1. Jakie są różnice między Safe Guard a modułem Full disk Encryption w produkcie Enduser Protection Web, Mail and Encryption?

   Kupując aktualnie bundle: Enduser Protection Web, Mail and Encryption otrzymujemy tak naprawdę kilka produktów, a z zakresu szyfrowania są to moduły Safe Guard:
   Encryption
   - SafeGuard Disk Encryption Advanced - SafeGuard Device Encryption, SafeGuard Native Device Encryption, SafeGuard Disk Encryption for Mac, Managment Center
   Czyli mamy szyfrowanie systemem Sophos, zarządzanie systemami szyfrowania natywnego oraz szyfrowanie dla Mac Os (starsze wersje).

2. Czy są jakieś mechanizmy dostępu do szyfrowanych danych z systemów Linux? Czy moduł dla Linux jest na road mapie?

   Na ten moment nie wiadomo nam nic o planach do wprowadzenia modułu szyfrowania dla Linux.

3. Czy architektura rozwiązania wymaga AD czy może się bez niej obyć (lub jakaś alternatywa) ?

   AD nie jest wymagane. Komputery mogą same odezwać się do serwera SGN po zainstalowaniu na nich klienta. Trafią wtedy do grupy Auto-registred.

4. Można użyć coś innego ? NetIQ eDirectory czy jakiś LDAP, RADIUS ...?

   Nie mam informacji o możliwości integracji z innymi bazami danych. Można jednak wykorzystać procedurę auto-rejestracji jak opisano w pkt. 3.

5. Jak ma się szyfrowanie (wolumenu, plików) do backupu?

   W wypadku szyfrowania na poziomie plików, backupowane pliki będą zaszyfrowane.

W wypadku backupu z szyfrowaniem na poziomie wolumenów backupowane dane nie będą szyfrowane, zostaną odszyfrowane w trakcie operacji kopiowania danych z dysku źródłowego na docelowy.