LogSentinel's audit trail functionalities grant full control over your business-critical data. Data is stored securely on the blockchain and process owners are notified as soon as anomalous behaviour is detected to enable swift action. Powerful visualization capabilities provide real-time monitoring of all business activity, combined with advanced slicing and dicing functionality that enables state-of-the-art business intelligence.
Payment Provider

Transactions Protection

Payment providers perform transactions on users’ behalf, and operate in a highly regulated market. There are significant requirements for information security, personal and payment data protection, and forensics capabilities both under EU regulations (e.g. PSD2) and under national ones. Additionally, security certificates such as the PCI DSS or ISO 27001 require concrete measures for protection.

Secure audit trail

By LogSentinel

Transactions performed by the payment providers need to be protected from tampering by adversaries, internal or external so that customer accounts are protected. Access to customer accounts by employees should be logged in a way that cannot be deleted in order to avoid employees from misusing information about customers. Compliance with relevant regulations needs to be demonstrated such that access to sensitive payment and personal data is monitored, tracked and investigated. In addition to that, LogSentinel provides fraud detection capabilities that aid risk management for all tiers of payment providers.
Bank Customer

Account Protection

The business process of banks often include a large number of employees who have access to customer accounts. They can browse the accounts as well as initiate transactions, thus gaining access to personal and payment data, and increasing the possibility for fraudulent behavior. System administrators are able to modify or delete the logs of who performed what, thus obliterating clearing all traces of wrongdoing.

Secure audit trail

By LogSentinel

Viewing an account and initiating a transaction should be stored securely so that even high-privileged actors cannot tamper with the logs. Thus, in case of information security accident, the bank can do full forensic investigation, obtain valid digital evidence for legal proceedings, and use the logs for improving security measures in the future. In case a customer sues the bank, the bank can prove that their logs are authentic, rather than purposefully created to help them in the trial. We at LogSentinel work with several banks to provide increased customer and transaction protection. The fraud detection capabilities – both rule-based and AI-driven - can be used to send alerts when anomalous behavior is detected.
A company operates with personal data and has to comply with GDPR or other data privacy regulations. Employees need access to customers’ data through internal information systems to do their jobs in a wide variety of functions such as marketing, HR, and operations.

Each time an employee accesses customers’ personal data, a log needs to be stored. Then, if the log is secured, the company can prove to the competent authorities on GDPR that nobody has accessed data apart from what has been logged and the log cannot be modified. LogSentinel is used as a tool to boost GDPR compliance, including real-time monitoring of data access, as well as integrated register of data processing activities as per article 30 of the GDPR.
Government Registers

Fraud Protection

Governments support many registers, including commercial registers, property registers, citizen registers, car register, public procurement registers. Data in these registers need to be authoritative and protected from unauthorized modification and access. Whenever transactions of high material interest exist, there is the possibility for fraudulent behavior.

Secure audit trail

By LogSentinel

If all access and modification to the data in these registers is logged securely, then tampering with the data will not be possible, as it will be detected, including via a configurable fraud detection.

Additionally LogSentinel provides real-time monitoring of all system activities for both information security purposes and possible process optimization.
Governments work with a lot of personal data and accessing that data should be restricted in order to protect the rights and freedoms of individuals. However, many government registers are based simply on relational databases without further data protection safeguards.

Direct database access as well as API based access to systems that store personal data (e.g., citizen register) should be logged securely in a way that the ones accessing the data cannot cover their tracks. This can be used as a deterrent to data abusers. LogSentinel is deployed to service this scenario in the Bulgarian government. The fraud detection capabilities can be used to send alerts when anomalous behavior is detected. Such initiatives increase both information privacy and government accountability and transparency.
Many companies rely on sensors to record data about the operation of connected machinery. Sometimes that data is used to prove some quality of service of uptime to customers or third parties (insurance agencies, banks, government bodies, etc.).

Data from sensors can be manipulated after being collected to suit the needs of the collector. This can reduce trust and increase transaction costs between them and customers or third parties. If data is securely logged, however, any organization can prove that it has not tampered with after being collected, thus solving the issues of trust and increased costs.
Ensuring Transparency
With Every Single Log

Some organizations need to prove to their customers that they are operating in a way they claim to be. These include banks (that want to prove to high profile customers what employees had access to their accounts), governments (that want to prove to citizens that their data is not being misused), firms that want to demonstrate ethical data use, etc.

Secure audit trail
By LogSentinel

A secure audit trail with limited public access can be used to increase transparency – if each customer or citizen had access not only to their data, but also to how their data was accessed and modified historically, and done so in a way they can do an independent verification, trust will be significantly increased.
ISO27001 and PCI-DSS
Ensuring Compliance

Organizations certified under ISO27001 or PCI-DSS use these certificates to prove to their customers that they apply the highest standards for security. The standards cover many aspects of information security and cardholder data protection, including the way logs are stored and protected.

Secure audit trail
By LogSentinel

While many companies are tempted to ignore the requirement for secure logs in ISO 27001 and PCI-DSS these requirements are there – it is not sufficient to simply have logs; they have to be protected from tampering, otherwise they give a false sense of security. Companies that wish to be truly compliant with the standards need to protect their logs with a solution like LogSentinel that makes tampering impossible through its advanced blockchain verification mechanism. In addition to that standards require improved risk management and fraud detection capabilities which LogSentinel offers.
Online Tenders

Proof of Legitimacy

Large corporations and government institutions do procurement using online information systems. The tenders are often time-sensitive, and participants want proof that no offers have been modified before being officially opened.

Secure audit trail

By LogSentinel

If there is a secure log entry for each document that enters the system, then it’s easy for the organization doing the tender to prove to all participants that no offer has been altered and that the order of submissions is preserved.

LogSentinel provides both the proof for lack of modification as well as a secure time-stamping facility fully compliant with Regulation EU 910/2014.
In manufacturing, every product has a number of source materials and processes needed for producing it. Usually all the supply chain and manufacturing steps are recorded and later analyzed for the purpose of financial and quality control.

Provided that the steps and source materials have a digital footprint, these records can be stored securely so that the manufacturing data cannot be tampered with. Apart from decreasing fraud, this will greatly help the process of internal financial audit.
Voting on national elections is a complicated task, both technically and legally. However, voting occurs on many more occasions, in corporations, NGOs, political parties. Such votes sometimes need not be anonymous, but the main security problem remains – how to guarantee that the results are not modified.

If each vote is logged securely in a way that cannot be tampered with without detection, in addition to other safeguards, then the end results cannot be easily disputed. Logging can happen either on the server receiving the votes, or even on the client device. The full voting record is ultimately tamper-protected. LogSentinel is deployed for internal elections in non-government organizations to cover this use-case.
WordPress

Finding the Missing Traces

WordPress is the most widely used software package on the web. Many e-commerce sites, news sites, blogs rely on WordPress and its plugins. Yet, the traceability of “who did what” in the system is low and underdeveloped and this causes issues for WordPress deployments operated by multiple people.

Secure audit trail
By LogSentinel

Every event that occurs in a WordPress installation can be forwarded to LogSentinel in order to log staff behavior. The forwarded logs give a nice overview of the activities on the websites as well as legal safeguards in case of fraud. For example, logging the opt-in consent is a must-have in terms of GDPR. LogSentinel allows integrity of data from different sources, which will help you store information such as opt-in and opt-out all in one place.

LogSentinel has made it easier by supporting its own Wordpress plugin, which can be downloaded for free.
CCTV Recordings

Guaranteeing Authenticity

CCTV is everywhere, inside and outside buildings. They are used for property protection and law enforcement in case of crimes and disputes. However, guaranteeing the authenticity of the recordings is not a trivial task, especially if they are to be used in court proceedings.

Once a video is transferred from the camera to a central location, it can be hashed and logged, thus making it impossible to change without the change being detected.

In case of investigation, if the hash of the recording matches the one stored in the audit trail, it is guaranteed that the record has not been modified.

Secure audit trail

By LogSentinel
Every organization has internal documents that it relies on – procedures, contracts, offers, schedules, product blueprints, etc. Some of these documents are critical and should not be changed without a proper and well communicated reason. More importantly some of those documents contain commercial secrets that are key to the organization’s competitive advantage.

Each new document, as well as each modification to a new document, represent an audit trail entry. If these entries are securely logged, no document can be modified without detection, so only legitimate document modifications can be carried out. If proper measures are in place it can be hard to access the document without being detected thus making the compromise of commercial secrets less likely, and in case it happens – opens the ability of the organization to press criminal charges against the perpetrator. The fraud detection capabilities of LogSentinel will also give an early warning of possibly suspicious behaviour.
Many software applications rely on a number of secrets and private keys for connecting to databases, search engines and external services. These secrets are often kept unprotected in text files thus allowing anyone who has access to the file system to use the secrets and pretend to perform queries to the external system on behalf of the application.

Other solutions provide a way to track access to such secrets. However, the audit trail that is bundled with Vault or similar solutions is insufficient, as privileged users can still tamper with it. In these cases, LogSentinel can be integrated in the process and have all the logs forwarded to it in order to make it impossible to modify the logs.
Billing Registers

Fraud Protection and Integrity

Some organizations maintain registers of all their customer with billing and payment details (e.g. utilities).

Typically, fraud is performed by employees selling “erasure” from those registers for a price lower than the sum that is due.

Secure audit trail

By LogSentinel

Secure audit trail would make it impossible even for internal privileged actors to erase data from the billing registers without being detected – all modifications to the register will be stored in a tamper-evident way and not only serve as a deterrent, but also allow reconstructing the original contents of the register.
Leaking public or private classified information is a criminal offense, but detecting such leaks often takes time, if at all possible. Documents lie in folders that either do no track access, or the access log can be modified without leaving a trace.

If the access to classified documents is logged securely, in a way that the person intending to leak the documents cannot modify, then detecting the leak through fraud detection and forensic investigation can be simplified and done a lot faster, thus increasing the security of information and raising the possibility of criminal investigation to the offender.
Many online payment providers, banks and exchanges need to perform “Know your customer” checks in order to comply with money laundering regulations. These checks include querying multiple sources, including public registers. Proving the KYC checks were performed dutifully is sometimes hard after the fact, especially in case of actual money laundering.

KYC checks with external and internal sources represent business events each of which can be securely stored in a way that can be used to later prove that indeed all required checks were performed at the time of registration of the customer. Analysing data using customer-related logs is a common practice which shouldn’t be underestimated. The advanced LogSentinel reporting tool allows a detailed overview for each particular event type that leads to a certain customer behavior. Thanks to the integrated anomaly detection a lot of anomalies can be detected and further analysed for different purposes – from money laundering to preparing consumer score cards.
Medical Records

Fraud Protection and Integrity

Medical information systems hold electronic health records of patients that contain sensitive information about diseases and lab results. Both access and modification of medical records should be restricted; however, system administrators can circumvent these restrictions and potentially learn sensitive health details or modify health records and thus do harm to patients. Another possible problem is the unauthorized sale or resale of medical data to private companies engaged in clinical research or health marketing.

Secure audit trail

By LogSentinel

If all access and modifications to the data is logged securely, and all health records and their updates are logged as well, both the integrity and the privacy of the health records will be protected and the risk for the patients significantly reduced. This is also enhanced by LogSentinel’s significant fraud detection functionality.
Cloud Providers

(IaaS, PaaS)

Cloud providers that offer infrastructure or platform as a service in which customers can start or terminate hardware or software resources (virtual machines, application servers, storage, etc.). They do that via administrative panels or via APIs that control the infrastructure. These are usually part of the contracts and SLAs and performance can be contested by the customer in order to gain financial compensation.

Secure audit trail

By LogSentinel

In order to provide full visibility over the lifecycle of the infrastructure, all administrator actions that modify the infrastructure should be securely logged so that the said administrators cannot modify them, thus making it harder to compromise the infrastructure as well as proving to the customer that performance is as per agreement.
Contact Us Today!

Let us know about your business needs and we’ll be happy to scope a plan to protect your data ensuring the highest quality!

Talk to us at contact@logsentinel.com