

# Boston Medical Center (BMC)

HP Enterprise Security Customer Case Study

**“The quick response capability that ArcSight TRM provides has prevented any major damage from occurring—every single time.”**

—Robert Monks, Network Manager, Boston Medical Center



## Customer Brief

Boston Medical Center is a private, not for profit, academic medical center located in Boston, Massachusetts. Emphasizing community-based care, BMC's mission is to provide consistently accessible health services to all.

## Product(s)

- ArcSight Threat Response Manager (TRM)

## Business Benefits

- Enables BMC to respond quickly to incidents and prevent any major damage from happening
- Helps ensure the overall safety and security of BMC's IP networks
- Successfully quarantines infected nodes before attacks can propagate



## HP Enterprise Security Customer Case Study:

ArcSight TRM enables non-profit Boston Medical Center to increase efficiency by providing dramatically faster and more effective incident response.

**Industry:** Healthcare

## Boston Medical Center's Challenge

Boston Medical Center operates a robust data network designed with security and stability in mind. The network consists of more than 10,000 nodes and contains a range of advanced technologies including voice over IP and wireless and network-enabled medical systems.

Despite a large investment in cyber-security prevention and detection technologies, BMC still had to respond to a proliferation of viruses, worms and other incidents. Cyber attacks occurred at all hours of the day. Network operators were expected to make quick decisions under pressure, and to take appropriate actions without endangering the availability of business systems and mission-critical traffic flows.

While a manual incident response plan had been put in place, the time it took to respond was simply not fast enough. First, a senior network engineer had to be contacted and informed of the incident. From there, the engineer had to analyze the network and determine which devices were impacted by the incident. Commands would then have to be issued to other



network devices to determine if the infected node was connected to any of them. After that, IT and business constituents had to be notified and all changes thoroughly documented.

Rapidly locating and quarantining infected nodes was a struggle and limited to a few senior engineers. By the time an engineer located and disconnected the infected node, the attack had propagated exponentially. The associated cost, loss of service and impact on patient safety from these incidents was too great to ignore.

## The ArcSight Solution

BMC had one primary goal with ArcSight Threat Response Manager™ (TRM): to eliminate time-consuming, manual procedures and replace them with a consistent, automated incident response strategy.

Shortly after deploying ArcSight TRM™, BMC was hit with a worm infection. This time, BMC staff was able to use ArcSight to quickly and easily quarantine the infected workstations before the attack could spread across the network—meeting and exceeding the medical center's greatest expectations.

BMC was also very impressed with how easy ArcSight TRM was to implement and how quickly it was able to benefit from the system. "ArcSight supported all our existing network devices. It was amazing that no changes to our device configurations were required, and we did not need to deploy any clients or agents on our desktops and servers," said Arsen Khouznoutdinov, a senior network engineer at BMC responsible for deploying the solution. "We were fully operational in just a few hours. Overall, ArcSight TRM was one of the easiest systems I have ever implemented."

## The ArcSight Impact

Thanks to ArcSight TRM, instant and effective incident response is now the norm at BMC, not the exception. The medical center is consistently able to contain and isolate infected nodes before there is any impact on its critical network. "Attacks occur despite our IPS/IDS solutions—that's a fact," said Robert Monks, network manager at BMC. "But the quick response capability that ArcSight provides has prevented any major damage from occurring—every single time."

BMC has benefited from many other features of the system beyond the quarantining of nodes. For instance, BMC is now able to leverage additional staff in the response process through the simple Web interface of ArcSight TRM. Moreover, the organization relies on the system's "self-documenting" feature to ensure all appropriate network configuration changes and incident details are automatically captured in a report.

"With the increased complexities of defending a mission-critical network, and the stakes being raised every day, it is clear that tools are needed to prevent, detect and react to problems," said Darren Dworkin, CTO of BMC. "ArcSight TRM enables us to round out our product portfolio by adding a strong reaction tool that helps us in our overall goal of ensuring that our IP networks are safe."

