LUMETA
DETECT WITH A HIGHER SENSE

SOLUTION BRIEF

REAL-TIME PUBLIC & HYBRID CLOUD SITUATIONAL AWARENESS WITH LUMETA SPECTRE

CYBER AWARENESS OF THE CLOUD AND ENTERPRISE IS ACHIEVABLE WITH LUMETA® SPECTRE.

Enterprise application development teams have embraced public multi- cloud environments like Amazon Web Services, Microsoft Azure, Google Cloud, VMware Cloud, IBM Cloud and other public cloud Infrastructure As A Service (IAAS) offerings to address their next- generation application development (devops), testing and deployment needs.

While cloud providers are responsible for security of their overall cloud infrastructure, you are responsible for your enterprise's security within your virtual private cloud instances. You need to be concerned with Shadow-IT that you don't know about, misconfigurations enabling unexpected paths to the internet and vulnerabilities or anomalous behavior invisible to your enterprise cyber security infrastructure.

HIGHLIGHTS

- Actively monitor from inside the Enterprsie to find unknown or new virtual private cloud (VPC) instances and virtual hosts running within them
- Actively monitor for unknown virtualized network functions such as forwarders within VPC instances that change the network topology.
- Eliminate unknown leak paths from cloud to the internet that may be used to exfiltrate corporate data or bypass enterprise policy enforcement
- Actively update the manifest of seen virtual endpoints in the cloud given into Enterprise Host Vulnerability Management (HVM) and Endpoint Detection and Response (EDR) tools, which allows existing Enterprise cyber security tools to see, scan cloud assets for vulnerabilities.

Key Benefits Lumeta Spectre Delivers:

- **Find unknown (e.g. Shadow IT) virtual private cloud instances via active host discovery interrogation from the enterprise.**
- **Leverage leak path discovery to find such paths directly to the internet coming from within a virtual private cloud instance.**
- **Identify Threatflows occurring from cloud virtual hosts to TOR and Command and control botnets**
- **Identify whether cloud VMs are known to/protected by enterprise EDR solutions such as McAfee ePO**

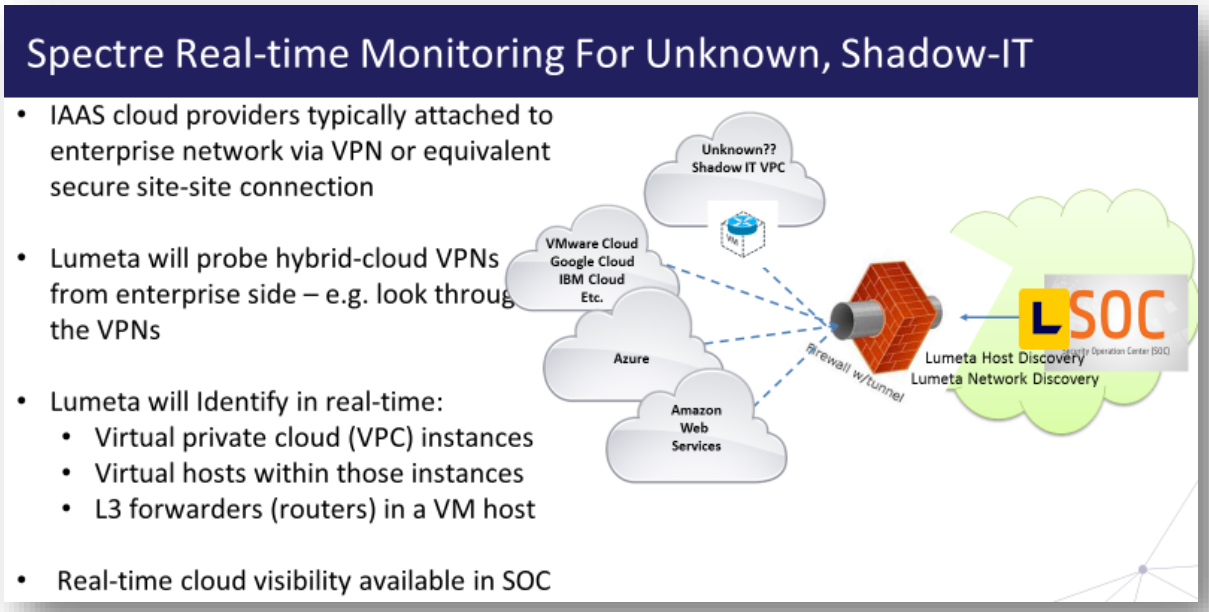
How It Works – Achieving a Comprehensive View

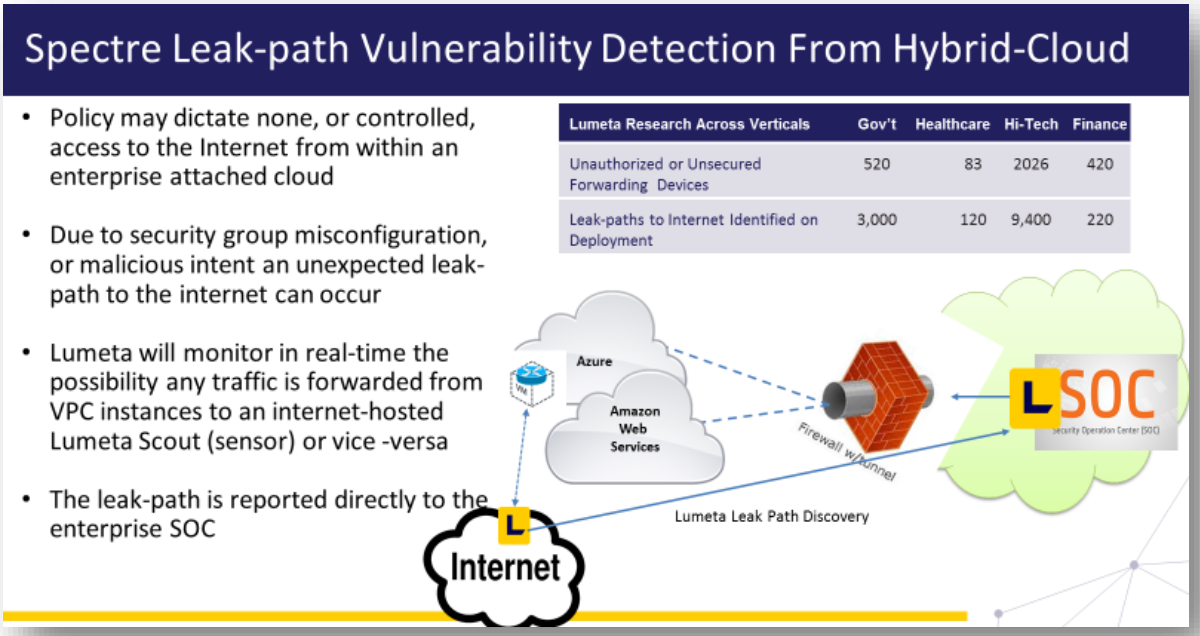
Comprised of multiple network crawling methods including network, host, enhanced perimeter and leak path discovery, Lumeta Spectre uses a combination of recursive network indexing techniques to find everything that's on the network (not just an IP range that is assumed to be in use by the administrator), resulting in a comprehensive, authoritative view of the entire infrastructure – including cloud instances and assets, all IP connections and devices. Spectre acts in real time to detect changes to the network's security.

INDEXING TYPE	WHAT IS THIS?	BENEFIT
Network Discovery (ND), Layer 2 Discovery	Actively index forwarders and paths using ICMP, TCP, UDP, DNS via TTL-tracing, responses. Index network infrastructure devices, route tables, ARP tables, switch TCAM, VLANs using SNMP, LLDP.	Authoritatively identifies the full address space in use and the edge of the managed enterprise network, through use of recursive additions of newly identified address targets.
Host Discovery	Actively index devices attached to network via ICMP, TCP, UDP, DNS, SNMP interrogation and responses	Provides the authoritative census of devices are there, now, connected to network.
Device Profiling (DP)	Actively fingerprints the indexed census of devices on the network using TCP (OS detection), CIFS, HTTP/S, SNMP	Provides a high confidence (agent-less) assessment of device type, manufacturer, OS, certificates and certificate status.
Service Port Discovery	Actively index ports within the profiled census of devices using a configured list or a full portscan by using TCP SYN/ACK response	Authoritatively identifies TCP ports in use and highlight deviations/violations from policy.
L3 Leak Discovery (LD)	Actively index leak-paths that exist in the L3 routed domain between network segments using Lumeta proprietary TCP packet spoofing.	Authoritatively identifies network segmentation violations between networks at L3.
L2 Leak Discovery	Index L2 bridging and forwarding devices using ARP listening to assemble candidate MAC/IP pairs and Lumeta proprietary active TCP packet injection targeting each MAC/IP pairs' default gateway.	Authoritatively identifies L2 bridging and forwarding violations within multi-homed hosts or devices with multiple interfaces.
Network Control Plane Context	Probe and index network change by participating in control domain using OSPF, BGP, ICMPv6, ARP, DHCP, DNS analysis (others to come).	Authoritatively identifies the presence of cloud, virtual/mobile devices and network infrastructure (NFVs) in real-time.

Visibility into the Dynamic Nature of the Cloud in Real Time

Lumeta Spectre discovers, maps and alerts about topology changes, including transitory endpoints, servers, virtual machines (VMs), AMIs and other virtualized network functions (gateways, switch/router/firewall and forwarding devices). Spectre forms a holistic view of both physical and virtual/cloud infrastructure, providing a holistic perspective of vulnerability to the enterprise security operations center.





Lumeta Spectre and Gigamon V-Series for Threat Protection

Real-time Monitoring For C2, TOR "Threat-Flows" in Cloud Environments

- Based on Lumeta Host Discovery finding new virtual machine hosts within minutes
- Lumeta will ingest & leverage:
  - Threat intelligence services like Accenture iDefense
  - Flow data from Gigamon Cloud Flow Collector
- Lumeta will Identify:
  - Connections from cloud VMs to TOR
  - Connections from cloud VMs to botnets
- Real-time visibility made available to SOC

For more information on Lumeta Spectre for the cloud visit http://www.lumeta.com/solutions/cloud-security/