Modern Logging for FinTech

FinTech companies face stringent and complex requirements for logging and auditing their systems. This challenge is compounded by the fact that more services are moving to public and private cloud computing environments. Regulations such as PCI DSS and PSD2 create compliance complexity with managing logs and it can be hard to keep up. Failing to meet these regulations can result in significant fines, or worse.

Here are some of the challenges the industry face when complying with regulations and how logging helps.

PCI DSS Compliance

Handling sensitive payment information means a proactive approach to security. Part of this process means thoroughly monitoring systems, applications, and infrastructure components for signs of vulnerabilities or breaches. Logs play a central role in this process by providing a constant stream of near real-time information on events taking place within your infrastructure.

Here are some important benefits:

Overseeing User and System Activity

One of the major requirements of PCI DSS is having the ability to track user actions across systems. This creates an audit trail of all user activity, allowing organizations to see what actions a user performed, trace their actions throughout a session, and generate alerts in case of suspicious activity. In case any data is compromised, organizations can use logs to determine how the user accessed the data and the scope of the breach.

To do this, organizations need to:

- Log all user access to system components (Requirement 10.1).
- Log all actions performed by users, especially administrators and other privileged users (Requirement 10.2).
- Log contextual information such as user and session IDs, the type of action performed, and any affected components (Requirement 10.3).

Since this also involves tracking access to cardholder data (Requirement 10.2.1), there is a risk of sensitive information making its way into log data. To protect cardholders, this information needs to be scrubbed or sanitized before being logged. Log management solutions like LogDNA often use rule sets to detect credit card numbers and other types of personally identifying data and mask them before storing them permanently.

Creating an Audit Trail

Logs are meant to be an immutable record of all events taking place on a system. They can and do contain business-critical operational information that can be used to troubleshoot and monitor sensitive activities. As such, access to logs should be strictly controlled to prevent malicious users from editing or deleting them, for example, in order to hide their steps (Requirement 10.5). Unless your logs are guaranteed to be immutable, they can't be trusted as an auditing tool.

Centralization plays a key role in this, as it helps ensure logs remain consistent even if the machine that generated them is compromised (Requirements 10.5.3 and 10.5.4). This means setting strong access control mechanisms such as role-based access controls (RBAC) for your centralization server and the logs stored in it (Requirement 10.5.2).

Centralized log management services like LogDNA enforce immutability, while also letting you control which users have access to sensitive log data.

PSD2 Compliance

The Second Payment Services Directive (PSD2) paved the way for greater flexibility and openness in banking and online payments. But like PCI DSS, it requires stronger policies for monitoring, auditing, and responding to security incidents. The European Banking Authority publishes guidelines on how payment service providers (PSPs) can satisfy PSD2 requirements. In terms of logging, there are two main areas of focus:

1) User Activity

Guidelines 4.10 and 4.11 suggest closely monitoring and limiting the access that users have to systems containing sensitive data, particularly payment data. User access should be thoroughly logged and periodically reviewed in order to detect unusual behaviors, especially for administrators and other high-privilege users.

2) Business Processes

In addition to user activity, PSPs should also monitor components that provide core business functions (Guideline 5.1) in order to detect unusual activity. This can include monitoring for changes to hardware or software, potential information leakages, malicious code, and security updates (Guideline 5.3). Logging this data over a period of time will help develop a baseline profile of operational activity, allowing you to set alerts and notifications for deviations.

How LogDNA can help

LogDNA leads the way in providing a fast and scalable log management solution that lets you centralize, analyze, and monitor logs from all of your applications and systems.

LogDNA is certified as a PCI Level 1 Service Provider and is compliant with a number of other regulations including GDPR, HIPAA, SOC 2, and Privacy Shield. Enterprises can also secure their logs with per-user access controls, OAuth sign-in and encryption of data in transit.

LogDNA has a flexible deployment model and it is easy to deploy no matter what your infrastructure needs, whether that is private cloud, on-premise or multi-cloud for greater control over your data. A standard LogDNA deployment can ingest several terabytes of log data per day, and supports search speeds of hundreds of gigabytes per second. The platform was made by developers for developers. LogDNA's streamlined interface allows users to navigate log data, perform natural language searches, and retrieve the fastest search results on the market.

With customers like IBM, CommonBond, Better Mortgage, LogDNA is enabling over 2,000 companies with their log management and compliance needs.

Check out logdna.com to learn more.

Deploy For Free Now

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.
Want a logging expert to assess your infrastructure? Contact us at onboarding@logdna.com