Solution Brief

Using Lumeta ESI to Provide Dynamic Validation of Network Segmentation Policies – in Real Time

Giving vendors, suppliers, partners and customers access to an organization's internal network poses risk. Every network connection does. Network architectures that segment a network to isolate risk and manage these connections carefully and continuously have become state of the art.

Lumeta®

The Security Risk of Third Parties

Highlights

Expose previously unknown network connectivity

Notification of changes to network topology as they occur

Comprehensive network visibility via combination of conventional and unique discovery methods

Identify network vulnerabilities that put the organization at risk

As more and more companies outsource nonstrategic activities to vendors, suppliers, partners and customers, they are growing increasingly dependent upon network-enabled partnerships. There are many advantages to connecting an outside/third party to your organization's internal network – it's an efficient way to do business and often saves money. But the additional risk this creates is ever present. Intruders can infiltrate an organization's internal network via a third party connection to potentially leak customer records or intellectual property out. It only takes one attack, one infiltration, and the organization could lose data, money, or reputation. The liabilities created from such a breach are increasing exponentially. Customer backlash, bad press, tarnished reputation, heavy fines for violations of industry regulations … what would a security breach cost your business?

Recent news reports on cyber security and data breaches point to so-called "backdoors" – connections exploited for data exfiltration – as being one of the most damaging and difficult to detect security hazards faced by organizations today. Network segmentation can significantly improve an organization's ability to manage the risk of exposing sensitive data to malicious users. But how do you police the network to make sure segmentation policies remain intact?

Network Segmentation: The Business (and Security) Value

Segmentation allows an organization to insulate each part of the network from unauthorized entry. Each network segment can be protected from the other segments by using firewalls, each employing its own set of rules, through which data moving between segments must pass.

Examples of situations in which networks are typically segmented include within a business (e.g., payroll and personnel data are not accessible to ordinary employees) and within governments (segregating classified information from non-classified information). Many organizations use a Demilitarized Zone (DMZ) network segment to separate their corporate intranet from the public Internet.

Often, the reason behind segmentation is operational efficiency or for business unit / enclave segregation. However, setting up segmentation once is not enough. Regularly monitoring network segments to ensure that new connections between networked devices aren't overlooked and that all-too-frequent changes in the network don't introduce new risk is required. Continual assurance that no new network changes have opened up connections affecting segmentation is critical.

Nail Down the Basics First

Enterprises lack sufficient network visibility into frequently exploited but easily remedied vulnerabilities. Most breach incidents can be avoided if basic security controls and best practices are in place.

The fact is, if you don't have visibility into every device and connection on your network – as your network changes – you're severely limited in how much control you have over your network security.

It's very important to keep careful tabs on IT inventory, as any device connected to the network is a potential gateway into or out of the network. A critical, foundational piece of intelligence is to be aware of network connections as they occur, in real time, to ensure there is no connectivity between certain network segments and/or connectivity between the network and external third party networks. If for some reason an unauthorized connection does occur, real time notification is needed to quickly address the problem.

Companies can learn from news of the latest breaches and take action to ensure segmentation, and to keep their own, and their customers', data safe.

Many companies have invested in point solutions in an effort to secure their network and remain compliant with industry regulations. But many of these companies still have gaps in their network security program … 10-20% of their network is "unknown" to them.

Not Just for External Networks

Insider threats can cause critical business disruptions. The risk of these types of malicious activity can be mitigated using network segmentation, too.

Whether you are a retailer protecting credit card data, a hospital guarding patient health records, a manufacturer that's invested billions of dollars in patented designs, an entertainment company producing a blockbuster movie, a financial institution with brokerage and advisory business units, a government agency safeguarding classified intelligence … all critical assets need to be protected. Network segmentation can help accomplish this goal.

Organizations are creating more of these "secure pockets" to ensure that sensitive data doesn't leave its discrete network segment without authorization, whether or not your company is required to do so by industry regulations such as PCI DSS or HIPAA.

Why? Because conventional security methods focus only the known IP address space. While that method is easiest, it is not the most comprehensive, and certainly not the most secure. Companies need to move beyond doing only what they must for regulatory compliance to ensure that the data they are entrusted with does not get compromised. Focus on real time changes in the network, and not just a checkbox on documentation supporting compliance to an “understand you network” requirement.

Network segmentation and access policies are important. But real-time monitoring of critical connections and pathways by which an attacker could access important data is an essential component to a company’s overall information security program.

Assuring Segmentation in Real Time – How Lumeta Can Help

You’re not alone … Lumeta commonly finds undiscovered vulnerabilities on enterprise networks because traditional network discovery products are typically only using conventional discovery methods and/or point security solutions.

Lumeta Enterprise Situational Intelligence (ESI) can detect security anomalies in real time, including leak path detection, to proactively stop potential leak paths before they can be exploited. Lumeta will discover not only authorized data paths, but uncover rogue paths between network segments.

Go Beyond Conventional Methods

Lumeta ESI discovers, defines and maps Layer 2 & Layer 3 (IPv4 and IPv6) networks, the secure network segments and all internal, wireless/BYOD, external, partner and Internet connections. As a result, organizations can:

- Identify and inventory all existing network connection points – uncovering leak paths, bypasses, and previously unknown backdoors in networks located on-premises or in the cloud
- Provide validation as connections are added / moved / changed / decommissioned
- Identify the true network perimeter to ensure properly managed entry points

- Test router / firewall access controls to ensure real time compliance to policy after network changes

- Identify vulnerable devices that are highly susceptible to a security breach

- Identify possible policy violations on individual devices

- Receive alerts in real-time any new connections or devices on the network

- View unique visualization technology – a precise image of the network, revealing the interconnectivity of the global network and easily identifying network segments as well as spurious connections

The end result is to expose connectivity you didn't know existed. With Lumeta, if a network connection exists to pass traffic, it will be found.

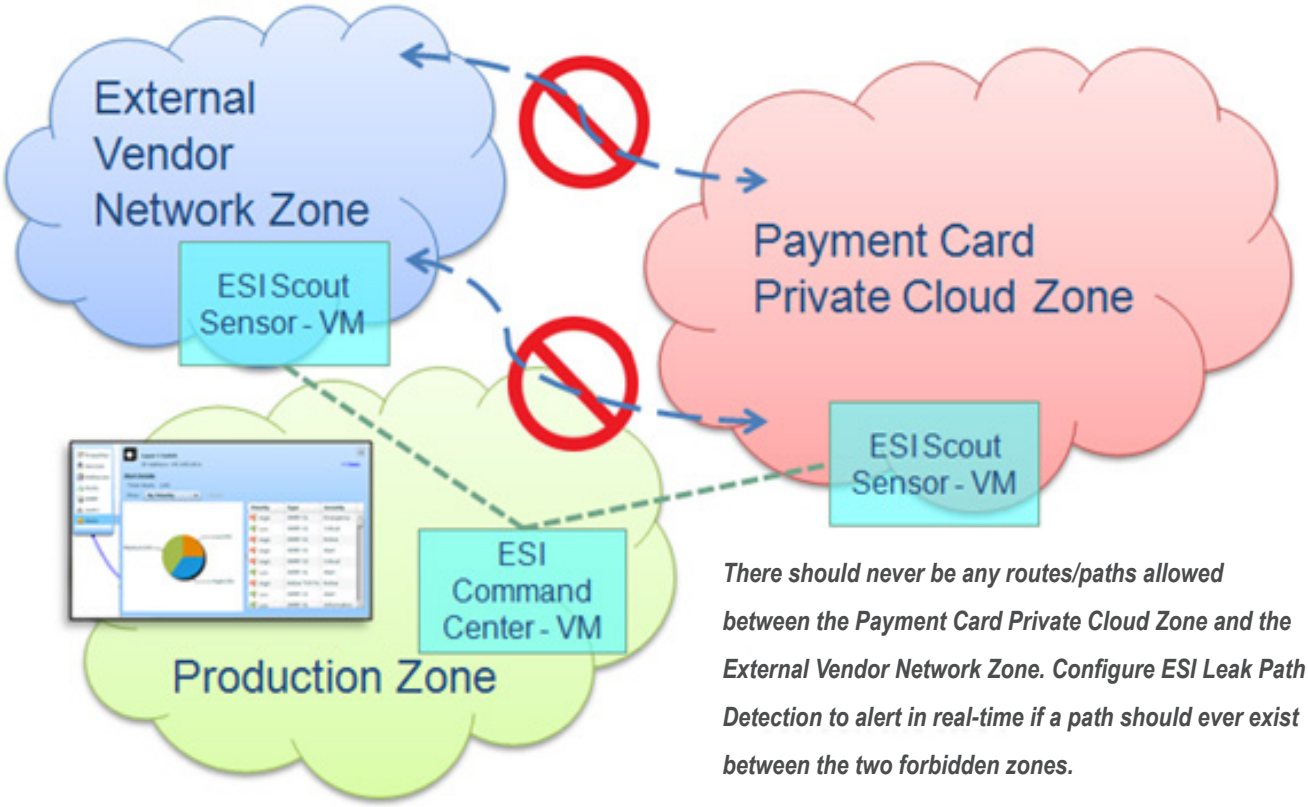
Monitor controls regularly, preferably in real-time as changes occur. Lumeta's network situational awareness solution is ideally suited to help organizations minimize risk amidst constant network change.

Maximize the Effectiveness of Security Tools

Lumeta provides foundational intelligence required for any network security program. It can provide a baseline as a starting point to understand the totality of the network, and then continuously update and alert about changes to the network, in real time.

Its findings can also be fed into existing security tools, such as device vulnerability scanners, IDS/IPS systems and SIEMs, enabling full utilization of their capabilities and therefore maximize their effectiveness (and the value of your investment in those tools). Security tools generally do what they do very well – but only on the supplied IP address space. Lumeta can feed the true network data into these security tools so that they are working off of complete network information.

Use Case: Assuring Segmentation in Real Time between Certain Zones



There should never be any routes/paths allowed between the Payment Card Private Cloud Zone and the External Vendor Network Zone. Configure ESI Leak Path Detection to alert in real-time if a path should ever exist between the two forbidden zones.

In this use case, the payment card database is segmented from the general corporate network. To comply with industry regulations and protect this payment card data, corporate policy states that there should never be any communication paths allowed directly between the Payment Card Private Cloud Zone (network segment) and the third party External Vendor Network Zone (segment) accessed via the Internet. Lumeta ESI monitors network segmentation in real time using its Leak Path Discovery module and sends an alert if it detects a path between the two "forbidden" zones.

While it's obvious to check for direct connections between the External Vendor zone and Payment Card zone, it is less obvious, and perhaps even more important, to check for covert pathways from External Vendor through the corporate Production zone (and potential connectivity between different sub-sections of Production zone) and then into Payment Card zone.

Lumeta ESI finds connectivity pathways that conventional discovery methods don't find.

Take the Next Step

One need only look at the very real costs incurred by companies that have suffered major data breaches or operational downtime to understand what's at risk. The most commonly discovered vulnerabilities, once detected, are easily remedied. The reason these security gaps can be exploited is because they are often undiscovered or unknown.

Lumeta is committed to helping you identify all connections on your network, be they internal connections between business units or segments of your network, or external connections with your suppliers and partners.

How do you implement network segmentation assurance using Lumeta ESI? Follow the configuration steps in this "Validating Network Segmentation" use case:

http://www.lumeta.com/solution/networksegmentation.html

Don't yet have Lumeta ESI? Contact Lumeta today to learn how your business can improve its security profile by assuring network segmentation in real time. For more information, please visit http://www.lumeta.com/company/contact.html