LUMETA
DETECT WITH A HIGHER SENSE

Lumeta Spectre for Managed Security Service Providers (MSSPs)

Enhance Your Service Portfolio and Increase Your Revenue with Cyber Situational Awareness

The global managed security services market is predicted to grow to $40.97 billion by 20221. There is a fast-growing market of enterprise- and midsize-class organizations (both commercial and government) actively looking for an enhanced set of security services to help them withstand targeted attacks that are constant. The migration to managed services is due to their ability to more efficiently leverage experienced security teams, centrally manage large volumes of complex security event data, apply security technologies at scale in order to protect critical resources, detect and analyze advanced threats and remediate problems quickly.

To be successful, MSSPs must deploy best-of-breed network security solutions to reliably and cost effectively protect client assets. In doing so, MSSPs are also challenged with differentiating their services, minimizing operational complexity and ensuring that the business is profitable.

Lumeta Spectre enables MSSPs to maximize their effectiveness in eliminating blind spots in infrastructure while providing unique real-time monitoring of network and virtual infrastructure changes to from the endpoint to the cloud to not only better protect customers from potential breaches, but also as a significant revenue driver. MSSP partners can use Lumeta Spectre, delivering Cyber Situational Awareness to:

- Quickly identify and help secure on average 20% unknown networks and endpoints, including VMs both on premise and within cloud-based networks. By bundling Lumeta Spectre into existing value-added services, an MSSP can further enhance its trusted security advisor status with its clients by eliminating blind spots that can be exploited by attackers, while generating additional revenues through the extended management of new infrastructure.

- Discover network leak paths, rogue infrastructure and shadow IT, previously unknown and in real-time by combining unique network infrastructure context with threat intelligence. Threat intelligence is also applied to network flows to create Lumeta Threatflows for faster identification of anomalous network behavior in real-time. Lumeta's patented active and passive monitoring capabilities, unlike other "continuous monitoring" solutions, do more than periodic interrogation of systems, great improves an MSSPs ability to protect client networks from breaches.

Multiple Use Cases for Enhancing Services offered by MSSPs

Pre-Sales: Before you scope out your entire client engagement, MSSP sales and pre-sales teams can use Lumeta Spectre to gain comprehensive visibility into the full infrastructure of the client's network. Spectre typically finds, on average, 20% more IP addresses (connections and endpoints on a network). By working from a larger network size, your engagement should command additional revenue – while maintaining customer satisfaction because you will be able to provide security services to protect all network connections and devices.

The baseline that Spectre provides creates a critical foundation for establishing a successful outsourced network management relationship and increased customer satisfaction. Automating the inventory discovery cycle results in greater customer confidence that all of the assets on their networks are effectively under management.

[1]*Source: Managed Security Services Market (Hosted or cloud-based MSS and On-premise or customer-premise equipment) - Global Opportunity*
Analysis and Industry Forecast, 2014 - 2022, Allied Market Research, Aug 2016

Multiple Use Cases for Enhancing Services offered by MSSPs

Real-Time Threat Detection, Rogue Activity and New and Dynamic Infrastructure Discovery: After you've officially engaged with a client, MSSP security operations teams can use Spectre to gain visibility into the complete network infrastructure to identify potential threats, but also monitor for suspicious behaviors, leak paths, unauthorized networks, endpoints and VMs along with identified Threatflows. In addition, as new infrastructure is introduced they can automatically be added to existing managed device contracts.
Critical Incident Response (IR): MSSP critical incident response teams get called in when there is a problem – hacking attempts, data breaches, malware outbreaks and distributed denial of service (DDoS) attacks. They need to quickly assess the client's situation and help to respond and recover. Spectre operates in real-time to get visibility into the client's full infrastructure and often attacks hit a network in the most vulnerable of places – via the unknown connection or device. Spectre can provide full visibility into all connections on a network, so MSSPs can understand the vulnerabilities. These capabilities are especially critical for IR teams post-incident in order to accelerate remediation and minimize future IT security incidents to meet the cyber threat defense/detection needs of their clients.
Security Audit: MSSP audit teams need to help clients ensure their readiness to achieve compliance (whether it be with PCI, HIPAA or the myriad other industry regulations). A key first step toward meeting the compliance needs of clients is to understand and take an inventory of the network. IPsonar can help MSSPs discover all that is on a network – all connections, devices and potential leak paths – across traditional and virtual IT infrastructure, as well as cloud environments.

Lumeta MSSP Program

- Market differentiation: Offer your clients unmatched visibility into their networks combined with threat intelligence, while enabling more services for you on larger, all-encompassing networks.
- Automated discovery: Fewer man-hours used to discover network segments to bring under management.
- Work with existing security stacks and network infrastructure to fill gaps in network visibility and threat detection : Lumeta integrates via open APIs with third-party security tools from McAfee, Cisco, Gigamon, Qualys, InfoBlox, Carbon Black and HP ArcSight, maximizing the effectiveness of the security operations team.
- Favorable pricing: MSSP-specific discounted pricing (includes sales support and training).
- Flexible deployment options: Deploy unlimited instances of the Lumeta solution via virtual machines within your own network – either spin up on an individual laptop while at a client site, or centralize it in your infrastructure for everyone to use during your security engagements

(MSSP internal use only). Add-on sales: As a customer gains value from Lumeta Spectre, an MSSP can benefit from reselling Lumeta Spectre direct to the client for permanent deployment post engagement. Add Lumeta Spectre to your portfolio to ensure high levels of security service delivery and expand your revenue opportunities. **See more at http://www.lumeta.com**

MSSP Benefits and Terms

MSSP Benefits	MSSP
The right to sell Lumeta products and services in a defined territory	•
Monthly pricing	•
Easily inserted into your current MSSP stack	•
Large Product Ecosystem	•
Lumeta generated leads	•
Marketing programs support	•
MSSP Partner Terms	**MSSP**
Have a signed MSSP Agreement in place with Lumeta	•
Actively sell and promote Lumeta solutions	•
Develop and receive agreement from Lumeta on a revenue, marketing and sales plan.	•
Actively promote Lumeta products on their website in accordance with the guidelines provided by Lumeta	•
Have 2 Certified Sales employee and 2 Certified Sales Engineers	•
Hold at least 4 dedicated Lumeta group selling events per year. This will be an agreed program of marketing activities and form part of their Business Plan.	•
Commitment Level (annual)	**MSSP Price/IP (monthly)**
None	$0.52
$100k	$0.34
$250k	$0.17

Key Messaging at a glance

Lumeta solutions enable your customers to:

Find and Eliminate ALL Blind Spots and See Changes in Real-Time
See, Discover and Monitor today's dynamic network and cloud infrastructure with real-time understanding of any changes

Apply Security Intelligence and Capabilities Everywhere
Full network context combined with best of breed security intelligence to identify threats across the darkest reaches of the network, the dynamic edge and into the cloud

Use, Validate, and Optimize Segmentation to be Proactive
Rather than just detect threats, more effectively control where authorized users can go, while limiting malicious users from accessing sensitive resources.

Lumeta Spectre: Cyber Situational Awareness Eliminates Blind Spots and Reveals THE Answers
Other Solutions CANNOT

- Prevents Breaches
- Are there any "threat" flows occurring to known bad-actor IP addresses on the Internet?
- Are there "zombie" devices I've lost control over?
- Are there "red" ports in use?

Protects Networks, Endpoint and Cloud Infrastructure

- Do I really know all my in-use address space?
- Do I know the edge of my network?
- Are there any rogue devices? Forwarders? VMs?Cloud?
- Can my security tools reach everything? **Understands, Validates and Optimizes Network Paths**

- Are there any leak-paths to the Internet?
- Are there any leak-paths in between enclaves?
- Are there any bridged connections or split-tunneling in multi-homed hosts?