LUMETA
DETECT WITH A HIGHER SENSE

CASE STUDY

FILLING MAJOR VISIBILITY GAPS IN PROTECTING PATIENT RECORDS AND SECURING IOT DEVICES AT THE LARGEST NON-PROFIT HEALTHCARE PROVIDER IN THE US

Overview

Typical to many healthcare organizations, our customer consistently carries and handles protected health information along with medical history, patient names, addresses, phone, personal email, credit card and social security numbers, all of which make healthcare institutions an attractive target for hackers and other cybercriminals. Our Customer was looking to take steps to improve their data protection strategies to meet regulatory requirements and secure health information against costly data breaches. Below we review some of their specific challenges and how Lumeta Spectre was instrumental in their ability to solve these challenges.

Business Challenges: Customer was Concerned with Increasing Lack of Visibility into Potentially Vulnerable Systems and Networked Medical Devices

- Our customer recognized the existing lack of visibility into their infrastructure when it came to undocumented systems (including legacy systems), medical devices and shadow IT infrastructure. In addition to wired devices (IoT), there was an increasing number of unapproved wireless medical devices connecting to the network. The Network Infrastructure team struggled to identify existing unmanaged assets leaving them unmonitored, unpatched and unsecured in many cases leaving them targets for compromise and a insertion point for further penetration and potential breach.
- With major cyberattacks such as WannaCry, they were also concerned that these unknown and unmanaged systems would be left vulnerable to exploits by threat actors, despite the customer's existing vulnerability management program. Many recent cyberattacks against healthcare organizations were successful by targeting vulnerabilities in unmanaged and undocumented systems, leaving them unpatched.

CUSTOMER PROFILE

BUSINESS: Large Non-profit Healthcare Provider
LOCATION: UNITED STATES of AMERICA SIZE: 12,500 Employees
REVENUES: $3.3B
NUMBER OF FACILITIES (Incl Acquisitions): 65
NUMBER OF ACQUISTIONS: 3

HIGHLIGHTS AND BENEFITS

Post Implementation benefits include:

- Readiness to monitor for the recent Ransomware attacks by knowing redundant legacy systems and IP diagnostic devices.
- With the on-going increase of IoT devices Lumeta is the only solution to find 100% of the IP devices, whether cloud, VM, mobile or network infrastructure joining and leaving the network in real-time.
- Augmenting existing vulnerability management programs to increase coverage across the entire enterprise network and touch every endpoint as well as identify newly added devices for assessment.
- Along with full asset identification and change monitoring, network segmentation violations can be seen on-premise and within the cloud to ensure the Healthcare provider can adhere to HIPAA and GDPR by knowing routes to data access both authorized and unauthorized. This includes leak (unauthorized) paths to the Internet.

- The customer was looking to manage the risk associated with recent acquisitions. The requirement to integrate multiple networks, patient systems, and medical devices made it more challenging for the Network Infrastructure team to keep track of target assets and monitor the network for unauthorized changes and activity. The customer was also concerned with potential vulnerabilities being introduced by the acquired assets thereby exposing the parent company to increased risk of a breach.

- The company direction to move further into cloud environments to gain economies of scale and reduce costs was causing their visibility gap to be exacerbated. The hosting and transmission of PII across on premise and cloud environments without infrastructure visibility created a greater challenge in complying with HIPAA requirements.

The Solution

When Lumeta was considered as a potential solution, the security team was working on a network visibility strategy as part of a long-term, system-wide security plan. Lumeta was selected based on the following criteria:

1. Find a solution that could provide them the most comprehensive visibility across the entire network including connectivity across distributed medical facilities

2. Harden all systems against attack by improving their vulnerability management (VM) program and limiting the exploitation of systems and medical devices that could lead to the possibility of a data breach.

3. Manage risk throughout the process of merging acquired companies' IT infrastructure as well as integrating partner systems to provide seamless network availability, while ensuring medical records are still protected from theft.

4. Match successful on-premise regulatory compliance with cloud-based adoption of hosted and managed infrastructure defined by HIPAA and GDPR compliance regulations.

Lumeta Spectre was selected versus existing vendors claiming visibility, such as current vulnerability management partners, network access control vendors (often claiming IoT system identification), and even packet capture tools due to Spectre's ability to identify every network and endpoint in the enterprise, including unknown, unmanaged, rogue and shadow IT to get a real understanding of the overall IT landscape and all the IP address ranges.

Results Achieved with Lumeta Spectre

Lumeta Spectre was able to ***find 27% more endpoints*** than existing and competitive solutions. This included traditional network monitoring tools, existing vulnerability management solutions, SIEM via log collection and endpoint solutions requiring agents. Lumeta was able to eliminate this blind spot gap and continue to find and identify "transient" medical devices that hop on and off the network including remote facilities and even extending into cloud environments using a combination of passive listening and patented unobtrusive active discovery techniques, all without the use of agents.

This critical information was then directly provided to their vulnerability management solution, Tenable Networks Tenable.io platform because they needed to know all the IP addresses that comprise the network and fully understand their risk posture. The issue with current vulnerability management solutions is that they cannot enable protection to devices that they don't see, and ***Lumeta Spectre generally finds an average of around 40% more devices on any network***. This visibility gap essentially restricts the capabilities of these solutions in providing a true picture of the network vulnerabilities. With Lumeta, the customer was able to pro-actively patch traditional endpoints but also any medical devices that our VM partners could scan and report on, including newly added wireless devices.

Lumeta Spectre is unique in preventing breaches by also identifying all existing leak paths, while also finding unknown IP devices/connections to the Internet, which could potentially lead to harmful leak paths. Lumeta Spectre, upon initial deployment, went even further to ***discover over 120 existing unknown, potentially malicious leak paths*** to the Internet, while monitoring in real-time for new leak paths. The customer was able to provide a monthly report regarding potential new leaks created at their facility networks.

Through its ability to recursively index and discover all network and networked assets, Lumeta Spectre was used to calculate the cost of taking on the new hospital systems and the ability to protect the new network assets with the appropriate endpoint solution or SIEM. Post-acquisition, the organization feels confidence in bringing the new entity into core operations through a continuous process of real-time monitoring, rediscovery and understanding what's changing in the IT landscape. Lumeta Spectre gave the Network Infrastructure team a true picture of the infrastructure and security risk and the necessary visibility to ensure protection of patient data.

LUMETA CORPORATION 300 ATRIUM DRIVE
SUITE 302 SOMERSET NJ 08873 USA +1.732.357.3500

www.lumeta.com