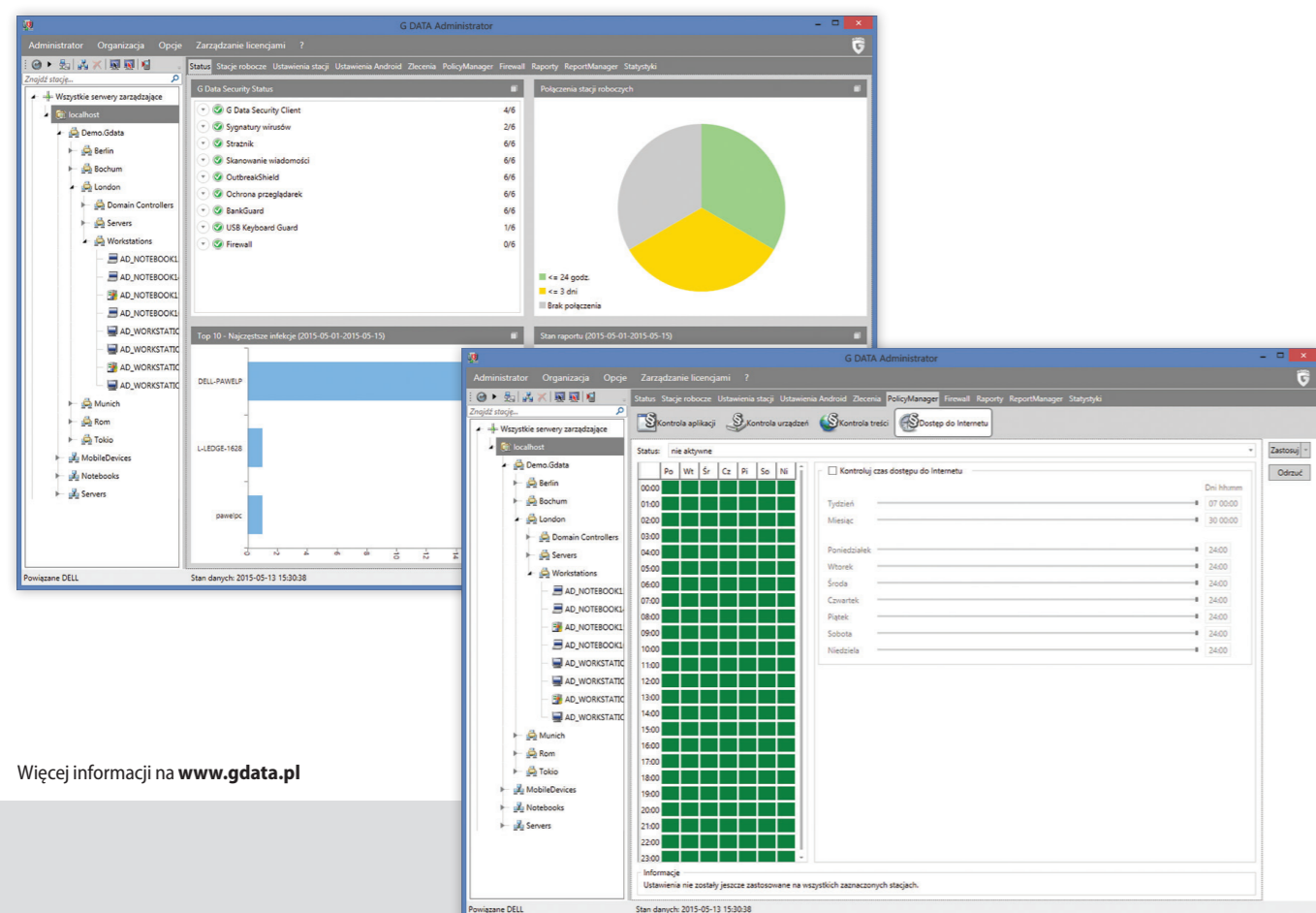
G DATA ENDPOINT PROTECTION BUSINESS

KOMPLEKSOWE BEZPIECZEŃSTWO DLA SIECI DOWOLNYCH ROZMIARÓW

G DATA ENDPOINT PROTECTION chroni Twoją sieć na wiele sposobów. Osiągnij najwyższy poziom bezpieczeństwa dzięki kombinacji aktywnej ochrony hybrydowej CloseGap oraz najlepszego czasu reakcji na najnowsze zagrożenia. Prócz ochrony antywirusowej, zapory sieciowej i antyspamu G Data oferuje moduł PolicyManager, który pozwala kontrolować dostęp pracowników do internetu, zainstalowanych programów czy zewnętrznych pamięci masowych.

Ochrona AntiSpam dedykowana dla serwerów Exchange, wsparcie dla większej liczby dystrybucji Linux oraz ochrona przed zmanipulowanymi napędami USB z wykorzystaniem G DATA USB KEYBOARD GUARD pozwoliły osiągnąć jeszcze wyższy poziom bezpieczeństwa dla Twojej sieci firmowej.

W G DATA od 30 lat prowadzimy badania nad cyfrowym bezpieczeństwem. Rezultatem jest wyjątkowa oraz kompleksowa ochrona stacji klienckich w sieciach firmowych. Łatwa instalacja, prosta obsługa i brak wpływu na wydajność chronionych urządzeń.



Więcej informacji na www.gdata.pl

KOMPLETNA OCHRONA STACJI KLIENCKICH

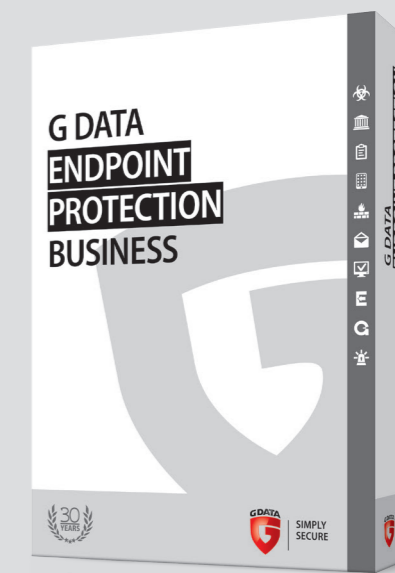
Technologia hybrydowa CloseGap	najlepsza ochrona dzięki ochronie proaktywnej oraz maksymalnie aktualnym bazom sygnatur.
G DATA BankGuard 2.0	bezpieczna bankowość bez potrzeby instalowania zbędnych dodatków do przeglądarki.
Kontrola zachowania	obrona przed nieznanymi zagrożeniami, szkodnikami, wirusami.
NOWOŚĆ Ochrona przed zmanipulowanymi urządzeniami USB	USB KEYBOARD GUARD zapewnia ochronę przed zmanipulowanymi urządzeniami podłączanymi pod porty USB.
Antywirus i antyspam poczty	wtyczka do Microsoft Outlook oraz ochrona kont POP3 i IMAP.
Wydajny firewall	monitoruje wszelkie połączenia przychodzące i wychodzące. Chroni przed atakami DoS, skanowaniem portów itp.
OPTIMALIZACJA Antywirus dla Linuxa	wsparcie dla jeszcze większej liczby dystrybucji.

CENTRALNE ZARZĄDZANIE

Prosta administracja i przejrzysty interfejs	zdalne instalacje, skanowanie i zarządzanie klientami w sieci.
Raport instalacji	status oraz historia dotychczasowych instalacji.
Zaprojektowany na nowo dashboard	intuicyjne okno do przeglądu wszelkich istotnych informacji o systemie wraz z podpowiedziami kontekstowymi.
Zdalne administrowanie	zarządzaj siecią z okna przeglądarki na urządzeniu mobilnym korzystając z zabezpieczonego połączenia.
Kontrola urządzeń	określa zasady dostępu do napędów USB, kart pamięci, napędów optycznych czy kamer internetowych.
Kontrola aplikacji	do ustalenia ogólnych zasad instalowania i korzystania z oprogramowania w sieci przedsiębiorstwa.
Kontrola treści	blokuje nieodpowiednie strony www.
Kontrola dostępu do internetu	możliwość określenia ram czasowych korzystania z sieci w firmie.
Synchronizacja z Active Directory	odzworowanie struktury organizacyjnej i automatyczna instalacja klientów.
NOWOŚĆ Mobile Device Management	centralne zarządzanie urządzeniami mobilnymi z iOS i Androidem w sieci firmowej - funkcje antykradzieżowe, kontrola instalowanych aplikacji, filtr połączeń.
Katalog sprzętu i oprogramowania	zestawienie wykorzystywanych urządzeń i zainstalowanego oprogramowania w sieci firmowej.
Aktualizacje i pomoc techniczna	darmowa aktualizacja do najnowszej wersji programu w ramach licencji oraz polskojęzyczna pomoc techniczna na wypadek kłopotów.

MODUŁY OPCJONALNE

OPTIMALIZACJA MailSecurity	centralny filtr spamu i zagrożeń (SMTP/POP3) dla dowolnego serwera poczty - Exchange, Domino itp. Zawiera plug-in dla MS Exchange od wersji 2007 do 2013.
Centralne kopie zapasowe	zabezpieczaj oraz zarządzaj danymi w sieci firmowej.
PatchManagement	centralne zarządzanie aktualizacjami oprogramowania na stacjach klienckich.
Antywirus dla Mac	kompleksowa ochrona dla komputerów z systemem Mac OS w Twojej sieci.



Wymagania
G DATA Security Client, Management Server, G DATA MailSecurity:
 Windows 8.1/8/7/Vista/XP (32-bit),
 Windows Server 2003/2008/2012, 1 GB RAM
G DATA Administrator, G DATA WebAdministrator, G DATA MailSecurity Administrator:
 Windows 8.1/8/7/Vista/XP (32-bit),
 Windows Server 2003/2008/2012, 1 GB RAM

G DATA Security for Linux (32-bit/64-bit):
 Debian 6.0 i 7, OpenSUSE 11.4, 12.2, 12.3 i 13.1,
 SUSE Linux Enterprise Server 10 SP4, SP3 11
 i 12, Red Hat Enterprise Linux 6.6 i 7.0 5.11
 Ubuntu 10.04.4 LTS, 12.04.5 LTS, 14.04.1 LTS
 i 14.10 CentOS 6.6 i 7.0 5.11, Fedora 19, 20 i 21