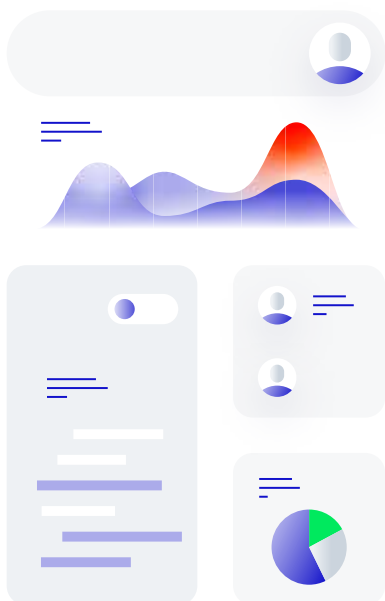


Datasheet



Logmanager je český nástroj pro správu logů obohacený o SIEM funkce, který výrazně zjednodušuje reakci na kybernetické hrozby, řešení problémů a zajištění souladu s předpisy.

Je dostupný buď jako hardwarové zařízení, nebo jako virtuální zařízení kompatibilní s platformami VMware a HyperV. Hardwarové požadavky pro virtuální zařízení jsou totožné se specifikací hardwarových modelů.

Podporované zdroje logů

Logmanager nativně podporuje více než 135 zdrojů dat napříč všemi IT nástroji, včetně bezpečnostních řešení, síťových prvků, virtualizací, operačních systémů, databází, cloudových aplikací a IoT zařízení. Tento rozsáhlý seznam se s každou aktualizací neustále rozšiřuje. Logmanager také podporuje standardizované strukturované formáty logů, jako jsou CEF, LEEF, RFP5424 a JSON. Pro starší zdroje umožňuje rychlou a snadnou tvorbu vlastních parserů.

Forwarder

Logmanager Forwarder je samostatné hardwarové nebo virtuální zařízení, které zajišťuje bezpečný a spolehlivý sběr logů ze vzdálených poboček a z Internetu/DMZ.

Logmanager hardwarová zařízení

Doporučené konfigurace pro virtuální zařízení

	Logmanager-XXL	Logmanager-XL	Logmanager-L	Logmanager-M	Logmanager-S	Logmanager Forwarder
Výkon v EPS ¹	10000	10000	5000	2000	1000	9000
Uchování dat ve dnech	~660-880	~440 - 660	~275 - 550	~230 - 460	~150	N/A; v režimu remote buffer
Úložiště	200 - 240 TB	120 - 160 TB	40 - 80 TB	12 - 24 TB	4TB	250GB
Operační paměť	128GB	128GB	128GB	64GB	64GB	8GB
RAID	RAID 6	RAID 6	RAID 6	RAID 5	RAID 1	N/A
Síťové karty	Dvě karty 2x10Gbps SFP+ redundantní, a 4x1Gbps RJ-45	Dvě karty 2x10Gbps SFP+ redundantní, a 4x1Gbps RJ-45	Jedna 2x10Gbps SFP+, a 4x1Gbps RJ-45	4x1Gbps RJ-45	4x1Gbps RJ-45	N/A
Hardwarové detaily	2U server, 2x PSU, Workload Accelerator, 5 let NBD RMA, obnova podpory po roce nebo 5-letá smlouva	2U server, 2x PSU, Workload Accelerator, 5 let NBD RMA, obnova podpory po roce nebo 5-letá smlouva	2U server, 2x PSU, 5y NBD RMA, obnova podpory po roce nebo 5-letá smlouva	1U server, 2x PSU, 5y NBD RMA, obnova podpory po roce nebo 5-letá smlouva	1U server, 1x PSU, 5y NBD RMA, obnova podpory po roce nebo 5-letá smlouva	MicroPC, 5y RMA, 4x 1Gbps SFP+ obnova podpory po roce nebo 5-letá smlouva

Volitelné doplňky a škálování

Cluster – Umožňuje vytvoření clusterů až do 4 jednotek, které podporují více než 10 000 EPS. Kapacita databáze clusteru se rovná součtu kapacit všech jednotek clusteru děleno dvěma.

¹ **Výkon v EPS** – Maximální udržitelný výkon měřený v událostech za sekundu (EPS) pro jednotku Logmanageru (Max Constant EPS). Směs surových logů s průměrnou velikostí 700 bajtů, testováno s plným parsováním. Peak EPS se rovná dvojnásobku Max Constant EPS po dobu 10 minut.

Licencování – Všechny verze zahrnují neomezený počet agentů, zdrojů a systémových uživatelů.