logentries
BY RAPID7

Using Logs to Address Compliance Standards

Prepared by
Netanium Security

logentries.com

Table of Contents

About Netanium

Effective security takes a team. Security Operations + Engineering + Analysis: Netanium provides the solutions, experience, and training necessary to develop a measurable and practical security program. When you are ready to think differently about solving complex cybersecurity challenges, Netanium will be here to help.

About Logentries

Logentries is one of the most popular log management tools used for real-time log centralization, search and analysis. DevOps, Security & IT professionals use Logentries to manage both logs and unstructured machine data for immediate visibility into their IT environments. By enabling users to securely collect logs, search for known events and provide audit trails, Logentries helps organizations meet the log management requirements of many common compliance standards. Learn more at logentries.com/security.

Understanding common log requirements

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA (Healthcare Insurance Portability and Accountability Act) requirements span across a multitude of categories to address the protection of data integrity, confidentiality and availability of protected health information (PHI) within the healthcare industry. PHI must be protected via a robust IT infrastructure that guarantees administrative, technical and workstation safeguards. This system must use effective encryption, and must instate verifiable authentication and access procedures.

This standard can be broken down into two specific rules: HIPAA Privacy Rule and HIPAA Security Rule. The Privacy Rule focuses on protocols around the saving, accessing and sharing of medical and personal data of individuals or patients, with emphasis on privacy of information. The HIPAA Security Rule instead focuses on security standards in regards to protecting the actual health data itself that is created, received, stored, or electronically transmitted. This is called electronic protected health information (ePHI).

In order for an organization or provider to be fully HIPAA compliant, a series of physical and technical safeguards must be in place:

Physical Safeguards

- Policies must be in place to address the use and access of all workstations and associated media in the facility.
- Access controls must be established to ensure that only authorized individuals are accessing the facility.

Technical safeguards and policies

Assurance of existing access controls that only allow authorized access to electronic protected health data includes:

- The usage and enforcement of unique user ID's, encryption and decryption and logging procedures.
- Controls to guarantee the integrity of the ePHI.
- IT disaster recovery, business continuity and reliable backup to ensure the protection and recovery of sensitive data.
- Full network security in terms of protection of data in motion throughout all transmission mechanisms, including email, web and movement to cloud storage.

Logging

Logging requirements include specific attention to the following topics:

- Risk Analysis
- Risk Management
- Malicious Software Detection and Protection
- Response and Reporting
- Information System Activity Review
- Authentication Monitoring
- Audit Controls
- Security Management Process
- Incident Procedures

In terms of Windows based systems, the Security Event Log holds the most valuable information pertaining to actions of users on the network. However, the following event logs also hold vital information that must be regularly monitored:

- Application Events
- Directory Services Events
- DNS Events
- System Events
- File Replication Service Events

The Security Rule and Privacy Rule of HIPAA mandates that the following areas must be logged, reported and monitored:

- User Access
- User Privileges
- NTFS Permissions
- Remote Access
- Role Permissions
- Auditing Enabling
- Password Policies

The following are recommendations for reports to run based on the above requirements:

- Account Management Success/Failure
- Directory Services Access Success/Failure
- System Events Success/Failure
- Group Management Modifications, Additions and Deletions
- Object Deletions
- Object Access Attempts Success/Failure
- Account Management
- Log On Failures to Active Directory
- Authentication Failures
- Elevated Access Actions
- Password Changes

Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) stands as a set of policies and procedures put in place to regulate organizations that process or store credit card data. The PCI DSS was created in 2004 by the credit card companies Visa, Discover, American Express, and Mastercard. Adherence to these standards is intended to increase the security of all transactions in the credit or debit card space, and to protect the cardholders from any misuse regarding their personal information.

Objectives

There are six major objectives that are outlined in detail by PCI DSS to ensure desired security of personal information:

1. **A secure network.** A robust infrastructure that includes the implementation of firewalls and related security measures are critical.

2. **Protection of card holder information.** Stored personal information must be completely secure against hackers and other misuse. Encryption is a necessary layer of protection that must be implemented.

3. **Anti-malware protections of systems touching card holder data.** All systems and applications should be patched regularly, and scans must be conducted frequently to detect any threats of viruses, malware, etc.

4. **System access restriction.** Any personnel who have a computer or workstation in the system must be identified by a unique ID, ensuring accountability in the case of an incident.

5. **Network monitoring and logging.** As personal data is exchanged over the network, it is vital that the network is constantly tested for security fortitude.

6. **Establishment of a formal security policy with explicit maintenance instructions.** All the previous objectives must be upheld and documented in formal documentation for both reference and auditing purposes.

Logging

PCI DSS includes several requirements that can be addressed through log management, including:

- The linking of individual, trackable users to both normal and elevated administrative privileges:
  - Confirm there are no shared accounts
- Establishing audit trails for the following events:

- All attempts to access card holder data
- Administrative and root access actions
- Creation and deletion of system-level objects
- Invalid logical access attempts

- Recording the following audit trail entries for all system components for each event:
  - Identification per user must be unique and documentable
  - Event type
  - Date and time
  - Authentication success or failure
  - Origination of event
  - Identified data, system component, or resource

- Ensuring the following actions are taken:
  - Secure audit trails so they cannot be altered
  - All actions taken regarding access to the logs must be documented and traceable to a unique identification
  - Daily log reviewal
  - Retainment of audit trail history for one year in a secure server
  - Audit trail history available online for three months at minimum

Sarbanes-Oxley (SOX)

The Sarbanes-Oxley Act of 2002 is a federal law in the United States implemented within the publicly-traded companies space, including boards and management. The act contains eleven sections that delve into corporate responsibilities and accountability, resources, white collar crime penalties and corporate fraud accountability, among others.

SOX requires publically-traded companies to put internal controls into place to protect the disclosure of confidential data and data tampering that could result in fraud. Specific to security, log management of anything related to financial statements and processing systems must be monitored. The collection, management and subsequent analysis of the resulting log data is vital to meet SOX requirements.

Section 302 of SOX specifically details the importance of establishing timelines, requiring all logs must be timestamped and stored within a secure archive. Any access to the logs must be tracked through verified and functional controls to ensure the integrity of the log data.

Logging

In order to be compliant with SOX regulations, the following parameters must be monitored, logged and audited:

- Account activity
- Database activity
- Network activity
- Login activity (both successes and failures)
- User activity
- Information access
- Internal controls

Examples of executable SOX reports are:

- User Log On
- User Log Off
- Log On Failure
- Audit Logs Access
- Object Access
- Host Session Status
- Account Management Changes
- Removal or Addition of Global Group
- Removal or Addition of Members of a Global Group
- Audit Policy Changes
- Successful User Account Validation
- Unsuccessful User Account Validation
- Individual User Action Report
- Network Device Change

Understanding what to look for in a log management tool

Given specific HIPAA, PCI and SOX requirements, it's clear that logs play a critical role in meeting compliance standards. For this reason, most organizations use tools and services to help them manage their logs. While the specifics of each regulation vary, the four categories of log management consistent across all standards are:

- *Log Collection*
- *Secure Retention*
- *Regular Search & Analysis*
- *Audit Trails*

Log Collection

What type of log events should be collected

Remember that when it comes to logging, compliance standards vary in specificity. Here's a recap of logging recommendations from section 1:

HIPAA	PCI	SOX
• Account Management Success/Failure • Directory Services Access • Success/Failure • System Events Success/ Failure • Group Management Modifications, Additions and Deletions • Object Deletions • Object Access Attempts Success/Failure • Account Management • Log On Failures to Active Directory • Authentication Failures • Elevated Access Actions • Password Changes	• All Individual Accesses to Card Holder Data • Administrative and Root Access Actions • Creation and Deletion of System-level Objects • Invalid Logical Access Attempts	• User Log On • User Log Off • Log On Failure • Audit Logs Access • Object Access • Host Session Status • Account Management Changes • Removal or Addition of Global Group • Removal or Addition of Members of a Global Group • Audit Policy Changes • Successful User Account Validation • Unsuccessful User Account Validation • Individual User Actions • Network Device Changes

Required data

PCI Standards also specifies what data must be contained within a log file. Even if you don't need to be PCI compliant, these are good practices to follow:

- Unique user identifiers
- Event type
- Date and time
- Authentication success or failure
- Origination of event
- Identified data, system component, or resource

Secure data transmission

It's essential that data sent from your system to any log management service is transmitted securely when traveling through secure networks. Be sure to check to see if the log management tool offers options for secure transmissions. For example, Logentries offers an endpoint for sending encrypted data via a TLS connection.

Secure Retention

All compliance regulations dictate that logs must reside in a secure, centralized location. The integrity of logs is vital, thus it must be provable they are unaltered after being collected. Most compliance regulations also specify requirements for how long logs must be stored. For example, PCI DSS requires logs remain searchable for up to 3 months and are retained for up to 1 year.

A log management tool can be used to consolidate all log events into a single, secure location. For example, a hosted log management service can help in the following ways:

- Store all logs remotely, separate from running systems
- Maintain an unaltered copy of log data to compare against local logs
- Offer direct integration with Amazon S3 for long-term storage
- Collect and centralize data from applications, systems and formats, including:
    - Applications
    - Workstations
    - Servers
    - Databases
    - Networks
    - Firewalls
    - Routers
    - Hosted Platforms

User Permissions

When working within a team, it may be necessary to give other team members access to your log management tool for search and analysis. When doing so, it's important to consider whether the team members should be able to make changes to your log management tool. In general, a log management

tool should:

1. Prevent any user (including admins) from deleting logs
2. Offer role permissions to prevent non-admins from changing which logs are collected or stored.

When considering a log management tool, ensure it offers some level of user permissions that can give read-only access.

Offsite vs. On-premises

Some logs contain sensitive data, such as private email addresses, that should not leave the corporate network. This is problematic if all logs are sent in an unaltered state to an external entity. To address this challenge, a hosted log management and search tool should provide the option to filter or obfuscate data based on patterns.

One example of a data obfuscation tool is Logentries' Datahub, which is hosted on a local server and configured to identify and scrub sensitive data before being sent off site. Datahub is used to match defined patterns and replace content within the log events with a hash value. For example, a customer's email address can be converted to a hash value before ever reaching Logentries. This sensitive data can always later be "unlocked" via a locally hosted browser extension, should the original value need to be viewed.

Search & Analysis Capabilities

Collecting and storing logs is only the first step of compliance regulations. Once successfully collected and stored, the log data must be regularly reviewed in a meaningful way. In most environments, this means enormous amounts of information must be analyzed and interpreted on a regular basis. Aggregations and correlations are essential to making sense of massive amounts of log data. Additionally, the ability to query logs for specific events based on known factors is required.

Using a query language

Traditionally, without a log management tool, querying logs would require a keen understanding of UNIX commands. For example, to search for a log event related to a login request, you may have to execute a command like the one below:

```
cat /var/log/httpd/access.log | grep “GET /login.php”
```

In the command above, the CAT command is used to specify which log file to look at. GREP is then used to search for specific text you believe to exist in the log event you want. While UNIX commands can be handy to know, they present a variety of challenges when querying logs:

- Difficult to learn
- Complex to type
- Lacks ability to calculate values
- Specific to only one log file

When considering log management tools, a powerful yet easy-to-use query language should be a leading factor in your evaluation. Let’s start by comparing the above Unix command with the equivalent command using a simpler log management query language:

UNIX:

```
/var/log/httpd/access.log | grep “GET /login.php”
```

vs.

Logentries:

```
login.php
```

With a tool like Logentries, you simply search for the keyword or pattern you’re looking for. What if you want to calculate values from a collection of log events? While your query syntax will vary slightly based on the format of your logs, here’s a common example of what a Logentries query would like if you are trying to count the number of 404 errors occurring within an apache web server:

```
where(status=404) groupby(status) calculate(count)
```

Custom Tags & Context

When looking at a large data set, it can be difficult to spot key log events. For this reason, using a tool that enables you to apply custom color-coded tags can make it significantly easier to interpret log data. When searching for data, results are often returned in a filtered format, showing you only the data you requested. Since logs are created in the order of which events occur, it can sometimes be helpful to see what happened just before the key event you’re searching. For example, let’s say you’re searching for the term “Login Failure” over the last 60 minutes. You identify the log event, but now want to see the actions taken by the offending user just before and just after the failure. How would you do so?

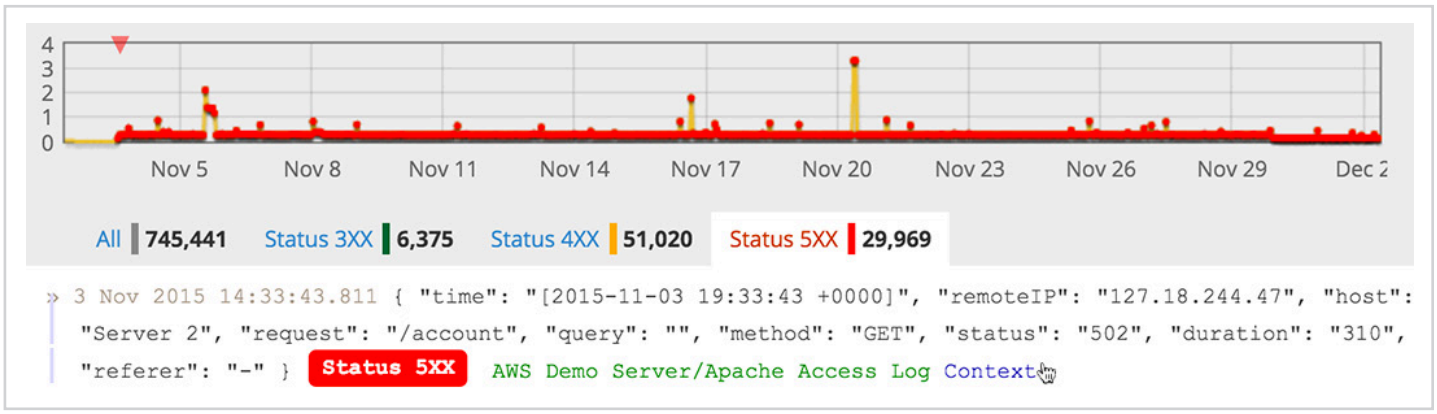

Figure: Tags & Context Link

When considering log management tools, look for one that offers the ability to "unfilter" events occurring just before/after your key event to enable further investigation of pertinent information, such as:

- IP addresses
- Remote hosts
- Usernames
- Commands executed
- Ports used

Using Regular Expressions

Sometimes, you know you're looking for a specific data pattern, but don't have a specific value to search for. For example, you're concerned one of the latest engineering deployments is inadvertently logging credit card numbers, which would be a violation of your PCI compliance policies. You don't have a specific credit card number to search your logs for, but you know that All Visa & Mastercards are 16 digits, while all AMEX are 15 digits. You also know that all Visa numbers start with a 4, all Mastercard start with 51 - 55, and all AMEX cards start with a 34 or 37. The example below demonstrates how you could use RegEx in Logentries to search for each card.

VISA

```
where(/4[0-9]{12}(?:[0-9]{3})?/)
```

AMEX

```
where(/5[1-5][0-9]{14}/)
```

Mastercard

```
where(/3[47][0-9]{13}/)
```

Some log management tools don't support regular expressions. When searching for a log management tool, consider one that offers full RegEx capabilities for extra flexibility when searching your logs.

Audit Trails

Once you've established a process for regularly reviewing your logs for known events and patterns that may indicate malicious activity, its important to establish an audit trail. In the event of a compliance audit, you'll need to be able to provide proof that regular log reviews occurred. There are a variety of ways organizations do this - some keep manual records of when logs were reviewed while others use a tool that creates an audit trail of when someone logged in to review the data. When exploring options for a log management tool for security & compliance, it's important to consider whether the tool provides audit trails of user activity.

Additional Value: Real-time alerts

Most log management tools offer basic alerts to notify you when specific events appear in your logs. Alerts can be incredibly useful by pinpointing issues soon after they occur, making it easier for you to investigate and reach a resolution. But what about when things that should happen, don't? And what about trends occurring over time? When considering a log management tool, look for one that offers the following alerting capabilities beyond standard alerts:

- **Field Level Threshold Alerting:** Often the number of times an event occurs within a given period of time can be an indicator of compromise. For example, you may want to set the threshold for number of failed logins across your environment within one hour to 50. If more than 50 failed logins occur within an hour, you'll be notified.
- **Inactivity Alerting:** Used to notify you when an expected event does not occur. For example, if a firewall goes silent for a determined amount of time, an inactivity alert can send you a notification. Since compliance regulations state that network and system activity are monitored, it is essential to detect when portions of the network architecture go down.
- **Anomaly Detection:** Used to notify you when a value exceeds its average by a specified amount. For example, a user might want to track the number of root sessions opened per day and ensure that number never exceeds its daily average by more than 25%. Anomaly detection would track the average number of root sessions per day and send an alert if that average is exceeded by more than 25%. Anomaly detection identifies trends that would be otherwise difficult for a human to spot as quickly.

A note on real-time: the amount of time that passes between when an event occurs and when an alert is triggered varies significantly across log management tools, with some taking as long as several minutes to be delivered. Be sure to look for a log management tool that checks for alert matches before processing & indexing your data. This means you receive alerts almost instantaneously. The difference between “immediately” and “several minutes” can equate to a quick resolution vs. a significant security compromise.

Examples

In this final section, we provide several specific examples of how to use a log management tool for investigating issues. In this section, we use Logentries as our example tool for log management.

Privileged Account Activity

Event types of particular interest across most compliance standards are actions taken by users with elevated privileges on a protected system. The example below is of an event for a session on a system in which a uniquely identified user with normal access logged in and elevated their privileges to root.

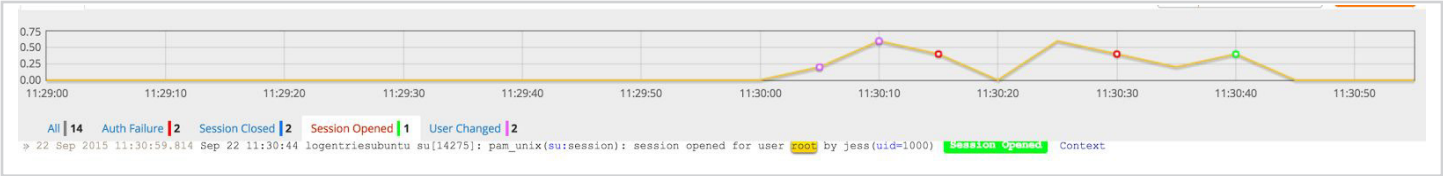

Figure: Collapsed View

At first glance this looks like normal behavior. Upon expanding the context of the entry, however, it can be seen that there were more interesting actions taken prior to the privilege escalation. There are a series of remote authentication failures, followed by an eventual success. From there, the user was able to immediately and successfully elevate their privileges and open a session as root.

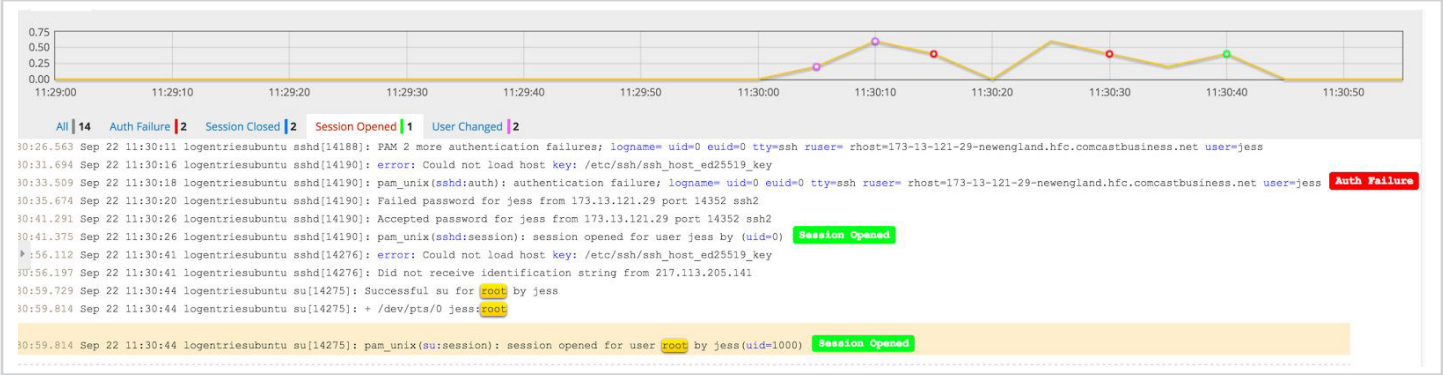

Figure: Expanded context view

While this might be an innocent case of a user entering in the incorrect password a few times, it could also be evidence of a malicious outsider gaining access and compromising the system. This level of comprehensive visibility allows for a better understanding of a chain of events.

Taking this event into consideration, another log analysis technique is to look at failed authentication in general. This provides a view of which user accounts are misconfigured or are potentially subject to brute force attacks. One way to do this is by querying for invalid users that have failed log ons.

GROUPS	COUNT
admin	1,016
administrator	712
test	315
user	147
cisco	141
guest	140
nagios	129
oracle	89
postgres	86
ubnt	71
pi	63
support	62
zabbix	60
ts3	51
ftpuser	49
ftp	48
default	47
git	44

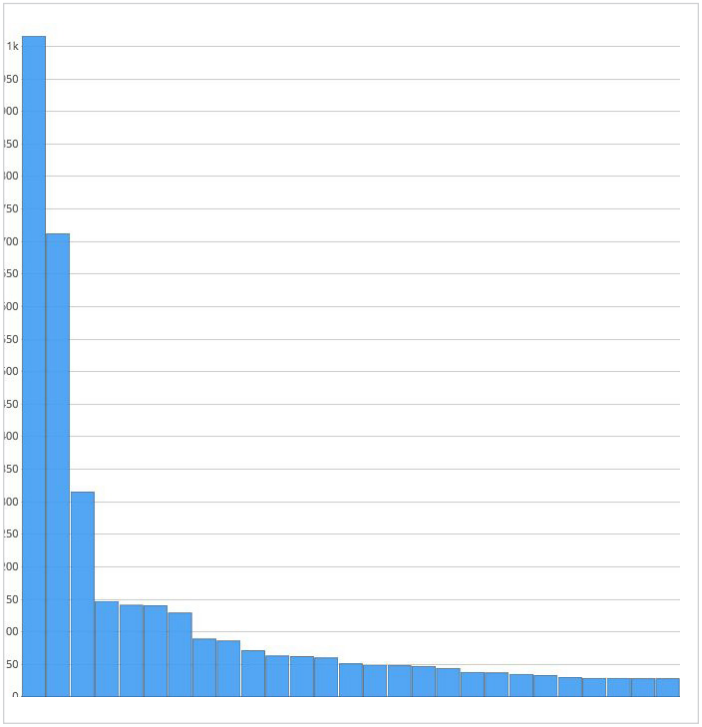

Figure: Count of remote users that have failed log on over a 30-day timespan.

This information shows that the username “admin” and “administrator” have the most failed login attempts. If the volume of failed logins for any accounts are significantly higher than expected, it could indicate a misconfiguration or attack.

Inactivity Alerts

Logentries’ Inactivity Alerts are particularly useful when something is not operating as expected. Many devices, like firewalls, generate a consistent stream of logs. If Logentries suddenly stopped receiving logs, it would indicate a problem somewhere in the path between the device and Logentries. This is especially concerning for regulated environments as missing logs can put a company out of compliance.

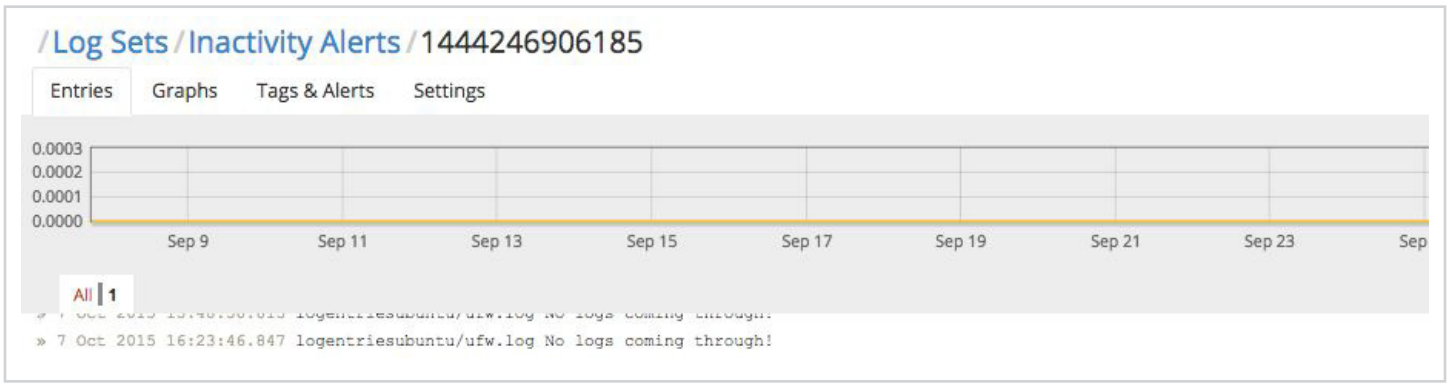

Figure: Inactivity Alerts

There are a number of reasons why logs would stop being received by Logentries, including a problem with the log source device or an issue with the network path that the logs are transmitted on. For this example, an alert triggered because the firewall on a protected server system went silent for more than 5 minutes. Looking at the logs just prior to the outage, there is a log message with the 'Modification of Local Firewall' tag attached. The log messages around this timeframe show that the user 'jess' elevated their privileges to root and disabled the local firewall. Quickly identifying issues like this are vital to ensuring regulated environments stay in compliance with logging and control requirements.

Figure: Expanded context view

Looking Forward

When it comes to compliance requirements related to log management, using a log management tool can significantly enhance your compliance efforts. While there are plenty of options for tools to help you become compliant, tools can vary significantly in terms of price, features, data accessibility and **usability**. A compliance tool that makes it difficult to search raw logs can impede your ability to resolve issues quickly. When considering a tool to meet the requirements outlined throughout this article, may product usability be a deciding factor in your evaluation process.

Start your 30-Day Logentries Free Trial Today.

Logentries can help you meet compliance standards with a suite of tools built for easy log centralization, investigation and reporting.

- ✔ Unlimited log centralization
- ✔ Secure data transmission
- ✔ Protection from log manipulation
- ✔ Easy search for known events & patterns
- ✔ Full RegEx Support
- ✔ Affordable plans
- ✔ Real-time Alerts
- ✔ Inactivity Alerts
- ✔ Anomaly Detection
- ✔ Data filtering & obfuscation
- ✔ Custom tagging of known events
- ✔ Custom retention policies

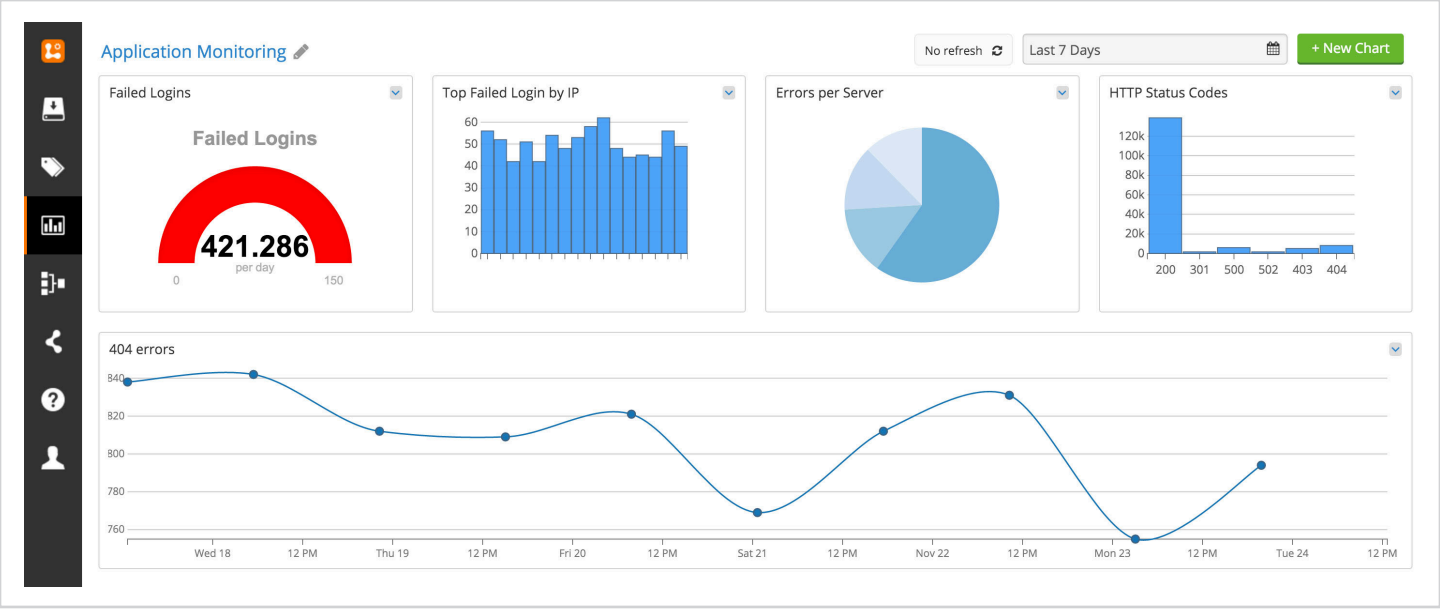

Figure: Customizable Dashboard view

Get started for free at logentries.com