AlienVault Competitive Comparison:
SolarWinds LEM (TriGeo)

Your Success is Our Mission!

"SolarWinds LEM or Alienvault USM--Which is right for me?"
We sometimes get asked by our customers to compare SolarWinds LEM to our USM platform. While this document is titled "competitive analysis", it is truly intended to illustrate the significant differences between SolarWinds Log & Event Manager (LEM) vs. AlienVault's Unified Security Manager (USM) and show that these solutions are very different and not competitive.

Today's Security Landscape
IT security is not a luxury; it's a necessity. That said, the challenge that almost every IT department faces is how to improve security with limited resources--budget, time, and staff. And, even those rare organizations with seemingly unlimited budgets and staff are too often finding themselves victims of attacks and becoming front-page news. The question so many IT professionals ask is "if those well-funded organizations struggle to secure their networks; what chance do the rest of us have?" It's a great question, and is exactly why AlienVault has become the market leader in helping organizations with limited resources secure their networks.

The issues associated with improving security visibility and accelerating threat detection and response are complex, and have frustrated organizations of all sizes for years. Solving those challenges requires a fundamentally different approach to deploying security technologies, especially for those organizations that are perpetually under-resourced.

We created this document to help you sort through the confusion that many SIEM (Security Information and Event Management) vendors and even log management vendors like SolarWinds have created around the topic of security visibility and threat detection. This document will clear up the confusion by examining how SolarWinds LEM (Log and Event Manager) and AlienVault's USM (Unified Security Management) are fundamentally different in five key areas:

- Security DNA
- Functionality
- Threat Intelligence
- Training / Education / Services
- Deployment Flexibility

SECURITY DNA
It's important to understand how the core competencies of an organization influence its collective behavior, its investment strategy, and ultimately what it delivers to the market.

SolarWinds

- SolarWinds acquired TriGeo. which offered a log management product, in June 2011. The

log management product is just one of many technologies acquired by SolarWinds. The SolarWinds team took this log management product and began to call it a SIEM to increase the total addressable market. Check the SolarWinds web site and you'll see that "SIEM" and "LEM" are used interchangeably in the SolarWinds documentation and website.

- SolarWinds' roots are in network and application management, not security. SolarWinds has failed to maintain its status in the Gartner SIEM Magic Quadrant, falling the bottom left quadrant with other "Niche Players". With more than 35 technologies in its product portfolio, almost all of which address network and application availability and performance, SolarWinds' core competence is not security.
- That being said, if you're looking for log management and not security visibility, threat detection or regulatory compliance – LEM may be a good option for your organization. And, if your organization is looking for any network or application-related solution, SolarWinds is at the very top of the value chain and should strongly be considered.

AlienVault

- AlienVault was founded in 2007 with a vision for a crowd-sourced approach to security visibility and threat detection. We brought the USM platform to market after seeing that the "security arms race" wasn't sustainable--organizations were making massive investments in technology and staff, and gaining only incremental gains in security.
- AlienVault's roots are in network security, and USM platform puts built-in, essential security controls and seamlessly integrated threat intelligence, powered by AlienVault Labs and the global Open Threat Exchange, into the hands of IT teams with limited resources. IT or Security practitioners can now deploy a single platform that accelerates threat detection and response by showing what threats are most important and how to mitigate them, on day one. The USM platform puts up-to-the-minute security and threat information about systems, data, and users at your fingertips, giving you complete security visibility and providing you with a unified threat detection and compliance management solution that is both easy-to-use and affordable.
- AlienVault continues to invest heavily in just our USM platform, and as a result is one of the fastest growing companies in the security market. Our focus remains the same since our founding: bring the most robust threat detection, response and regulatory compliance capabilities to organizations with limited resources (as our user community of more than 17,000 [and growing] demonstrates).

FUNCTIONALITY:

The following table illustrates the wide disparity of technology between what's provided in the USM platform and missing in the LEM solution. It's important to note that Log Management solutions aren't expected to have security elements in them. This is less about the deficiencies in the SolarWinds solution than the functions organizations require to have full threat detection and incident response capabilities.

The orchestration (rich integration) of these security applications into the USM platform means that AlienVault threat researchers can deliver high value alerts, alarms and correlation by virtue of the rich contextual data these applications provide. Because we own both the data sources as well as the management platform, our threat experts have a comprehensive understanding of the interactions between the different data types being correlated and analyzed as well as the latest attack techniques. We embed this expertise in the built-in security controls and seamlessly integrated threat intelligence we deliver, to allow you to detect the latest threats as well as instruct you on how to mitigate the

threats quickly and effectively, regardless of your network environment. The unfair advantage we give to organizations, large and small, all revolves around this predictable application security stack.

Capability	Technology	AlienVault USM	SolarWinds LEM
Asset Discovery - Discover and track hosts, services, and installed software present in the environment for improved correlation and context for incident response		**YES**	**NO**
	Passive Network Discovery - identify hosts with passive network monitoring	**YES**	**NO**
	Active Network Scanning - actively scan the network to identify and version running services without local access to the machine	**YES**	**NO**
	Host-based Software Inventory - provide full binary-level inventory of software packages running on assets	**YES**	**NO**
Vulnerability Assessment - identify vulnerabilities in the monitored environment and track historical record for compliance purposes		**YES**	**NO**
	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	**YES**	**NO**
	Active Network Scanning - actively scan the network to identify vulnerable services. Both authenticated and unauthenticated scanning are available depending on the target.	**YES**	**NO**
Intrusion Detection - monitor the environment for threats, identifying known attack vectors, attack patterns, payload signatures and behavioral identification of exploits and malware.		**YES**	**NO**

	Network IDS - perform deep-packet inspection of the network traffic in order to identify attacks, behaviors of compromised systems, policy violations, and more.	**YES**	**NO**
	Host IDS - monitor the operating system level activity of a host to identify indicators of compromise, such as rootkits, malware, or abuse of system services	**YES**	**NO**
	File Integrity Monitoring (FIM) - monitor changes to critical files to identify potential security issues on critical hosts.	**YES**	**NO**
Behavioral Monitoring - monitor the ongoing behavior of observed systems to provide context for forensic investigation and identification of potential security incidents		**YES**	**NO**
	Netflow Analysis - identify network activity throughout your environment. Identifies protocol usage, and volume of traffic between hosts in monitored environments.	**YES**	**NO**
	Service Availability Monitoring - identify service availability in the environment to detect disruptions in availability which could indicate a successful attack or compromise.	**YES**	**NO**
SIEM - aggregate and analyze information from all the security controls and environment in order to correlate disparate behavior and provide a platform for forensic investigation.		**YES**	**NO**
	Log Management - provides a consolidated interface for reporting and querying activity occurring in the monitored environments. Critical for most compliance use cases.	**YES**	**YES**

	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.	**YES**	**NO**
	Reporting Engine - a customizable engine to generate status and compliance reports based on the information in the system. Includes over 150 customizable, preconfigured reports and over 2,200 report elements you can use to create custom reports.	**YES**	**NO**
Threat Intelligence - emerging threat analysis and research which leverages more than 26,000 participants 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 and respond to threats.	**YES**	**NO**

THREAT INTELLIGENCE

Time is of the essence when protecting your organization's critical information assets against cyber threats. The process of finding security intelligence that matters to your organization can consume precious time and strain in-house resources already stretched too thin. Whether it is up-to-date information about IP addresses communicating with their systems, correlation rules that link seemingly random events to indicate potential compromise, or detailed analysis of the latest attack techniques, IT teams need relevant, actionable security intelligence. Additionally, today's security tools are very effective at generating a steady stream of alerts about important (and not so important) activity. IT teams without deep security expertise are then required to conduct research into each alert to understand its significance and criticality, and what to do about it.

At times, days or even months can pass before you have time to conduct even routine activities like deploying patches to remediate known vulnerabilities in your environment. This delay increases your business risk and expands the window of exposure, increasing your chances of being victim to a successful exploitation of that vulnerability Having a partner who can deliver actionable threat intelligence is critical to securing your environment and achieving compliance.

SolarWinds

- SolarWinds has no threat intelligence, which fundamentally suggests that this is not a true security solution, but rather a log management solution. SolarWinds LEM provides statistical

analytics which is largely meaningless when looking to identify and respond to those threats that are imminent in one's environment. This gap alone renders it nearly useless for the purpose of security and threat detection. Created to monitor user activities rather than external threats, Log Management products (including LEM) have been in the market for some time. Unfortunately log management isn't enough if security/compliance is your goal.

AlienVault

- AlienVault has changed the way companies approach the topics of threat intelligence and threat detection. We did this by first with OTX, the world's most authoritative crowd-sourced threat intelligence exchange. AlienVault Open Threat Exchange (OTX) is an open threat information sharing and analysis network, created to put effective security measures within the reach of all organizations. Unlike invitation-only threat sharing networks, OTX provides real-time, actionable information to all who want to participate. The Open Threat Exchange facilitates global threat sharing and collaboration of data on emerging threats between all participants in the community.
- The fidelity of our threat data has caused other security companies to want to participate in AlienVault's threat intelligence program. These companies include Intel Security (McAfee), HP, and many others. Our threat exchange is leveraged by major financial institutions, the US DoD, Intelligence communities and many of the largest companies in the world.
- AlienVault Labs threat research team spends countless hours mapping out the different types of attacks, the latest threats, suspicious behavior, vulnerabilities and exploits they uncover across the entire threat landscape. They leverage the power of OTX to provide global insight into attack trends and bad actors. The AlienVault Labs Threat Intelligence publishes threat intelligence updates to the USM platform that includes correlation directives, IDS signatures, vulnerability audits, asset discovery signatures, IP reputation data, data source plugins, and report templates.
- The automation of this threat intelligence means that your organization can consume and take action on this information to detect threats in real-time. Every 30 minutes you receive proactive, actionable intelligence tailored to your environment:
    - Clear, concise threat and vulnerability analysis
    - Detailed remediation information and recommendations
    - Consultation with our threat experts
    - On-demand access to extensive threat and vulnerability databases used by the largest and most advanced security companies around the world.

- Your team is not left with the responsibility of constantly tuning your SIEM to the constant changes to your internal network or the ever-evolving threat landscape. AlienVault provides Log Management plus Asset Discovery, Vulnerability Assessment, Threat Detection, Behavioral Analysis, and Security Intelligence. These integrated features are powered by up-to-the-minute threat intelligence from AlienVault Labs and our Open Threat Exchange. AlienVault offers the only Unified Security Management solution to unify these five essential security capabilities. With essential security controls built-in, AlienVault USM puts complete security visibility within fast and easy reach, which translates into rapid time to value.

TRAINING / EDUCATION / SERVICES

Customer training and certification is an essential aspect of any technology acquisition, because it gives

customers the tools they need to be successful. By not investing in training and education programs for customers, a vendor is making it more difficult for you to secure your organization from threats and breaches. Organizations that have been trained on technology products are on average 30% more proficient and their return on investment is significantly faster than those not trained.

SolarWinds
SolarWinds does not offer formal training, education or certification for its LEM solution. You will need to seek out a third party to get training or certified on the product.

AlienVault
AlienVault understands that product training and certification are fundamental to placing your team in the very best position to protect your organization's resources, reputation, and intellectual property. With this understanding, AlienVault provides training at NO cost to all customers who purchase our Unified Security Management solution. This training is a one-day course that can be taken within the first 30 days of purchase. You can also purchase a five-day training course (delivered at the customer premise or "Live-Online") that helps organizations of all sizes to quickly detect and effectively respond to the latest threats. And, if you want to demonstrate your expertise, you can earn certification through online testing or at testing centers worldwide. Led by security professionals, AlienVault training classes provide the instruction and hands-on practice needed to design, install, deploy, configure, and operate our USM products.

Need help deploying or customizing your deployment from your vendor? Only AlienVault offers deployment services without requiring you to have to sub-contract with another vendor for these services. We stand behind everything we do.

DEPLOYMENT FLEXIBILITY
The last topic to discuss is the deployment of your LEM or USM instance. Although deployment flexibility is often overlooked during the evaluation process, it is a relevant (and even critical) factor to consider, depending on the location of the assets you want to monitor/manage. For example, while most organizations have on-premise assets (for example, in a datacenter or remote location), many have migrated some portion of their assets to the cloud while others have embraced virtualization.

Some questions you should ask yourself to determine your deployment requirements:

- Do you anticipate having applications that need to be monitored in the cloud?
- Do you anticipate needing a hardware appliance that can be managed by your vendor?
- Do you anticipate needing to move from a virtual appliance to a cloud appliance, or from a physical appliance to a virtual appliance?

SolarWinds
SolarWinds offers its LEM solution in a virtual appliance only. There are no hardware options and no cloud options for LEM.

AlienVault
Only AlienVault offers a very extensible solution to help you meet today's requirements (as well future requirements) with the freedom to exchange deployment types, without incurring additional fees. Think you will move from a virtual appliance to a physical appliance? Do you have changing preferences or anticipate future network expansion? All can be accommodated by AlienVault.

ABOUT ALIENVAULT

AlienVault's mission is to enable organizations with limited resources to accelerate and simplify their ability to detect and respond to the growing landscape of cyber threats. Our Unified Security Management (USM) platform provides all of the essential security controls required for complete security visibility, and is designed to enable any IT or security practitioner to benefit from results on day one. Powered by threat intelligence from AlienVault Labs and the AlienVault Open Threat Exchange— the world's largest crowd-sourced threat intelligence network — AlienVault USM delivers a unified, simple and affordable solution for threat detection, incident response and compliance management. AlienVault is a privately held company headquartered in Silicon Valley and backed by Trident Capital, Kleiner Perkins Caufield & Byers, GGV Capital, Intel Capital, Sigma West, Adara Venture Partners, Top Tier Capital and Correlation Ventures. For more information visit www.AlienVault.com or follow us on Twitter.

To learn more, visit: www.alienvault.com