AlienVault® USM Appliance Logger

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

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

The USM Appliance Logger is the secure data archival component of the USM Appliance™ 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, Intrusion Detection, Behavioral Monitoring, and Security Information and Event Management (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 USM Appliance Logger performs a simple, but critical, task – it forensically stores all of the logs your organization produces. In addition to the numerous compliance requirements related to maintaining raw log data, it is important for forensic purposes to have full visibility into the historical record. The USM Appliance 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.

The USM Appliance Logger stores large volumes of data while ensuring its admissibility as forensic evidence in a court of law. You can further increase the security of your data transport by implementing encrypted tunnels between the USM Appliance Logger and the event source. The USM Appliance Logger supports most common encryption schemes and includes a VPN client for use on network hosts.

At times, forensic analysis triggers research on a related event or changes to current security practices. The USM Appliance Logger enables forensic analysis and is fully integrated into the USM Appliance platform, giving you seamless access to historical log data from the same threat management console as asset discovery, vulnerability assessment, intrusion detection, behavioral monitoring, and SIEM.

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.

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