# Geisinger Customer Story

How Geisinger Implemented ThreatSTOP DNS Firewall to Eliminate Security Breaches

ThreatSTOP

Geisinger

## Customer Overview:

Geisinger Health System is an integrated health services organization widely recognized for its innovative use of the electronic health record and their development of cutting-edge care delivery models. As one of the nation's largest health service organizations, Geisinger serves more than 3 million residents. The physician-led system is comprised of approximately 30,000 employees, including 1,600 employed physicians, 12 hospital campuses, two research centers and a 510,000-member health plan.

## Security Challenges:

Geisinger's DNS servers had limited security capability, and provided very little visibility into the network. Detecting and stopping malware and botnet infections across vast and varied endpoints was a serious challenge, and was driving up risk.

## Why They Chose ThreatSTOP

Geisinger selected ThreatSTOP to stop threats that other controls had missed. The automated and cloud-based solution added zero footprint, required no hardware, and deployed quickly. ThreatSTOP provided critical network visibility that revealed and proactively blocked unknown malware in the network.

## Solution Impact

**Full Visibility**
For monitoring and remediation

**DNS Protection**
of 50K devices against attacks

**Remediation**
of compromised medical device

> *“ThreatSTOP caught the most threats, has the best interface, and is able to determine threat activity at the device level."*
>
> Rich Quinlan, Senior Technical Analyst

## The Problem

The Geisinger Network IT department had systems in place to protect their network from security threats, but had limited visibility into where threats may reside, and limited mechanisms to protect their DNS servers from attack. Geisinger began looking to add an additional layer of protection and functionality with a DNS firewall, conducting a bakeoff of solutions to choose the right one for them.

The team tested a competing cloud-based service and found it lacking because it could not identify which machine made the request for a tainted domain. Rich Quinlan, a Senior Technical Analyst in the Network IT department, stated that although he now knows that there is malware in the network, "with 50,000 devices, we need to know which device requires remediation." They needed a solution that would provide visibility.

*"In the spirit of it all, the ThreatSTOP DNS Firewall is one of those products that if you are not just trying to meet the letter of the law, but protect your environment, it just makes a ton of sense."*

## The Solution

During the ThreatSTOP DNS Firewall proof of concept, Rich's team identified that a clinical device—an ultrasound machine—was making queries to a command and control server in a foreign country. The machine was later determined to have been infected by a vendor during a service call to install patches via a USB drive. Rich stated, "The ThreatSTOP DNS firewall prevented the attack and gave us visibility into a large number of DNS queries that were being blocked. It also enabled us to quickly track down the infected ultrasound making the calls. That sold the product."

In addition to protecting clinical equipment, employee machines and servers, the ThreatSTOP DNS firewall also safeguards users of the guest network. "On our guest network, we see a lot of activity, but there is not much we can do about those machines. At least we can block malicious domains and protect guests' machines while they're using our network."

## Results - Effective Protection and Peace of Mind

The Geisinger team is using a combination of the ThreatSTOP threat intelligence service and the ThreatSTOP DNS Firewall. In a medical environment with many devices, and many devices types—including medical equipment that cannot be updated with new security rules or policies—ThreatSTOP provides a unique and powerful layer of security at the perimeter that protects every device on the network from inbound attacks and data theft. It blocks all malware types from reaching end-user and network equipment with an automated, cloud-based service that provides detailed reports on what was blocked, and the machines affected for quick remediation.