FROST & SULLIVAN

Lumeta and McAfee:

Eliminating 100% of Your Blind Spots to Secure the Entire Network and Optimize Security Operations Across the Entire Threat Defense Lifecycle

A Frost & Sullivan White Paper

www.frost.com

50 Years of Growth, Innovation and Leadership

INTRODUCTION

Today's enterprise networks are dynamic, since the network changes as guest, employee, and IoT devices enter and exit the network, and cloud environments host applications to expand capacity and functionality. This diversity and dynamism in the enterprise network gives rise to potentially vulnerable endpoints and introduces new threat vectors. These factors make the jobs of enterprise network cybersecurity professionals even more challenging.

To add to the complexity, in many organizations, IT, operations, and security operate in separate silos, with personnel who are in short supply. Although many of these organizations have a Security Operations Centers (SOC) the following is needed to ensure effectiveness:

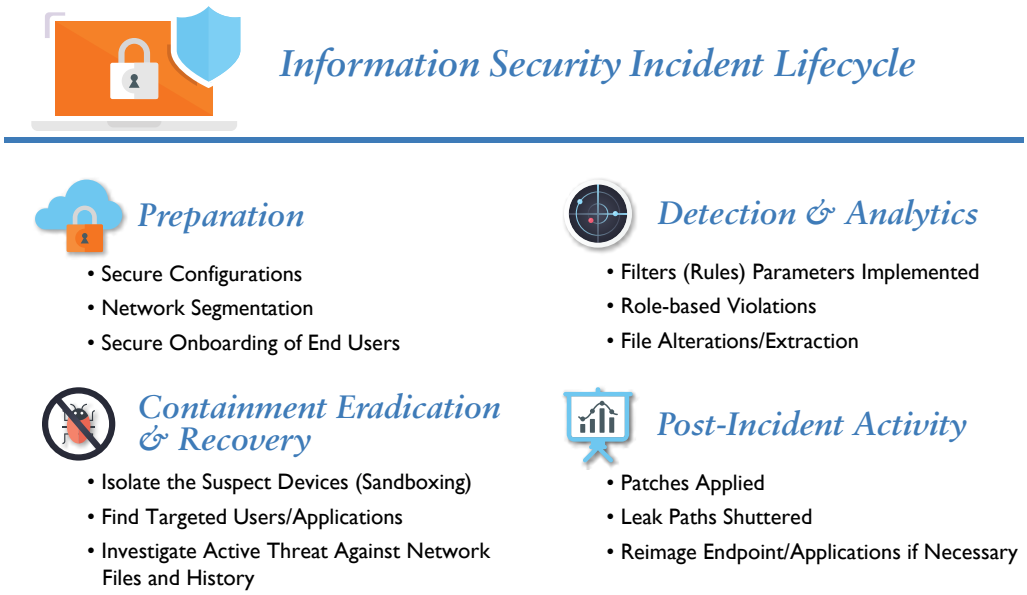
- Baseline (and hopefully optimized) ultimate visibility
- Monitoring
- Threat detection capabilities

In addition, a SOC should have a platform that provides dynamic discovery of endpoints and cloud environments, improves the efficacy of existing tools, analyzes incoming/outgoing traffic to identify indicators of compromise (IOC) in network security forensics, identify and monitor the constant network and endpoint changes in real-time that are common in today's environments and utilizes threat intelligence and analytics to determine anomalous network behaviors that are part of an overall attack pattern.

INCIDENT DETECTION AND RESPONSE LIFECYCLE

The term IDR lifecycle is more than just an operational function because network security requires constant vigilance. Presented below is an image of the taxonomy of the Security Incident Lifecycle as defined by National Institute of Standards and Technology (NIST 800.61). The four cycles shown are a reasonable facsimile of what typically happens in the security operation center (SOC).

Figure 1. Information Security Incident Lifecycle (NIST 800.61 Model)



Source: NIST 800.61 framework, Frost & Sullivan

An exhaustive review of each step in the IDR lifecycle would be lengthy. However, a fundamental understanding of these four stages is instructive:

- **Preparation.** The preparation stage within an enterprise network involves secure software development environments, secure onboarding of end users, network segmentation for security of logical business functions, and secure configurations of endpoints.
- **Detection and Analysis.** This phase is a little bit tricky. Incident detection can be described in four basic premises—known bad IP signatures attempting network intrusion (malware), rule-based violations, role-based violations, and the detection of file alteration or extraction.
- **Containment, Eradication, and Recovery.** In the diagram above, the Detection phase and Containment phase are inextricably linked, and with good reason. The Detection phase must be thorough in providing insight into where a threat came from and what systems/end users are endangered. The Containment phase is the art of working backward to mitigate the threat, and then make the necessary repairs. Eradication and recovery are necessary procedures that conclude remediation.
- **Post-incident Recovery.** Trust but verify. Even if infected endpoints are quarantined and reimaged, the proper patch management is applied, and OS and software upgrades occur smoothly, an incident may be believed to be fixed, but the desired mitigation did not actually take effect due to misconfigurations, network events, or simple human error.

In each of these four phases of IDR, Lumeta Spectre can be used to improve visibility, enhance threat detection, and improve the overall posture of the network.

LUMETA

Lumeta provides cybersecurity and network performance monitoring software solutions. Lumeta Spectre, the flagship product, discovers every unknown, unmanaged, rogue and shadow IP enabled device and associated infrastructure even into the cloud. This visibility offers comprehensive, real-time network monitoring to hunt for new or changed infrastructure, routes, paths, and devices. When combined with security threat intelligence, Lumeta Spectre provides breach detection in virtual, cloud, mobile and software-defined networks. Lumeta also complements and optimizes existing network and security product investments by providing accurate, real-time, comprehensive network intelligence, allowing these solutions to also better detect attack activity.

Below is a summary of the types of data the Lumeta Spectre provides around unique network context and monitoring for threats across the entire network infrastructure:

- **Visibility over blind spots.** Spectre makes use of patented active (non-invasive interrogation and response) and passive listening techniques. Protocols include ICMP, TCP, UDP, DNS, and SNMP to name a few.
- **Monitors dynamic network changes.** Spectre can see any network change, router or switch configuration change, new network paths being created, leak paths across enclaves or to the internet, and endpoint, including virtual machines.
- **Device profiling.** Spectre uses multiple techniques to identify device types. The platform matches device responses with over 26,000 endpoint patterns.
- **Dynamic network path mapping.** With Lumeta Spectre, the security team can discover, map, and visualize the Layer-2 and Layer-3 infrastructure. Spectre also creates and monitors switch tables. Through these and other active indexing techniques, it can determine segmentation violations and leak paths.
- **Incident Detection and Response.** Based on complete discovery and change monitoring, Lumeta Spectre ingests and applies threat intelligence data to this real-time network context to identify suspicious traffic network behavior like threat flows, Command and Control activity (C2), callbacks to malware hosts, TOR communications, and anomalous ports in use and zombie and TOR nodes.
- **Builds network infrastructure indices.** Lumeta determines if there are unknown or stealth routers. The platform has summary services of DNS, and common Web services and IP address utilization. If something fishy is going on, on the network, Lumeta will see it. This includes the ability to determine if a router or switch as has been compromised and is setup for illegal forwarding paths. This is almost impossible for traditional IDR tools to determine.

Lumeta Spectre can also be deployed as a part of defense-in-depth strategy or an open platform strategy with other cybersecurity platforms. Second, in an optimal security operations center (SOC) architecture, bidirectional communications can improve the efficacy of each platform.[1]

1 For example, malware evades antivirus platforms and somehow evades a NGFW, but is detected as a rule or role violation on a SIEM. If an API or communications fabric between the SIEM and the NGFW is established, the NGFW can be dynamically updated to block IP traffic with the same malware signature in the future.

LUMETA INTEGRATION WITH McAfee

Along these lines, Lumeta Spectre and McAfee ePolicy Orchestrator (ePO) offer a unique certified integration. Through ePO, McAfee Endpoint Threat Protection and McAfee Active Response conduct endpoint management and endpoint detection and response (EDR). Active Response prioritizes threats, provides continuous monitoring, and automates threat responses to not only streamline analyst activities in the SOC, but also increase output and produce better security outcomes. The platform incorporates workflow, visibility, investigation, and corrective measures onto a single pane of glass, with single-click actions.

At MPOWER 2017, McAfee CEO Chris Young said that McAfee was absolutely dedicated to stopping the cyber adversary. So much so that McAfee are also committed to working with integration partners to offer a more comprehensive security stack to customers.

In this case, the actions are better than the platitudes. For cybersecurity companies to share information, McAfee developed the Data Exchange Layer (McAfee DXL). McAfee DXL offers many important benefits:

- DXL offers both an open and secure software development kit (SDK). The SDK allows developers to reuse code over multiple instances instead of having to write/rewrite APIs to make multiple point-to-point product interconnections.
- DXL can be used to connect solutions from third-party vendors, Innovation Alliance Partners, external threat exchange data providers and in-house applications to McAfee products and services.
- The way that companies use the DXL can create new IT/security paradigms. Ticketing products can be combined with threat detection platforms. Endpoint products can be combined with SIEM for analysis alongside correlated logs and packet captures.

The integration between Lumeta and McAfee provides end-users additional capabilities in visibility and control. The following sections present use cases of how Lumeta is used either as a standalone appliance or as part of a cybersecurity stack to improve processes in the IDR lifecycle.

Preparation

The ability to discover the entire infrastructure even into the cloud or OT environments is almost impossible with full knowledge of even rogue or shadow IT infrastructure that is obscured from most technologies network and security technologies. Recursive Network Indexing is a proprietary technology within Spectre that not only discovers all of your assets, but also looks for dynamic changes in the network. Recursion is a type of learning that builds upon persistent processes. In this case, Spectre uses a recursive cycle of targeting, indexing, tracing, monitoring, profiling, to represent and correlate the network's current state. A sub-text is that Spectre uses passive indexing to find new assets, rogue devices, and unmanaged assets. Active indexing is used to provide additional network and device context to aid in threat investigations.

Starting with prevention, one of the key technologies used in the SOC is vulnerability management (VM). VM scans uncover unpatched and vulnerable software on endpoints, infrastructure equipment, and in vulnerable code. Additionally, VM vendors use known threat libraries to initiate vulnerability assessment scans against endpoints. The main objective is to discover and patch vulnerabilities before a breach occurs. In addition, many hosts that enter the network need the latest endpoint management and protection suites as endpoint compromises, even virtual, are the traditional entry point that is the start of an advanced attack.

In addition to McAfee ePO and via DXL, Lumeta Spectre can be integrated with different cybersecurity tools. Key partnerships include integration with Qualys, Cisco, Splunk, InfoBlox, and many other partners, to better identify vulnerabilities, protect all endpoints and track dynamic network changes at the SOC. With these integrations, Spectre helps to optimize vulnerability assessment scans to account for all devices (managed or unmanaged) and also trigger the VM solution to initiate scans based upon detecting changes in infrastructure or when new endpoints are discovered. In addition, endpoint protection solutions, such as Endpoint Threat Detection and Response (ETDR) or Next Generation Anti-Virus (NGAV), can quickly be installed on newly discovered systems to that can scan for malware or viruses before those systems can start to spread and infect other parts of the network. This can ensure that McAfee and Lumeta, together, can ensure every single endpoint is protected across the entire infrastructure. Even a single unprotected or unpatched system is easily vulnerable to compromise and is often targeted by attackers for that very reason.

Independent of other product integrations, Spectre identifies leak paths that may be related to misconfigurations that need to be locked down before a breach. The recent North Korea attack and breach of South Korean stealing joint SK and US military plans is a great example of leak-paths used in a successful breach. This includes leak-paths from cloud infrastructure to the Internet that violate security policies.

As a standalone device, Spectre uses probes (called Scouts) to index the network control plane. By creating a virtual map of the Layer-3 network and Layer-2 bridges between communicating devices, security analyst gain visibility that cannot be achieved by vulnerability scanners or from the investigation of alerts from cybersecurity platforms.

Detection and Analysis

In terms of overall network security, real-time visibility is the strongest singular attribute offered by Lumeta Spectre. In this context, visibility is more than just the fluid discovery and inventory of devices and infrastructure equipment; it also entails traffic paths between devices. Lumeta Spectre's combination of network visibility analytics, identification of known/unknown network devices, correlation of inventories with endpoint solutions, and analysis of traffic paths can have stunning results:

- **Command of the control plane.** Spectre keeps a record of the type of traffic patterns in L2-L3 OSI layers. The effect is two-fold. Lumeta can find evidence of exfiltration to C2C servers by using IP threat reputation scoring to find leak paths. Second, often lateral movement goes undetected, but Spectre will find anomalous behavior of endpoints on the network or in irregular network clusters.
- **Validation of segmentation policies.** Earlier, we mentioned that one of the important preventative security techniques was establishing network segmentation. If a platform has rule and role-based filters that helps determine logical network segments, the corollary to that is if segmentation policy are being violated, this may be an IOC. Worth noting, Spectre provide insights into whether segmentation policies are being violated or misconfigured in addition to discovering if illegal paths are being created. Spectre is also integrated with Cisco Identity Service Engine (ISE) via pxGrid for device profiling or deeper segmentation hierarchies.

Spectre looks for IOC from leak-paths from enclaves to the Internet, hidden communications over TOR, and rogue or zombie devices. Unlike on-premises security devices, and because Spectre discovers endpoints and monitors traffic flows, Spectre discovers virtual machines, cloud applications, and zombie devices that may not be visible otherwise.

Containment, Eradication, and Recovery

An important transition happens between the Detection and Analysis phase, and the Containment, Eradication, and Recovery phase of IDR. In rough terms, determining that a threat is real is the Detection phase. Finding out what the parameters of the active threat are (targeted user groups, OS, or applications) is the Containment phase. Obviously, once the threat is fully fleshed out, the appropriate patch/response/or sandbox technique can be applied.

Ideally, if breach activity is discovered, the damage can be prevented or impact significantly reduced. Often attacks are still successful at exfiltration or some other activity as the time delta between threat discovery and remediation is too wide. If an incident can be contained, theoretically, any leak-paths should be eliminated or enough network context can be leveraged for security teams to work more closely with network teams to lock down the infrastructure. This is where Lumeta provides a unique level of network context and understanding.

Lumeta Spectre is vital in that it not only catalogs and discovers existing, new, rogue, shadow networks and endpoints, but also tracks the communications and paths through the network. It is simplistic and overlooked, but is fundamental to making sure that a network is safe and seeing changes in real-time provides the necessary visibility and insights to today's dynamic networks and potential threats that exploit this change. Here is how Lumeta Spectre accomplishes these lofty goals:

- Lumeta maps every network, all network paths and devices, including "leak-paths", not just connected devices.
- Lumeta finds real-time network changes or change in paths indicating leaky and rogue network paths.
- Lumeta will identify Layer-2 bridging and forwarding devices with hosts honing to multiple locations, or devices with multiple interfaces.

THE POWER OF McAfee + LUMETA IN THE IDR PROCESS

At the McAfee MPOWER 2017 industry event, Lumeta was named the best new Security Innovation (SIA) Partner. The award was given for the integration between Lumeta Spectre and McAfee ePolicy Orchestrator (ePO). ePO is renowned for its ability to facilitate and coordinate activities related to visibility into and then management of endpoints. The capabilities of Lumeta-McAfee platform integrations include:

- **Elimination of blind spots.** The combination of Lumeta recursive passive/listening with McAfee endpoint detection and response (EDR) capabilities minimize the possibility of hidden endpoints. Each platform has different vantage points. Lumeta uses a patented combination of active and passive listening techniques to map the network, without using an agent or credentials. With McAfee EDR, agents are installed for control and visibility. This creates two separate inventories of devices that can be observed and correlated.
- **Direct integration with McAfee® Active Response.** McAfee Active Response uses predefined and user-customizable collectors to investigate all accessible systems for indicators of attack (IoAs). Lumeta Spectre analytics already segment the network by devices and event types, and these groups can be segmented for investigation and containment. Active Response gives the analyst comprehension not only of running processes, but also of processes that may lie dormant.

- **McAfee Active Response is already a closed-loop process.** Active Response is able to prioritize threats, provide continuous monitoring, and automated threat responses. What is ultimately important about Active Response is it can reduce protection postures, correlate multiple security appliances, and direct SOC analyst activities toward a singular outcome.

The integration with McAfee is strategic for Lumeta because of McAfee's reputation as a strong threat detection and mitigation company. The flagship product offered to enterprises for cyber defense is McAfee Endpoint Threat Protection. McAfee Endpoint Threat Protection combines several cybersecurity disciplines and creates new opportunities for collaboration:

- **ePolicy Orchestrator.** ePolicy Orchestrator provides the management, policy enforcement and orchestration used by McAfee and in integration with other industry leading cybersecurity platforms for visibility, segmentation, management, and control.
- **Endpoint protection is not an isolated event.** McAfee offers integration modules for threat exchange data (McAfee Threat Intelligence Exchange is the best example), Web control, and firewall protections.
- **Complete threat detection.** McAfee combines structured, signature-based threat detection with behavior and machine learning threat detection to account for unidentified but nefarious behavior.
- **Endpoint control.** McAfee Endpoint Threat Protection can be integrated with EDR platforms, so that threat response activities can be automated and executed with or without human input. Additional, threat protection is adaptive as information from the IDR lifecycle is used to make dynamic changes in the security posture.

Worth noting is new integration between Lumeta Spectre and McAfee DXL is on the horizon. The McAfee DXL fabric makes it possible for multiple security platforms to interoperate as a single super-solution set. Possible expansion ideas for Lumeta's network visibility and control, with McAfee's endpoint visibility, management, and control could include tighter workflow management, control and visibility for specific environments like manufacturing, or 'as-a-service' modules and support.

CONCLUSION

Network security is not easy to achieve, but mastery of these fundamentals outlined above is a good place to start. Network security begins with visibility and detection of anomalous behavior in order to secure configurations. Security analysts must then assemble contextual awareness of the device, the end user, and external threat feeds to determine if network anomalies rise to the level of a threat. If an investigation of an alert reveals a possible exposure, the platform must also determine if and what damage is done, and it must close the vulnerability. Only a thorough understanding of the last known good configuration of the network compared to the network security posture after remediation confirms if closed-loop remediation is in fact closed.

The strength of Lumeta Spectre is the combination of visibility, historical context, and analytics used to detect anomalous behavior and threat detection. Lumeta Spectre in integration with McAfee technology empowers network security practitioners to do more with the limited resources that they have:

- Continuous threat detection and remediation.
- Dynamic discovery of assets
- Device profiling
- Network segmentation
- Network control plane context
- Historical context (behavioral, traffic patterns, threat analysis)

Perhaps one last point can be made, the integration between Lumeta and McAfee is only the tip of the iceberg. With McAfee Threat Intelligence Exchange, enterprise networks can add global threat data to the contextual awareness of each endpoint. McAfee DXL will make Lumeta and McAfee integrations even more extensible and facilitate integrations of other likeminded cybersecurity vendors for new use cases.

FROST & SULLIVAN

Silicon Valley
3211 Scott Blvd
Santa Clara, CA 95054
Tel +1 650.475.4500
Fax +1 650.475.1571

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel +1 210.348.1000
Fax +1 210.348.1003

London
Floor 3 - Building 5,
Chiswick Business Park
566 Chiswick High Road,
London W4 5YF
Tel +44 (0)20 8996 8500
Fax +44 (0)20 8994 1389

877.GoFrost • myfrost@frost.com
http://www.frost.com

NEXT STEPS

Schedule a meeting with our global team to experience our thought leadership and to integrate your ideas, opportunities and challenges into the discussion.

Interested in learning more about the topics covered in this white paper? Call us at 877.GoFrost and reference the paper you're interested in. We'll have an analyst get in touch with you.

Visit our **Digital Transformation** web page.

Attend one of our **Growth Innovation & Leadership (GIL)** events to unearth hidden growth opportunities.

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?