ESG Lab First Look

Lumeta: Cyber Situational Awareness

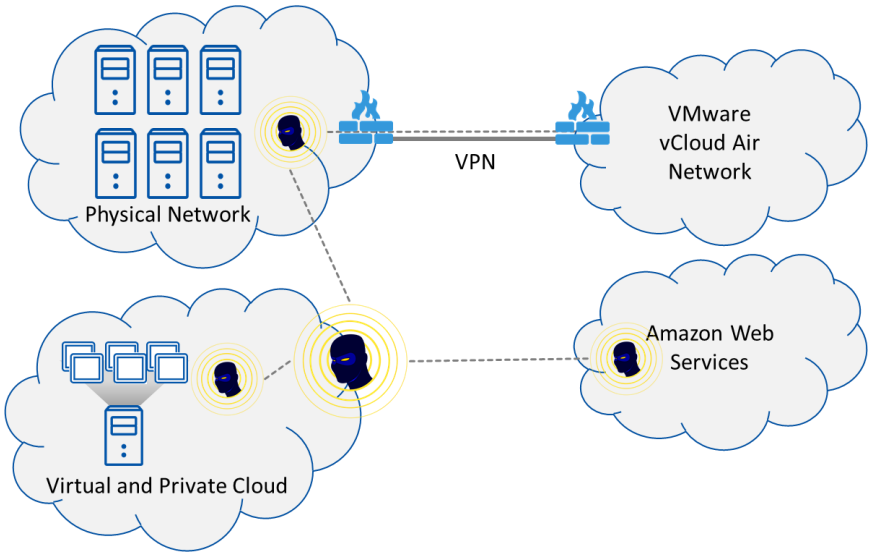
Date: June 2017 Author: Tony Palmer, Senior Lab Analyst

Cybersecurity Challenges:[1,2]

45% The percentage of organizations that believe they have ***a problematic shortage of cybersecurity skills*** in 2017.

54% The percentage that report that *the cybersecurity skills shortage* ***increased their workload***; 35% said it led to **an inability to utilize security technologies to their fullest potential**.

Network security can be an intimidating discipline for most organizations, and information security professionals would readily admit that today's virtualized enterprise IT infrastructure—leveraging private, public, or hybrid clouds—makes managing or even seeing everything on the network a challenge. With more enterprise network users doing business on mobile platforms—smartphones, tablets, and notebooks—detecting and stopping persistent cyber-adversaries is a difficult challenge. Traditional security and vulnerability assessment (VA) products aren't designed to search for the unknown, and so it's not surprising that they miss a significant percentage of endpoints and devices connected to the network. Organizations are trying to cope with these challenges while operating within the constraints posed by the global cybersecurity skills shortage.



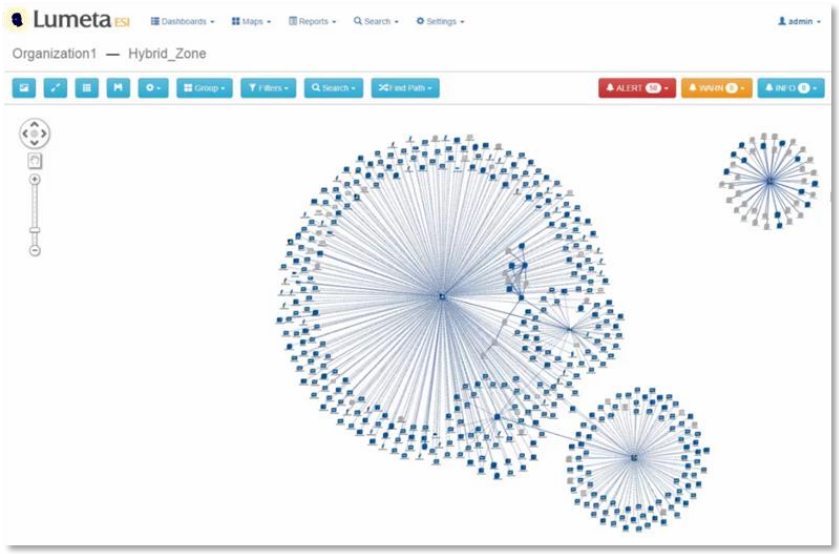
Lumeta Enterprise Situational Intelligence

Lumeta Spectre, (formerly Lumeta ESI) is designed to offer real-time, context-driven security intelligence to address these problems. By enhancing Lumeta's Recursive Network Indexing techniques with the context of network state change via analysis of network control plane protocols (OSPF, BGP, ARP, DHCP, DNS, ICMPv6, and others), Lumeta Spectre provides cyber situational awareness in real-time, as mobile, virtual, cloud assets, and even the physical/software-defined network changes. Lumeta Spectre hunts for anomalous behavior to provide context and to quickly prioritize issues for remediation. Spectre includes the ability to ingest third-party threat intelligence feeds—an Accenture iDefense subscription is included—to correlate with network data to find threat flows—live communication with malicious command and control servers, discover internal use of known malicious ports, and to hunt for unauthorized communication to known bad actor sites.

Lumeta Spectre hunts for dynamic changes to the network edge and changes caused by virtual, cloud, and mobile assets on the network. Recursive Network Indexing provides a real-time, authoritative view of network infrastructure. This enables organizations to gain a true view of all network devices, i.e.: the total address space and everything in it. Lumeta Spectre can also identify leak paths—unauthorized communication to the internet or between firewalled segments.

[1] Source: ESG Brief, 2017 Cybersecurity Spending Trends, March 2017.
[2] Source: ESG/ISSA Research Report, Through the Eyes of Cyber Security Professionals: Annual Research Report (Part II), December 2016.

ESG Lab Validation Highlights



ESG Lab performed hands-on testing of Lumeta Spectre, looking at how Lumeta's real-time, always-on monitoring and integration with best-of-breed cybersecurity tools can enable organizations to gain complete visibility into their network, enabling detection, prevention, and remediation of threats and vulnerabilities. The full ESG Lab Review will be published in June 2017.

ESG Lab Testing

- ESG Lab looked at a live network environment using Lumeta Spectre. With a couple of clicks we were able to see the entire network and all devices on it. The *Breach Detection* dashboard showed all devices on the network identifying zombie devices, dark web (Tor) nodes.
- Spectre also identified threat flows, peer to peer transactions between inside devices communicating with IP addresses identified as P2P nodes.
- Spectre also identified all devices at IP addresses not managed by the organization's endpoint and threat management solutions. Spectre can drill down into the details for these devices for identification and remediation.
- ESG also looked at the custom query builder. Spectre provides a visual query builder that enables users to build complex analytic queries by dragging and dropping elements, with no SQL required.

First Impressions

Today's IT infrastructure, featuring the cloud, digital transformations of the business, and a mobile workforce, is evolving at a pace that's exceeding the capabilities of legacy security approaches. Network security has proven to lack the visibility, control, and intelligence necessary to keep up with changing needs. Infrastructures are left exposed to a dangerous threat landscape where persistent cyber-attackers have proven adept at bypassing aging security mechanisms, presenting an increased risk to the business.

To shrink an organization's attack surface and reduce potential avenues of compromise, security teams should look to improve their network visibility and enforcement capabilities. After all, it's impossible to protect users and their endpoint devices when you don't know who they are, what they've connected to, and what they allowed to do.

ESG Lab testing revealed that Lumeta Spectre provides real-time visibility into organizations' on premise and cloud infrastructure, exposing previously unknown devices and vulnerabilities. ESG Lab was able validate early and predictive breach detection by correlating real time network visibility with threat intelligence feeds. Lumeta Spectre also demonstrated the ability to detect real-time network configuration changes, exposing leaky and unauthorized network paths.

Given the need for network visibility, tight access controls, continuous monitoring, and real-time security policy flexibility, ESG believes that Lumeta's integrated security solutions, including integrated network discovery, monitoring, and analytics can act as a comprehensive platform for addressing evolving network security requirements.