UNIVERSITY OF BALTIMORE

# CUSTOMER STORY

***How UBalt** Strengthened Their Endpoint Security and Saved a Drowning Help Desk*


## CUSTOMER OVERVIEW

The University of Baltimore is part of the University System of Maryland with approximately 6,400 undergraduate and graduate students in law, business, public affairs, the applied liberal arts and sciences. Its law school is the nation's sixth largest public law school. Its network consists of several data centers firewalled by Juniper Services Gateways and a Cisco router and switch network environment. The primary security product used prior to ThreatSTOP was Symantec antivirus.

## SOLUTION IMPACT

**Full Visibility**
in to the network

**Over 180K**
attacks blocked per week

**90% Drop**
in help desk tickets

### SECURITY CHALLENGES

Despite ongoing user education efforts and security controls in place, users continued to respond to phishing and visit malicious websites which led to infected hosts. This forced constant blacklisting of IP addresses as well as cleaning malware infections that were getting through perimeter defenses.

### WHY THEY CHOSE THREATSTOP

The university's team 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, solving their help desk ticket overflow problem.

*"Our Help Desk team was overwhelmed. The whole malware problem was over-utilizing vital resources"*

*- **Mike Connors**, Information Security Analyst*

# THE PROBLEM

Like most higher education institutions, University of Baltimore provides an open academic environment for learning and knowledge sharing, which makes information security a particularly tough challenge. It was expending significant security, network, and desktop resources to manually keep up with blacklisting IP addresses as well as cleaning malware infections that were getting through perimeter defenses. Despite ongoing user education efforts and other security controls in place, users would continue to respond to phishing and visit malicious websites which led to infected hosts. The university needed a way to limit users' ability to interact with phishing and exposure to bad sites while maintaining an open academic environment, as well as a way to automatically block threats that were getting through, freeing staff for other tasks not associated with malware infections.

# THE SOLUTION

After months of evaluation, University of Baltimore selected Juniper SRX Services Gateways and ThreatSTOP Shield for its firewall upgrade project. Other products such as OpenDNS were evaluated but didn't satisfy UB's need. OpenDNS only blocks by domain names, which is not granular enough, and UB receives a lot of malicious traffic via bad IPs.

In one instance during their initial roll-out, a high-privileged user was discovered to be "botted." ThreatSTOP stopped the bot from "calling home" and activating a breach. This allowed UB's IT help desk to quarantine the machine before any damage was done. The ThreatSTOP service includes web-based reports parsed from customers' firewall logfiles, enabling them to discover, analyze and remediate malware infestations - fast.

> *"The decrease in malware/virus incidents has allowed our team to focus on other tasks."*
>
> *- Dave Wells, Call Center Manager*

# 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.