# Specifikace funkcionalit bezpečnostního softwaru Varonis

## I. Přehled funkcionalit a popis jednotlivých modulů

### a) Obousměrná viditelnost oprávnění k datům uloženým ve spravovaných systémech

- Systém umožňuje zobrazit přístupová práva k uloženým datům (složky, dokumenty, klasifikované soubory) pro všechny spravované uživatele a skupiny. Stejně tak umožňuje zobrazovat přístupová práva pro jednotlivé objekty uložených dat (složky, klasifikované dokumenty,) na jednotlivé uživatele a skupiny.
- Informace o uživatelích jsou přímo propojeny s metadaty o řízení přístupu k jednotlivým datovým objektům.
- Systém jednoduše zobrazuje u uživatele všechny skupiny a podskupiny ve kterých se nachází.
- V systému je na první pohled jasné, zdali daný učet je v AD „enable“ či „disable“

### b) Kompletní auditní záznamy

- Systém pro všechny sledované servery pořizuje o každé operaci prováděné nad datovým objektem auditní záznam.
- Auditní záznam obsahuje kompletní informace o prováděných operacích.
- Systém audituje veškeré operace prováděné v samotném managementu bezpečnostního SW. Tento údaj obsahuje informace o dané události, a především identitu účtu, který operaci vykonal.
- V auditních záznamech nad dokumenty jsou viditelné záznamy, zdali se jedná o klasifikovaný soubor s informací o klasifikačním pravidle. Např.: dokument obsahuje rodné číslo, datum narození atp.
- Nad auditními záznamy je možno provádět vyhledávání, filtrování a třídění.
- Sběr dat má minimální dopad na výkonnost serveru. Klasifikace dat není prováděna na zdrojových uložištích. Může se používat jiný dedikovaný výpočetní výkon.
- Sběr dat je prováděn skrze agenty/služby nainstalované na jednotlivých informačních systémech nebo skrze standardní přístupová práva s nastavením čtení Security Event Logu jednotlivých doménových kontrolérů.

### c) Systém doporučení a modelování situací

- Systém na základě pravidelně prováděných auditů navrhuje proaktivní zásahy administrátorům. Tím je například myšlena identifikace přístupových

práv, které se aktivně nevyužívají po nastavitelnou dobu např. 180 dní. Systém proaktivně připravuje odebrání těchto změn, aby administrátoři pouze potvrdili jejich odebrání.
- Systém umožnuje administrátorům modelovat stavy nastavení oprávnění bez vlivu na skutečná práva spravovaných systémů. „tzv. sandbox“
- Systém umožnuje správu veškerých oprávnění včetně správy samotného Active Directory.
- Systém umožnuje po omezenou dobu vrácení dané změny přístupových oprávnění pro případ opravy špatného nastavení.

**d) Centrální správa systému**

- Systém umožnuje komplexní správu v heterogenním prostředí prostřednictvím jednoho jednotného dedikovaného GUI.
- Centrální hlášení anomálií chování uživatele.
- Systémové hlášení pro administrátory.
- Libovolné nastavení systému hlášení, různým skupinám, uživatelům, složkám
- Systém přehledů a sestav pro management, administrátory a bezpečnostní administrátory
- Možnost vytváření šablon přehledů a sestav.
- Export vyhledávaných a filtrovaných dat
- Auditovaní AD
- Vysoce škálovatelné prostředí
- Výsledky klasifikace jsou zobrazeny v centrálním managementu přímo u daných složek, tak aby na první pohled bylo zřejmé, jaké data konkrétní složka obsahuje.
- Centrální management disponuje možností rozdělení oprávnění pro samotné administrátory či jednotlivé role v rámci organizace. Např.: Administrátoři, auditoři, helpdesk, Data Protection Officer, Security IT atp.

**e) Identifikace vlastníků informací**

- Systém navrhuje potencionální vlastníky složek/dat, a to na základě četnosti práce se samotnými daty.
- Systém umožňuje nastavení vlastníků/garantů pro jednotlivé složky. Tyto vlastníci jsou vedeni pouze v bezpečnostním softwaru a nemají žádný dopad na vlastnictví složek z pohledu základního systému např.: Microsoft File System.
- Složky či zdroje umožňují více vlastníků
- Systém umožňuje automaticky rozesílat auditní záznamy a reporty vlastníkům/garantům dat. (běžní uživatelé)
- Systém umožňuje automatické rozesílání reportů na jednotlivé vlastníky. Tím je myšleno, že systém vyhledá nad zdroji jednotlivé vlastníky, následně vygeneruje jednotlivé reporty a ty jim rozešle. Z pohledu administrace se

jedná o nastavení jednoho reportu, který bude automaticky distribuován na jednotlivé vlastníky.

**f) Klasifikace informací**

- Systém umožňuje automaticky klasifikovat nestrukturovaná data skrze regulární výrazy
- Systém umožňuje validaci těchto nálezů skrze matematický algoritmus např.: české rodné číslo identifikuje skrze regulární výraz. Po shodě formátu čísla provede jeho ověření skrze matematickou funkci. Tímto je zamezeno identifikování falešných rodných čísel a systém maximálně identifikuje osobní údaje.
- Systém umožňuje kategorizaci dat na základě jejich metadat, např.: identifikace dat dle jejich formátu *.pdf, *.doc, *.cad a veškeré multimediální soubory.
- Systém na základě klasifikování metadat umožňuje klasifikování souborů, které jsou starší než např.: 180 dní a mají velikost větší než xx a žádný uživatel s nimi nepracuje.
- Systém umožňuje nastavení na citlivá a necitlivá klasifikační pravidla z důvodu nezkreslování výsledných reportů při klasifikaci multimediálních a starých souborů.
- Systém umožňuje sledovat a vyhodnocovat nesrovnalosti s politikami řízení přístupu k elektronickým informacím dle jejich klasifikace. Tím je myšleno např.: Pokud jsou klasifikována personální data zaměstnanců, systém upozorňuje na nakládání s těmito daty pracovníky, kteří nejsou z personálního oddělení. Toto tzv. křížení rolí je možné individuálně nastavovat.
- Možnost hledání klíčových slov a frází v elektronických dokumentech.
- Možnost vytvářet vlastní slovníky, které budou použity při klasifikování dat.
- Systém umožňuje vyhledání regulárního výrazu s kombinací klíčových slov, kde umožňuje nastavení vzdálenosti klíčového slova od regulárního výrazu např.: 5-10 slov, včetně jeho umístění před, za či z obou stran regulárního výrazu.
- Systém umožňuje nastavení negativních klíčových slov
- Systém umožňuje nastavení výjimek k regulárním výrazům
- Jedno centrální rozhraní.

**g) Alertování událostí v „reálném čase“ a případná integrace se SW třetích stran**

- Alerty umožňují reakci na veškeré zalogované události, veškeré změny přístupových oprávnění včetně práce s klasifikovanými dokumenty.
- Alertní systém může být integrovatelný s produkty třetích stran např. SIEM.
- Alertní systém umožňuje vykonat akce:
  - Zaslání emailu

    - SYSLOG message
    - Event Log
    - SNMP Trap
    - Spuštění aplikace nebo skriptu
- Systém má definovatelnou strukturu výše uvedených akcí
- Systém již obsahuje předdefinovaná základní pravidla
    - Identifikace generických hrozeb typu RANSOMWARE
    - Vykopírovaní klasifikovaných dat
    - Vytváření administrátorských účtů
- Systém je přístupný skrze webový přístup k vyhodnocování jednotlivých alertů a anomálií, tzv. Dashboard.

**h) Webové rozhraní pro řízení přístupových práv samotnými uživateli**

- Systém umožňuje uživatelům přístup do webového rozhraní, kde mohou řídit svá přístupová práva
- Systém umožňuje přístup do webového portálu s ověřením vůči LDAP – Microsoft Active Directory
- Systém umožňuje řídit práva na Microsoft File Systemech a Microsoft AD skupinách
- Systém umožňuje výběr složek, které budou řiditelné tímto rozhraním
- Systém umožňuje rozdělení uživatelů do min. 3 rolí:
    - **Běžný uživatel**
      Umožňuje pouze viditelnost vybraných složek, žádost o práva na tyto složky, přehled vlastních žádostí daného uživatele
    - **Autorizující osoba**
      Je osoba nad konkrétní složkou, která může schválit konkrétní žádost běžného uživatele, musí mít přehled o všech žádostech
    - **Vlastník/garant dat**
      Systém vlastníkovi dat umožňuje plné řízení přístupových práv, schvalování žádostí, přehled o aktuálních přístupových právech, kompletní zobrazení veškerých událostí s daty, dále umožňuje revize přístupových práv, kde systém sám navrhuje odebrání přístupových práv při jejich nepoužívání např. 90 dní.

- Systém umožňuje generování reportu o tom, kdo neudělal revize nad vlastněnými složkami
- Systém veškeré žádosti zasílá v el. podobě formou emailu
- Systém loguje veškeré žádosti včetně jejich schválení či zamítnutí
- Webové rozhraní může být provozované na HTTPS
- Webové rozhraní pro koncové uživatele je k dispozici v českém a anglickém jazyce

**i) Bezpečné a relevantní prohledávání souborových serverů Windows a MS SharePointů**

- Systém umí vyhledávat přesné a relevantní výsledky založené na uživatelských přístupech a metadatech
- Systém má jednoduché webové rozhraní

- Výsledky vyhledávání systém umí vyřazovat na základě doporučení metadat samotných dokumentů a pravidel klasifikace dat tzn. například vyloučit citlivá data z vyhledávání
- Efektivní indexování na základě přírůstkového skenování
- Rozsah indexování podle aktivity na příslušných datech, přírůstková indexace
- Systém funguje na stávající infrastruktuře bez potřeby dalších investic

## II. Detailní parametry modulů Varonis

### Logované typy událostí v AD

| Parametr | Požadovaná hodnota |
|---|---|
| Podporované události v rámci Active Directory | Vytvoření a vymazání všech objektů |
| | Změny v členství ve skupině |
| | Změny vlastností objektu v AD pro všechny vlastníky. |
| | Vyresetování hesla |
| | Uzamknou/odemknout účet |
| | Žádost o přístup |
| | Vytvoření/smazání účtu |
| | Autentifikace ověření účtu |
| | Povolit/zakázat účet |
| | Změny členství ve skupinách |
| | Změna nastavení GPO |
| | Vytvoření odkazu na GPO |
| | Změna odkazu na GPO |
| | Smazání odkazu na GPO |
| | Přidání oprávnění na objekt v AD |
| | Odebrání oprávnění na objekt v AD |
| | Změna vlastníka objektu v AD |
| Typy objektů, které jsou auditovány | Počítač |
| | Kontakt |
| | Kontejner |
| | Doména |
| | Ostatní objekty |
| | Exchange - dynamické distribuční seznam |
| | Zabezpečení cizího objektu |
| | Skupina |
| | Politika skupiny |
| | Organizační jednotka |
| | Tiskárna |
| | Sdílená složka |
| | Uživatel |

**Logované typy událostí pro MS SharePoint Server**

| Parametr | Požadovaná hodnota |
|---|---|
| Možnosti auditu MS SharePoint 2010, 2013, 2016 | Vytvoření souboru |
| | Smazání souboru |
| | Otevření souboru |
| | Přejmenování souboru |
| | Změna souboru |
| | Změna oprávnění, auditování a vlastníka souboru |
| | Vytvoření složky |
| | Smazání složky |
| | Přejmenování složky |
| | Vytvoření „site“ |
| | Změna oprávnění, auditování a vlastníka složky |
| | Nastavení role |
| | Vytvoření seznamu |
| | Smazání seznamu |
| | Vytvoření položky seznamu |
| | Smazání položky seznamu |
| | Otevření položky seznamu |
| | Přejmenování položky seznamu |
| | Změna oprávnění, auditování a vlastníka položky seznamu |
| | Změna položky seznamu |
| | Změna oprávnění, auditování a vlastníka seznamu |
| | Přejmenování „website“ |
| | Smazání „website“ |
| | Změna oprávnění, auditování a vlastníka seznamu „website“ |
| | Vytvoření přílohy |
| | Smazání přílohy |
| | Otevření přílohy |
| | Změna oprávnění, auditování a vlastníka seznamu knihovny |
| | Vytvoření knihovny |
| | Smazání knihovny |
| Možnosti auditu MS SharePoint Online a OneDrive | Vytvoření souboru |
| | Úprava/změna souboru |
| | Otevření souboru |
| | Smazání souboru |
| | Přejmenování souboru |
| | Smazání složky |
| | Přejmenování složky |
| | Smazání položky seznamu |

**Logované typy událostí pro MS Exchange Server**

| Parametr | Požadovaná hodnota |
|---|---|
| Podporované události v rámci MS Exchange Server | Otevřít složku |
| | Vytvořit adresář |
| | Smazat adresář |
| | Přejmenovat adresář |
| | Přidat oprávnění adresáře |
| | Odstranit oprávnění adresáře |
| | Změnit oprávnění adresáře |
| | Přesunout adresář |
| | Vyprázdnit adresář |
| | Kopírovat adresář |
| | Označit vše jako přečtené |
| | Otevření zprávy |
| | Odeslání zprávy |
| | Odeslání zprávy (jménem XY) |
| | Odeslání zprávy (jako XY) |
| | Přijetí zprávy (do schránky) |
| | Editace zprávy |
| | Smazání zprávy |
| | Kopírování zprávy |
| | Přesunutí zprávy |
| | Vytvoření zprávy |
| | Označení zprávy jako nepřečtená |
| | Označení zprávy jako přečtená |
| | Přihlášení |

**Logované typy událostí pro MS File Server (CIFS)**

| Parametr | Požadovaná hodnota |
|---|---|
| MS Windows 2000 a vyšší (2012 R2 NTFS i ReFS) | Vytvoření souboru |
| | Smazání souboru |
| | Otevření souboru |
| | Přejmenování souboru |
| | Změna souboru |
| | Nastavení oprávnění souboru |
| | Změna vlastníka souboru |
| | Přidat oprávnění k souboru |
| | Odebrat oprávnění k souboru |
| | Přidání ochrany souboru |
| | Odebrání ochrany souboru |
| | Vytvoření adresáře |
| | Smazání adresáře |
| | Přejmenování adresáře |
| | Nastavení oprávnění adresáře |
| | Změna vlastníka adresáře |
| | Přidat oprávnění adresáře |
| | Odebrat oprávnění adresáře |
| | Přidání ochrany adresáře |
| | Odebrání ochrany adresáře |
| Události odmítnutí přístupu | Smazání souboru |
| | Otevření souboru |
| | Smazání adresáře |
| | Otevření adresáře |
| | Změna oprávnění, auditování a vlastníka souboru |
| | Změna oprávnění, auditování a vlastníka adresáře |