

## PRZEGLĄD PRODUKTÓW

### G DATA TOTAL SECURITY 2010

John Hawes

Firma *G Data Software*, założona w roku 1989 w Bochum (Niemcy), działa w branży oprogramowania antywirusowego już od ponad dwudziestu lat. Oprócz swojego sztanदारowego produktu, obecnego od dawna na rynku, a znanego wcześniej jako *AntiVirusKit (AVK)*, firma oferuje aktualnie całą gamę zabezpieczeń antywirusowych, łącznie z oprogramowaniem zabezpieczającym przeznaczonym dla biznesu, i nadal zwiększa swoją obecność na rynkach na całym świecie.

Być może nie posiada ona, przynajmniej poza ojczystymi Niemcami, tak mocno ugruntowanej pozycji wśród firm produkujących oprogramowanie antywirusowe, to jednak jej nazwa jest dobrze znana częstym czytelnikom VB, dzięki konsekwentnie utrzymującym się doskonałym wynikach w próbach VB100. Produkty firmy stworzyły imponującą serię pozytywnych wyników z zaledwie dwoma wynikami negatywnymi od 2003 roku (jeden z nich otrzymany za fałszywe rozpoznanie zagrożenia o stosunkowo niewielkiej wadze, a drugi za problem ze skanowaniem stacji dyskiety - wtedy takie rzeczy wciąż jeszcze były ważne). W ostatnich przeglądach porównawczych nasz nowy system oceniania reaktywnego i proaktywnego (RAP) podkreślił wspaniały potencjał wykrywania zagrożeń otrzymany dzięki wykorzystaniu przez producenta podejścia z dwoma silnikami, a co za tym idzie, umieszczenie go wśród wiodących systemów w naszych ćwiartkach RAP. Podobnie imponujące

wyniki osiągnięte zostały w innych, niezależnych testach. Zdecydowaliśmy przyrzeć się dokładniej najnowszemu produktowi zawierającemu kompletny zestaw funkcji obiecujący szeroką gamę elementów nadprogramowych, dodatków do najwyższej klasy ochrony przed złośliwym oprogramowaniem.

### OBECNOŚĆ W SIECI, INFORMACJA I WSPARCIE TECHNICZNE

Firma posiada znaczną liczbę stron internetowych w różnych językach z macierzystą, angielskojęzyczną stroną znajdującą się na [gdatasoftware.com](http://gdatasoftware.com). Rozpoczynając z tego miejsca, użytkownicy mogą przejść do strony zlokalizowanej dla ich regionu, przy czym większość wersji językowych oferuje te same wrażenia: strona jest prosta, przejrzysta, poprawnie reaguje na działania użytkownika i działa bez zarzutu pomimo wyłączonej możliwości uruchamiania skryptów – będącej szczegółem uznawanym przez zbyt wiele firm jako przeszkoda nie do zaakceptowania w ich działaniach marketingowych. Strona główna jest mocno skoncentrowana na produktach. Zawiera listę oferowanej gamy produktów umieszczoną na honorowym miejscu tuż pod kolorową reklamą najnowszej wersji 2010. Dołączono szczegóły aktualnych przychylnych recenzji, informacje o możliwości modernizacji już zakupionych produktów, a także wybór najnowszych informacji dotyczących zagadnień bezpieczeństwa. Zestaw linków prowadzący do głównych podsekcji strony - pierwszy z nich to oczywiście sklep internetowy oraz dostęp do darmowych wersji próbnych, które wydają się obejmować większość

produktów przeznaczonych do użytku domowego.

Następna sekcja to wsparcie techniczne, której jasny i prosty układ jest kontynuacją układu reszty stron: duże i wyraźne pole wyszukiwania jest jego głównym elementem, a numery kontaktowe, tak często dziś usuwane z zasięgu wzroku, żeby uniemożliwić jakąkolwiek formę kontaktu z producentem, umieszczone są bardzo wyraźnie na górze każdej strony dotyczącej zagadnień wsparcia technicznego. Dostępny jest także formularz kontaktu online, razem ze szczegółowymi danymi teleadresowymi zarówno do biur lokalnych, jak i do biura głównego. Do rozwiązywania nieco bardziej standardowych zagadnień przygotowano bardzo porządną zaopatrzoną sekcję *Najczęściej zadawanych pytań*, zawierającą szeroki zestaw często spotykanych problemów oraz jasnych i sensownych rozwiązań, a wszystko to z możliwością łatwego wyszukiwania potrzebnych haseł. Sekcja pobierania zapewnia dostęp do bardziej szczegółowych instrukcji obsługi (choć niektóre z nich nie są jeszcze dostępne dla edycji 2010), jak również wybór dodatkowych narzędzi, łącznie ze startowym obrazem CD wykorzystywanym przy bardziej skomplikowanym oczyszczeniu systemu.

Sekcja pt. „Laboratorium bezpieczeństwa” zawiera bardziej ogólny zestaw porad i pomocy, a także informacje o złośliwym oprogramowaniu i dotyczących go kwestiach, dobrze zaopatrzoną w wiadomości i alerty bibliotekę, zestaw pomocnych wskazówek i trików pomagających wzmocnić ogólne bezpieczeństwo, takich jak wybór hasła czy też robienie kopii zapasowych dla

danych. Dostępne są też zabawne statystyki, niektóre w postaci map i wykresów obrazujących ataki przeprowadzone przez złośliwe oprogramowanie i spam (łącznie z zabawnym pomiarem „masywności” ataków), liczbę aktywnych zombie itp. Na koniec w kilku słowach przedstawiono dane na temat firmy oraz jej partnerów biznesowych, a także imponującą listę rekomendacji pochodzących od obecnych klientów, głównie z Niemiec. Dostępna jest także lista współpracujących partnerów technologicznych, na której znajdują się wiodące firmy zajmujące się bezpieczeństwem. Po przeglądnięciu informacji dostępnych online, a nie mając jeszcze pomysłu na testowanie systemu, wzięliśmy do laboratorium naszą kopię pierwszego produktu na liście: *Total Security*.

## INSTALACJA, KONFIGURACJA I POMOC

Instalacja produktu jest dość prosta. W przypadku systemów o mniejszej mocy, zatrzymuje się w kilku miejscach, ale generalnie działa dość szybko. Możliwe jest zainstalowanie dodatkowych komponentów takich jak nadzór rodzicielski czy niszcarka danych. Także na tym poziomie możliwe jest dołączenie (lub nie) standardowego obecnie systemu społecznościowego. Chwilę później wszystko już działa, ale oczywiście konieczne jest jeszcze zainstalowanie aktualizacji, aby przyspieszyć działanie. Zaskakujące jest to, że pakiet przeznaczony do pobrania najwyraźniej nie zawiera danych odnośnie wykrywania nowych zagrożeń dodanych na przestrzeni ostatnich kilku miesięcy, w związku z czym konieczna jest dość długo trwająca aktualizacja. Wydaje się,

że dodatkowa praca potrzebna, aby utrzymywać względnie na bieżąco standardowy pakiet instalacyjny dostępny online, zostanie zrekompensovana przez mniejsze obciążenie serwerów z aktualizacjami oraz lepszą natychmiastową ochronę zapewnianą użytkownikom, to jednak bez wątpienia istnieją inne czynniki mające wpływ na podjętą przez producenta taką, a nie inną decyzję.



Kiedy już wszystko działa, produkt prezentuje bardzo atrakcyjny interfejs oddający wrażenie spokojnej obecności firmy w sieci. Jego wygląd jest dość standardowy: zawiera listę różnych komponentów i modułów, razem z informacją o ich stanie, linkami do ich konfiguracji i zarządzania. Po lewej stronie panelu sporo miejsca zajmują informacje dotyczące licencji, a także ładne, małe wykresy obciążenia systemu i skanera. Szybkie sprawdzenie różnych opcje menu natychmiast pokazało, że dostępne możliwości sterowania na głębszych poziomach są godne pochwały. Na pierwszy rzut oka całość wyglądała na logicznie ułożoną i przystępną, zdecydowaliśmy więc przyrzeć się później dokładniej niższym poziomom każdej z sekcji, zatrzymując się tylko po to, by spojrzeć pobieżnie na system pomocy.

Do systemu pomocy można przejść dzięki linkowi umieszczonemu w głównym oknie interfejsu użytkownika (jest to możliwe tylko ze strony głównej). Istnieje także kilka linków kontekstowych znajdujących się w różnych podsekcjach dotyczących kontroli, co jest często szybkim i użytecznym sposobem na dotarcie do informacji na konkretny temat. Podane informacje są dogłębne i ogólnie jasne i klarowne. Czasem zdarzają się jedynie drobne usterki stylowe i gramatyczne powstałe podczas tłumaczenia. Choć nie ma zbyt wiele zrzutów ekranu czy też linków do obszaru kontroli nad głównym produktem, tematy opracowane są doskonale i uzupełnione są bardzo dobrym zbiorem „wskazówek” prowadzących użytkownika podczas wykonywania konkretnych zadań, zamiast, jak to czasem bywa, wyszczególniać, jakie jest zadanie każdego z poszczególnych przycisków. Reasumując, produkt wydaje się być dobrze zaprojektowany i zaprezentowany. Nadszedł czas, żeby sprawdzić, co takiego kryje się wewnątrz.

## OCHRONA SYSTEMU I WYKRYWANIE ZŁOŚLIWEGO OPROGRAMOWANIA

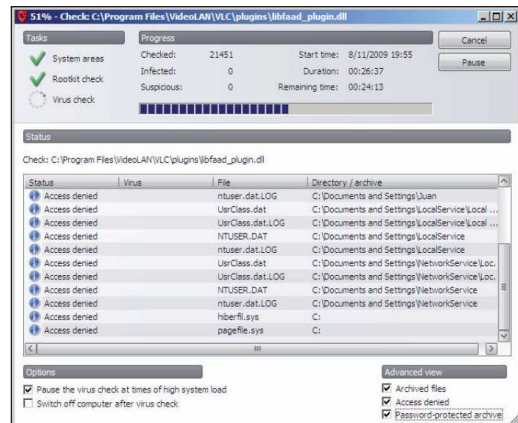
Zauważyliśmy już spójną doskonałość *G Daty* w kwestii wykrywania złośliwego oprogramowania, czego dowodem są doskonale wyniki działania w VB100 i innych testach. Wysoki poziom wykrywania zapewniono dzięki wykorzystaniu dwóch osobnych mechanizmów, które były już stosowane w przeszłości, przez co warto wspomnieć o niektórych programistach i laboratoriach. Dawniej to mechanizm Kaspersky’ego, tak popularnego dzięki swoim produktom OEM, był podporą

komponentów, ale tym razem firma *G Data* postanowiła przenieść się na nowy teren, łącząc mechanizmy *BitDefender* i *Alwil*. Sądząc po naszych najnowszych pomiarach w testach porównawczych VB100, obydwa te mechanizmy dawały sobie doskonale radę, ich kombinacja obiecywała więc zapewnić równie dobre, jeśli nie lepsze poziomy wykrywalności, przy okazji redukując w niektórych przypadkach znacznie czasy skanowania.

Uruchomienie produktu dla naszego próbnego zbioru okazało się być warte swojej ceny - skaner z łatwością poradził sobie ze wszystkim, z czym kazaliśmy się mu zmierzyć. Biorąc pod uwagę nasze improwizowane próby, wydaje się, że *G Data* jest gotowa do dalszego ulepszania jeszcze przez najbliższe kilka miesięcy swojej już i tak doskonałej pozycji na naszych wykresach wycinkowych RAP. Skanowanie okazało się być wiarygodne i stabilne, dające sobie bez żadnego problemu radę z grupami trudnych do usunięcia wadliwych plików, które w przeszłości zmyliły wielu, a monitor dostępu dzielnie się trzymał nawet podczas wyjątkowo silnego bombardowania go z różnych stron żądaniami.

Do produktu nie dołączono blokowania typu HIPS ani blokowania behawioralnego, ale posiadając dwa mechanizmy osiągające ostatnio wspaniałe wyniki w reakcyjnej części naszych zestawów RAP, ochrona zapewniana przeciwko nowemu i nieznanemu złośliwemu oprogramowaniu powinna być prawie tak dobra, jak w przypadku skanowania statycznego wykorzystującego zaawansowane heurystyczne i generyczne rozpoznanie. Stwierdziliśmy również, że podane koszty ogólne są całkiem rozsądne, pomimo

dwustronnego podejścia, wzięwszy pod uwagę fakt, że większość systemów działa doskonale - nawet netbooki o mniejszej mocy nie pracowały wolniej niż normalnie.



Skanowanie na żądanie, zaprojektowane tak, by było szybkie i możliwie jak najdokładniejsze, nakłada jednak znaczne ograniczenia na system pod kątem jednoczesnego wykorzystywania zasobów do innych celów w czasie, gdy wykonywane jest sprawdzenie. Istnieje jednakże możliwość przekazania kontroli, jeśli użytkownik chce kontynuować inne działania. Możliwość przekazania kontroli może także zostać włączona w trakcie skanowania i choć potrzeba na to kilku chwil, to urządzenie zaraz powraca do pracy z maksymalną prędkością i wznowia skanowanie wysokiej mocy kiedy tylko zwolnią się zasoby. System cache jest także całkiem przyzwoity, dzięki czemu wcześniej przeskanowane lub znajdując się na białych listach pliki są ignorowane – ta technologia nie jest jeszcze dokładnie brana pod uwagę w naszych porównawczych pomiarach prędkości, ale mamy nadzieję, że w niedalekiej przyszłości wprowadzimy aktualizacje do naszego systemu. Sprawdzając jednak w sposób zupełnie nienaukowy,

wydaje się dość oczywistym, że skaner znacznie przyspieszył po tym, jak zdążył poznać lokalny system.

Ograniczeni jak zwykle brakiem czasu, nie mieliśmy możliwości wejść zbyt głęboko w szczegóły, a mając do przygotowania jeszcze jedno porównanie na szybko zbliżającą się roczną konferencję VB, nie przyjrzelśmy się tak dokładnie, jak byśmy chcieli usuwaniu i szczepionkom. Jednakże te elementy, które zainstalowaliśmy w systemie mogły być dokładnie i do czysta usunięte po tym, jak już wszystkie niezbędne definicje zostały zaktualizowane, zapewniając poprawne wykrywanie. System okazał się być zarówno prosty w obsłudze, jak i zadziwiająco dokładny – nie udało nam się wymyślić żadnej opcji, której albo by brakowało albo też byłaby ciężka do znalezienia. Zarówno w przypadku monitorów dostępu, jak i skanowania na żądanie istnieje możliwość używania jednego lub drugiego silnika (skromnie nazywanych „Silnikiem A” i „Silnikiem B”), przy czym domyślne ustawienia zakładają wykorzystywanie obydwu silników w obydwu trybach. „Silnik A” jest przedstawiony jako lepiej wykrywający zagrożenia, lecz pracujący nieco wolniej, natomiast „Silnik B” jest polecany do szybkiego skanowania i nie tak dokładnego wyszukiwania. Prostota operacji dotyczy także ochrony poczty elektronicznej i internetu, która co prawda posiada osobną sekcję w głównym interfejsie, to jednak jest ściśle powiązana ze skanerem wykrywającym złośliwe oprogramowanie. Komunikacja po HTTP, IM oraz wymiana poczty elektronicznej są skanowane i mają kilka konfigurowalnych wartości takich, jak limit rozmiaru dla skanowanych plików i załączników, dodawanie portów do skanowania itp. Ponadto, użytkownik

może wybrać opcję raportowania zainfekowanych stron właścicielom, aby zwiększyć ochronę całej społeczności. Biorąc pod uwagę inny ważny element ochrony, pakiet zawiera oczywiście obowiązkową teraz zaporę ogniową. W tej dziedzinie obowiązują pewne proste zasady osiągnięcia sukcesu: skuteczność ustawień standardowych, inwazyjność (lub jej brak) wynikająca z doświadczenia użytkownika oraz, w przypadku bardziej zaawansowanych użytkowników, przydatność precyzyjnego dostrajania. W przypadku każdego z tych trzech czynników *G Data* otrzymuje bardzo wysokie oceny. Domyślnie, zaporę ogniową działa wyłącznie na „autopilocie”, trzymając się wybranych standardowych zasad i tworząc nowe zestawy dla jakiegokolwiek znalezionego w systemie działającego oprogramowania, które korzysta z sieci. Wygląda na to, że całość jest całkiem niezłe przemyślana i skuteczna, a zgromadzone doświadczenie wydaje się nie istnieć z punktu widzenia użytkownika, podobnie jak procesy uczenia się i ciągły natłok próśb o pozwolenie na wykonanie, tak lubiane przez wiele systemów. Dla przeciętnego użytkownika zapewniany jest bardzo zadowalający poziom zabezpieczenia przed atakami z sieci w sposób niewymagający od niego żadnego wysiłku.



Dla tych bardziej doświadczonych (lub też bardziej obsesyjnych) istnieje oczywiście możliwość głębszego wnikięcia w ustawienia i skonfigurowania produktu dokładnie według własnych upodobań. Tego typu systemy są często skomplikowane i wprawiające w zakłopotanie, a jednak w tym przypadku, należy to podkreślić raz jeszcze, *G Data* dołożyła wszelkich starań, aby zapewnić dostęp do regulacji nawet tym użytkownikom, którzy posiadają mniej doświadczenia i wiedzy. Prosty i przyjemny kreator przeprowadza użytkownika przez proces projektowania i tworzenia zasad lub zestawu zasad bazujących na kategoriach – włączając w to aplikacje, połączenia sieciowe i usługi, a także sterowanie instrukcjami itp. Jedyną brakującą rzeczą byłaby możliwość łączenia konkretnych aplikacji i zachowań w bloki na poziomie lokalnym, aby móc je zmienić w pełnoprawny i wysoce użyteczny system do zarządzania aplikacjami oraz do wykrywania i zapobiegania włamaniom z poziomu hosta (HIPS). Poza tymi uproszczonymi ustawieniami, zapewniono także pełną i szczegółową konfigurację w zaawansowanej zakładce, która również jest przejrzysta i klarowna. Funkcja logowania jest kompletna i szczegółowa, z przyjemnie

jasnym podsumowaniem, dostępnym dla każdego wykrytego incydentu, bez względu na to, czy został on oznaczony jako zablokowany czy też dozwolony.

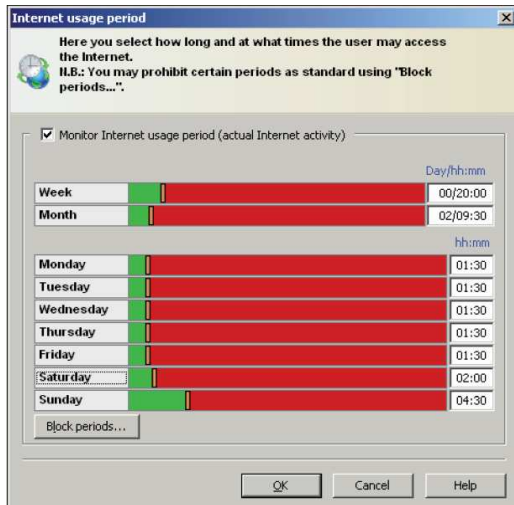
## INNE FUNKCJONALNOŚCI

Produkt nazywa się „Pełna ochrona” i oczywiście w pewnym sensie wychodzi poza wymienione do tej pory standardowe komponenty. Posiada, oczywiście, filtr antyspamowy – inny obowiązkowy w dzisiejszych czasach element ochrony. W tym przypadku, filtr antyspamowy posiada swój własny podrzędny interfejs użytkownika, dokładnie tak, jak elementy zapory ogniowej i w podobny sposób wyposażony jest w opcje i kontrolki. To kolejny element, którego nie byliśmy w stanie dogłębnie przetestować – nasze testy dla komponentów antyspamowych są bardziej nastawione na korporacje i ochronę na poziomie serwerów niż na domowego użytkownika końcowego, ale przeglądając jego rozplanowanie doszliśmy do wniosku, że oferuje on wszystko, czego można zapragnąć: od prostych list zezwalających i blokujących dostęp do szczegółowych kontrolki czułości oraz odpowiedzi na potencjalne zagrożenia. Elementy znajdujące się w niższej części głównego interfejsu dotyczą funkcji dostępnych tylko w bardzo dokładnych pakietach. Pierwsza z nich, i prawdopodobnie najbardziej powszechna, to system nadzoru rodzicielskiego służący do chronienia dzieci przed niewłaściwą zawartością stron internetowych. Testując ten fragment całkiem dobrze się bawiliśmy, z czego można ponownie wywnioskować, że interfejs został wyjątkowo dobrze zaprojektowany. Obszar, w którym definiuje się dozwoloną liczbę godzin pracy bazującą

na konkretnych przedziałach czasowych i/lub tygodniowych czy miesięcznych limitach, jest szczególnie łatwy do zaimplementowania. Istnieje nawet rozróżnienie pomiędzy korzystaniem z internetu a wykorzystaniem komputera w trybie bez połączenia. Wbudowane ustawienia oferują filtrację całej gamy niechcianych tematów, rozpoznawanych na podstawie zarówno niedozwolonych stron, jak i słów kluczy, a także podejście w stylu „otoczonego murem ogrodu”, w którym dostępne mogą być jedynie strony umieszczone na liście znanych, dozwolonych miejsc. Lista wydaje się być całkiem sensownie wypełniona, jest dość łatwa do rozszerzenia o nowe strony i całe nowe kategorie, więc zaangażowany i staranny rodzic może ją wypełnić tak, jak tylko sobie tego zażyczy. System blokowania jest równie prosty, polegający na dodawaniu w prosty sposób nowych niechcianych adresów stron lub słów kluczy.

Jednakże od strony implementacji zagadnienie wydaje się być nieco mniej kompletne, gdyż podczas testowania wykryto kilka dziwnych zachowań. Zdarza się czasem, że strony znajdujące się na liście stron dozwolonych nie są wyświetlane, a kolejne odwiedzane strony wydają się podszywać pod brakującą stronę, zaś niektóre miejsca i kategorie wyświetlane były w innych językach, co wskazuje na to, że lokalizacja tej sekcji jest niekompletna. Jest się prawdopodobne, że pożytek z tego narzędzia będzie zależał od lokalizacji użytkownika. Metoda odwrotna, tj. blokowanie niechcianej zawartości przy jednoczesnym ogólnym zezwoleniu na dostęp również pokazała kilka osobliwości: nie zaliczyła testu „Scunthorpe’a” i najwyraźniej usuwała niektóre bloki, jeśli na tej samej stronie

znaleziono zabronione słowo kluczowe. A więc całkiem przyzwoita próba stworzenia systemu kontroli z doskonałymi możliwościami konfiguracji, połączona z niewielkim brakiem wyrafinowania w przypadku najbardziej zaawansowanych przykładów tego gatunku. Dostępne jest oczywiście pełne logowanie wykonywanych czynności. Idąc dalej, znaleźliśmy sekcję oznaczoną jako „dostrajacz”, która oferuje znacznie więcej niż tylko proste czyszczenie nadmiaru plików, dostępne także w niektórych z innych branż pod uwagę pakietów. Nie tylko czyszczone są liczne elementy czasowe i te przechowywane w pamięci cache, które można spotkać na dysku długo i intensywnie używanego urządzenia, ale także przeglądane są rejestry w poszukiwaniu niepotrzebnych odpadków oraz sprawdzane są ustawienia systemowe, aby upewnić się, że stosowane są podstawowe środki bezpieczeństwa. Rozdzielając powyżej wymienione na kwestie bezpieczeństwa, wydajności oraz związane z prywatnością, każda z nich jest ustawiona domyślnie jako aktywna, jednakże z możliwością wyłączenia. Można przeprowadzić sprawdzenie próbne, na podstawie którego zostanie stworzona lista (bez rzeczywistej implementacji) zmian uważanych za konieczne.



Zapewnione jest pełne harmonogramowanie i logowanie, a funkcja „cofania” umożliwia anulowanie zmian, które po wykonaniu zostały uznane za niewłaściwe. Wszystko to wydaje się dość dokładne, niezawierające żadnych potencjalnie szkodliwych elementów i działa zadziwiająco szybko. Po uruchomieniu tej funkcji na starym, wysłużonym netbooku, który widział już niejedno instalowane i usuwane oprogramowanie, rzeczywiście zdawała się dostrzegalnie poprawiać działanie systemu, i wyczyściła wszystkie nadmiarowe a potencjalnie wrażliwe informacje, które przyszło nam do głowy sprawdzić. Ostatnia opcja dostępna z głównego interfejsu to możliwość sporządzenia kopii zapasowej, posiadająca również własny interfejs, zgodny pod względem projektu i układu z resztą produktu. Proste kopie, wykonywane na żądanie lub zaplanowane, mogą być sporządzane, aby archiwizować konkretne, wymagane obszary i typy plików, a także zapisywane w dowolnym, sprecyzowanym przez użytkownika miejscu (choć w tym przypadku lokalne partycje dysku nie są

polecanyimi obszarami). Preferowane jest przechowywanie kopii na dyskach sieciowych, włączając opcje umieszczania ich na stronach za pośrednictwem FTP, choć lokalne kopie mogą być także tworzone i zapisywane (jeśli użytkownik tak woli) na płycie CD. I ponownie, konfiguracja jest zarówno w wysokim stopniu dogłębna i prosta w nawigacji, a dodatkowo także dokładnie logowana. Istnieje nawet system do administrowania wcześniejszych kopii zapasowych, aby móc usuwać starsze i niepotrzebne już wersje.

Przełęczając tak szeroki zakres możliwości, myśleliśmy, że powinniśmy się znajdować w okolicach końca funkcji oferowanych przez *G Data*. Mimo tego jednak pozostała jeszcze jedna opcja, na którą warto zwrócić uwagę: wspomniana pobieżnie w czasie instalacji niszcarka. Nie posiada ona swojego osobnego miejsca w interfejsie głównym, a jedynie ikonkę na pulpicie, nad którą można przeciągnąć obiekty do bezpiecznego usunięcia. Wydaje się nie mieć żadnego rodzaju konfiguracji, rezygnując z uzależnienia od decyzji użytkownika w kwestii wyboru metody niszczenia plików (co jest oferowane przez niektóre podobne narzędzia), ale wykonuje swoje zadanie w prosty i idealnie skuteczny sposób, nie sprawiając kłopotu użytkownikowi koniecznością wyboru, której wersji wojskowego, certyfikowanego przez Departament obrony USA, wielopoziomowego rodzaju nadpisywania użyć.

## WNIOSKI

Dotarliśmy do końca niniejszego przeglądu nieco przytłoczeni przez rozmach tego pakietu i pozostajemy nadal pod jego głębokim wrażeniem.

Połączenie dokładnej ochrony wynikającej z dwusilnikowego podejścia i równie precyzyjnych dodatkowych komponentów bez wątpienia przemówi w zdecydowany sposób do bardziej wymagających użytkowników, którzy nie znajdują tu pola do narzekań, może poza brakiem w pełnowymiarowego hostowego systemu wykrywania i zapobiegania włamaniom (HIPS). Jednakże punktem, w którym *G Data* naprawę zaimponowała jest układ i projekt produktu, dzięki którym produkt udostępnia swoje niesamowite możliwości znacznie szerszemu gronu odbiorców niż wąska grupa technicznych zapaleńców. Wśród szerokiej gamy produktów, które przechodzą przez nasze laboratorium VB, widać silną tendencję do poświęcania możliwości konfiguracyjnych na rzecz użyteczności, lub na odwrót, a kiedy jakiś produkt jest w stanie efektywnie połączyć te dwa elementy, wtedy zdecydowanie wybija się z tłumu. Pakiety zabezpieczające dojrzewają jako typ oprogramowania i stają się standardowymi elementami na każdej stacji roboczej, a zakres oferowanych przez nie narzędzi stale się powiększa, przy jednoczesnym doskonaleniu ich jakości. Podczas gdy niektóre z przedstawionych tu słabszych elementów ciągle jeszcze znajdują się nieco z tyłu pod względem wykonania w stosunku do najlepszych z danej dziedziny, zestawienie tak szerokiej gamy narzędzi w pojedynczym pakiecie, który na dodatek posiada jedno, wspólne podejście do działania i zarządzania, otwiera nowe horyzonty bezpieczeństwa dla szerszej grupy odbiorców. Innym szczegółem wartym nadmienienia jest udoskonalenie szybkości działania i zmniejszenie wykorzystywanych

zasobów. Podczas gdy poprzednie wersje mogły niektórym użytkownikom wydawać się zbyt potężne, a zwiększająca się moc systemów komputerowych doprowadziła niektórych programistów do przekonania, że uda im się uniknąć wzrostu kosztów ogólnych, *G Data* zdecydowanie poprawiła wydajność swoich produktów, nie osłabiając zarazem możliwości ochrony użytkowników. Koniec wyobrażenia powolnych i obojętnych systemów, które wielu wskazałoby jako główną przyczynę unikania podejścia dwusilnikowego, mogłby oznaczać pojawienie się firmy *G Data* jako istotnego gracza na scenie produktów oprogramowania antywirusowego.

**Szczegóły techniczne:**

*G Data Total Security 2010* był testowany na:

*Intel Pentium 4 1.6 GHz, 512 MB RAM, system operacyjny Microsoft Windows XP Professional SP2.*

*AMD Athlon64 3800+ o podwójnym rdzeniu, 1GB RAM, system operacyjny Microsoft XP Professional SP3 oraz Windows Vista Business Edition SP2.*

*Intel Atom 1.6 GHz netbook, 256 MB RAM, system operacyjny Microsoft Windows XP Professional SP3.*