



Keeping A Major Teaching Hospital Healthy

CounterStorm-1™ delivers unparalleled internal network security to one of the world's largest hospital systems.

The Challenge

This major teaching hospital with three campuses and more than 15,000 employees, had a network security challenge that existing security solutions were unable to address. While the hospital already deployed a perimeter solution that protected its network from the outside, there still was the potential for security breaches to occur from inside the network. A combination of worms and botnets could threaten the integrity of the internal network and put confidential digital assets and patient information at risk.

Healthcare Requirements

The hospital had several requirements for an internal network security solution which were common to the healthcare industry:

- **Third party access:**

The hospital had to offer flexible network access to physicians, medical students, consultants and vendors, all using devices not owned or managed by the hospital. These devices could potentially be infected with worms, botnets and viruses.

- **Securing unpatched medical devices:**

The hospital needed to quickly and easily secure unpatched devices. However, in some cases these devices could not be taken offline to either patch or upgrade, the legacy hardware could not support the new patch, upgrading was too expensive, or an upgrade/patch invalidated the manufacturer's warranty.

- **HIPAA requirements:**

The hospital was required to meet a series of HIPAA regulation compliance dates. The main challenge in the legislation was keeping patient information accessible, but confidential. They needed a solution that protected against compromises and potential patient information leakage in order to comply with HIPAA regulations.

- **Protecting high-valued assets and life critical services:**

The hospital needed to identify attacks accurately and within seconds. Once identified, it was essential to quarantine the malicious computer or device, in order to isolate it from the network, and eliminate any possibility of infection propagation. While all enterprises have mission critical services, the hospital was faced with ensuring that "life critical" service remained online and fully functional at all times.

The Solution

The hospital deployed CounterStorm-1 in its network to address each of its requirements. CounterStorm ensures that the hospital's mission critical services stay up and running during attacks by protecting its online assets, including confidential data and records.

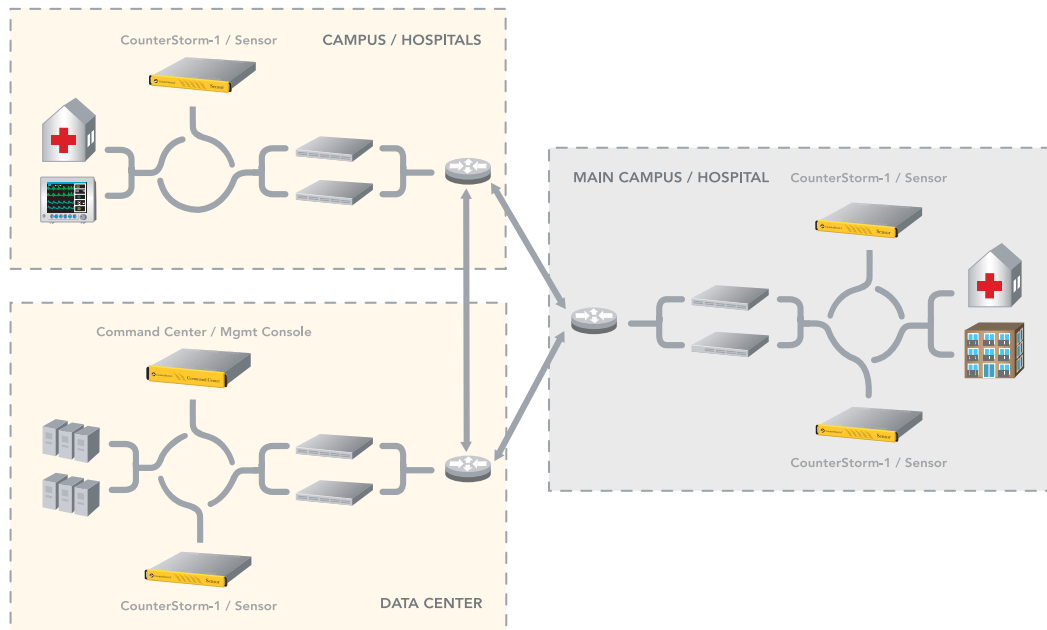
"False positives are a costly and time-consuming problem, and having a technology in place that greatly reduces this issue is very important to our organization."

Information Security Officer

Deployment

CounterStorm was deployed across three campuses. Suspect traffic was immediately and accurately identified and devices were quarantined in seconds for remediation.

At the main campus, CounterStorm-1 protects the hospital and dormitory facilities. At additional hospital campuses, CounterStorm-1 protects the hospital and medical devices. At the data center, CounterStorm-1 protects mission critical/high value devices and services. The Command Center is also deployed at the data center and provides full visibility and control to the entire deployment.



RESULTS & BENEFITS

By deploying CounterStorm-1, the hospital achieved:

- **Immediate identification (within seconds)** of attacks that may be introduced on the internal network and could have disabled large portions of the network. In many cases, this is a challenge that existing security solutions are unable to address.
- **Unparalleled accuracy** in identifying real attacks, giving the IT department a greater assurance that they will not be deluged with large numbers of false positive alarms.
- The ability to **quarantine infected devices in real-time** to quickly stop attack propagation and eliminate the spread of attacks to mission critical services.

Differentiators

- **Real-time internal network attack detection**
"CounterStorm protects our multi-tiered network by identifying internal network threats and offers the ability to neutralize them immediately."*

- **Highly accurate**

"False positives are a costly and time-consuming problem, and having a technology in place that greatly reduces this issue is very important to our organization."*

- **Immediate ability to stop/quarantine attacks**

"[CounterStorm] is instrumental in detecting and remediating worms and other malicious or accidental attacks aimed at our network, [and it's] particularly relevant for the complex security and availability requirements for medical devices."*

- **Delivering valuable protection to the healthcare industry**

"CounterStorm-1 provides an essential function to our overall internal network defense, which allows us to maintain the security of the campus, as well as ensure our compliance with HIPAA regulations."*

About CounterStorm

Based in New York City, CounterStorm, Inc. is the maker of CounterStorm-1, the only internal network security solution that effectively stops zero-day and targeted attacks in seconds. This unprecedented protection is being used by a wide variety of government agencies and global enterprises, as CounterStorm-1 is the fastest and most accurate network attack detection and blocking device available.

For more information, please visit <http://www.counterstorm.com> or call us at (212) 206-1900.

* Quotes from the hospital Information Security Officer