NETWORK TESTING LABS REVIEW

Network Situational Awareness

Lumeta's Enterprise Situational Intelligence (ESI) tells you who's using your network, it identifies rogue or stealthy devices and ESI detects unintended leak paths that bare your network's sensitive data to the outside world.

Executive Summary

Lumeta's Enterprise Situational Intelligence (ESI):

- Accurately discovered every computer, device and route
- Revealed unintended network paths to sensitive data
- Gave us an up-to-date, real-time map of our network
- Identified our IPv6 devices and routes
- Was easier to use

Lumeta's Enterprise Situational Intelligence could not have been easier to set up and configure. Impressively, it used network resources frugally as it discovered our network, profiled devices and identified potential security problems. It easily wins the Network Testing Labs World Class Award for best network-wide situational awareness tool.

Your Changing Network

Your network has become highly dynamic. Mobile devices and endpoint client computers are constantly joining and leaving your company's network. Administrators are making configuration changes to routers and switches. Traffic volumes swell as your servers respond to increasing myriads of data requests.

Most of the activity on your network is legitimate. Employees and company visitors authenticate themselves, act appropriately in making business-oriented inquiries and treat the results with respect.

However, a growing percentage of network activity is illegitimate. Hackers use specialized software tools to crack passwords, defeat firewalls and extract sensitive, valuable data.

Your first line of defense against exposure of sensitive data is intelligence. You need to know who is accessing your network and from where. You also need to know that wireless visitor devices have no network access path to sensitive data.

Two market-leading vendors, Tenable Network Security and Lumeta Corporation, offer network intelligence to help protect your data.

We evaluated Tenable's Nessus Enterprise 6.1 and Lumeta ESI 2.1 in both our Alabama network laboratory and at various customer sites to find out which one is best and that we could recommend to you.

Tenable licenses its Nessus Enterprise product as a model 100 or 200 hardware appliance, an Internet-based managed service or as a virtual machine for Microsoft HyperV and VMware environments. Tenable's components are Nessus Enterprise, a Passive Vulnerability Scanner (PVS) and a SecurityCenter central console.

Key Findings and Conclusions

- Lumeta ESI's device discovery was more accurate
- Lumeta ESI used the network more frugally
- Lumeta ESI's reports and graphs clearly revealed network activity
- Lumeta ESI showed us leak paths to sensitive data
- Lumeta ESI and Tenable Nessus Enterprise are complementary

Similarly, Lumeta licenses ESI in the form of an appliance, a virtual machine and an Amazon AWS Cloud service.

Lumeta ESI's superior device discovery, its clear, comprehensive reports and its leak path detection earned ESI top honors in this review. Lumeta ESI wins the Network Testing Labs World Class award for best network situational awareness product.

Discovery

ESI's device discovery was more accurate than that of Nessus Enterprise, as Figure 1 shows.

Impressively, ESI identified 100% of the devices on the network. In contrast, Nessus Enterprise achieved only a 94% success rate across our tests.

From an enterprise perspective, what do ESI's and Nessus Enterprise's device discovery rates mean? On a network of 100,000 IP addresses, Nessus Enterprise would miss about 6,000 devices.

ESI was especially effective at identifying transient mobile devices on the perimeter of our network.

ESI's discovery of leak paths was a unique feature that further set it apart from Nessus Enterprise in our tests. ESI unerringly alerted us to network paths and connections that inadvertently gave hackers access to our network's sensitive data. We concluded that this one feature alone made Lumeta ESI worth buying.

ESI used a combination of Passive Discovery (listening) and Active Discovery (scanning) to see devices as they joined and subsequently left the network. Passive Discovery used ARP packets, ESI's own analysis of the routing plane, DHCP packets and other network activity to know and understand the breadth and scope of the network. Active Discovery used multi-protocol pings, Time-to-Live (TTL) data and the results from Passive Discovery to "see" all our network's perimeters.

Nessus Enterprise's approach to device discovery used multiple scanning agents scattered across the network to identify devices.

To our delight, in real time, ESI efficiently identified IPv6-enabled devices, found IPv6 network paths, located rogue IPv6 devices and highlighted devices for which IPv6 had been unintentionally enabled.

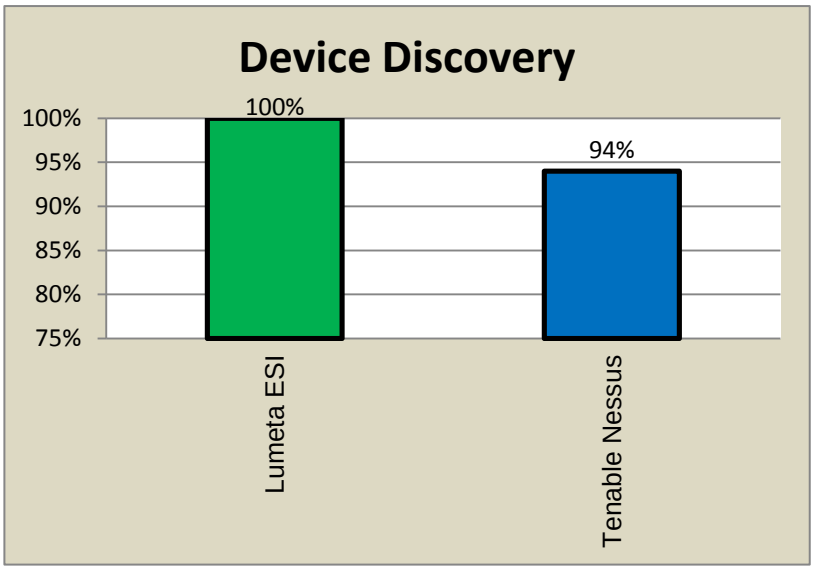


Figure 1. ESI vs. Nessus Enterprise Discovery

Nessus Enterprise also supports IPv6, but, without the extra-cost PVS option, it lacks ESI's ability to deeply probe IPv6 devices for issues and anomalies.

Interestingly, we were able to use the results of ESI's discovery to tell Nessus Enterprise and the Passive Vulnerability Scanner about the farther reaches of our network. The synergistic combination of Lumeta ESI and Tenable Nessus Enterprise gave us the best of both worlds … ESI's accurate device and node discovery plus ESI's own reports, blended with Nessus Enterprise's compliance reports and Nessus Enterprise's malware detection. In fact, we found Nessus Enterprise and the Passive Vulnerability Scanner to be accurately and reliably useful only when used in conjunction with ESI.

Lumeta ESI correctly mapped all subnets and connections to reveal our network's perimeters, including previously unknown (i.e., undocumented) sections of the network. It also identified partner connections and cloud links.

ESI also excelled at identifying newly-created virtual machines. Just as quickly as we initiated a new VM, ESI reported its existence to us.

While Nessus Enterprise also gave us a census of virtual environments, ESI's alerts were more timely and we found them more useful and informative.

ESI's ability to spot and warn us about stealthy VM-based routers – i.e., the configuration of VM network ports (whether intended or not) to allow a VM to act as a network router – was another feature that made Lumeta ESI particularly useful on our network.

Like Nessus Enterprise and its Passive Vulnerability Scanner, ESI identified and reported on network nodes responding to public SNMP queries as well as the existence of expired digital certificates.

Performance

Lumeta ESI was far more frugal than Tenable Nessus Enterprise in its use of the network, as depicted in Figure 2.

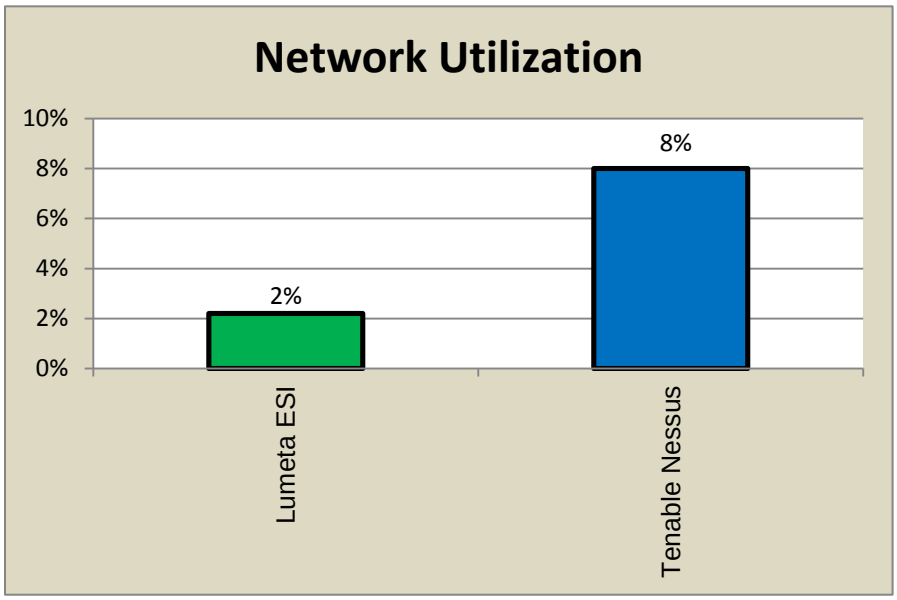


Figure 2. ESI vs. Nessus Enterprise Network Usage

Lumeta ESI's rather intelligent Passive Discovery technology caused absolutely no network traffic whatsoever, and its Active Discovery's network utilization was only 2%. Tenable Nessus Enterprise's scanners caused four times as much network traffic – 8% – yet discovered fewer devices.

Ease of Use

While ESI – based on its continuous discovery of devices, hosts and leak paths – focuses on immediately actionable network data, Nessus Enterprise is more oriented toward compliance reports, such as for Payment Card Industry (PCI) standards and Sarbanes-Oxley. Nessus Enterprise reports track adherence to standards and policies that you set up.

ESI's reports, which can also be used for government and industry standards compliance and auditing, are additionally appropriate for best practices verification through the use of risk metrics that you specify.

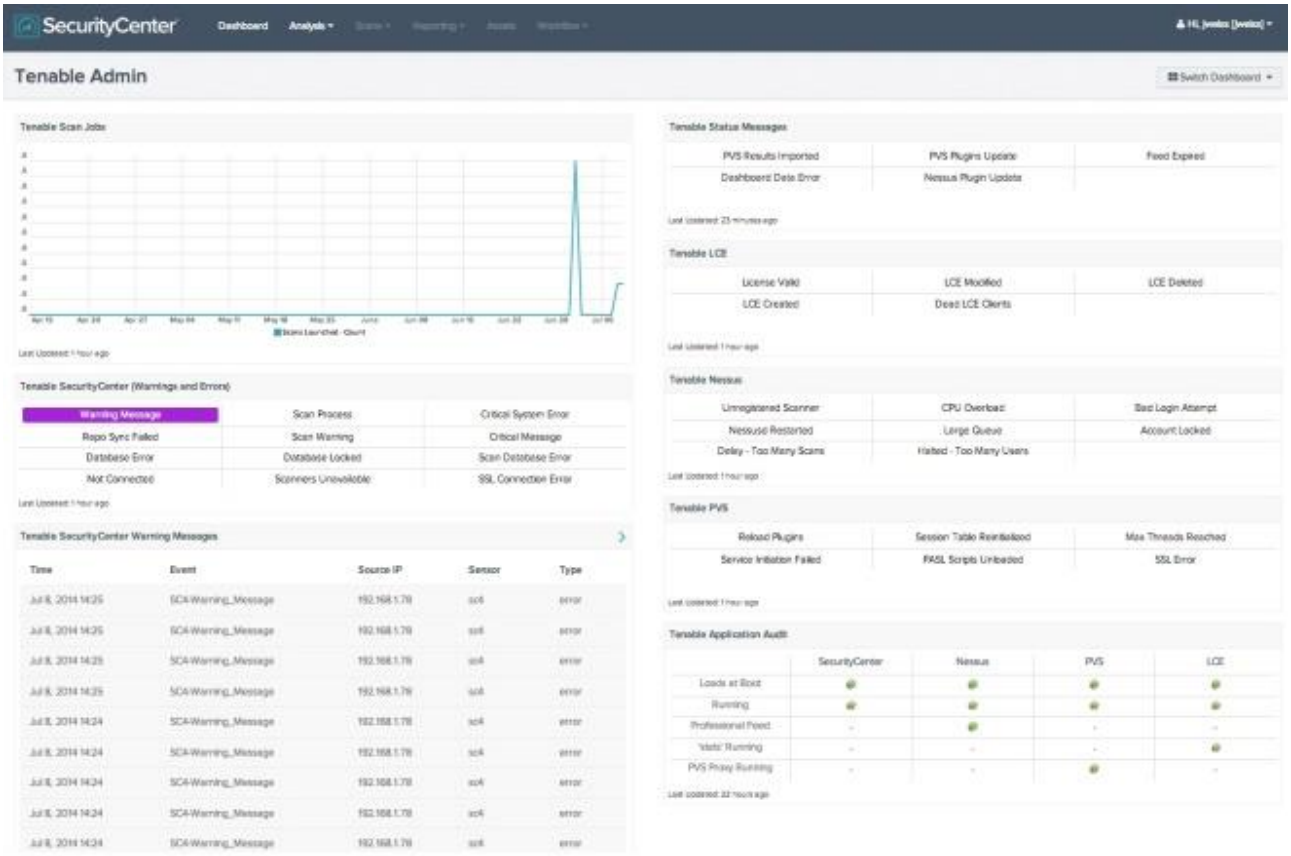
Uniquely, Nessus Enterprise scans individual files for malware by calculating an MD5 hash value or checksum for each file. Nessus Enterprise flags a file as suspicious if its MD5 hash value matches Nessus Enterprise's list of malware MD5 values. However, we found that Nessus Enterprise malware scans were not nearly as accurate nor its list of MD5 malware ID values as up-to-date as, say, those offered by a security vendor like Intel-McAfee.

Both ESI and Nessus Enterprise are quite scalable, capable of deployment across the largest of networks.

ESI's real-time, always-up-to-date, zone-based network map, illustrated in Figure 3, is exactly what a network administrator needs to see when he or she is watching for rogue mobile devices joining or leaving the network. The ESI network map also helps administrators intuitively and clearly understand the network's breadth of devices, connections and configurations.

Figure 3. ESI Network Map

Figure 4. Nessus Enterprise



SecurityCenter

Tenable's Security Center, depicted in Figure 4, reflects a chart of scanner launch times, a number of status, warning and error messages, some Tenable license warning messages and a status report on the overall health of the Nessus Enterprise software.

With ESI's user interface, you designate zones and, within each zone, one or more collectors. A zone might denote "Critical Servers" or perhaps an IP address subnet. A collector uses the protocols you choose, the schedule you set up and the IP address range you specify to examine the network. Each collector can be Passive or Active.

In the Nessus Enterprise /PVS/SecurityCenter interface, you create Policies. Each Policy has five sections of configuration settings: Basic, Discovery, Assessment, Report and Advanced.

The Basic section names the Policy, the Discovery section specifies host discovery and port scanning parameters, the Assessment section contains security-related parameters, the Report section controls how Nessus Enterprise /PVS/SecurityCenter should handle scan results and the Advanced section groups a range of miscellaneous parameters for that Policy.

Setting up and managing ESI's parameters, we found, was an intuitive and easily-navigated process. In contrast, dealing with the Nessus Enterprise /PVS/SecurityCenter interface was cumbersome, confusing, tedious and error-prone.

Moreover, the Nessus Enterprise manual has too many double-negatives, such as "…note that not enabling 'Scan web applications' will not enable the options in the UI."

Licensing

Lower licensing costs are another of Lumeta ESI's advantages over Tenable Nessus Enterprise. Table 1 shows the MSRP for some of each vendor's offerings.

	MSRP
Lumeta ESI virtual machine	$7,200/year for 1,000 IP addresses
Lumeta ESI Saas cloud access	$7,200/year for 1,000 IP addresses
Tenable Nessus Enterprise, PVS and Security Center	$37,000/year for 1,000 IP addresses
Tenable Nessus Enterprise, PVS and Security Center cloud access	$5,000/year for 1,000 IP addresses (plus AWS EC2 charges)

Table 1. Lumeta and Tenable Prices

How We Tested

The testbed network consisted of thirty-five Gigabit Ethernet subnet domains connected by Cisco routers. Our lab's 1,500 clients (endpoints) consisted of computing platforms that included Windows 2000/2003/2012 and Windows Vista/7/8, Macintosh 10.x and Red Hat Linux (both server and workstation editions). Our remote testing took place across T3 and OC-9 WAN links.

The relational databases on the network were Oracle and both Microsoft SQL Server 2008 and SQL Server 2012. The network also contained two Web servers (Microsoft IIS and Apache), three e-mail servers (Exchange, Notes and iMail) and several file servers (Windows 2003, Windows 2008 and Windows 2012 servers).

Our virtual computing environments consisted of VMware, XenServer and Microsoft Hyper-V.

The servers in our simulated data center consisted of a group of forty PowerEdge R720 servers with Dual Xeon E5-26xx processors, 384 GB RAM and 32 TB disk storage and running Windows 2003 Server, Windows 2008 Server and Red Hat Enterprise Linux.

Vendor Info

Enterprise Situational Intelligence (ESI)

Lumeta Corporation
732-357-3500
www.Lumeta.com

Nessus Enterprise, Passive Vulnerability Scanner (PVS) and SecurityCenter console

Tenable Network Security, Inc.
410-872-0555
www.Tenable.com

Conclusion

Lumeta ESI easily emerged the winner in our tests.

ESI offers by far the most accurate, real-time device discovery of any product in the industry. It revealed unintended network paths to sensitive data, gave us an up-to-date, intuitive map of our network and identified our IPv6 devices and routes. ESI was easier to set up, configure and use, and it used network resources frugally as it discovered our network, profiled devices and identified potential security problems.

We recommend Lumeta ESI to any organization that needs to have situational awareness of its network activity.

Report Card

	Discovery (40%)	Ease of use (20%)	Reports (20%)	Installation & documentation (20%)	**Overall score**
Lumeta Enterprise Situational Intelligence	A	A	B	A --	A --
Tenable Network Security Nessus, PVS and SecurityCenter	C	C	B	B	C

About the Author

Barry Nance is a networking expert, magazine columnist, book author and application architect. He has more than 29 years experience with IT technologies, methodologies and products.

Over the past dozen years, working on behalf of Network Testing Labs, he has evaluated thousands of hardware and software products for ComputerWorld, BYTE Magazine, Government Computer News, PC Magazine, Network Computing, Network World and many other publications. He's authored thousands of magazine articles as well as popular books such as *Introduction to Networking* (4th Edition), *Network Programming in C* and *Client/Server LAN Programming*.

He's also designed successful e-commerce Web-based applications, created database and network benchmark tools, written a variety of network diagnostic software utilities and developed a number of special-purpose networking protocols.

You can e-mail him at barryn@erols.com.

About Network Testing Labs

Network Testing Labs performs independent technology research and product evaluations. Its network laboratory connects myriads of types of computers and virtually every kind of network device in an ever-changing variety of ways. Its authors are networking experts who write clearly and plainly about complex technologies and products.

Network Testing Labs' experts have written hardware and software product reviews, state-of-the-art analyses, feature articles, in-depth technology workshops, cover stories, buyer's guides and in-depth technology outlooks. Our experts have spoken on a number of topics at Comdex, PC Expo and other venues. In addition, they've created industry standard network benchmark software, database benchmark software and network diagnostic utilities.