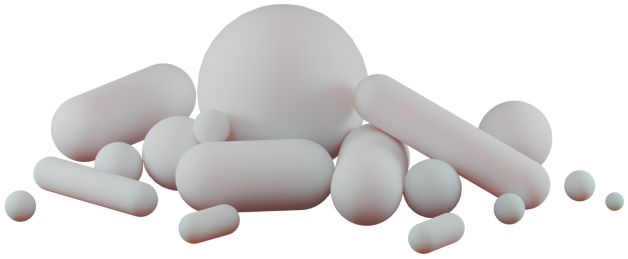
Logmanager

Machine data is a challenge

In today's over-technological world, information is a critical resource enabling the right decision at the right time. In contrast to this is the fact that important data is distributed across the entire organization, not always in an understandable format and with different availability. The unification of machine data from many sources, the setting rules for the data management, their translation into a human-readable format and their indisputability are therefore key requirements for the effectiveness of the security and operational activities of every company. When you add a clear interpretation in a compact and a powerful tool, detection and analysis functions, you have a tool for making the right decisions. And such tool is the Logmanager.



Logmanager description

Logmanager is a SEM/SIEM solution for centralized machine data management from any sources. It uses a powerful database with appropriately sized capacity, fast search in "big data" and immediate visualization of requested data. Its task is the collection, trusted storage and comprehensive analysis of the organization's machine data. Allows you to search aggregated data in real time, create analyses, reports and event alerts correlated from multi-sourced data. It can also easily enrich the obtained data. Logmanager also facilitates regulatory compliance. When implemented, it can help organizations to achieve compliance with various Cyber Security Acts or standards. However, Logmanager is not designed exclusively for IT security departments and it is neither just a mandatory tool to meet regulatory compliance for its own sake.

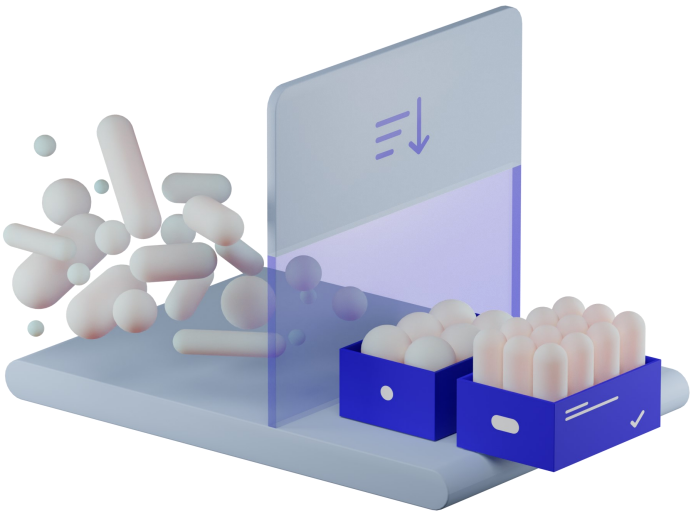
During the development of Logmanager, great emphasis is placed on the radical simplicity of use and its real contribution to IT in general. Logmanager collects operational and diagnostic data from all company systems in one place. Thanks to consistent data normalization, data from different sources can be easily connected within a single visualization pane and thus gain the necessary overview. The IT operator has the opportunity to find out in a few seconds information about operational statuses and possible problems, which he would otherwise have to search in distributed resources. Thanks to the increased visibility into the Microsoft environment is also automatically informed about suspicious events and can thus prevent security incidents.

Supported source

Logmanager natively supports more than 135 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

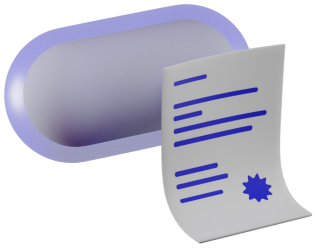
- ⇒ Centralized repository for logs and machine data
- ⇒ Consolidation of any log formats into human intelligible form
- ⇒ Processing and visualization of incoming data in near real time
- ⇒ Fast data searches without the need to learn SQL syntax
- ⇒ Many SIEM & Extended detection functionalities
- ⇒ 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:
  - NIS2 EU Directive
  - Country specific Cyber Security Acts and legislations
  - ISO 27001:2013 on retention of audit trail records
  - GDPR
- ⇒ Licensing restrictions not applied
- ⇒ Streamlined integration and license saving on SOC integration



Radical Simplicity and Performance

- ⇒ Ability to handle up to 25,000 EPS on a continuous basis*
- ⇒ All-in-one solution with minimal deployment effort
- ⇒ High-availability data storage for up to 320 TB of logs*
- ⇒ Supports variety of source devices, operating systems and apps
- ⇒ A centrally managed client for collection of Windows OS logs
- ⇒ Enhanced visibility into Microsoft events driven by Sysmon
- ⇒ 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

** cluster setup*



Typical use-cases

Compliance

Need a central system for machine data management, analysis and long-term storage of audit trails and operational data? You require a cost-effective solution without licensing restrictions that fill the "tick-box" in your audit and corporate security policy...

SIEM features and integration

Logmanager includes generic SIEM functions. However, if you decide to deploy an external SOC in the future, Logmanager makes it easy. Keep all data locally and share only security related. Save on license fees for 3rd party tools or SOC services and simplify integration...

Improve Microsoft security

By implementing extended visibility in the Microsoft environment, Logmanager allows you to get more details, clearly identify suspicious processes and investigate. Responses can be planned and a thorough forensic analysis can be performed...

Security monitoring

Need to look after all security systems, but your company is using various brands. A dedicated solution is expensive and supports only some platforms. Consolidate the logs and audit records to a uniform format...

Tracking config changes

Who, when and with what result did changes in the settings across company network, servers and applications. What happened a year ago or today, fresh audit data and regular reports in your email...

Monitoring file servers

Who read, copied or deleted sensitive data from file servers? From what computer, what IP address, and what was the true username? Keep operations on all the file servers under control...

Network access control

Do you deploy wired and wireless network access with 802.1X and need universal visibility. Merge authentication logs from network, MS AD or RADIUS, DHCP, FW and other related sources with radical simplicity...

Application access monitoring

Need to process any applications logs? Who, when, and with what result performed access and operations in your applications and databases. Logmanager can directly read those data and provide results in real-time...

Trusted store for any data

Need a platform for creating reliable datasets or reports and collected machine data must not be deleted or modified. Logmanager assign trusted time stamp, unique identifier, backup is digitally signed...

Technical specification of the Logmanager appliances

Logmanager appliance with software 3.9.x and newer (minimal values)						
CPU	Memory	Disks	DB Capacity	Data Retency (Average EPS[3]-days)	MAX Constant EPS[3]	Peak EPS[3]
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 HT/MT @3.2GHz	128GB	12 in RAID 6	120/160[2]TB	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)						
2x16core HT/MT @2.8GHz	128GB	12 in RAID 6	40/80[2]TB	3000EPS - 275 (550[2])days	5000 (6000[1])	10000/10min
Logmanager-M based on DELL server 1U size. (5 years NBD RMA, 1 or 5 year SW renewal, 1x Logmanager-VF)						
1x16core HT/MT @3GHz	64GB	4 in RAID 5	12TB	1000EPS - 230days	2000	4000/10min
Logmanager-Demo based on MicroPC platform - only as a nonproduction unit for LAB or PoC. (3 years RMA, 1 year SW renewal, 1x Logmanager-VF)						
1x8core HT/MT @2.6GHz	32GB	1	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	1 vDisk	8/16/128GB	N/A; act as remote buffer	9000	18000/10min
Logmanager-HF Physical Forwarder based on MicroPC platform. (3 years RMA, 1 year SW renewal)						
1x8core HT/MT @2.6GHz	8GB	1	250GB	N/A; act as remote buffer	9000	18000/10min
Optional addons and Scaling						
Workload Accelerator[1] - NVMe 6.4TB module to accelerate processing of near-realtime operations, optional in Logmanager-L and by-default embedded in 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 2 or 4*SFP+ for Logmanager-L and XL. Optional SFP+ transceivers available.						
Cluster - Logmanager allows creation of cluster up to 4 units. Each addition unit in cluster adds 40% processing and 80% search performance.						
DB Capacity in cluster - Cluster DB capacity equals sum of all cluster members capacity divided by two.						
Performance in EPS[3] - Events Per Second for standalone Logmanager unit. RAW log mix with average size 700Byte, tested with full parsing.						

About the manufacturer and customer references

Logmanager is 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. Do not hesitate to contact us for more detailed customer references directly from area of your business. We will be happy to provide contacts to existing customers who have agreed to be included on our list of references.