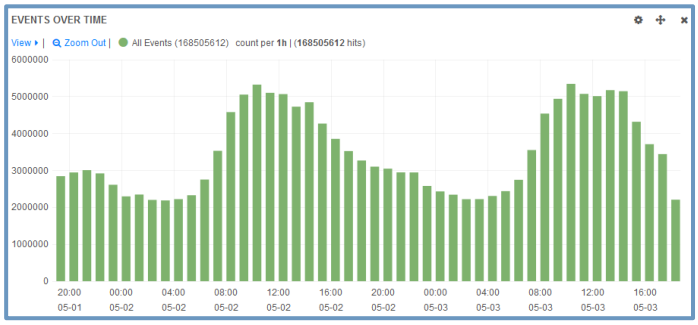
LOGmanager

> Central Log Repository
> Affordable SIEM

HELP TO RESOLVE CRITICAL IT INCIDENT

LOGmanager

In today's world driven by technologies, information becomes a critical resource for making the right decisions at the right time. This contrasts with the fact that vital information is scattered across devices and applications within the entire organization, often with varying levels of accessibility and in formats that may not be easy to understand. Consolidation of information from multiple sources, conversion into human intelligible form, setting up of fixed rules for handling of information and protection of its integrity are thus key for ensuring safety and efficiency of operational activities in every organization. When complemented with clear interpretation of the collected information through a compact and powerful tool, IT organizations acquire means for putting right decisions in practice. LOGmanager, a system developed in the Czech Republic, is such a tool.



LOGmanager description

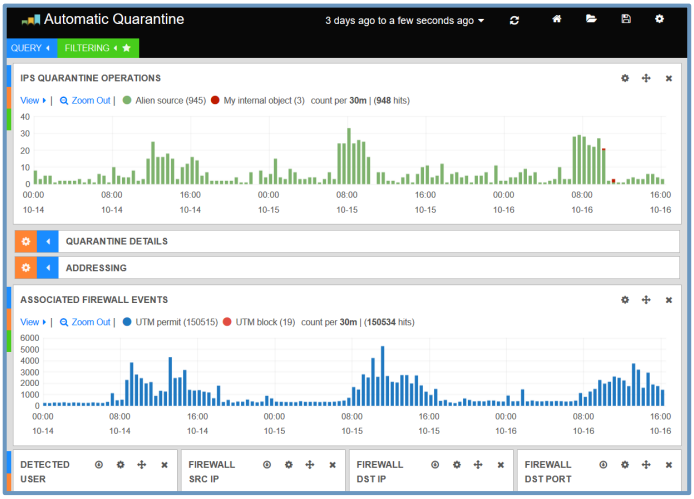
LOGmanager is an HW appliance for centralized management of logs and other machine data from any sources. It uses a powerful database with extremely large storage capacity and offers blazing fast searches on big data and instantaneous visualization of query results. It is a solution for collection, long-term storage with data integrity protection, and analysis of machine data. It allows organizations perform real-time searches on aggregated big data and generate statistical analyses, reports and alerts triggered by event data correlated from multiple sources. LOGmanager also facilitates regulatory compliance. When duly implemented, it can help organizations achieve compliance with ISO 27001:2013 on retention of audit trail records and also with the requirements of the GDPR or the Cyber Security Acts. LOGmanager is not designed exclusively for IT security departments and it is neither just a mandatory tool to meet regulatory requirements for their own sake. Great emphasis has been placed during its development on tangible benefits for the IT operations as such. LOGmanager greatly contributes to IT operations by aggregating operational data from all vital systems. IT administrators are thus able to retrieve within a few seconds information about operational statuses or potential defects for which they would otherwise have to search with big effort across distributed sources. They are also automatically informed about tracked events, which helps them prevent IT or security incidents.

Supported sources

LOGmanager natively supports more than 125 sources from all areas of IT including security solutions, networking, virtualization, operating systems, databases or cloud applications. The list is very extensive and it keeps growing with each update. LOGmanager also supports standardized structured log formats such as CEF, LEEF, RFP5424 or JSON. For legacy sources, it supports quick and easy creation of customized parsers.

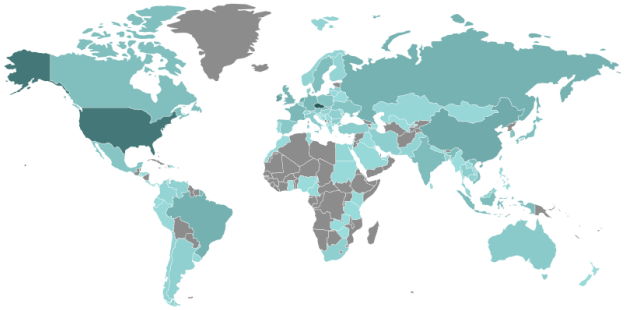
Key features

- Centralized repository for logs and machine data in an organization
- Consolidation of source log formats into human intelligible form
- Processing and visualization of incoming data in near real time
- Fast data searches without the need to learn SQL syntax
- Basic SIEM functionality. Alerts with thresholds and correlations
- Unique configuration and programming GUI
- Uncompromising ease of use and user-friendliness
- Easy creation of audit and other reports in real time
- Makes regulatory compliance easier including:
  - GDPR
  - The Cyber Security Act and related implementing legislation
  - ISO 27001:2013 on retention of audit trail records
  - PCI DSS 3.2
- No licensing restrictions on sources, performance, or stored data
- Streamlined integration with 3rd party SIEM/UBA products



Competitive advantages

- Ability to handle up to 13,000 EPS on a continuous basis
- Peak performance of up to 26,000 EPS for 10 minutes
- Appliance with embedded disk storage for up to 160 TB of logs
- Supports variety of source devices, operating systems and apps
- A centrally managed client for collection of Windows OS logs
- High-availability active-active cluster configuration
- Rapid deployment and easy training for standard operations
- Designed with specific requirements of CEE countries in mind
- No licensing equals no additional hidden costs for acquisition, operation and maintenance



Typical user cases

Compliance

Your business needs a centralized system for management, analysis, and long-term storage of audit and operational data. You require a cost-effective solution without licensing restrictions that would populate the "tickbox" in your audit plan and your corporate security policy...

Network access control

You plan to deploy a centralized solution for controlling access to wired and wireless networks and your IT operations need a monitoring system for 802.1X. You need to be able to aggregate authentication logs from active network elements, single sign-on via Active Directory, RADIUS server messages...

Monitoring file servers

Who copied or deleted sensitive data from file servers? You need to keep operations on file servers under control and you need to know what operations were performed, by whom and when. Your organization was affected by ransomware and you need targeted restoration of the files that had been encrypted. But you don't know what had been encrypted...

Security monitoring

You need to monitor security systems, but you are using multiple platforms and you need to consolidate the logs and audit records to a uniform format. A dedicated solution is too expensive and supports only selected vendors. LOGmanager processes and analyses logs from all sources with no restrictions...

Tracking configuration changes

Who, when, and with what result performed configuration changes to active elements, operating systems and applications. You need to have the latest audit data and reports in your email. You need to be able to know what a particular administrator modified six months ago across your IT infrastructure...

Features and integration

LOGmanager deliver basic SIEM features. If you later decide to deploy 3rd party analytics tool like SIEM or UBA, LOGmanager will still help. It allows selectively share structured data in many formats with third-party products. You save on license fees for these instruments and integration is easy...

Compliance verification

You need to verify whether the setup of the rules in your security systems is in accordance with your company policies...

Application access monitoring

Who, when, and with what result performed operations in your applications and databases...

Protection of information

Once machine data is stored in LOGmanager, it cannot be altered. Due to system design and certification (ISO 27001:2013), this solution is an ideal platform for creating reports and forensic analysis...

Technical specification of the LOGmanager appliances

CPU	Memory	Disk	RAID	DB Capacity	Data Retency (Average EPS[3]-days)	MAX Constant EPS[3]	Peak EPS[3]
LOGmanager appliance with software 3.6.0 and newer							
LOGmanager-XL based on DELL server 2U size, with natively integrated Workload Accelerator[1] (5 years NBD RMA, 1 or 5 year SW renewal, 1x LOGmanager-VF)							
2x16core Intel Xeon@2.9GHz	128GB	12*12TB	6	120TB	5000EPS - 440 (580[2])days	10000	20000/10min
LOGmanager-L based on DELL server 2U size. (5 years NBD RMA, 1 or 5 year SW renewal, 1x LOGmanager-VF)							
2x12core Intel Xeon@2.2GHz	128GB	12*4TB	6	40TB	3000EPS - 275 (550[2])days	5000 (6000[1])	10000/10min
LOGmanager-M based on DELL server 1U size. (3 years NBD RMA, 1 or 3 year SW renewal, 1x LOGmanager-VF)							
1x12core Intel Xeon@2.2GHz	64GB	4*4TB	5	12TB	1000EPS - 230days	2000	4000/10min
LOGmanager-S based on DELL Tower server. (3 years NBD RMA, 1 or 3 year SW renewal, 1x LOGmanager-VF)							
1x2core Intel G5500@3.8GHz	32GB	2*4TB	1	4TB	250EPS - 310days	500	1000/10min
LOGmanager-Demo based on Intel NUC platform - only as a nonproduction unit for LAB or PoC. (3 years RMA, 1 year SW renewal, 1x LOGmanager-VF)							
1x2core Intel i5@2.9GHz	16GB	1*500GB	N/A	490GB	250EPS - 30days	500	1000/10min
LOGmanager Forwarder appliance (solution for secure and reliable log colletion from remote branches and Internet/DMZ)							
LOGmanager-VF Virtual Forwarder with 8, 16 or 128GB disk space - virtual appliance for Hyper-V or VMWARE. (1 year SW renewal)							
2*vCPU	4GB	8/16/128GB vDisk	N/A	8/16/128GB	N/A; act as remote buffer	9000	18000/10min
LOGmanager-HF Physical Forwarder based on Intel NUC platform. (3 years RMA, 1 year SW renewal)							
1x2core Intel i3@2.6GHz	8GB	256GB	N/A	256GB	N/A; act as remote buffer	9000	18000/10min
Optional addons							
Workload Accelerator[1] - NVMe 6.4TB module to accelerate processing of near-realtime operations in LOGmanager-L and XL.							
DB extension[2] - Option to expand DB Capacity by another 40TB (LOGmanager-L to 80TB and XL to 160TB). Must be ordered with LOGmanager init. order.							
Network port extension - Option to extend the network ports with 4*SFP+ for LOGmanager-L and XL.							
Performance in EPS[3] - Events Per Second, RAW log mix with average size 700Byte; In an HA cluster, performance increases to 130% of single unit performance.							

About the manufacturer and customer references

LOGmanager has been developed since 2014 as a flagship product of Sirwisa a.s., a company based in Prague. You can find selected customer references at www.logmanager.com. Our customers include not only government authorities but also businesses of all sizes from all sectors, business corporations, banking organizations and more. Do not hesitate to contact us for more detailed customer references directly from your area of business. We will be happy to provide contacts to existing customers who have agreed to be included on our list of references .