



# AreaGuard Neo

Ochrana důvěrných osobních i firemních informací se stává součástí našeho života, a v mnoha státech po celém světě její povinnost stanovuje i zákon. **Neoprávněné získání citlivých informací** může znamenat pro jakoukoli organizaci **citelnou finanční ztrátu** pramenící ze ztráty konkurenční výhody, důvěry zákazníků, negativní publicity a v konečném důsledku i z postihů vyplývajících z porušení zákonů a vyhlášek o ochraně osobních údajů.

Podle statistik bývá více než polovina firemních dat uložena bez jakékoliv ochrany na koncových zařízeních jako jsou desktopové počítače nebo notebooky. Citlivá data, mezi které mohou patřit například informace o zákaznících, obchodní tajemství, smlouvy nebo dokumenty shromažďující duševní vlastnictví jsou tak vystavena vysokému riziku ztráty nebo odcizení. Jednoduchý přístup uživatelů/zaměstnanců k přenosným diskovým zařízením s rozhraním USB (např. populární flash-disky nebo i MP3 přehrávače a fotografické aparáty) pak toto riziko ještě dále zvyšuje. Organizace a firmy tak stojí před nutností chránit svá data i za firemním firewallem uvnitř firemního prostředí.

## OBLASTI OCHRANY DAT A JEJICH SPRÁVA

- Ochrana dat online šifrováním
- Omezení nežádoucího používání výměnných médií
- Monitoring používání dat a chování uživatele
- Proaktivní návrhy nastavení bezpečnostních politik
- Snadné nasazení a centrální management

## JAK FUNGUJE AREAGUARD NEO

AreaGuard Neo zajišťuje ochranu informací a dat na koncových stanicích ve více vrstvách. Kombinuje ochranu dat online transparentním šifrováním s omezením nežádoucího používání výměnných médií. Pomocí centrální vzdálené správy lze snadno chránit data na notebookech, koncových stanicích uživatelů a zároveň účelně omezovat využívání výměnných zařízení uživateli. Snadná implementace a jednoduché ovládání jsou hlavními rysy produktu. AreaGuard Neo nevyžaduje přímou interakci uživatele a nepožaduje tak po něm jakoukoliv změnu zaříteného stylu práce. Pokrokový způsob proaktivního poskytování informací umožňuje mít přehled například o tom, jaká data má uživatel uložena na počítači a kde, jak často s těmito daty pracuje, popřípadě zda se blíží konec platnosti šifrovacích klíčů. Nová nastavení jsou automaticky aplikována na klienty, bez jakékoliv interakce uživatele.

AreaGuard Neo je postaven na minimální náročnosti na implementaci, provoz, správu a používání. Nízké hardwarové nároky umožňují provoz prakticky v jakémkoliv prostředí. Jde o zcela nový produkt z rodiny AreaGuard postavený na moderních technologiích, maximálně provázaný s doménovým prostředím (Active Directory) a operačním systémem Windows.

## Klientská část

### Ochrana dat šifrováním

Přístup zaměstnance k citlivým datům uvnitř firmy a jejich následná ztráta nebo odcizení patří k nejčastějším příčinám bezpečnostního incidentu. I prostý servisní zásah může znamenat, že se vaše data společně s notebookem nebo jen s pevným diskem dostanou mimo chráněné firemní prostředí. AreaGuard Neo tato rizika eliminuje online šifrováním v okamžiku ukládání souborů na lokální disky. Přístup k souborům je umožněn pouze dešifrováním autorizovaným uživatelům.

### Správa výměnných zařízení

Výměnná zařízení jsou díky své fyzické velikosti, kapacitě a obtížné sledovatelnosti velmi častým způsobem úniku dat. AreaGuard Neo umožňuje organizacím monitorovat a řídit přístup k výměnným zařízením na koncových stanicích uživatelů. Lze tak učinit v závislosti na typu zařízení a/nebo jeho výrobním čísle a to i v okamžiku, kdy není daný počítač připojen k firemní síti.

## Serverová část

### Centrální správa snadno a efektivně

Plné napojení na firemní doménové prostředí (Active Directory) s důrazem na rychlé nasazení, maximálně jednoduchý provoz a celkové usnadnění práce. Všechny administrátorské úkony lze provádět z jediné administrátorské konzole prostřednictvím domény. Distribuce klientů a aktualizací na koncové stanice, tvorba, modifikace a distribuce bezpečnostních politik je tak řešena z jednoho místa a v rámci jednoho prostředí.

### Správa šifrovacích klíčů

Efektivní správa šifrovacích klíčů v AreaGuard Neo umožňuje oprávněným uživatelům bezpečně a snadno přistupovat k datům na jejich pracovních stanicích a notebookech. Centrální správa poskytuje snadný způsob správy vydaných šifrovacích klíčů, a jejich bezpečné uložení a obnovu v různorodém prostředí organizace.

### Průběžný monitoring a proaktivní logování

Komplexní ochrana informací a dat v podnikových prostředích s různými koncovými zařízeními a operačními systémy může být náročná. Pokud zaměstnanci a obchodní partneři organizace mají přístup k datům z mnoha míst, zařízení a aplikací, nelze se bez centralizovaného vyhodnocení rizik obejít. AreaGuard Neo zajišťuje průběžný sběr, zpracování a vyhodnocení provozních informací získávaných z klientských stanic do přehledů, které umožňují správci reaktivní nastavení optimálních bezpečnostních politik a následně ověřování jejich dodržení. Bezpečnostní politika tak lze snadno nastavit, vynutit a kontrolovat s cílem snížit bezpečnostní rizika na minimum. Veškeré případné bezpečnostní incidenty jsou zaznamenávány pro vyhodnocení rizik.





# AreaGuard Neo

## PŘEHLED KLÍČOVÝCH FUNKCÍ A ZÁKLADNÍCH TECHNICKÝCH ÚDAJŮ

- Plná podpora doménového prostředí (Microsoft Active Directory).
- Přehledná centrální správa nabízí správci inteligentní nástroje pro rychlá a efektivní rozhodnutí s možností vynucení jejich dodržování a zpětné kontroly. Výsledkem je celkové snížení provozních nákladů na ochranu informací a dat společnosti.

### Klientská část

- Ochrana dat uživatele prostřednictvím online transparentního šifrování souborů na koncové stanici (symetrická kryptografie, použití silného algoritmu AES 256bit). Všechna data v uživatelském profilu jsou automaticky šifrována. V případě zcizení nebo ztráty zařízení tak zůstávají chráněna.
- Audit lokálních disků poskytující informaci o dalších úložištích uživatelských dat, jejich typech četnosti použití. Díky tomu lze ochránit jakákoliv uživatelská data, ať už jsou uložena na disku kdekoliv.
- Sledování a možnost omezení pohybu dat na výměnných zařízeních v organizaci pomocí restrikcí. Přístup k zařízení může být blokován nebo povolen v závislosti na typu zařízení a/nebo jeho výrobním čísle.
- Minimální požadavky na znalosti uživatele. Produkt nevyžaduje přímou interakci a nesnižuje tak produktivitu práce.

### Serverová část

- Centrální správa bezpečnostních politik napříč organizací prostřednictvím administrátorské konzole.
- Snadná distribuce klientů a aktualizací na koncové stanice prostřednictvím domény/patch klienta.
- Snadné nastavení politik díky proaktivnímu logování a vyhodnocení aktivit uživatele.
- Automatizovaná evidence, záloha a přidělení šifrovacích klíčů uživateli (depozitář šifrovacích klíčů).
- Monitoring a vyhodnocení aktuálního stavu ochrany dat na koncových stanicích. Jednoduchá možnost nastavení tzv. white-listů pro přístup k výměnným zařízením.
- V případě ztráty notebooku lze díky průběžnému logování stavu ochrany provést zpětný audit a prokazatelně zjistit/doložit, že nedošlo k úniku nešifrovaných dat.
- Databáze postavená na efektivním nástroji Microsoft SQL.

## SYSTÉMOVÉ POŽADAVKY

### Klientská část

- Windows XP SP3, Windows Vista 32/64bit, Windows 7 32/64bit
- .NET framework minimálně 2.0.
- Počítače a uživatelé v doméně Windows.

### Serverová část

- 32/64bitová edice Windows Server 2003, 2003 R2, 2008, 2008 R2, možnost použít i na SBS edici.
- Microsoft SQL server 2005 a vyšší, možnost použít i edici Express.
- Dostupný server s Active Directory Domain Services.

## DALŠÍ INFORMACE

### O SPOLEČNOSTI SODATSW s.r.o.

SODATSW s.r.o. je výrobce a dodavatel originálních řešení určených pro správu a bezpečnost pracovních stanic. Profesionální ochraně dat a monitoringu činností na počítačích se věnujeme již od roku 1993. Naše šifrování dat využívá například Ministerstvo vnitra ČR a Ministerstvo financí ČR. Data pomáháme chránit i dalším orgánům státní správy a samosprávy, školám, zdravotnickým zařízením stejně tak jako bankám a malým i velkým firmám. Jen v České republice chrání naše technologie více než 50.000 počítačů.

Pro další informace navštivte prosím náš web:

na [www.sodatSW.cz/neo](http://www.sodatSW.cz/neo) nebo kontaktujte obchodní oddělení na tel. **543 236 177** případně využijte mail [sales@sodatSW.cz](mailto:sales@sodatSW.cz).

Jsme Microsoft Certified Gold Partner. Úspěšně jsme absolvovali certifikační audit systému kvality mezinárodního standardu ISO 9001:2009 pro systém managementu kvality vývoje, technické podpory a implementace a ISO/IEC 27001:2006 pro systém managementu bezpečnosti informací. Disponujeme osvědčením podnikatele od NBÚ pro seznamování se s utajovanými informacemi do stupně utajení Důvěrně.