LOGmanager

> Central Log Repository
> Affordable SIEM

HELP TO RESOLVE CRITICAL IT INCIDENT

Why everyone needs log management?

In today's IT dependent age every organization heavily relies on its underlying IT infrastructure. As businesses grow, so its infrastructure — even a small organization can have webs comprised of hundreds of interconnected components: Servers, Applications, Databases, Endpoints, IoT devices etc. And each of those components can speak with us via machine data it produce - informing us about config changes, operational statuses, user activities, diagnostics and more. Having the right log data is vital for many important tasks like monitoring, diagnostics, audit, forensics, reporting, compliance with regulations. Everyone who would like to process log data needs to consider few **challenges**:

- ### Understand log data

There is no common agreement on how the machine data should look like. Dozen od competing standards and still, each vendor has its own approach. Even worse, each system update could bring changes to existing log format. All this makes manual log processing very hard. Adapting to different formats and its constant changes quickly is mandatory.

- ### Deletion and changes

New logs overwrite older, so they might not be there when you need them. And if security breach happens, it is guaranteed that attackers will cover their tracks by deleting them instantly.

- ### Regulations

Having log management solution is crucial for achieving compliance with various standards, regulations and country specific cyber-security related laws.

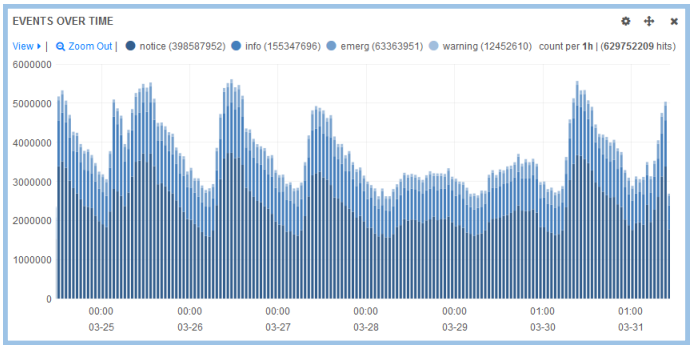
- ### No central search

Keeping logs on device which produces them, makes them much harder to track—thus making any incident remediation effort slower. And as everyone knows time = money .

Given above issues, it is clear that every organization needs a log management. Traditional log managements were specifically designed for large enterprise needs. Resulting in complex systems requiring hi-level skills and big teams. This, in combination with high price, forced mid and small-sized companies to use open-source solutions. But open-source is often hard to implement, maintain and work with, or lack critical functionalities. Modern log management system is the answer.

Log management contributes IT in all major areas

Without understanding machine data, there is always a gap. Log management is a widely accepted solution designed to fill this gap. And LOGmanager is made for small to mid-sized organizations, easy to use, maintain and implement. It is equipped with all critical log management functionalities. And with the best price/value ratio on the market due to embedded hardware and no-license policy.



Even the small log management deployment need to cope with large amount of data. Rapid processing and sufficient storage space is a "must have" to deal such big data.

Following text describes in detail each of log management problematic areas

IT Operations

A critical IT incident is the pivotal term in today's IT world; just like taxes or death, it cannot be evaded, because sooner or later it is inevitable. First of all, what is a critical IT incident – it is a situation whereby a business application or infrastructure linked to that application becomes non-functional. Such a situation calls for immediate response and the organization's IT team needs to be able to collaborate on a speedy removal of the defect according to the nature of the incident. In this context, two concepts are typically used – **MTTR** (Mean Time To Repair) and **RCA** (Root Cause Analysis). The role of the IT Department is to find the underlying cause as quickly as possible, eliminate it, and subsequently analyze the reasons of the outage including its context and determine corrective actions to prevent occurrence of an identical or similar issue in the future.

Format unification and centralization of logs. Distribution of logs across different systems and devices, different retention times and different language used in the logs can potentially cause issues. Every device takes a different approach to log management, records logs in a different machine language and uses different amount of internal storage to keep logs locally. This results in different retention periods, for which the logs are preserved. If you are looking for a particular record because you need to address an operational issue, you'll need to go through logs stored on different devices. Understand where to look for the information you need and keep searching. Makes sense to deploy a centralized log management system.

A centralized system such as LOGmanager conveniently collects logs from all devices and stores them in a single place. Furthermore, it uses parsers to translate the logs into a common format that is easy to understand and index all records to enable fast searching.

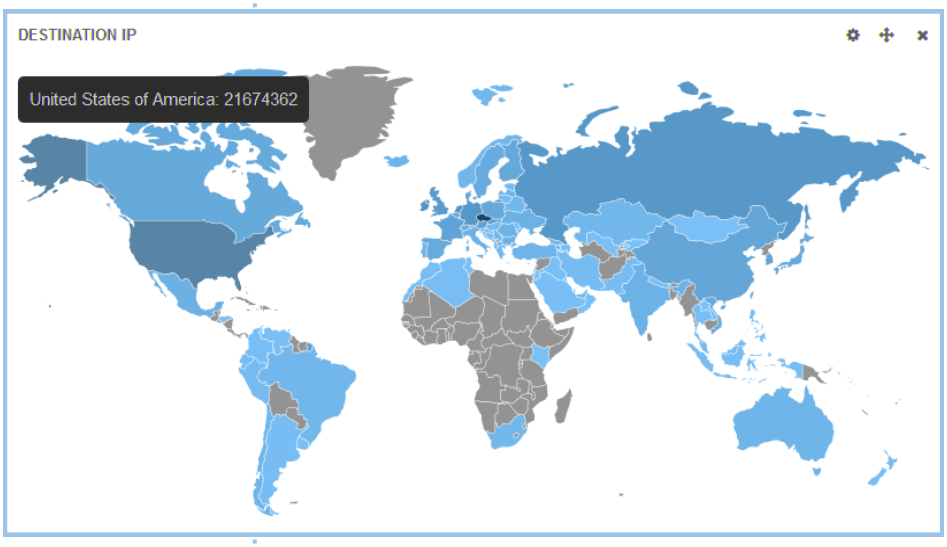
When you later need to deal with an operational issue, you have a single source of information to turn to - where you can review logs generated by infrastructure, security, servers and applications that became inaccessible, and you can identify the cause of the issues quickly and efficiently.

Fast data analysis thanks to centralized logs. Thanks to the centralization of logs in LOGmanager, IT operators can quickly analyze multiple sources of information without having to obtain administrator access to each of the systems. Logs stored in LOGmanager cannot be deleted or modified. Therefore, the technical staff without administrator privileges are able to review logs from most of the operational systems without needing to access the systems themselves. As part of their job, they can thus analyze routine operational issues and communicate requests for their resolution upstream in the IT hierarchy.

Security

The most significant benefits in the area of security are **the protection of logs against tampering** and the ability to proactively identify potential security risks, fine-tune configurations and track changes. Once a record is stored in LOGmanager, it cannot be deleted or modified. Organizations dealing with security issues often find out that the attacker deleted all records about malicious activity in the systems and devices to which he obtained unauthorized access. Therefore, it can be very difficult to get detailed data about the attacker's activities and make such information available for a thorough forensic analysis of the incident.

Let **actionable cyber threat data** interact with own machine data. Cyber threats are constantly evolving and having a right insight can ease prediction of cyber incidents and initiate a quick and focused response. LOGmanager uses its own Reputation database co-developed with Czech operator of national e-infrastructure for science, research, development and education - CESNET.



Proactive approach

Log management allows you to set up custom alerts which will detect single events, such as deletion of critical files. Modern ones should correlate multiple events allowing you to detect series of events and alert only while reaching defined threshold. Alerting will enable your organization to quickly respond to any issues as they appear. LOGmanager collects information about changes implemented in individual systems, which allows you to easily identify who made a change and what was the result. You can also monitor failed logon attempts to systems, in which sensitive data are stored, attempts to test security rules within the network, and so on.

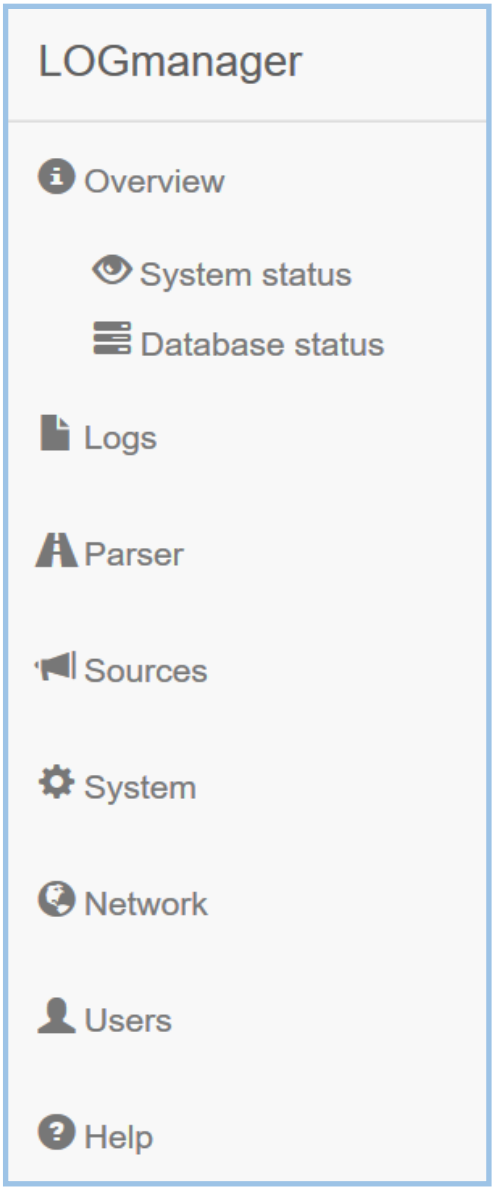
Compliance

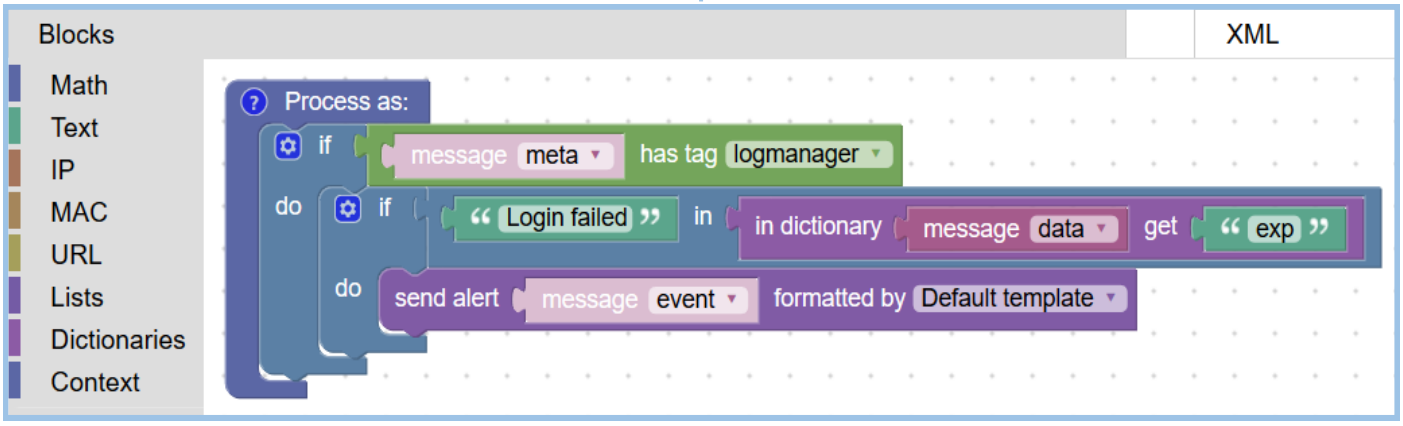
There are always many challenges in the area of regulatory compliance. Organizations are required to archive and analyze logs, capture activities, as well as long term store logs from critical systems and resources. **GDPR, NIST CSF, PCI-DSS, ISO 27001:2013, NISD 2016/1148/EU, HIPPA?** – it does not matter which regulatory compliance your company would like to achieve; proper log management is always part of solution.

Audit/Reports – When a security audit is performed in an organization, it is essential to have a system capable of generating reports based on the auditor's requirements. LOGmanager allows you to generate reports not only in a graphic form, but also in the CSV format with a structure according to the auditor's requirements. You can select any log stored in the database and include them in the report. You can even export a file with hundreds of thousands of lines, if needed. LOGmanager further supports the option to access the log database directly via REST-API and process database queries directly from your own reporting tool.

Radical Simplicity

Lack of resources can doom even the best projects. Log management should not exhaust your internal human resources. Typical log management values are quick implementation, short training cycle and simple integrated interface, which even a junior operator can handle.





LOGmanager unique feature is visual programming, allowing users to edit-write any code by using simplified graphical approach.

Frequently Asked Questions:

Log management or SIEM?

Many IT experts will claim that SIEM is “a must have” solution for each mid-size company. We found this claim partially false. Consider that SIEM focuses primarily on cyber security. If a company’s IT security team does not exist yet, or it is small, investing a big sum of money into the SIEM is counter-productive. While having limited man-days left to learn and handle complexity of SIEM product, it will be abandoned sooner or later anyway. Modern log management can substitute many SIEM functionalities with reduced cost and smaller effort. Starting with dynamic dashboards, embedded and custom alerting and correlations, security events reporting, actionable cyber threat data up to forensics. And if a company still considers SIEM, modern log management solution can be used as a major cost cutter.

Simply – log management in real-time collects/stores all logs but forward only security related logs to SIEM. Such approach increases overall functionality and reduces logs received by SIEM, thus made SIEM license cheaper.

What machine data do we need to collect?

The answer lies in the understanding of the main purpose of collecting machine data. A rule of thumb is that everything that has some value for the purpose of the collection, should be processed. There are three main purposes – operational, security and legal. The settings of each source systems need to be modified accordingly. This is a continuous activity because new systems are added and existing ones modified or removed on an ongoing basis. It is necessary to constantly monitor changes in the IT structures and incorporate also Logging and Audit items in the change management system. As far as the volume of data is concerned it is always better to collect as much information as possible and to collect the data in the highest level of detail. Filtering out irrelevant data is easy with LOGmanager. A comparison can be used: when you have a proper tool available, it will be easy to find a needle in a haystack; however, you will not be able to find it, if it has not been put in the haystack in the first place. Therefore, LOGmanager detailed documentation contains guides how to properly configure typical log source devices (including complex guide for Microsoft Audit policies).

How long should we keep machine data?

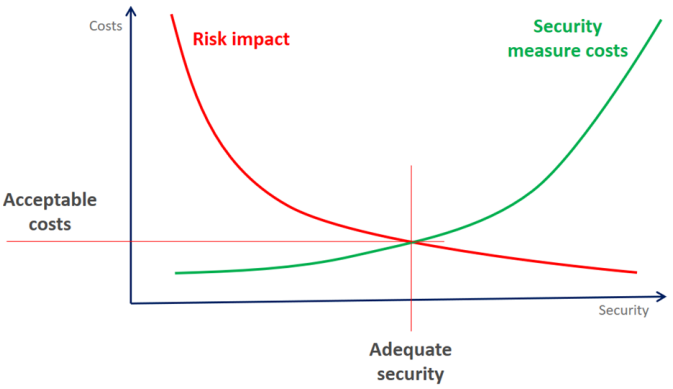
Here the answer is easy. LOGmanager provides more than sufficient, quickly accessible internal storage capacity. Such approach fulfills almost every regulation requirement or recognized advisory. Next to it, LOGmanager allows automated backup of the collected daily data on cheap external storage systems for virtually unlimited retention period.

Is it expensive?

Answer is relative of course, but generally LOGmanager is a system with **no hidden costs**. Most important—LOGmanager does not use any licensing model. It works up to the maximum hardware performance and even beyond (due to the unique buffering subsystem). The quoted price covers whole solution including optimized hardware from trusted vendor, as well as onsite HW replacement. Software upgrade and technical support for the first year is included in the price. The price for extended support period is set as low as 15% of the product’s purchase price.

How to consider right solution for us?

Evaluate. Have a test drive and try different solutions. If interested in LOGmanager - just contact our partner, request LOGmanager demo unit and run a proof of concept test in your environment. Consider the price/value ratio of the evaluated products as whole. Don’t forget the cost of the adequate hardware and storage, installation, training, hardware maintenance and software upgrade service.



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 .