CASE STUDY Regional Medical Facility

The medical facility is one of the largest private hospitals in the country offering a full range of advanced medical services, including oncology, surgery, and rehabilitation services. It employs nearly 1000 medical and other employees.

> *"We were really surprised by MENDEL. We thought we would see what happened after the free 30 day trial but ended up choosing it because it allowed our team to solve a huge amount of the issues we had been having immediately, without the expensive and lengthy search for new members of the team."* (David F. CIO)

Challenges

Despite its size, the facility's IT team is made up of only three members. Its network uses a variety of existing network security solutions, including endpoint security, enterprise firewalls (though some of these were outdated), and includes a well-segmented network structure, including a public wi-fi for patients, internal administrative segment, a segment for VOIP and emergency dispatch, internal medical data segment, and others.

While well designed, the facility network still faced several challenges. The IT team still missed out on network visibility as to the devices in the network at any given time, and had experienced several rare, but troubling security incidents. Though these had not resulted in data loss, they were alarming. The network faced chronic performance issues. The IT team lacked sufficient time and resources to handle the detected security incidents, and performance issues.

Objectives

The facility was looking for a security monitoring solution – specifically to perform security functions across the network, provide visibility and performance monitoring, and secure confidential patient data.

Advantages

The firm heard several presentations from other security companies, some of which focus on flow monitoring. None of these could match MENDEL's ability to provide security, visibility, and answer the challenges posed by the regulatory demands of medical practice.

Results

The firm is using the MENDEL All-in-One hardware appliance.

- MENDEL identified several security incidents both on the public Wi-Fi network and some on the internal network, which would have taken significant time to discover within MENDEL.
- The root of the performance issues was discovered and resolved
- A number of misconfigurations (which presented a security risk) were identified
- MENDEL served as an additional stop-gap measure by integrating with the facility's firewalls until a new firewall could be purchased.

Customer Summary

- IT & network administration team of 3
- 1000 employees
- Currently using endpoint security, enterprise firewall, well segmented network (Wi-Fi for patients, OT network, sensitive data), etc.

Challenges

- Lack of visibility into network traffic
- Rare security incidents w/o significant data leaks
- Older model of firewall
- Lack of time and tools to investigate security incidents
- Frequent/chronic performance issues reported by users

Results

- Easy to solve, but hard to detect security incidents discovered
- Root of chronic performance issues found and solved
- A number of misconfigurations with security risk were discovered and corrected
- Integration with existing firewall allowed for security during search for new hardware.

GREYCORTEX

GREYCORTEX uses advanced artificial intelligence, machine learning, and data mining methods to help organizations make their IT operations secure and reliable. MENDEL, GREYCORTEX's network traffic analysis solution, helps corporations, governments, and the critical infrastructure sector protect their futures by detecting cyber threats to sensitive data, networks, trade secrets, and reputations, which other network security products can miss.

Purkyňova 127, 612 00 Brno, Czech Republic, +420 511 205 216, info@greycortex.com, www.greycortex.com