# AlienVault & Splunk: *Which should I be purchasing?*

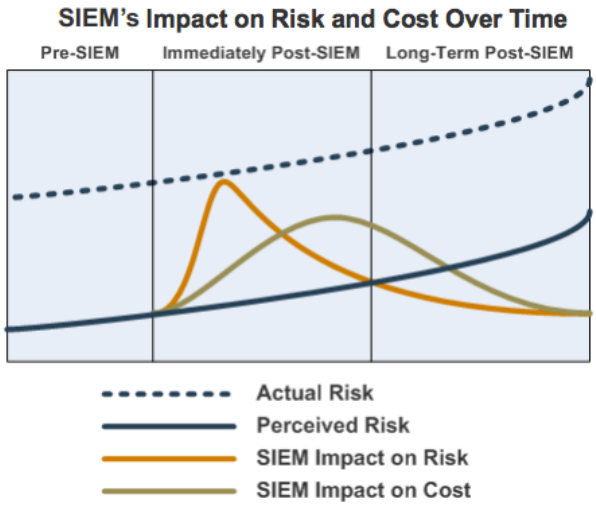
**About AlienVault**
**Founded:** 2006
**Headquarters:**
**Global:** San Mateo, California
**EMEA/APAC:** Cork, Ireland
**Ownership:** Privately held
**Customers:** 5,500+
**Employees:** 115+

It's a great question, and one AlienVault gets all the time. **The purpose of this document is to offer an overview as to why you, the operator, might invest in one OR the other as well as why you might buy one AND the other**. To offer a complete picture it has been valuable for some customers to provide context around the SIEM market and how AlienVault and Splunk truly differentiate from those in the SIEM category.

## What's wrong with SIEM?

Many IT security teams have made a significant investment in both money and people to support a traditional SIEM, only for the SIEM to fall short of vendor promises and never be fully deployed. The reasons for the broken promises are numerous. They are often tied to the dated architectures of traditional SIEMs, which typically use a SQL database with a fixed schema. This database is a single point of failure with scale and performance limitations. Customers with failed SIEM deployments commonly complain that it is difficult to get data into the SIEM and that queries can take hours to run, often never finishing. To get around performance issues, SIEM vendors often sell one product for raw logs and yet another product with a SQL database containing a subset of this raw data for SIEM use cases. This "data reduction" process inevitably hampers future incident investigations or advanced threat detection, when all the original data is needed to get to the root cause or to find the tiny fingerprints of an advanced threat. This unfortunately is only the beginning. Further issues that plague SIEM vendors include:

1. **Implementation and tuning** – It is difficult to strike the right balance between correlation rules that catch all possible attacks and correlation rules that produce too many false-positive alerts. Tuning often requires a professional services engagement and on-going expenses, and industry analysts report speaking with customers for whom, "...a year of tuning was required". This will continue to plague the SIEM vendors as the complexity of managing all of the moves, adds, edits to the data sources that feed them is not



something they can solve for. (Figure 1 right). The risk that organizations feel is real…as the threats are very real. The reality is that the "perceived" threat is much less than the "actual" threat. Scary right? The dirty little secret in the SIEM industry is that most SIEM solutions have a shelf life of approximately 18-24 months before organizations give up on the promise of SIEM and unfortunately look for another SIEM solution. It's NOT the SIEM solution. It's the inability of organizations to Implement and Tune that threatens the long-term value of SIEM.

2. **Trending and analytics** – *If the tuning doesn't get you the failure of consumable analytics will*. SIEMs often have a selection of canned reports but new report creation is not flexible enough to adjust to changing conditions. Canned reports can be useful, and may look great initially, but relying on a canned report to understand the end-to-end implications of a security event from the edge router to the application simply doesn't work.

3. The **"Rules-based" approach** – When a correlated security event is presented to the security analyst, it's reasonable to expect the analyst to limit his or her investigation to the data sources reported by the alert. A "Rules-based" approach supports only a go-forward view of security data, ***if you get a correlation rule wrong***, you can't adjust the model and re-analyze the data, because events that didn't match the old rule have already been discarded. Not the desired outcome… certainly not for what these SIEM solutions cost.

4. **Cost** – SIEM is expensive. It's expensive because large enterprise organizations continue to pay hefty prices for these solutions. SIEM has in most cases been cost-prohibitive for the mid-market customer who is looking to also secure their organization. Costs associated to:

   - ✓ Initial Licensing Costs
   - ✓ Implementation / Optimization Costs
   - ✓ Ongoing Management Costs
   - ✓ Renewal Costs
   - ✓ Integration of all the security technologies
   - ✓ Training of personnel/incoming personnel

   The hidden costs are what usually result in the demise of the traditional SIEM strategy; the painful issue of **resourcing**. The very real costs associated to deploying, integrating, using, tuning, *cursing*, and potentially expanding the deployment.

These are the areas that have led to such dissatisfaction with the traditional SIEM approach. These are very real and evident in almost every organization who has had experience with SIEM. AlienVault only had to listen to its customers to know that something had to change. This was the primary driver in introducing Unified Security Management (USM).

## So "What is difference" between SIEM and Unified Security Management (USM)?

The answer is really in AlienVault's approach. What we can all agree on is despite the Billions (with a "B") being spent every year on security these things hold true:

- More and more organizations are finding themselves in the crosshairs of various bad actors for a variety of reasons, most often to steal money, IP or smear one's reputation.
- The "security arms race" cannot continue indefinitely as the economics of securing your organization is stacked so heavily in favor of those launching the attacks that incremental security investments are seen as impractical.
- 32% of those who have purchased a SIEM are/would consider replacing their existing SIEM solution for a better cost-savings (time and money).
- 44% of those leveraging SIEM solutions suggest that their SIEM lacks integration with other products and that correlation is far too difficult to manage and maintain.

So as an organization, what options do you have OTHER than SIEM?

IT organizations of all shapes and sizes have embraced Unified Security Management (USM) to reduce the cost and accelerate security visibility & threat detection. Customers need access to security solutions that offer significant time to value while increasing their overall security posture. At AlienVault we're committed to unifying best-of-breed technology with shared intelligence for a truly open and collaborative security. AlienVault's Unified Security Management™ (USM) platform gives organizations a solution that stands up to the most sophisticated, expensive, enterprise-level security products. Unlike any other security solution on the market, AlienVault's USM platform has dramatically reduced the cost and complexity related to buying and deploying all of the essential security controls required for comprehensive security visibility. This is what that looks like. All 5 essential security capabilities provided in a Unified platform we call USM.

AlienVault offers the only unified security management solution to unify the five essential security capabilities you need for complete security visibility. This translates into rapid time to value – faster and easier audits, targeted remediation, and more seamless incident response.


## "One Splunk. Many Uses" – But Security?

At the simplest level, Splunk gives you a single interface to search, report, and alert on all your IT data, across your entire IT infrastructure. Splunk can be applied to any unstructured data. Organizations use it for things as diverse as web analytics, telecoms call records, and earthquake data. On the fly you can assemble search results into larger and more familiar concepts like 'ip

addresses' or 'failed transactions', and from there you can calculate statistics and email people pretty charts. So how does that fit into the security discussion? Security is one of the use cases, but not the principle focus of Splunk.

Splunk allows the user to quickly work with all machine data without filtering or reduction. Events are stored in flat files using a real-time indexing algorithm invented specifically for IT data, and users issue queries in a natural search language with a rich layer of analytical commands. The mechanism of search supports the ability to extract knowledge from events, create visualizations, alerts, and dashboards and enable real-time data capture and display. Splunk can collect data in any format, without requiring parsers or connectors. Get all the data including custom application logs and other non-traditional data sources including registry changes, performance metrics, process tables, and file system changes.

Given this explanation, this is why we often see organizations leveraging Splunk AND AlienVault. So if we were to focus on the Security Use Case here's how Splunk would compare with AlienVault.

| **Capability** | **Technology** | **AlienVault** | **Splunk** |
|---|---|---|---|
| **Asset Discovery** - Discover and track hosts, services, and installed software present in the environment for improved correlation and context for incident response | | ✓ | * |
| | **Passive Network Discovery** - identify hosts with passive network monitoring | ✓ | * |
| | **Active Network Scanning** - actively scan the network to identify and version running services without local access to the machine | ✓ | * |
| | **Host-based Software Inventory -** provide full binary-level inventory of software packages running on assets | ✓ | * |
| **Vulnerability Assessment -** identify vulnerabilities in the monitored environment and track historical record for compliance purposes | | ✓ | * |
| | **Continuous Vulnerability Monitoring** - using data from the asset discovery capabilities, correlate the latest known vulnerability feeds with the existing asset inventory information to identify vulnerable services without active scanning | ✓ | * |

| | | | |
|---|---|---|---|
| | **Active Network Scanning** - actively scan the network to identify vulnerable services. Both authenticated and unauthenticated scanning are available depending on the target. | ✓ | * |
| **Threat Detection** - monitor the environment for threats, identifying known attack vectors, attack patterns, payload signatures and behavioral identification of exploits and malware. | | ✓ | * |
| | **Network IDS** - perform deep-packet inspection of the network traffic in order to identify attacks, behaviors of compromised systems, policy violations, and more. | ✓ | * |
| | **Host-based IDS** - monitor the operating system level activity of a host to identify indicators of compromise, such as rootkits, malware, or abuse of system services | ✓ | * |
| | **File Integrity Monitoring -** monitor changes to critical files to identify potential security issues on critical hosts. | ✓ | * |
| | **Wireless IDS** - monitor environments for rogue access points to identify potentially unauthorized access to networks. | ✓ | * |
| **Behavioral Monitoring -** monitor the ongoing behavior of observed systems to provide context for forensic investigation and identification of potential security incidents | | ✓ | * |
| | **Netflow Analysis** - identify network activity throughout your environment. Identifies protocol usage, and volume of traffic between hosts in monitored environments. | ✓ | * |
| | **Service Availability Monitoring** - identify service availability in the environment to detect disruptions in availability, which could indicate a successful attack or compromise. | ✓ | * |

| | | | |
|---|---|---|---|
| **Security Intelligence** - aggregate and analyze information from all the security controls and environment in order to correlate disparate behavior and provide a platform for forensic investigation. | | ✓ | ✓ |
| | **Log Management** - provides a consolidated interface for reporting and querying activity occurring in the monitored environments. Critical for most compliance use cases. | ✓ | ✓ |
| | **Correlation Engine** - performs correlation across disparate data sets to identify malicious activity in the environment. Generates alarms on Environment Information, Reconnaissance and Probing, Delivery and Attack, Exploit and Installation, and System Compromise. | ✓ | ✓ |
| | **Reporting Engine** - a customizable engine to generate status and compliance reports based on the information in the system. | ✓ | ✓ |
| **Threat Intelligence** - emerging threat analysis and research which leverages more than 9,500 global collection points across more than 140 countries, within the world's largest crowd-sourced threat intelligence exchange. | **Includes:** event correlation rules, IDS signatures, asset inventory and vulnerability database updates, reporting modules and templates, as well as dynamic incident response templates with "how to" guidance on how to investigate threats. | ✓ | * |

***Further clarification of the chart above:***

**Correlation.** Splunk correlates using a powerful search language. This serves as a distinct advantage of traditional SIEM vendors like ArcSight, Q1, or Nitro, etc. These rules that might take hours or days to build might only take 15 minutes in Splunk. Great feature; however compared to AlienVault, Splunk and those very same SIEM vendors have serious limitations. As an example, the way AlienVault tiers the correlation rules to generate a staged alert is not something Splunk can do. These same 'tiered' alerts prove near impossible within the SIEM community. These products simply doesn't work that way. This is critical if security is your objective. This is not a knock on the Splunk solution necessarily is you keep in mind that Splunk was never meant to be a security solution. Security is only a use-case and this serves as a serious gap. Most log management solutions follow suit in trying to make the leap to provide security; however it becomes obvious when the product lacks the DNA to deliver against even fairly basic security problems.

**Asset Management.** Splunk does have a simplistic asset and identity correlation engine built in to their security product. It allows them to capture basic asset information through integration with LDAP or other identity and access management systems and correlate along those dimensions when reporting on, analyzing, or generating alerts on data patterns. The often over-looked problem is that this is really just a lookup table on the backend. It's not terribly secure and is hard to maintain relationships with other entities. The asset system in AlienVault is far superior as security largely relies on the operators understanding of the assets in their environment hence a major area of focus for AlienVault.

## A difference in Licensing (i.e. "Cost")

Splunk leverages a volume-based or index-based licensing model. Volume or indexed-based licensing models mean that the license size will be determined by a metric that will vary based on network, server and application activity. Normal activity can generate multiple Gigabytes of log data. As you might imagine, if you have a substantial amount of log data ~ Splunk get's very expensive. This cost can also be very elastic (unpredictable) depending on how dynamic your environment is. AlienVault leverages a perpetual licensing model that means you're only making investments in the solution year one (1) and then paying for support and maintenance moving forward. This model is highly predictable which is always more appealing to an organization.

## Threat Intelligence vs "BYOI" (Bring Your Own Threat Intelligence)

With Splunk, "security" includes about eight threat feeds out of the box. They can be updated periodically by pulling down the feeds from various Internet sources. Once in Splunk they are stored as a lookup file. Once they are in a lookup file they are available in any search, report, or correlation. Recently, they integrated the product with a reputation product called Norse Corp. The feed provides reputation-based information about Internet IPs. This is what AlienVault refers to as "BYOI" (Bring our own intelligence) as without threat data, you're leaving yourself in a very reactionary mode. AlienVault's Open-Threat-Exchange becomes a game-changer for most organizations as behind all the threats that are collected all over the world, AlienVault provides a team of engineers that are solely responsible for curating, maintaining, and expanding the intelligence and distributing it to all users of the AlienVault solution – so you don't have to be exposed to the issue prior to solving for it. Hugely advantageous for AlienVault and the customers that they serve.

## What specifically is AlienVault's Threat Intelligence/Labs?

AlienVault Labs Threat Intelligence maximizes the efficiency of your security-monitoring program, by delivering the following directly to your AlienVault Unified Security Management (USM) installation. This team of security experts delivers the following every 30 minutes:

- Weekly updates that cover 8 coordinated rule-sets:
    - Network-based & Host-based IDS signatures – which detect the latest threats in your environment.
    - Asset discovery and inventory database updates – identifies the latest OS'es, applications and device types
    - Vulnerability database updates – dual database coverage to find the latest

vulnerabilities on all your systems

- Event correlation rules – translation of raw events into actionable remediation tasks.

- Report modules and templates – providing new ways of viewing data in your environment

- Incident response templates / "how to" guidance for each alarm in USM

Traditional SIEM solutions would leave all this work up to you. AlienVault understands that most organizations don't have the time, resources or expertise in house to develop, manage and monitor all of these areas of their environment. With this easily consumable threat intelligence fueling your USM platform, you'll be able to detect the latest threats and prioritize your response efforts. Specifically, you'll extend your security program with:

- **Real-time botnet detection –** identifies infection and misuse of corporate assets
- **Data exfiltration detection –** prevents leakage of sensitive and proprietary data
- **Command-and-control traffic (C&C) identification –** identifies compromised systems communicating with malicious actors
- **IP, URL, and domain reputation data –** prioritizes response efforts by identifying known bad actors and infected sites
- **APT (Advanced Persistent Threat) detection –** detects targeted attacks often missed by other defenses
- **Dynamic incident response and investigation guidance –** provides customized instructions on how to respond and investigate each alert

## Point Solutions for Log Management – Not for Security

This is where AlienVault further differentiates in approach and strategy that organizations might choose to take. Point solutions for log analysis and log management are very good at data management; none better than Splunk. Rather than producing the data that contributes to the full context of threat analysis (asset info, vulnerability data, IDS, Netflow, etc.), Splunk relies upon the quality and content of the logs that are delivered to them. If you don't have these logs; Splunk can't help you. You'll need to go out and make those point purchases in order to leverage the data management/correlation engine that Splunk delivers. In other words, to deliver the same set of functionality as AlienVault's USM, these tools would require YOU to integrate the log data of asset discovery tools, vulnerability scanners, netflow analysis tools, IDS tools, and then have the event correlation analysis in place to make sense of it. AlienVault doesn't believe that should be your responsibility or problem to tackle. Even the largest organizations in the world today struggle with this as all of these point solutions simply don't play nicely together.

Most pure play log analysis and log management tools lack event correlation and threat intelligence, relying on the customer to decide how they want to translate the raw log data. These tools, like Splunk, may have impressive storage capabilities and fast query times, but they expect you, the customer, to know what questions to ask of the log data, or under what conditions to trigger an alert. There are limited event correlation rules, policies, and directives

to make sense of it all.  For example, compared to the 1500+ event correlation rules provided in AlienVault's USM engine, Splunk only offers about 50.  And these aren't curated by a security research organization like AlienVault Labs, because Splunk lacks one.

At AlienVault, we believe that open and collaborative is the best way for all companies to gain the security visibility they need. Built on proven security controls and updated continuously with the latest threat intelligence, AlienVault's Unified Security Management (USM) platform provides a complete, simple and affordable way for organizations with limited security staff and budget to address compliance and threat management. With the essential security capabilities already built-in, USM puts enterprise-class security visibility within easy reach of security teams who need to do more with less. For more information visit **www.AlienVault.com** or follow us on Twitter.