

► KASPERSKY SECURITY FOR STORAGE

Výkonná ochrana pro úložiště EMC a NetApp

ÚVOD

Smrtící malware se může v organizaci šířit děsivou rychlostí a zneužívat vzájemné propojení moderních sítí. Při stále narůstající škále hrozeb může jediný nakažený soubor omylem nahraný do úložiště vystavit bezprostřednímu riziku všechny síťové uzly.

Aplikace Kaspersky Security for Storage poskytuje robustní, výkonnou a škálovatelnou ochranu cenným a citlivým firemním datům nahraným do systémů úložišť EMC™ VNX™ a NetApp.

- Ochrana proti malwaru v reálném čase
- Ochrana pro systémy EMC VNX a NetApp
- Podporuje speciální úlohy pro skenování důležitých oblastí systému
- Flexibilní konfigurace skenování
- Škálovatelnost a odolnost proti poruchám
- Adaptabilní využívání systémových zdrojů
- Ochrana terminálových serverů
- Podpora clusterů serverů
- Certifikována jako kompatibilní s platformou VMware
- Obsahuje optimalizaci antivirového skenování iSwift a iChecker
- Správa konzole Kaspersky Security Center
- Hlášení o výkonu aplikace
- Podporuje správu sítě SNMP/MOM

NEJDŮLEŽITĚJŠÍ INFORMACE

VÝKONNÁ OCHRANA PROTI MALWARU V REÁLNÉM ČASE

Nepřetržitá aktivní ochrana pro řešení úložišť připojených k síti (NAS). Výkonná ochrana proti malwaru společnosti Kaspersky skenuje všechny spuštěné či upravované soubory, jestli neobsahují jakoukoliv formu malwaru včetně virů, červů a trojských koní. Pokročilá heuristická analýza identifikuje i nové a neznámé hrozby.

OPTIMALIZOVANÝ VÝKON

Výkonné skenování, nabízející optimalizovanou skenovací technologii a pružné nastavení výjimek, zajišťuje maximální ochranu a zároveň minimalizuje dopad na výkon systému.

SPOLEHLIVOST

Výjimečné odolnosti proti poruchám je dosaženo pomocí jednoduché architektury využívající jednotné komponenty navržené a sestavené tak, aby hladce spolupracovaly. Výsledkem je stabilní a odolné řešení, které v případě nuceného vypnutí provede automatický restart a zajistí spolehlivou nepřetržitou ochranu.

SNADNÁ SPRÁVA

Servery se instalují vzdáleně a jsou chráněné ihned bez potřeby restartu. Spravovány jsou společně prostřednictvím jednoduché a intuitivní centrální konzole – Kaspersky Security Center – společně s dalšími řešeními zabezpečení společnosti Kaspersky.

FUNKCE

NEPŘETRŽITÉ AKTIVNÍ ZABEZPEČENÍ

Špičkový engine pro skenování malwaru společnosti Kaspersky, sestavený odborníky na získávání informací o hrozbách z celého světa, poskytuje aktivní ochranu proti vznikajícím a potenciálním hrozbám prostřednictvím inteligentních technologií pokročilé detekce.

AUTOMATICKÉ AKTUALIZACE

Antimalwarové databáze se aktualizují automaticky bez narušení skenování, čímž se zajišťuje nepřetržitá ochrana a minimalizuje pracovní zátěž správce.

VYJMUTÉ PROCESY A DŮVĚRYHODNÉ ZÓNY

Skenovací výkon lze vyladit vytvořením důvěryhodných zón, které lze spolu s definovanými formáty souborů a procesy (jako například zálohování dat) ze skenování vyjmout.

SKENOVÁNÍ OBJEKTŮ AUTOMATICKÉHO SPUŠTĚNÍ

Za účelem zvýšení ochrany serveru lze skenovat soubory automatického spuštění a operačního systému, aby se malware nemohl aktivovat při spuštění systému.

SPRÁVA

CENTRALIZOVANÁ INSTALACE A SPRÁVA

Vzdálená instalace, konfigurace a správa včetně upozornění, aktualizací a flexibilních hlášení se ovládají prostřednictvím intuitivní konzole Kaspersky Security Center. V případě potřeby je dostupná i správa z příkazového řádku.

KONTROLA NAD OPRÁVNĚNÍMI SPRÁVCŮ

Každému správci serveru lze přiřadit různé úrovně oprávnění, což umožňuje soulad se specifickými firemními zásadami zabezpečení IT.

SYSTÉMOVÉ POŽADAVKY

HARDWARE:

- systémy x86 v konfiguracích s jedním nebo více procesory,
- systémy x86-64 v konfiguracích s jedním nebo více procesory.

MÍSTO NA DISKU:

- k instalaci všech komponent aplikace: 70 MB,
- k ukládání objektů do karantény a jejich zálohování: 400 MB (doporučeno),
- k ukládání protokolů: 1 GB (doporučeno),
- k ukládání databází: 2 GB (doporučeno).

MINIMÁLNÍ KONFIGURACE:

- procesor – 1 jádro; rychlost 1,4 GHz,
- RAM: 1 GB,
- 4 GB místa na pevném disku.

DOPORUČENÁ KONFIGURACE:

- procesor – 4 jádra; rychlost 2,4 GHz,
- RAM: 2 GB,
- 4 GB místa na pevném disku.

FLEXIBILNÍ SKENOVÁNÍ UMOŽŇUJÍCÍ OPTIMALIZOVANÝ VÝKON

Zkracuje dobu skenování a konfigurace a posiluje vyrovnávání zatížení, čímž pomáhá optimalizovat výkon serveru. Správce může určit a řídit hloubku, šířku a načasování skenování a definovat, které typy souborů a oblasti je nutné skenovat. Skenování na vyžádání lze naplánovat na období nízké aktivity serveru.

CHRÁNÍ ŘEŠENÍ HSM A DAS

Podporuje režimy skenování offline zajišťující účinnou ochranu systémů HSM (Hierarchical Storage Management). Ochrana DAS (Direct Attached Storage) také podporuje využívání nízkonákladových řešení úložišť.

OCHRANA VIRTUÁLNÍCH SYSTÉMŮ A TERMINÁLOVÝCH SERVERŮ

Součástí flexibilního zabezpečení je ochrana virtuálních operačních systémů (hostů) ve virtuálních prostředích Hyper-V a VMware a terminálových infrastruktur Microsoft a Citrix.

FLEXIBILNÍ HLÁŠENÍ

Informace lze předávat prostřednictvím grafických hlášení nebo pomocí protokolů událostí systému Microsoft Windows® či konzole Kaspersky Security Center. Nástroje pro hledání a filtrování poskytují rychlý přístup k datům v objemných protokolech.

SOFTWARE:

- Microsoft Windows Server 2003 / 2003 R2 x86 / x64 Standard / Enterprise Edition,
- Microsoft Windows Server 2008 / 2008 R2 x86 / x64 Standard / Enterprise / Datacenter Edition,
- Microsoft Windows Server 2012 / 2012 R2 Essentials / Standard / Foundation / Datacenter,
- Microsoft Windows Hyper-V Server 2008 R2,
- Microsoft Windows Hyper-V Server 2012 / 2012 R2.

SERVERY:

- Microsoft Terminal Services s Windows 2003 Server,
- Microsoft Terminal Services s Windows 2008 Server,
- Microsoft Terminal Services s Windows 2012 / 2012 R2 Server,
- Citrix Presentation Server 4.0, 4.5,
- Citrix XenApp 4.5, 5.0, 6.0, 6.5,
- Citrix XenDesktop 7.0, 7.1, 7.5.

PLATFORMY ÚLOŽIŠŤ:

Úložiště souborů EMC Celerra / VNX:

- EMC DART 6.0.36 nebo novější,
- Celerra Antivirus Agent (CAVA) 4.5.2.3 nebo novější.

Požadavky na úložiště NetApp:

- Data ONTAP 7.x a Data ONTAP 8.x v režimu 7-mode,
- Data ONTAP 8.2.1 nebo novější v režimu cluster-mode.

