The AlienVault Logger

Security organizations must protect the infrastructure from a rapidly evolving threat landscape and ensure compliance — all while conforming to demanding service level requirements.

- **FORENSIC CONSOLE FOR INCIDENT INVESTIGATION**
- **DIGITALLY SIGNED LONG TERM LOG STORAGE FOR REGULATORY COMPLIANCE**
- **HORIZONTALLY-DISTRIBUTED SCALABILITY WITH ACCESS FROM A SINGLE CONSOLE**

Logging is an important security capability; however it alone does little more than enable forensics and compliance reporting. AlienVault's Logger, together with the Sensor and Server components, provides more comprehensive and effective security than standalone logging products in meeting increasingly demanding security and compliance requirements.

The Logger is the secure data archival component of the Unified Security Management (USM™) platform. USM enables you to more easily and efficiently configure, manage, and operate the five essential security capabilities that no company should be without: Asset Discovery, Vulnerability Assessment, Threat Detection, Behavioral Monitoring, and Security Intelligence / SIEM. Unifying these essential security capabilities within a single platform simplifies management and reduces complexity, allowing you to spend more time securing the network and less time learning, deploying, and configuring tools.

AlienVault's Logger performs a simple, but critical, task – it forensically stores all of the logs an organization produces. Regardless of the numerous compliance obligations to maintain raw log data, it is important for forensic purposes to have full visibility into the historical record. The AlienVault Logger stores information according to strict security market standards. It collects data in its native format, digitally signs and time-stamps the data, and securely stores the raw format, preserving data integrity. You can easily navigate and isolate data of interest through the integrated search function.

Logger stores large volumes of data while ensuring its admissibility as forensic evidence in a court of law. Data transport can further be forensically secured by implementing encrypted tunnels between the Logger and the event source. AlienVault Logger supports most common encryption schemes and includes the OpenVPN client for use on network hosts.

At times forensic analysis triggers research on a related event or changes to current security practices. Logger enables forensic analysis and is fully integrated into the AlienVault Unified Security Management platform making for seamless access to historical log data from the same interface as incident management, vulnerability assessment, behavioral monitoring, and threat detection.

	FEATURE	BENEFIT
LOGGER	Digitally signed storage	Ensures admissibility as forensic evidence in a court of law.
	5:1 compression[1]	Reduces storage costs.
	Integrated Search	Easily find data of interest.
	Central Retention Policies	Enforce corporate or regulatory data retention requirements.

CONTACT US TO LEARN MORE

WWW.ALIENVAULT.COM

[1] 5:1 compression ratio is the average experienced by our customers. Actual compression may be higher or lower depending on specific log data.