



OSSEC (Open Source Security) is a powerful open source host based intrusion detection system that was developed to detect and prevent malicious activities on systems. It can monitor all kinds of environments such as Windows, Mac OS X, Linux, and Solaris systems.

OSSEC consists of 3 components: the manager, the agent and the local OSSEC server.

1. The manager is responsible for the agents that monitor the activity on the systems and report back to the manager. The manager then compiles the reports, and finally combines them with any rules, tests or alerts if there are any security issues.
2. The agent monitors the systems to catch any changes or anomalies throughout the traffic that could possibly be a malicious attack; they also look for unauthorized changes to files or configurations that could indicate a breach of security.
3. The local OSSEC server is responsible for analyzing data from the agents and taking action based on what is detected. This looks like sending out alerts, blocking traffic, performing forensic analysis and within the company.

OSSEC is considered an invaluable asset for organizations looking to secure their networks from threats both outside and within the company.

Resources:[

 [OSSEC Variants \(OSSEC/WAZUH/ATOMIC\)](#)]( [OSSEC Variants \(OSSEC/WAZUH/ATOMIC\)](#) "smartCard-inline")