The Universal Gap in Preventing Breaches: Leak Path Detection and Mitigation

LUMETA RESEARCH WHITE PAPER

Sanjay Raja, CMO

LUMETA
DETECT WITH A HIGHER SENSE

Table of Contents

Executive Summary

Perimeter defenses are well-tested protective elements that have been used for thousands of years. Instead of protecting each house in a city against invaders, walls were built around the city, and well-guarded gates controlled access to the city. Often, there were lesser entry points through the walls, for convenience or special uses. These included “postern gates,” which were small entrances far from the main gates. There are numerous tales of cities that fell because their perimeter defenses were subverted by these little-known entry points. Spies on the inside, who find these long-forgotten “postern gates”, provide an entry point for hiding malicious activity leading and including a breach.

These unknown or unauthorized entry points are leaks – a means to malicious or unauthorized entry across the network perimeter. Firewalls and intrusion detection systems serve as gatekeepers to defend the network; nevertheless, circumvention can and does happen. Unlike data leaks, which represent the egress of sensitive information from an organization’s control, Internet leaks are unrestricted pathways into and/or out of an organization’s network perimeter. Malicious attackers use these paths to infiltrate networks, compromise endpoints, shuttle additional malware, install encryption software for ransomware, move laterally to find sensitive data, and even take over additional systems through more infections. According to a **Ponemon Institute and an IBM survey** enterprise losses from attack activities, which use worms, viruses, spyware, and other attack vectors, average $3.6M annually in 2017. If one includes additional recovery and reputation costs, that figure grows even larger.

Why Are Leaks So Common?

Continuous changes to the network landscape, including infrastructure, operating systems, and applications can cause organizational security policy and network defense configuration to become misaligned, contributing to a proliferation of leaks. And it only takes one leak to allow malicious intrusion into a network.

The root of some of the most dangerous leaks comes courtesy of manufacturers, according to SANS.[1] The SANS ‘Top 20'[2] identifies the most critical and/or common vulnerabilities in Windows, UNIX, and Linux environments, many of which are likely to create leaking ports. For example, vulnerable ports may be open by default, creating holes that are the easiest and most convenient route for attackers to exploit. The Blaster, Code Red, and Slammer worms can be attributed to these vulnerabilities. In addition, vendor products may be defaulted to enable routing and remote access. If these are not properly secured, the impact of these vulnerabilities can include denial of

[1] *The SANS™ Institute (SysAdmin,Audit,Network, Security). Bethesda,Maryland.www.sans.org.*

[2] *SANS Top-20 Internet Security AttackTargets (2006 Annual Update). The SANS Institute.*

service attacks, exposure or compromise of sensitive files and data, random command execution on the server, or complete server intrusion. Until all software is one hundred percent hardened by default, it is essential to evaluate the configurations of servers and enable only the features and services required.

At the same time, outside manufacturers cannot take all the blame. With today's overly complex network infrastructures, it is understandable that we commonly see Improperly configured VPNs, routers, and switches that all leave networks susceptible to unauthorized access to host or end- point devices. In addition, host computers may be enabled to allow IP forwarding without proper packet filtering configurations. All the cases reflect the ease at which defense configuration can become misaligned with security policy. In modern decentralized organizations, control over business units and the management of IT assets often becomes disconnected. As an increasing number of network configuration and connectivity decisions are made by more people, disparate management controls combine with inconsistent enforcement of security policies to compromise access control lists that govern connectivity both to and from the Internet.

A third issue is outsourcing. Outsourcing, whether an organization's entire IT infrastructure or just security services, has become a widely adopted, cost-conscious business practice. However, outsourcing configuration errors, where the perimeter of one or more networks are not secure, can allow "bleeding" of one outsource customer's network into another. This kind of misconfiguration can allow outsiders to find pathways into a network. Not monitoring the security of out- sourced connections can have dire consequences and ultimately decrease security, compliance and availability of core business infrastructure – the very areas that outsourcing is designed to optimize.

Lastly, the proliferation of unknown and rogue connections creates a breeding ground for leaks. Common sources of rogue connections include acquired business units that do not have accurate network documentation, divested business units where connections were not terminated in accordance with the new business structure, unsanctioned wireless network connections, and remote network connections established by even the least technically-savvy end users such as a simple wireless access point.

Proactive identification of leaks and exposed network zones allows effective prioritization of remedial resources to prevent network subversions. The only answer comes down to real-time leak discovery as a powerful mechanism for comprehensively protecting an organization's network.

Inbound vs. Outbound Leaks

Leaks can allow traffic to bypass security provisions into and out of a company's enterprise network. Hence, they are generally referred to as "inbound" and "outbound" leaks, respectively. These unsafe passageways provide hackers, worms, viruses, and other unwanted web flotsam free access to enterprise resources.

Inbound Leaks

Most companies restrict inbound traffic to minimize the company's vulnerability to worms, real-time hacking, and other attacks. Inbound leaks almost always pose a significant threat. Detection of an inbound leak is an indicator that security controls have been bypassed. Every security policy will have guidance to block unauthorized connectivity since the advent of the fire- wall and DMZ, however these solutions are only as effective as their individual configurations.

Outbound Leaks

Companies vary in how stringent they are about what exists inside their networks. While some feel that if they control inbound traffic, they are sufficiently protected, others endeavor to maintain higher control of outbound traffic to help prevent internal infections from leaving the company and attacking elsewhere, particularly in today's environment of increasing insider threats. These are scenarios that could result in negative publicity or legal consequences. Reducing the number of outbound leaks significantly minimizes the likelihood that an intruder can compromise a system within a network and launch further attacks on the outside – resulting in a situation in which the company's system appears to be at fault.

Outbound leaks are often seen as less critical than inbound leaks. Nevertheless, organizations often use the lists of outbound leaks to validate stated corporate security policies used by divisions or sub-groups within the organization. Outbound leaks also show the Network Address Translation (NAT) devices in the network. If multiple rows in the table have a corresponding IP address, then that is probably the IP address of the device that is performing NAT for a portion of the network.

Methodology

Real-time monitoring for both inbound and outbound connectivity to and from the Internet via multiple protocols including User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), Simple Network Management Protocol (SNMP), Domain Name System (DNS), and user-specified Transmission Control Protocol (TCP) and UDP ports. From there, re- ports should be generated to clearly and accurately present the gathered data for informed task prioritization.

Only through collection of a comprehensive set of network facts, including tests from every port using multiple protocols, can organizations discover and ultimately remediate leaks.

Inbound Leak Discovery

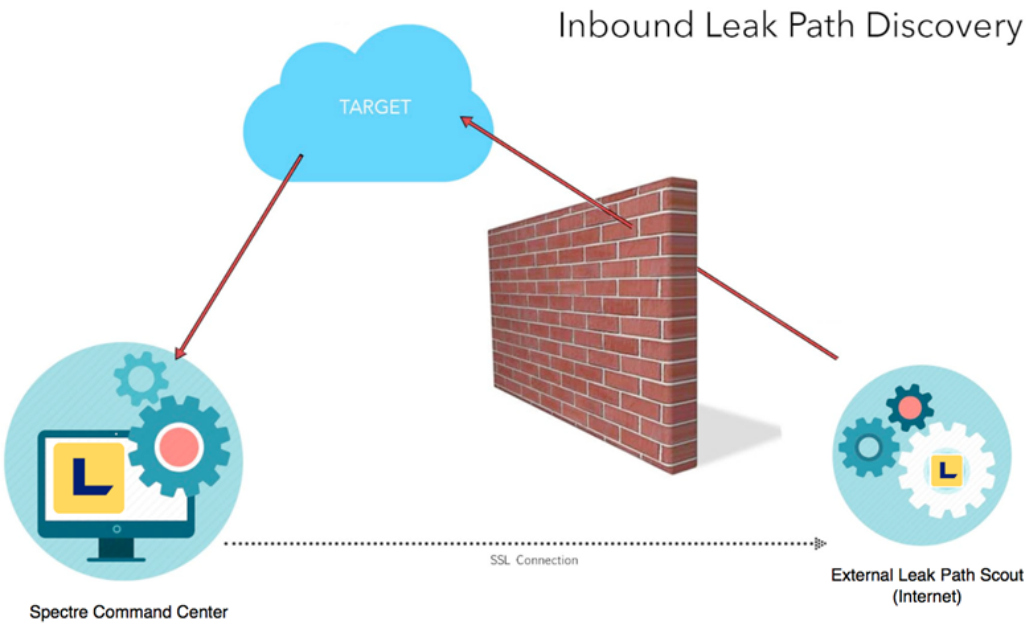


Figure 1: Discovering inbound leaks – A request sent from outside the network bypasses a firewall and is received, indicating an insecure port of entry – and the possibility that an unauthorized source can view the network from outside.

Outbound Leak Discovery

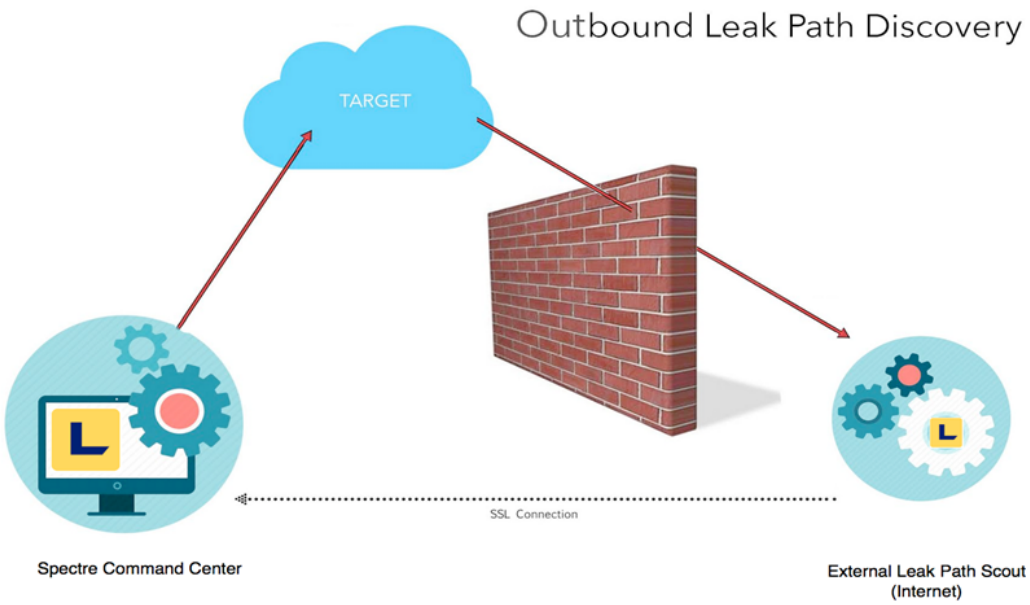


Figure 2: Discovering outbound leaks – Spoofed IP requests pass through nodes on the network. Leaking packets not blocked by the firewall are collected and reported.

Prioritized Patch Management and Data Leak Prevention with Leak Discovery

The results of inbound leak discovery enable organizations to see not only where leaks are present, but also which devices and hosts require the most critical response to control viruses that attack a port, such as the Slammer worm. Many organizations are reluctant to begin rolling out untested patches quickly in response to a spreading virus (often with good cause), since an untested patch could cause malfunctions in the network and may cause more harm than good. While a newly released patch is being tested, organizations can use Network Assurance scan results to rapidly identify which devices are running the port(s) vulnerable to the attack and which of those devices has leaks to and from the Internet.

Having identified the most vulnerable devices, organizations can take action to filter inbound traffic on the ports targeted by the virus. Once all of the leaking devices that use the targeted ports are protected, the organization can address the remainder of the non-leaking devices that run the targeted port. Prioritizing efforts and closing the most dangerous holes first ensures that critical devices that have a documented need to run particular services are running them safely. The solution also provides a well-defined list of devices that will need patching once the new releases have been sufficiently tested.

Patching and access restriction, driven by leak detection, also have an additional advantage as they repair or restrict potentially significant avenues for data leakage. If sensitive data resides on a system that leaks to the Internet, for example, it may be exploited and used in unauthorized data transmission or access (a “data leak”). This results in significant risk exposure for the organization – many of which have unfortunately been exploited with the exposures documented in the media. While data leaks can happen in a number of ways, proactive network leak prevention protects a potentially high exposure channel in the defense of sensitive data.

Mitigation Enables Lower Risk and Stronger Compliance

The structured detection, documentation, and remediation of leaking devices provides auditors with demonstrable justification that controls are in place to protect an enterprise or agency against any reasonable threats to network integrity and operations.

Leak discovery provides powerful capabilities for any public, private or government entity that must develop a compliant security policy for business risk assessment and incident response. Detecting and documenting leaks enables security organizations to get advanced level insight into vulnerabilities in the network and their potential

impact. Organizations should pay special attention to inbound leaks discovered and take great care in describing the measures and technologies that are being taken to protect these leaking devices against unauthorized logical access.

Leaks in the Broader Context of Network Assurance

Discovering leaks is a vital element of a proactive Network Assurance program. The ever- changing nature of today's networks creates constant changes in connectivity, infrastructure, and defense configuration. Security organizations can no longer afford to relegate vulnerability assessments to times of convenience – leak discovery must become a continuous process.

As important as leak discovery is, handling leaks is just part of the bigger picture. To create a fully secure network, organizations must have a full range of network capabilities, so they can:

- Make a baseline of network information
- Understand the true network perimeter
- Discover all unknown connectivity and unknown assets
- Shore up all leaks
- Handle rogue wireless devices

Network Assurance addresses dangerous gaps produced in risk management processes as rapid network change causes organizational security policy and network defense configuration to become misaligned. With the implementation of a comprehensive Network Assurance program, organizations can quantify risk from a network perspective, based on this comprehensive set of network facts. Using Network Assurance, companies can also prioritize remediation efforts based on a complete view of connectivity and risk. This is a critical requirement for validating policies and controls put into place to stop and prevent leaks, among otherissues.

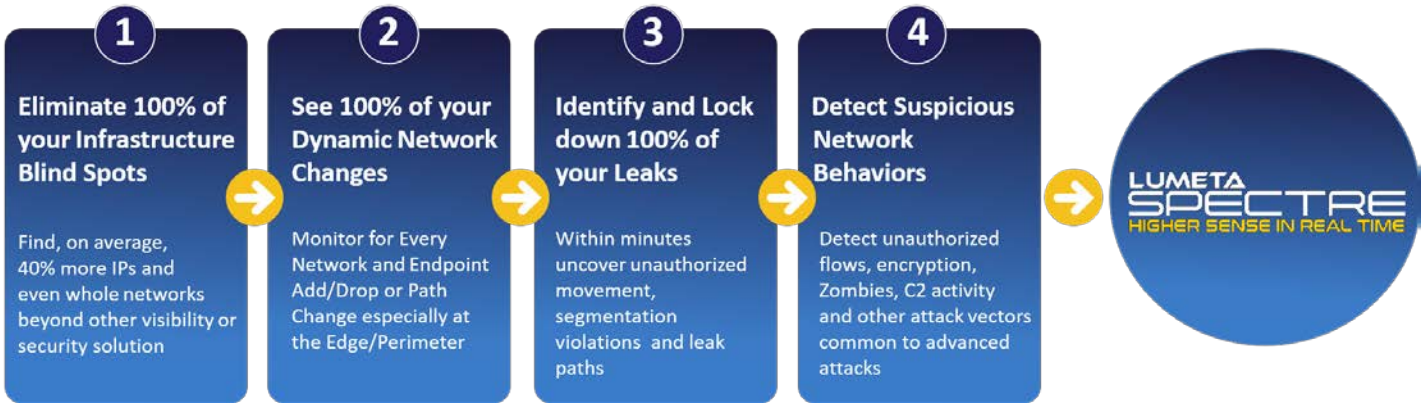
Continual internal and external forces keep network vulnerability in a never-ending state of flux. Although security products and policy management guidelines continue to evolve, there is ultimately no single proven solution to prevent all network leaks. However, consistent testing and assessment help bring companies as close as possible to achieving comprehensive security.

Leaks Detection and Mitigation in Real-Time

Research by Lumeta determined that over 40 percent of today's dynamic networks, endpoints, cloud infrastructure are unknown, unmanaged, rogue or participating in shadow IT, leading to significant infrastructure blind spots and network leaks by enterprise and government departments alike. Most often, these blind spots result from not having a comprehensive understanding of the entire network infrastructure, including leak paths that go undetected.

Lumeta Spectre for Eliminating Blind Spots and Detecting Leaks

Lumeta Spectre extends seamlessly and comprehensively across the entire enterprise infrastructure and into the cloud deliver full visibility, detecting leak paths, malicious network activity and ensuring segmentation. The platform's real-time change monitoring capabilities can detect segmentation and communication violations, leak paths and anomalous activity and threats with the potential to cause major damage to critical operations. Lumeta Spectre provides the following capabilities to eliminate infrastructure blind spots, detect changes and identify leaks:



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.

100% Real-Time Leak Path Detection

Identify ALL leak paths that you have today and in real-time not only to identify existing leak paths, but also new leak paths created in real-time. Adding threat intelligence, as described below, provides security context on leak paths being unauthorized, specific attack activity, misconfigurations or actual authorized change.

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 is the only solution to deliver 100% real-time IP infrastructure visibility, real-time network change monitoring and threat detection for preventing successful breaches in these critical environments. Lumeta Spectre provides unmatched *real-time* cyber situational awareness enabling network and security teams to not only identify even the darkest corners of your IP enabled, including dynamic network elements, endpoints, virtual machines and even cloud-based infrastructure paired with threat intelligence critical infrastructure but also monitor for changes or unusual behaviors without agents to detect and prevent threats that target these common gaps in visibility.

Lumeta Spectre can help organizations both protect and optimize the segmentation of sensitive areas of the network and critical infrastructure. In addition, Lumeta can help IT security teams validate segmentation policies and monitor for unexpected paths, lateral movement or any sort of changes, all in real-time.

To learn more contact Lumeta today to get more information or organize your POC.

http://www.lumeta.com/solutions/audit-compliance/

LUMETA
DETECT WITH A HIGHER SENSE