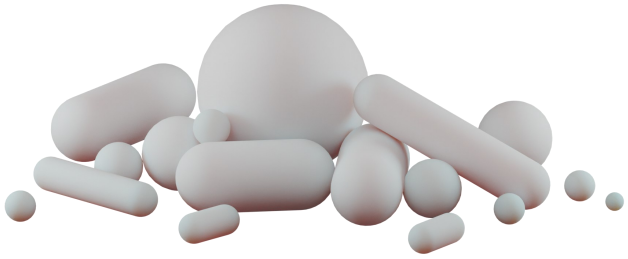
Logmanager

Strojová data jsou výzva

V dnešním přetechnizovaném světě jsou informace kritickým zdrojem umožňujícím správné rozhodnutí v pravý čas. V protikladu k tomu stojí fakt, že důležitá data jsou rozmístěna napříč celou organizací, ne vždy ve srozumitelném formátu a s rozdílnou dostupností. Sjednocení strojových dat z mnoha zdrojů, nastavení pevných pravidel při jejich správě, přeložení do lidsky čitelného formátu a jejich nezpochybnitelnost jsou proto klíčové požadavky pro efektivitu bezpečnostních i operativních činností každé firmy. Když se k tomu přidá přehledná interpretace v kompaktním a výkonném nástroji, detekční i analytické funkce, získá IT organizace nástroj pro realizaci správných rozhodnutí. A tímto nástrojem je český systém Logmanager.



Určení systému Logmanager

Logmanager je SEM/SIEM řešení pro centralizovanou správu logů a jiných strojových dat z libovolných zdrojů. Je založen na výkonné databázi s vhodně dimenzovanou kapacitou, rychlým vyhledáváním ve “velkých datech” a okamžitou vizualizací vyžádaných dat.

Jeho úkolem je sběr, nezpochybnitelné uložení a všestranná analýza strojových dat organizace. Umožňuje prohledávat agregovaná data v reálném čase, vytvářet analýzy, reporty i upozornění na události korelované z dat více zdrojů. Dokáže snadno obohacovat získaná data. Nedílnou součástí řešení Logmanager je taktéž podpora souladu s požadavky zákonných norem. Při správné implementaci pomůže organizaci k zajištění shody se Zákonem o kybernetické bezpečnosti, ČSN/ISO 27001:2013, nebo i nově připravovanou NIS2 EU Direktivou.

Logmanager však není určen pouze pro oddělení bezpečnosti IT.

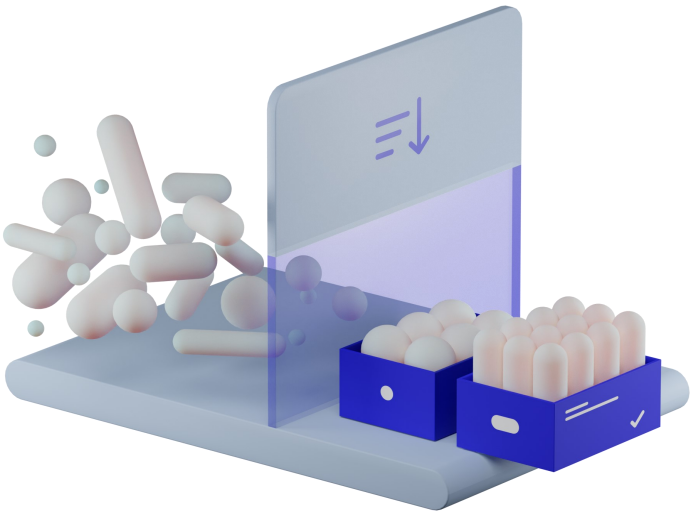
Při vývoji Logmanageru je kladen velký důraz na radikální jednoduchost užívání a jeho reálný přínos pro IT obecně. Logmanager na jednom místě shromáždí provozní i diagnostická data ze všech systémů firmy. Díky důsledné normalizaci dat lze v rámci jedné vizualizace snadno propojit data z různých zdrojů a získat tak potřebný nadhled. Operátor IT má možnost zjistit během několika sekund informace o provozních stavech i případných problémech, které by jinak musel komplikovaně vyhledávat v distribuovaných zdrojích. Díky rozšířené viditelnosti do prostředí Microsoft je i automaticky informován o podezřelých událostech a může tak předcházet bezpečnostním incidentům.

Podporovaná zařízení

Logmanager nativně podporuje více než 135 zdrojů ze všech oblastí IT, od bezpečnostních řešení, přes sítě, virtualizace, operační systémy, databáze, až po cloud aplikace. Seznam zdrojů se každou novou aktualizací rozšiřuje. Logmanager podporuje i standardizované strukturované formáty logů jako jsou CEF, LEEF, RFC5424 a JSON. Pro unikátní zdroje dat umožňuje Logmanager rychlé a snadné vytvoření nové integrace.

Klíčové vlastnosti

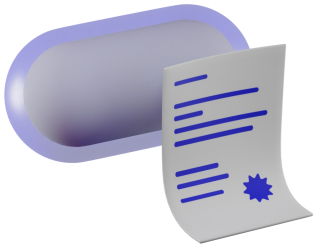
- ⇒ Centrální úložiště strojových dat organizace a jejich analýza
- ⇒ Sjednocení formátu libovolných dat do definované struktury
- ⇒ Zpracování, vizualizace i upozornění v reálném čase
- ⇒ Rychlé prohledávání dat bez nutnosti znalosti SQL jazyka
- ⇒ SIEM/XDR funkce, upozornění s limity a korelacemi
- ⇒ Unikátní grafické konfigurační a programovací rozhraní
- ⇒ Radikální jednoduchost a uživatelská přívětivost
- ⇒ Snadné vytváření reportů a auditních zpráv za běhu
- ⇒ Umožní snadnější splnění požadavku na shodu s regulacemi:
  - Připravovaná NIS2 EU Direktiva
  - Zákon o kybernetické bezpečnosti a návazné vyhlášky
  - ČSN/ISO 27001:2013 pro pořizování auditních záznamů
  - GDPR
- ⇒ Bez licenčních omezení na zdroje, výkon i uložená data
- ⇒ Úspora na poplatcích při napojení na externí SOC



Radikální jednoduchost a výkon

- ⇒ Trvalé zpracování více než 25 000 událostí za sekundu*
- ⇒ Řešení „vše v jednom“ - Server, OS, Databáze i Aplikace
- ⇒ Odolné diskové úložiště pro až 320 TB logů *
- ⇒ Možnost horizontálního i vertikálního škálování
- ⇒ Podpora velkého množství zdrojových zařízení, OS a aplikací
- ⇒ Centrálně řízený klient pro sběr logů z MS Windows
- ⇒ Integrované rozšíření bezpečnostních událostí v prostředí MS
- ⇒ Snadná integrace s externím SOC nebo SIEM/EUBA systémy
- ⇒ Rychlé nasazení a snadné zaškolení pro běžné operace
- ⇒ Rozhraní i kompletní dokumentace v českém jazyce
- ⇒ Rozsáhlá síť spolehlivých a technicky zdatných partnerů
- ⇒ Přímá technická podpora výrobcem a možnost testování zdarma

**hodnoty clusteru*



Typické uživatelské případy

Shoda s předpisy

Potřebujete vzhledem ke svému působení centrální systém pro správu, analýzu a dlouhodobé uložení auditních i provozních dat. Požadujete cenově efektivní řešení bez licenčních omezení, které naplní „tickboxy“ ve Vašem auditním plánu a firemní bezpečnostní politice...

SIEM funkce i snadná integrace

Logmanager obsahuje SIEM funkce. Pokud se však v budoucnosti rozhodnete pro nasazení externího SOC, Logmanager to zjednoduší. Umožňuje snadno sdílet pouze vybraná data v mnoha formátech s produkty třetích stran. Šetří na licenčních poplatcích za nástroje nebo služby a zjednodušuje jejich integraci...

Pokročilá detekce

Díky implementaci rozšířené viditelnosti do událostí v prostředí Microsoft, Logmanager umožňuje získat více detailů, jednoznačně identifikovat podezřelé procesy a snadno provádět vyhodnocení. S těmito informacemi lze plánovat odpovědi a v případě potřeby provést i důkladnou forenzní analýzu...

Monitoring bezpečnosti

Chcete monitorovat bezpečnostní systémy, ale máte více platforem, ze kterých plánujete sjednotit logy a audity do jednoho formátu. Specializované řešení může být složité a má podporu pouze na dané výrobce...

Sledování konfiguračních změn

Kdo, kdy a s jakým výsledkem prováděl změny v nastavení aktivních prvků, operačních systémů a aplikací. Potřebujete vždy čerstvá auditní data a pravidelné reporty ve svém emailu...

Dohled nad SMB servery

Kdo kopíroval nebo mazal citlivá data ze souborových serverů? Chcete mít pod kontrolou operace na SMB serverech a vědět kdy, kdo a jaké operace s citlivými soubory prováděl...

Dohled nad přístupem k síti

Potřebujete dohledový systém pro řízení přístupu k drátové a bezdrátové síti s 802.1X. Chcete sloučit logy z ověřování v aktivních prvcích sítě, jednotného přihlášení v MS AD nebo RADIUS, logy z DHCP, FW...

Sledování operací v aplikacích

Potřebujete zpracovat libovolné aplikační logy? Kdo, kdy a s jakým výsledkem prováděl operace ve vašich aplikacích nebo jejich vnořených databázích...

Ochrana pořízených informací

Strojová data nelze mazat ani modifikovat. Obsahují důvěryhodné časové razítko, unikátní identifikátor, proto lze Logmanager použít jako platformu pro vytváření požadovaných důvěryhodných reportů...

Technická specifikace jednotlivých produktů Logmanager

Procesor	Paměť	Disky	Kapacita DB	Odhad retence EPS[3] - dní	Trvalé EPS[3]	Špičkové EPS[3]
Logmanager Appliance se software 3.9.x a výše (minimální hodnoty)						
Logmanager-XL na DELL nebo HPE serveru 2U výšky s integrovaným Workload Akcelerátorem[1]. (5 let NBD RMA, 1 nebo 5 let SW aktualizace, 1x LOGmanager-VF)						
2x16core HT/MT @3.2GHz	128GB	12 v RAID 6	120/160[2]TB	5000EPS - 440 (580[2]) dní	10000	20000/10min
Logmanager-L na DELL nebo HPE serveru 2U výšky. (5 let NBD RMA, 1 nebo 5 let SW aktualizace, 1x LOGmanager-VF)						
2x16core HT/MT @2.8GHz	128GB	12 v RAID 6	40/80[2]TB	3000EPS - 275 (550[2]) dní	5000 (6000[1])	10000/10min
Logmanager-M DELL nebo HPE server 1U výšky. (5 let NBD RMA, 1 nebo 5 let SW aktualizace, 1x LOGmanager-VF)						
1x16core HT/MT @3GHz	64GB	4 v RAID 5	12TB	1000EPS - 230dní	2000	4000/10min
Logmanager-Demo ve formátu MicroPC - pouze jako neprodukční box pro lab nebo na PoC. (3 roky NBD RMA, 3 roky SW aktualizace, 1x LOGmanager-VF)						
1x8core HT/MT @2.6GHz	32GB	1	490GB	250EPS - 30dní	500	1000/10min
Logmanager Forwarder (řešení pro bezpečný a spolehlivý sběr logů ze vzdálených poboček a z Internetu/DMZ)						
Logmanager-VF Virtuální forwarder s 8, 16 nebo 128GB diskového prostoru ve verzi pro HyperV a VMWARE. (1 rok SW aktualizace)						
2*vCPU	4GB vRAM	1 vDisk	8/16/128GB	N/A; pracuje pouze jako mezipaměť	9000	18000/10min
Logmanager-HF Fyzický forwarder ve formátu MicroPC. (3 roky NBD RMA, 1 rok SW aktualizace)						
1x8core HT/MT @2.6GHz	8GB	1	250GB	N/A; pracuje pouze jako mezipaměť	9000	18000/10min
Rozšíření a škálování (pro navýšení výkonu, úložné kapacity a vysokou dostupnost)						
Workload Akcelerátor[1] - Přídavný NVMe modul k akceleraci zpracování near-realtime operací - integrován v Logmanager-XL a volitelný pro Logmanager-L.						
DB rozšíření[2] - Volitelné rozšíření kapacity DB o dalších 40TB pro LOGmanager-L na 80TB a XL na 160TB. (nutno objednat s objednávkou Logmanager).						
Síťové rozšíření - Volitelné rozšíření síťového rozhraní o 2* nebo 4*SFP+ porty pro Logmanager-L a XL. Volitelně i vhodné SFP+ transceivery.						
Cluster - Lze vytvořit cluster ve vysoké dostupnosti až o 4 jednotkách. Každá další jednotka clusteru přidává 40% výkonu na zpracování a 80% výkonu prohledávání.						
Velikost databáze Clusteru - Velikost databáze clusteru je součtem kapacit všech členů clusteru děleno dvěma.						
Výkon v EPS[3] - očekávané množství události za sekundu na samostatný Logmanager, log mix s RAW velikostí logů průměrně 700Byte.						

Informace o výrobci a reference

Logmanager je vyvíjen od roku 2014 jako nosný produkt firmy Sirwisa a.s., která sídlí v Praze. Na stránkách www.logmanager.cz naleznete vybrané reference. Pro podrobnější list referencí přímo z oblasti Vaší činnosti nás neváhejte poptat. Příslušné kontakty na stávající zákazníky, kteří souhlasí s uváděním na referenčním listu, rádi předáme.