TRAPX SECURITY

CASE STUDY

John Muir Health MODERNIZES CYBER RISK MANAGEMENT WITH DECEPTION TECHNOLOGY

TrapX DeceptionGrid™ Provides Visibility to IT and OT Networks

> **“We immediately identified things on the network that shouldn’t be there and were able to very quickly address them. If new things come up, we have a high degree of visibility to be able to detect them at the network level. We treat it like an early warning system. If something is moving around on the network, generally speaking, we’ll see it.”**
> — Thomas August, VP and Chief Information Security Officer (CISO) at John Muir Health

Cybersecurity Challenges Within the Healthcare System

Headquartered in Walnut Creek, California, John Muir Health is an integrated system of professionals, facilities, and services. The extensive network serves thousands in the region and includes two of the largest medical centers in Contra Costa County. John Muir Health leadership is committed to protecting sensitive assets and patient safety. The organization equates information security with the well-being of those they serve. Quality of care and safety remains a priority as John Muir Health strives to keep up with sophisticated attacks.

Hospitals and other medical organizations deal with a high number of devices such as servers, workstations, machines, and medical devices. Each component requires specific configurations and are managed in a variety of ways. Network visibility is a challenge due to this large volume of unique assets. As risk levels vary from device to device, a way to observe malicious traffic is essential to cybersecurity effectiveness.

Tom August, Vice President and Chief Information Security Officer, decided to fight cyberattacks through a risk-based program beyond standard compliance. Upon taking his position, August determined a layered, threat modeling based approach would reflect a more modern view of risk management. “Gaining visibility into the network became our first priority. We reviewed what the options were to determine which tools were available to do the job,” he said. As a result, the Vice President and Chief Information Security Officer turned to TrapX for a solution.

TrapX Provided a Preventive and Proactive Solution

Infection through outside vendors or inside devices and users is a growing threat within the healthcare sector. TrapX is a leader in deception technology providing real-time visibility throughout all IT and OT environments. TrapX actively attracts, isolates, and exploits threats via strategically-placed traps disguised as system assets. TrapX decoys pinpoint malicious threats to provide actionable intelligence when disturbed. This form of real-time breach detection is a proven method for private and public enterprises around the world.

TrapX DeceptionGrid™ fully integrated with John Muir Health logging systems to provide insight into system activity. Traps immediately alerted John Muir Health’s security team to suspicious activity due to malware infection or misconfigured devices. Adjustability was key as the platform recognized threats and misconfigurations before damage could occur. The unobtrusive nature of TrapX made this a viable solution within even the most sensitive of environments.

CASE STUDY

John Muir Health Expanded the TrapX Deployment to Every Corner of Their Network

"It was important for us to get visibility into what was happening on the network so we could determine whether any attacks were occurring. An easy way to assess whether you have malicious activity going on at the network level is to deploy honey pots," said Tom August, Vice President and Chief Information Security Officer of John Muir Health. **"For us, TrapX's product acts as an intelligent honey pot that can be customized to look like it belongs to the network."**

"When we initially deployed TrapX, we immediately identified things on the network that shouldn't be there and were able to very quickly address them," August reported. TrapX's ability to detect, deceive, and adjust to a variety of cyber threats reduced cyber risk.

CYBERSECURITY CHALLENGES IN THE HEALTHCARE SECTOR

- Older or unpatched operating systems
- Many devices with unique configuration requirements
- Lack of access to systems managed by third-party vendors
- Impact of cyberattacks on medical services and facilities
- Lower patient care quality and efficiency
- Failed processes or unexpected performance
- High exposure of sensitive patient information
- Damage to provider reputation

KEY BENEFITS OF TRAPX'S DECEPTIONGRID

- An affordable and scalable early warning cybersecurity solution
- A reduction in reliance on disruption-based cybersecurity measures
- An ability to integrate itself with existing processes and operations
- Improved detection focused the security team on real threats
- Real-time analysis enables immediate action against incoming cyber threats

TrapX Security, Inc.
303 Wyman Street
Suite 300
Waltham, MA 02451

+1–855–249–4453
www.trapx.com

sales@trapx.com
partners@trapx.com
support@trapx.com

About TrapX Security

TrapX has created a new generation of deception technology that provides real-time breach detection and prevention. Our proven solution immerses real IT assets in a virtual minefield of traps that misinform and misdirect would-be attackers, alerting you to any malicious activity with actionable intelligence immediately. Our solutions enable our customers to rapidly isolate, fingerprint and disable new zero day attacks and APTs in real-time. TrapX Security has thousands of government and Global 2000 users around the world, servicing customers in defense, health care, finance, energy, consumer products and other key industries.