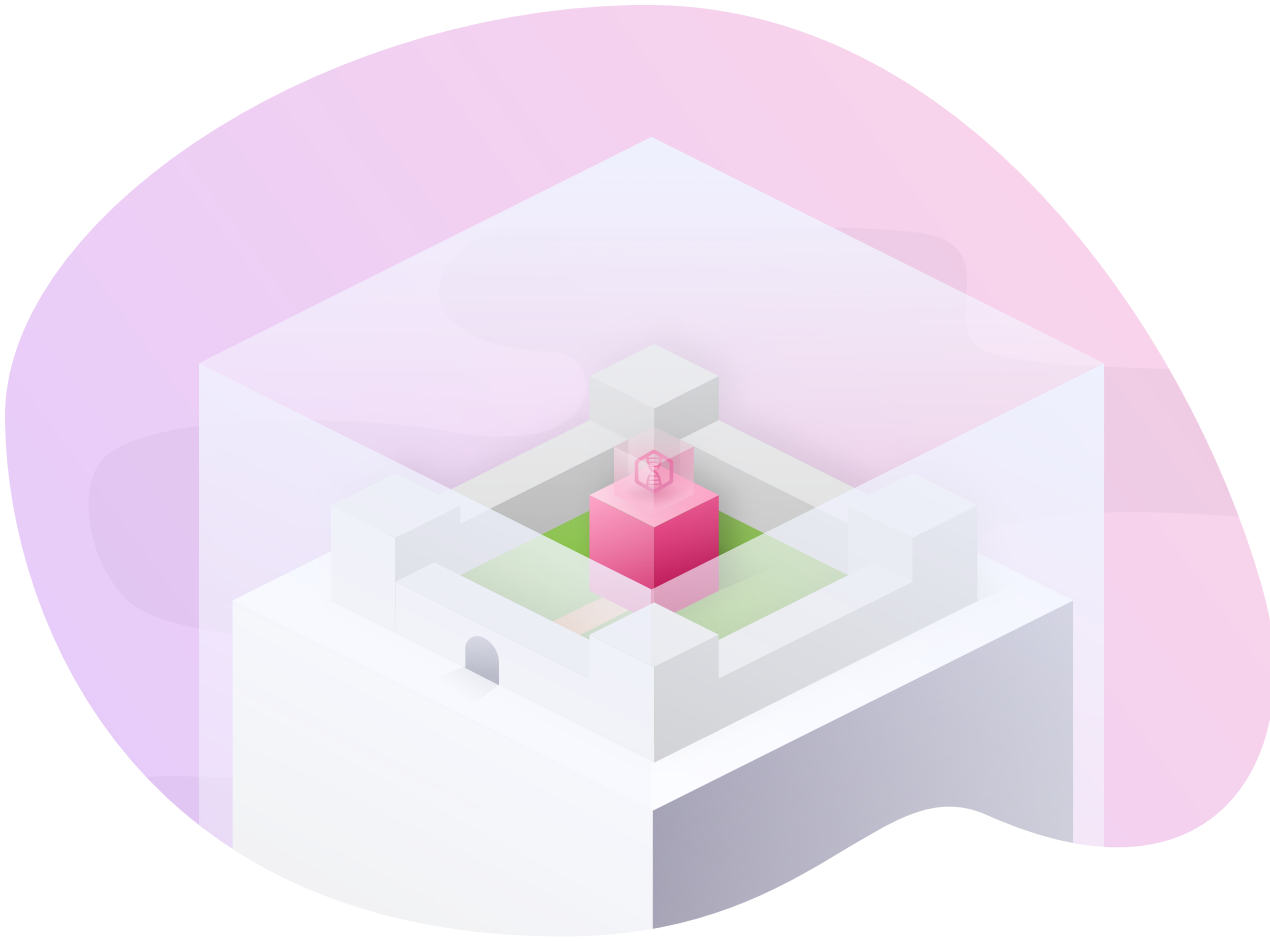
WHITEPAPER

Logging Platform Buyers Guide

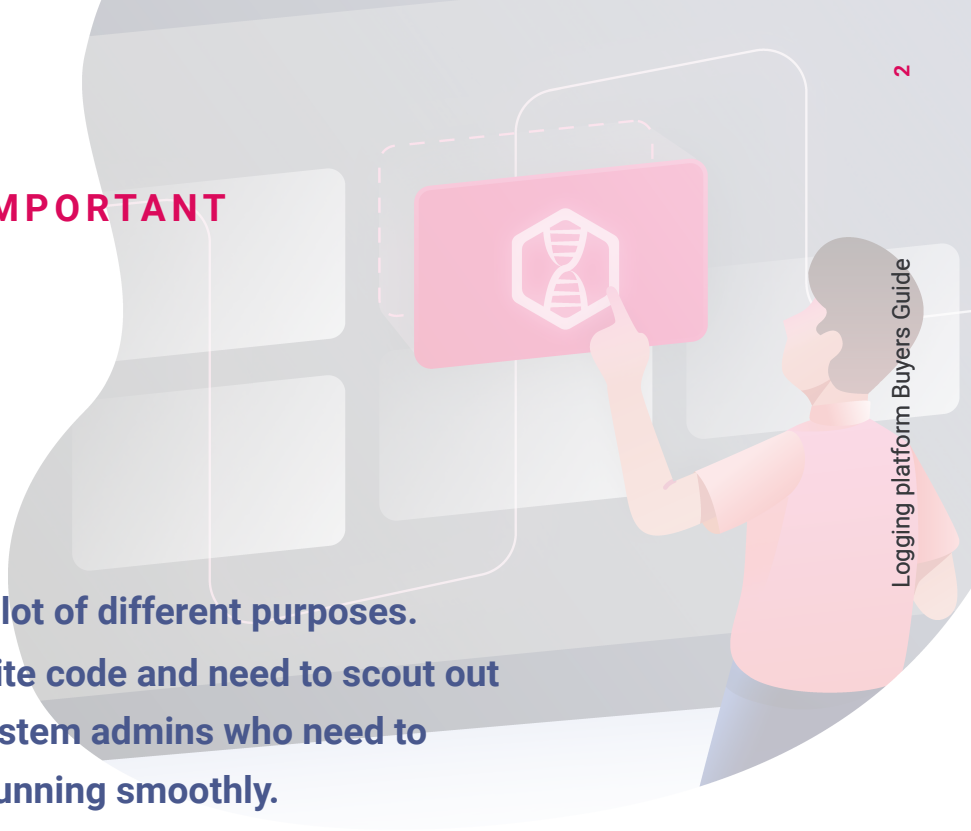
All fortresses require gatekeepers and guards. From the locks on your doors to the digital sentries manning the firewalls. Businesses of all kinds also have something special inside their electronic systems. We're talking about the sentry inside – log monitoring.

Log monitoring oversees important activity within your infrastructure, inspects events, logs user actions, and provides you with alerts in the event of a data breach. These raw files are known as logs and the practice of managing them called Logging.



logdna

WHY LOGGING IS IMPORTANT



A log can be useful for a lot of different purposes. From developers who write code and need to scout out for potential issues to system admins who need to make sure everything's running smoothly.

Logging can provide real time insight into production applications. Most of the time, logging tools are deployed to developers who might not have access for direct debugging. Some of these log messages can then be used to localize potential issues. If a regular log isn't enough, developers can turn on their debug logs and go into greater details on what's happening in real-time. The goal of every system administrator is to make sure their systems are running at full capacity. Logs give operators the ability to check and see if everything is under control. It also significantly reduces downtime as they can catch problems before they happen and potentially bring down a network.

Often times engineers need this crucial information as it can shorten development cycles. They're working on making sure their applications run smoothly and dealing with security at the same time. They're utilizing logs to create reports, scout out for malware and using them to find potential security problems. Wearing multiple hats as a security operator and developer gives DevOps the ability to see the broader picture when overviewing their systems or applications.

Logging can also help you understand how your customers are using your products. Logs give you the direct ability to watch crucial user actions. With this added availability, you can see what works best for the customer. Say you wanted to implement a new layout and do some A/B testing to improve something in the UI. After implementing this new development or design change, you'll be able to directly watch user actions pertaining to this new change and use that information to come to a decision.

There may be millions of individual actions taking place – this data isn't just static noise. It can be grouped, analyzed and managed. You'll gain a greater insight into the intricacies of your customer base and your business. The trick is knowing how you should gather everything and get connected with the information that really matters.

TYPES OF LOG MANAGEMENT

It's important to get a log management solution that works well with your company's unique needs and helps empower your business to work more efficiently. There are a few different types of management platforms. These include: purely cloud based solutions, on-premise server management, hybrid on-site/cloud, and a self managed system – essentially building your own logging management platform through a service like **AWS**.

CLOUD LOGGING

Logs are not always the easiest to deal with, but they are an important part of any system. When you're faced with a development issue, one of the easiest things you can use is a dedicated log management solution. You don't want to have to circle through endless text-files in a scattered and chaotic manner.

One of the best advantages of cloud management tools is that they can be used to easily pinpoint the main cause of any software or application error, within one simple search. This also applies to security-related issues, where some cloud logging platforms will help give your IT team the ability to prevent attacks before they happen. Another great factor is that you'll be equipped with a visual overview of how your customers are using your software. All of this information in one packaged and single dashboard can help tremendously in terms of productivity.

DEPLOYING ON YOUR OWN SERVER & HYBRIDIZATION

Businesses today need to be able to collect and secure data in a fast and efficient manner. This can be done on your own servers. As an example, you can use Amazon S3, as it is an object storage that's built to store and take data from anything and anywhere. This includes mobile apps, enterprise applications, device log databases and IoT sensors. S3 gives users the ability to create your own storage solutions in a unique way. It provides functionality that allows you to run analytics directly on your data through S3 query solutions. It's also the most supported storage platform around.

Amazon S3 can also be used in tandem with an internal logging solution on your server. S3 combined with your own server can put these things together at once. While this option for log management will work – it's going to require a lot more setup and individual ingenuity rather than using pre existing log management solution.

ELK SELF MANAGEMENT

Many opt to self manage through Elasticsearch, Logstash, and Kibana, basically building your own log management service in the process. Before implementing a custom solution like this, it's important to consider the costs that come with maintaining and managing your own system. There will be a lot of positive things to note as there will be greater design flexibility, but at the cost of much higher operational complexity. Let's take a look at each component of the ELK stack.

Elasticsearch is an open source distributed search and analytics engine. It is one of the most popular types of search engines and one its main uses is for log analytics. It is a full-text search tool and provides real time analytics for large volumes of data. It's a popular solution as its highly customizable with easy to use APIs that allow you to integrate and add search capabilities to your apps.

Kibana is coupled with Elasticsearch to form the visualization end of the spectrum. It's used for analytics, operational intelligence and application monitoring. Kibana has built in histograms, line graphs, heat maps, and pie charts. The visual and textual side are then completed with Logstash as its the data pipeline that brings it all together. Logstash feeds and loads data into Elasticsearch and as 200 plus open source plugins that help you index data your own way.

When choosing a log management platform, it's important to evaluate your current company operations. Decide whether or not you need to be individually flexible, need an enterprise solution or can get away with running a tight ship with a small logging operation.

HOW TO DETERMINE THE BUSINESS NEEDS

For a lot of different companies, there is a regulatory and mandatory need to take proper control and order over your data. This includes logs. Two of the major regulatory functions that need to be met are as follows.

- **SOC 2**
- **HIPAA**

SOC2 was developed by AICPA and designed for service providers that store customer data in the cloud. What this means is that the majority of SaaS companies and any business that stores their customer's data in the cloud, must align with these specific requirements.

Cloud vendors only had to deal with SOC 1 (SSAE) compliance records before 2014. It's important to know **what SOC2 actually is**. SOC2 requires businesses to follow a strict security policy and protocol that secures data from the time of processing to the final destination of storage. SOC2 is becoming a necessity for a wide number of companies. Here are a few major things you need to have accomplished in order to have SOC 2 compliance.

- You're monitoring unusual activity within your system
- Checking on authorized & unauthorized internal configurations
- Monitoring user access levels of management

You have to be able to monitor for known malicious activity, as well as being prepared for the unknown. This is a standard most companies will have to meet. For specialized companies, mostly healthcare ones – there is a need to meet HIPAA compliance.

HIPAA LOGGING

HIPAA Compliance

Healthcare data is incredibly sensitive and important to keep track of and protected. Before the cloud existed the Health Insurance Portability and Accountability Act of 1996 Title II (HIPAA) was the first important law that addressed these concerns.

Regulations through the Hitech Act amendment have been created to protect electronic health information and patient information. Log management and auditing requirements are covered extensively by **HIPAA** as well.

- Protected information being changed/exchanged
- Who accessed what information when
- Employee logins
- Software and security updates
- User and system activity
- Irregular Usage patterns

It's grown increasingly more important for healthcare professionals and business partners alike to maintain HIPAA compliance indefinitely. Log files (where healthcare data may exist) must be collected, protected, stored and ready to be audited at all times. A data breach can end up costing a company millions of dollars.

You must also keep in mind that you're going to need to know how long you need to keep your data with a logging provider and what your daily log intake is going to be. These will be sent into the log management system on a daily basis for processing.

PROVIDER RESEARCH

There are few things to keep in mind when looking for a provider. The cost is going to be an important deciding factor. Pay per gig is one of the most flexible and smartest ways of using a logging platform. Companies are a dynamic vehicle and you could go from processing a few hundred thousand logs a day to a few million overnight. The goal is to always be growing your company, and your log management must be able to scale with you in both dynamic ability and cost!

COST (TCO)

Pay per gig eliminates any issues with being able to forecast your data volumes and allows you to only pay for what you use.

Here is a good checklist to think about when determining your costs and what you'll need out of a Logging management platform.

- Free trial & easy installation
- Limited free plan availability
- Ability to track how much you've logged Storage retention costs per paid tier
- User limits & plan of action if they're exceeded
- Features offered per each plan
- Granular billing rate

HOW TO COMPARE AN ELK STACK VS. A CLOUD BASED SOLUTION

There are hidden costs when it comes to self-managed solutions such as an ELK stack. It will require someone to manage the system indefinitely. This is why it's hard to pin down the exact costs for this stack.

While it is open source and technically "free" it still requires hardware maintenance and cloud storage costs. Setting up the entire stack, which includes the ES servers, Kibana and mapping API should take an average engineer (familiar with an ELK stack,) only 5 days to set up.

This consultation alone could cost around $500 daily, this is based off of an average salary of an engineer. Monthly maintenance needs to be done around 3 days per month.

On average this could end up costing a company $1500 monthly for just maintenance paying a variety of consultants. This cost will fluctuate as this does not include any crises or change requests from within the company. Additionally, you'll need to hire engineering support. Without one central solution, prices will vary a lot due to specific business use cases.

Here are some things to consider and ask yourself when choosing a solution:

- Do you already have an on-premise solution or preexisting cloud setup?
- Are your users all developers?
- How many different services do you want to connect to the stack?

What's an average amount of time for data retention? If your use cases are changing and expanding fast over time, complex scenarios are expected, multiple channels inside your company need log management, then ELK deployment is going to be the more complex option. A regular ELK installation won't be the best way to go here. Keep in mind that you'll either need to have an independent deployment or officially managed system either way.

While an independently run ELK stack gives you more flexibility and control, you risk having to dedicate or hire an engineer to become the full time ELK manager. Paid management gets rid of these concerns right off the bat.

PROVIDER RESEARCH

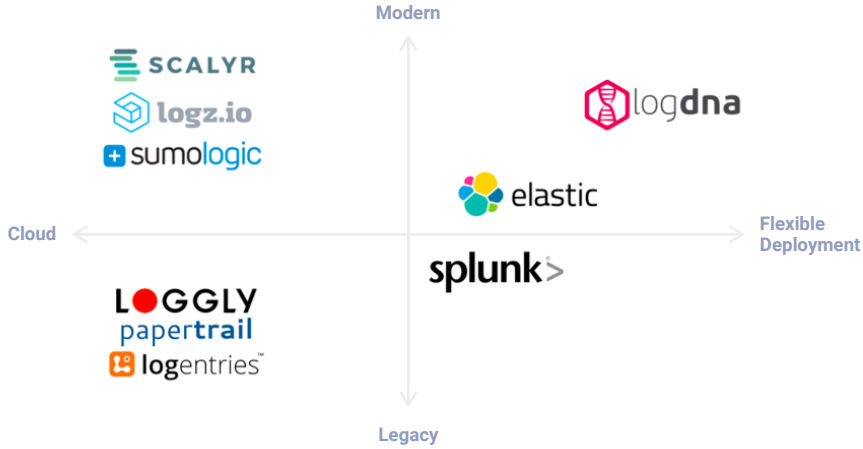
SCALE, SPEED & INTEGRATION

As an application grows up – as inevitably they will if successful, storage needs for logging will change. From the humble backwoods of grep to the open source search engine. As services and company needs grow, companies will face new challenges involving scalability, search speed and integration with third party plugins. Even established companies can struggle with working out the kinks if not properly prepared. These next ten principles and abilities should be available for the platform and logging solution that you pick.

1. Use a framework with flexible output options
2. Utilize standard format like JSON
3. Visualization of console logs without direct server access
4. Custom format for storage outside your data center
5. User experience intuitive for all users
6. Low latency for live monitoring
7. Test search performance at full query capacity
8. Ingestion time less than a few seconds
9. Automatically parsed logs at ingestion
10. Easy onboarding and integration for pre existing systems

COMPETITOR LANDSCAPE

A great log management solution isn't just a storage place. It's a framework that is going to change the dynamics of your business.



PROVIDER RESEARCH

LogDNA prides itself on blazing fast search and an intuitive design practice. In a quantitative world system filled with computer-speak and opaque log messages – knowing what you're doing and looking for with plain language is a god send. Everything needs to fast and efficient. From the integration into your pre existing systems to the search for a specific log. We do the heavy legwork when it comes to speed and management.

LOG FROM ANYWHERE

From Kubernetes, python library to REST API, we support over 30+ integrations to ingest log data. Start logging in as little as 2 minutes. Identify the root cause of issues quickly, so you can get back to work. Debug in real-time since your data arrives nearly instantly with live streaming tail.

LOGDNA SUPPORTS COMMON LOG FORMATS

- Apache
- AWS ELB
- AWS S3
- Cron
- HAProxy
- Heroku
- JSON
- Logfmt
- MongoDB
- Nagios
- Nginx
- PostgreSQL
- Kubes
- Docker
- Ruby/Rails
- Syslog
- Tomcat

Additional Log Types Supported +++

PAY PER GIG PRICING

LogDNA makes it easy for smaller companies with the **"pay as you grow"** pricing structure. It reduces costs as it doesn't have to be stored on premise. You also don't have to worry about fixed storage buckets.

LOGDNA SOLUTION

Constrained usage buckets are wrought with inefficiencies. No one has an absolute accurate view of their own log volume. This thought alone puts paralysis on deciding what type of plan you're going to use. For data-based companies, it's crucial to have scalable pricing. Customer data usage is going to change accordingly to company size, growth, and internal data collecting decisions within the company.

Additionally, management costs go down as the platform takes over that job. LogDNA has created a system with proactive monitoring, a sleek user-interface, technical capabilities that integrate with standard logs across countless platforms and continues to innovate with the latest in logging technology. The pricing system is innovative and has set a precedent that cannot be beat.

BUILT FOR SCALE

Our platform is capable of handling hundreds of thousands of log events per second, and dozens of terabytes per customer per day. Whether you run 1 or 100,000 containers, we scale with you – from 1GB to 10PB we have you covered.

SECURE COMPLIANCE

With SOC 2 compliance and HIPAA/HiTech – all avenues are covered in regards to regulation.

For HIPAA, our distinctly tiered system takes into account how many team members (users) will be using LogDNA on the same instance and length of retention (historical log data access for metrics and analytic purposes.) Additionally we also have our scaled pricing tier – HIPAA compliant for protected health information (which includes a Business Associate Agreement, or BAA, for handling sensitive data).

KEY TAKEAWAYS

Overall, a logging platform has to meet your business unique needs, be compatible with your plugins and systems and be able to effectively manage and scale for a dynamic growing business.

You should also keep these questions in mind before choosing your platform.

What is my initial log volume going to look like? Where is my application in the development lifecycle? And finally, what management solution aligns best with my overall business strategy?

Let this information and these questions guide you to a future of log management success.

START SAVING TODAY

To see how easy it is to get started with LogDNA, sign up for a **free 14-day trial** and start managing your logs today. If you would like to run LogDNA as an on-premise solution, please **contact us** for an assessment or demo.

logdna

GET YOUR FREE TRIAL

CONTACT US