Product Brief

Logentries

Immediate Answers from Real-Time Machine Data Investigation

Logentries by Rapid7 is the easiest way to centralize logs in real-time and analyze machine data so you can get answers to your security and operations questions quickly.

With Logentries, you can manage both logs and unstructured machine data to get instant access to your data for security, DevOps, and IT operations. Protect your logs from manipulation to create a solid audit trail. Receive instant notifications about system failures or malicious activity, track system activities in real time, and easily search across raw logs for known patterns with intuitive search queries to quickly identify the root cause of issues.

Effortlessly centralize all your log and machine data

Organize your logs for secure accessibility

With Logentries, logs from across your entire environment are safely stored in a central location to be easily and securely accessed by your team, regardless of data format or source.

Enable teams with access to the data they need

Because all logs are centrally accessible in Logentries, your entire team has access to logs without having SSH access to production servers. Limiting access is a security best practice and reduces the risk of human error.

Create a secure audit trail

With Logentries' log centralization, you have a permanent record of exactly what happened in your environment. Rather than disappearing when servers crash or attackers cover their tracks, logs centralized in Logentries will always be there to provide answers.

Automatically scale with your environments

Use Logentries with configuration automation tools or Docker containers to ensure that new servers or containers are automatically added to Logentries' log collection, preventing the risk of missing data.

Reduce time to accessing data

Unlike other log management tools, Logentries doesn't require you to specify log types or create your own indexes, thus giving you access to your data faster.

Maintain compliance with centralization, search, and audit trails

A significant part of meeting regulatory compliance standards includes centralizing log data for a specified period and providing proof of regular log reviews. With Logentries, you can centralize your data, specify exactly how long you wish to retain it and perform regular reviews with detailed audit trails.

Be the first to know about security and operational issues

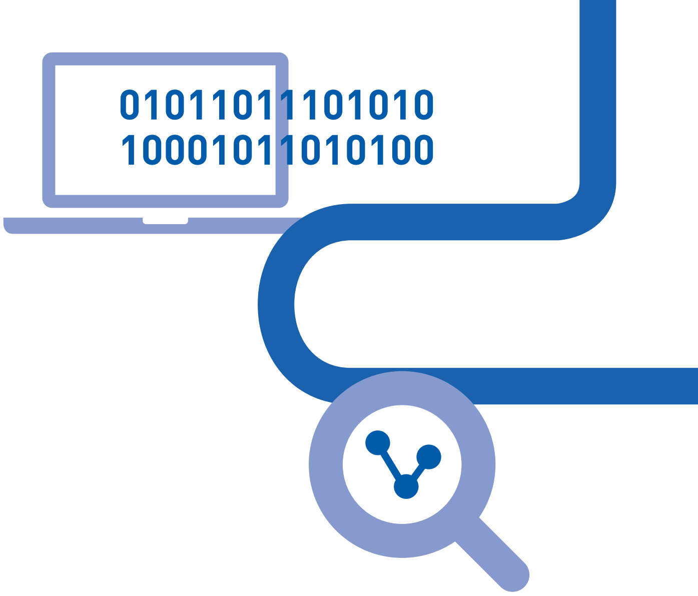
Catch issues as they occur

Logentries notifies you of issues within seconds rather than minutes because it triggers alerts by pre-processing data as it enters the system, helping you take immediate action. You have full control over alert frequencies and thresholds to avoid alert fatigue.

Know what's not happening – but should be

Sometimes, the most urgent events

> “Using Logentries we transformed log data from routers and switches into a prominent tool for proactively preventing outages, improving response time to outages when they occur, and getting a visualized understanding of what our baselines are.”
>
> – Michael Dieter, Senior Systems Engineer, Loyola University



are those that don’t happen. Whether it’s an important backup process or a scheduled scan, Inactivity Alerts tell you immediately when things don’t happen as they should.

Realize trending threats with anomaly detection

Logentries is constantly analyzing your log behavior. With Anomaly Detection, you’ll be notified if something unusual occurs or system behavior changes. You have full control over which events Logentries analyzes and alert thresholds.

Empower your team to take action

What good are alerts if your team doesn’t see them? Logentries integrates with your favorite team communication tools, including Slack, HipChat, and PagerDuty. You can also send notifications to webhooks for further integrations.

Spot hidden insights with data visualization

Dashboards create powerful data visualizations for spotting trends and patterns. Whether it’s an unusual spike in login failures or memory usage trending high, Dashboards built from Logentries’ powerful query language help you reveal insights you may have previously missed.

Resolve security and operational incidents with fast investigations

Investigate attacks on your network

When investigating a security incident, Logentries enables you to search historical log data for indicators of compromise, such as changes to root privileges or users SSH’ing into production environments. Searches can be performed across your entire environment to help identify all affected systems.

Watch events in real-time for incident response or troubleshooting

Tail all of your aggregated log files from one location in real-time. Live Tail mode enables you to watch a stream of your log events as they occur for up-to-the-second monitoring and investigation – whether you’re hunting an intruder play-by-play or troubleshooting an operational issue.

Analyze log data with an intuitive query language

Logentries’ query language is easy to use and enables you to perform deep queries and group data by specific values like user IDs, IP addresses, or hostnames to enhance your investigation. If you’ve worked with SQL, you’ll pick up Logentries’ Query Language (LEQL) in a heartbeat and without effort.

Analyze unstructured data with Regular Expressions

Derive insight from even unstructured data with Logentries’ full support of Regular Expressions.

Get context for discovering an issue’s root cause

Once you’ve queried your logs to filter for significant events, use the Context button to reveal surrounding events and understand what occurred before and after to identify root cause.

Make it easy to spot issues with Custom Tags

With Custom Tags, it’s easy to identify the events that are the most meaningful to you and your team. Custom Tags act as visual markers within your log stream and timeline.

Learn more about Logentries and start your free 30-day trial at:
www.rapid7.com/products/logentries