ThreatSTOP™

Customer Stories:
FireHost

“Decrease the number of total attacks against our customers by about 40 percent.”

firehost™
SECURE CLOUD HOSTING

FireHost
Richardson, TX

The Problem

- Protect FireHost and its customers against botnets, phishing, zero-day attacks and other advanced threats.
- Provide security required for customers with HIPAA, PCI or other compliance requirements..
- Filter malicious attacks at the network perimeter layer.

www.threatstop.com
sales@threatstop.com
US: 760-542-1550

Customer Overview

FireHost is the leader in secure cloud hosting, protecting sensitive data and brand reputations for some of the largest companies in the world. FireHost’s cloud infrastructure was purpose-built for security, compliance, performance and service. FireHost’s managed cloud IaaS services are provided from data centers in Dallas, Phoenix, London and Amsterdam.

FireHost focuses on serving hundreds of customers in the healthcare, retail, e-commerce and markets that **need to comply with HIPAA, PCI** and other regulatory mandates. As a leading cloud hosting provider that hosts critical financial and personal health data, FireHost is a constant target for cyber criminals and “bad actors”.

Examining the Issue

To provide customers the most secure cloud hosting available, FireHost needed a solution to filter and block communication with untrustworthy IP addresses. Even with existing firewalls and security solutions, FireHost felt exposed as it continued to witness attacks originating from Asia, Russia and Eastern Europe. As FireHost has customers around the globe, geographic IP blocking wasn’t an option.

How ThreatStop solved it:

FireHost recognized that by blocking communication with known “bad actors”, that an IP reputation management based approach would help provide needed additional protection and improve network utilization.

Due to its effectiveness and flexibility versus other IP reputation services and approaches, FireHost quickly decided on the ThreatSTOP IP reputation solution. ThreatSTOP is now fully deployed and providing protection for all of FireHost’s global data centers.

Results:

With ThreatSTOP, FireHost is now able to block inbound attacks before they reach the firewall, reducing risks to its operations while also reducing demands on compute and network resources required by existing solutions. ThreatSTOP now filters approximately 41% of the attacks on FireHost across all of its data centers, providing the following benefits:

- Over 138,000 daily attacks on FireHost and its customers now blocked.
- Improvement in overall network performance and utilization.
- No additional servers or infrastructure required.

Through the first half of 2013, ThreatSTOP has already blocked nearly *24 million attacks.* By blocking attacks at the perimeter, FireHost is also able to extend the life of existing network infrastructure by improving overall utilization and performance. ThreatSTOP is now a key component of the best-in-class security technology and expert configurations that comprise FireHost’s Intelligent Security Model™.

> *“ThreatSTOP filters many types of illegitimate traffic including botnet command and control servers, botnet zombies, phishing attempts, spam and other malicious sources. Implementing this system has helped to decrease the number of total attacks against our customers by about 40 percent.”*

-Chris Drake
Founder, CTO FireHost

ThreatSTOP™

The Solution

- Over 138,000 daily attacks on FireHost now blocked..
- Improvement in overall network performance and utilization.
- No additional servers or infrastructure required.

www.threatstop.com
sales@threatstop.com
US: 760-542-1550