ThreatSTOP™

Customer Stories: Cirrus Tech

"They were knocking down the door faster than we could respond."

Cirrus Tech
Toronto, ON, Canada

The Problem

- Protect Cirrus and its customers against DDOS, brute force, zero-day and other advanced threats.
- Provide protection required by gov't and health care customers.
- Identify geographic sources of suspicious network traffic.

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

Customer Overview

Cirrus Tech is one of Canada's largest web hosting companies and a leading provider of comprehensive Internet services. Cirrus cloud hosting services, named CloudTO, provide customers elastic cloud hosting, cloud VMs and private cloud environments. Founded in 1999, Cirrus Tech has been named a Top 10 cloud hosting provider by HostReview.

Cirrus Tech hosts nearly 100,000 domains and thousands of VMs, with customers relying on Cirrus Tech to host their websites, web applications, email, VPS hosting and other managed IT services. As all infrastructure is public-facing, Cirrus Tech is a constant target for cyber criminals and "bad actors". Attacks come in a wide variety of forms, including brute force and distributed denial-of-service (DDOS) attacks, as well as attacks on customer applications.

Examining the Issue

ICirrus Tech operates three data centers in the Toronto that support its web and hosting operations. To satisfy the requirements of customers in the government and health care sectors, Cirrus Tech needed to provide protection against DDOS, brute force, zero-day attacks, APTs and other advanced threats.

Even with existing firewalls and security solutions, Cirrus Tech still felt exposed. As Cirrus Tech has customers not just in Canada but around the globe, geographic blocking wasn't an option.

How ThreatStop solved it:

Cirrus Tech recognized that an IP reputation-based approach would help provide needed additional protection and make Cirrus virtually invisible to hackers, criminals and other "bad actors". Due to its ease of configuration and use versus other IP reputation services, Cirrus quickly decided on the ThreatSTOP IP reputation solution. Once purchased, ThreatSTOP was fully deployed and providing protection for Cirrus Tech's datacenters in less than an hour:

Results:

With ThreatSTOP, Cirrus Tech is now able to block communication with "bad" IP addresses associate with DDOS and brute force attacks, reducing risks to its operations while also reducing demands on compute and network resources required by existing solutions. After deploying ThreatSTOP Cirrus Tech has realized the following benefits:

- 60-70% daily reduction in DDOS and brute force attacks.
- Elimination of network slowdowns due to attacks and hacking activity.
- Overall improvement in network performance and utilization.

With ThreatSTOP's industry leading IP reputation solution, Cirrus Tech has protected itself and its customers from the risks from DDOS and brute force attacks that antivirus, malware and other security solutions fail to address. It now has the protection required to address the security and compliance needs of government and health care customers, particularly as they begin to consider Cirrus Tech's cloud services.

The Solution

- Up to 70% daily reduction in DDOS other brute force attacks.
- Virtual elimination in network slowdowns due to attacks and hacking..
- Improvement in network performance and utilization.

"With customers in the government and healthcare sectors, Cirrus needs to provide the highest level of protection against DDOS and brute force attacks. ThreatSTOP's IP reputation service provides invaluable protection for Cirrus Tech and our customers against threats that other solutions fail to address."

Ehsan Mirdamadi
CEO, Cirrus Tech

ThreatSTOP™

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