



Dzisiejsze przedsiębiorstwa muszą pro-aktywnie chronić swoje zasoby oraz infrastrukturę IT przed rosnącą ilością zagrożeń i możliwych ataków. Ciągłe głównym obszarem, na którym skupiają się polityki bezpieczeństwa przedsiębiorstwa jest ochrona przed zagrożeniami płynącymi z sieci. Jednak w chwili obecnej coraz poważniej traktowane są ryzyka związane z wewnętrznymi zagrożeniami. Urządzenia mobilne, nośniki pamięci podłączone bez kontroli do infrastruktury przez uniwersalne porty USB, Firewire, Wi-Fi narażają organizację na możliwość utraty lub wycieku danych co może spowodować szkody zarówno finansowe jak i wizerunkowe oraz spowodować naruszenie praw i regulacji ustawowych (np. Ustawa o Ochronie Danych Osobowych).



Bezpieczeństwo stacji roboczych (komputerów, urządzeń mobilnych) jest narastającym problemem dla organizacji. Wiele firm już dzisiaj doświadcza skutków braku kompleksowej ochrony swoich komputerów i danych na nich zawartych:



- Według Gartner'a - „Pamięci USB, odtwarzacze mp3 i temu podobne mogą doprowadzić do naruszenia bezpieczeństwa i utraty danych.”
- Średni koszt incydentu utraty danych dla przedsiębiorstwa to 6,6M\$¹
- Do 50% naruszeń polityk bezpieczeństwa w firmie pochodzi z wewnątrz organizacji²
- „70% naruszeń polityk bezpieczeństwa które spowodowały straty ponad 100.000\$ pochodziły z wewnątrz organizacji”

✘ Wielu szefów IT wierzy, że ich dotychczasowe rozwiązania zapewniają ochronę end-point'a - niestety jest to mylne pojęcie. Kontrola end-point'a przez systemy operacyjne MS Windows, oprogramowanie do zarządzania domenami oraz rozwiązania typu firewall ograniczają się w najlepszym przypadku do ochrony typu włącz/wyłącz. W nowoczesnej organizacji, która zna wartość swoich informacji oraz respektuje regulacje konieczne jest wprowadzenie dodatkowych, komplementarnych rozwiązań w celu zapewnienia kompleksowej i elastycznej kontroli nad wrażliwymi informacjami.



Safend Data Protection Suite to zaawansowane i kompleksowe rozwiązanie, wysoce skalowalne, posiadające „lekkiego” klienta oraz rozdystrybuowaną i w pełni redundantną architekturę zarządzania. Jest intuicyjny i bardzo prosty w zarządzaniu, nie zaburza wydajności end-pointa i jego bezpieczeństwa.

Dla Firmy poszukującej rozwiązań, które utrzymują równowagę między wydajnością pracowników, a zapewnieniem wysokiego poziomu bezpieczeństwa danych - rozwiązaniem jest **Safend's Data Protection Suite**:

- Łatwy w zarządzaniu, poprzez przyjazny interfejs który umożliwia kreowanie polityk dla end-point'a dla dowolnych domen,

grup, komputerów, jednostek organizacyjnych lub użytkowników ze szczegółową kontrolą rodzajów urządzeń, modeli urządzeń lub unikalnych numerów seryjnych

- Wszystkie end-pointy oraz podłączone do nich pamięci przenośne są zabezpieczone domyślnie, niezależnie czy end-point jest w sieci, czy jest off-line.

Wszystkie funkcjonalności są dostarczane na *jednej* platformie serwerowej, *jednej* konsoli zarządzającej i *jednym* lekkim agencie

Safend Data Protection Suite posiada certyfikaty zgodności m.in.:



- 1) Ponemon Institute, '2008 Annual Study: Cost of a Data Breach'.
- 2) 2005 FBI/CSI Computer Crime and Security Survey.
- 3) Vista Research.

© 2009 Safend Inc. All rights reserved. Safend and the Safend logo are either registered trademarks or trademarks of Safend, Inc. in the United States and/or other countries.

© 2011 Wise Networks Sp. z o.o. - Wszelkie prawa zastrzeżone

Zdjęcia produktu

Inne rozwiązania producenta

Podobne produkty

- [Varonis Data Governance Suite](#)
- [Metasploit](#)
- [AppWall](#)
- [QRadar SIEM](#)
- [CA SiteMinder](#)
- [AppDirector](#)
- [SourceFire 3D IPS](#)
- [Nexpose](#)