OTAVA

DATA SHEET

DAILY LOG REVIEW

Detect and prevent abnormal user behavior

Monitoring and analyzing user and system activity can help detect patterns of normal use and potentially malicious users. Log monitoring tools review network and systems activity, inspect all monitored events, provide alerts for suspicious activity or anomalies, and record system user activities.

Daily log review is the process of regularly reviewing and reporting on log activity. These log messages and alerts provide insight into anomalies in your system network and managed devices - including failed login attempts or other indicators of possible intrusions.

You're a perfect fit for Otava Daily Log Review if...

- You're concerned with security and need to be PCI compliant. That could be credit card data, financial data, social security numbers, health care records; anyone with sensitive information needs daily log review.
- Your business is in the medical, dental, or insurance fields, or any other healthcare support business, that is required to protect ePHI (Electronic protected health information) under HIPAA privacy rules.
- Your business is governed by Sarbanes-Oxley financial reporting requirements to provide an audit capability for access to sensitive business and financial information.
- You need to detect attacks and security failures before they become data breaches.

Why Otava Daily Log Review?

Clearer, more regular system insight

Daily Log Review provides regular insight into your monitored systems, instead of auditing devices after an event occurs. With consistent monitoring and analysis, you can pinpoint a potential data breach and remediate faster and more effectively.

Condense and easily review critical data

Daily Log Review provides a system that condenses huge logs of data from the system network and managed devices so it's easier to digest and separate normal activities from suspicious activities.

Improves security and system awareness

Daily Log Review improves security through increased system awareness and the recording of abnormalities. These same records can supply the digital evidence of computer hacking, data theft or business fraud should such an event occur.

How is Daily Log Review Configured?

A simple, dependable software solution

Otava deploys our real-time log review platform to review logs from your managed devices.

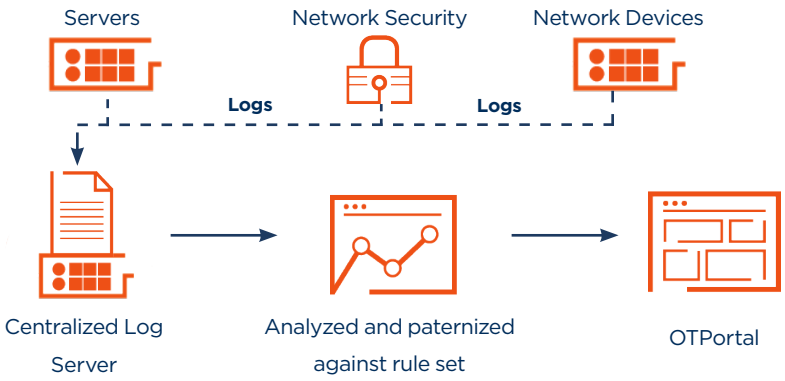
Monitoring

Otava's Daily Log Review solution, based on OSSEC from Trend Micro, monitors, identifies trends and recurring issues, and records log activity and events. Reports are retained by Otava for 12 months.

Reporting

Reports of daily log reviews will be available monthly in our client portal, OTPortal®. In compliance with PCI requirement 10.7, Otava maintains up to a year of archived messages.

How Daily Log Review Works



Otava's Daily Log Review and Compliance

PCI DSS

PCI requirement 10.6 requires log review:

Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).

PCI requirement 10.3 mandates that you must:

Record at least the following audit trail entries for all system components for each event – including user ID, type of event, data and time, success or failure indication, etc.

PCI requirement 10.7:

Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).

HIPAA

HIPAA §164.308(a)(5)(ii)(C)- HIPAA Security Standards Administrative Safeguards:

Requires the ability to monitor log-in attempts and reporting discrepancies.

HIPAA §164.308(a)(5)- Security Awareness and Training Standard:

Log-in monitoring requires tracking failed log-in attempts to make workforce members aware of password management and system use.

Sarbanes–Oxley (SOX)

SOX requirements (Sec 302 (a)(4)(C) and (D):

Logging user access to systems and sensitive data contributes to the level of internal controls assurance mandated by SOX.

Otava's Daily Log Review Benefits:

- **Easily review log data through a system that condenses and analyzes data for you.**
- **Detect system and network changes earlier, instead of auditing devices after an issue is raised.**
- **Be more proactive in preventing and resolving issues.**
- **Decrease your risk of security breaches, malware, loss and legal liabilities.**

OTAVA
EXPECT EXCEPTIONAL

OTAVA provides secure, compliant hybrid cloud solutions for service providers, channel partners and enterprise clients. By actively aggregating best-of-breed cloud companies and investing in people, tools, and processes, Otava's global footprint continues to expand. The company provides its customers with a clear path to transformation through its highly effective solutions and broad portfolio of hybrid cloud, data protection, disaster recovery, security and colocation services, all championed by its exceptional support team. Learn more at www.otava.com.

READY FOR IMPROVED COMPLIANCE & ADDED SERCURITY OF DAILY LOG REVIEW?
Talk to a specialist now.

OTAVA.com (877) 740-5028 solutions@otava.com