Operation Smile

CUSTOMER STORY

How a Medical Charity Got Ahead of Advanced Threats Attacking Their Network

CUSTOMER OVERVIEW

Operation Smile is an international medical charity that has provided hundreds of thousands of free surgeries for children and young adults in developing countries who are born with cleft lip, cleft palate or other facial deformities. Founded in 1982, Operation Smile has extended its global reach to more than 60 countries through its network of credentialed surgeons, pediatricians, doctors, nurses, and student volunteers. It is one of the oldest and largest volunteer-based organizations dedicated to improving the health and lives of children worldwide through access to surgical care.

SECURITY CHALLENGES

The charity was in need of a security solution that would adequately protect their headquarter network, as well as their large databases of patient data from 60 different countries stored on Azure servers.

WHY THEY CHOSE THREATSTOP

The Operation Smile team selected ThreatSTOP because its cloud-based security solution offers quick, reliable and automatic protection from malicious inbound IP and DNS attacks, and allows them to manage and protect both on-premise and Azure databases.

"When we began using the product on premise, we immediately saw what was hitting our firewall on a regular basis. Definitely a success story for us."

- Christopher Ackerman, Application System Analyst

SOLUTION IMPACT

Full Visibility
into the network

Attacks Blocked
automatically

Azure Protection
for data on the cloud

ThreatSTOP

THE PROBLEM

The Operation Smile IT team manages and secures the largest database of patient data in the world, across 60 countries. The charity supports both clinics and missions. They manage data on premise at brick and mortar locations and Azure in countries where they do not have a physical location. Operation Smile then brings anonymized data from all locations and the cloud to a central database in Azure for analysis to make smarter choices on how to deploy surgical teams for missions and look for trends in healthcare needs.

The team was looking for a way to secure all of the patient data from its network of on premise and Azure databases around the world. According to Christopher Ackerman, Operation Smile's Application System Analyst, “medical data is a highly valuable target for hackers. In the past 12 months a number of charities and non-profits have been targeted by hackers. Terrorists have also tried to hack medical data and hold it for ransom. We are trying to stay ahead of that.”

THE SOLUTION

Operation Smile originally deployed ThreatSTOP’s IP Firewall at its headquarters to block both inbound attacks and prevent outbound communications with threat actors, immediately seeing results. To secure electronic medical records in Azure, Operation Smile is using ThreatSTOP’s DNS Firewall. DNS Firewall protects cloud workloads by automatically delivering continuous threat intelligence to Azure DNS servers based on user-defined policies to prevent data theft and corruption by stopping malware from “phoning home” to threat actors.

Adding DNS Firewall to their security platform was an easy choice. Since the team was already using ThreatSTOP on premise, it was the clear choice to continue using ThreatSTOP for Azure in the cloud. This allowed Operation Smile to keep the same security policies across on premise and cloud databases. “Azure has become an extension of our on premise datacenter. We leverage the compute power on the cloud." According to Ackerman, “**Working with ThreatSTOP really makes sense for us from a business standpoint. We have a relatively small IT team for an organization of our size. With ThreatSTOP, we can stay ahead of the hackers**.”

"The ability to manage and protect both on premise and Azure with ThreatSTOP is beneficial and crucial for what we do."

RESULTS - *Effective Protection and Peace of Mind*

The ThreatSTOP platform is a proven, easy and cost-effective cloud service that stops the pervasive botnet and malware problem at the gateway before damage is done. Automatically aggregating over 900 threat intelligence sources, it protects against all cyberthreats and data theft without the cost, time and complexity of a forklift upgrade that most other solutions require. ThreatSTOP's web-based reports provide a simple and effective diagnostic as well as remediation tool for IT and security professionals to protect their networks.