One F500's journey to find the perfect DNS protection software

> ***Cisco Umbrella allowed users to access over 50% of the threats*** *our software blocked.*

An F500 company using Cisco Umbrella questioned how reliable the software was for threat detection.

They saw the rising security threat data breaches posed to their business, both financially and as a threat to their company image. With over 13,000 employees in offices around the globe, they needed the most secure DNS protection software available

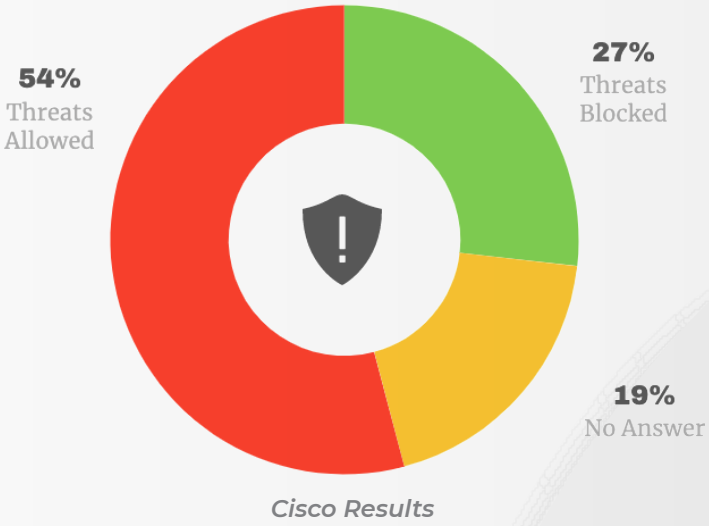
This F500 company came to DNSFilter. They wanted to see how we matched up against Cisco Umbrella, so we performed a head-to-head comparison of threats prevented by Cisco Umbrella and DNSFilter.

Here are our findings.

Experiment 1:
DNSFilter's blocked threats

DNSFilter took a 24-hour report of domains marked as a threat by its AI and then accessed those same domains using Cisco Umbrella.

Of the 432 domains blocked by DNSFilter, Cisco Umbrella only blocked 26.8% of those threats. 19.1% of the threats caused an error and no response, while **54.1%** of the domains that DNSFilter blocked, Cisco Umbrella allowed.

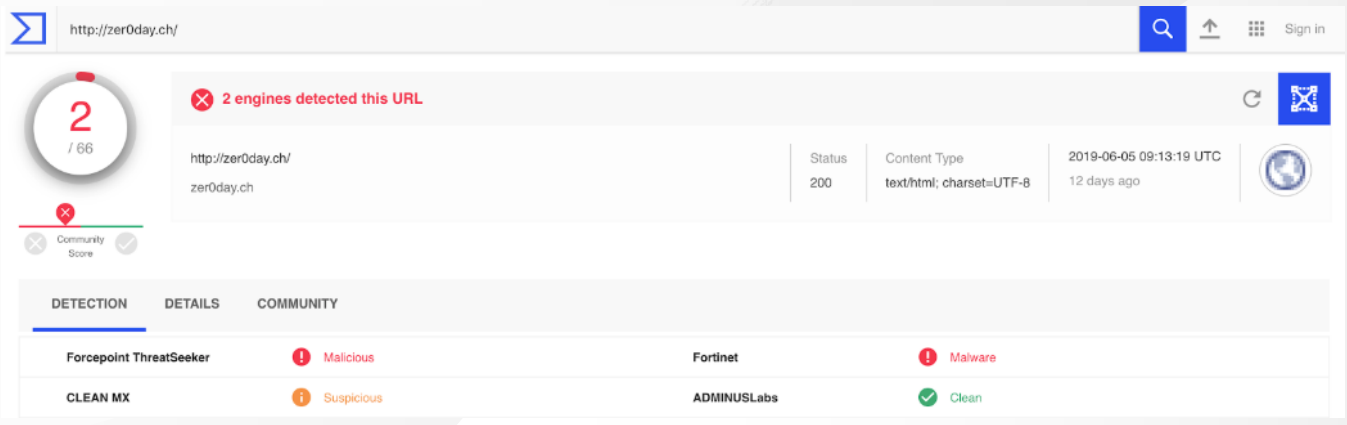


The **results**

VirusTotal is a collaboration of over 150 anti-virus and domain scanning tools. We used this aggregate tool as a benchmark for our results. To measure the efficacy of DNS protection software, the domains blocked by that software should match closely with the domains marked as a threat by VirusTotal.

We ran the DNSFilter-blocked domains list against VirusTotal to validate our results. This review led to us revealing that only 12 out of our 432 domains were false positives. This means of the threats blocked by DNSFilter in a 24-hour period, we had a 97% match rate with VirusTotal.

It also confirmed our findings that Cisco Umbrella allowed users to blocked. access over 50% of the threats our software



Experiment 2:
Cisco Umbrella's blocked threats

We then reversed the experiment and obtained a list of threats blocked by Cisco Umbrella over a 24-hour period. The list had 447 domains. Of the Cisco Umbrella-blocked domains, DNSFilter only agreed with 5% of them. DNSFilter allowed users to access 90% of what Cisco deemed a "threat".

But what were those sites that DNSFilter wasn't blocking that Cisco Umbrella was?

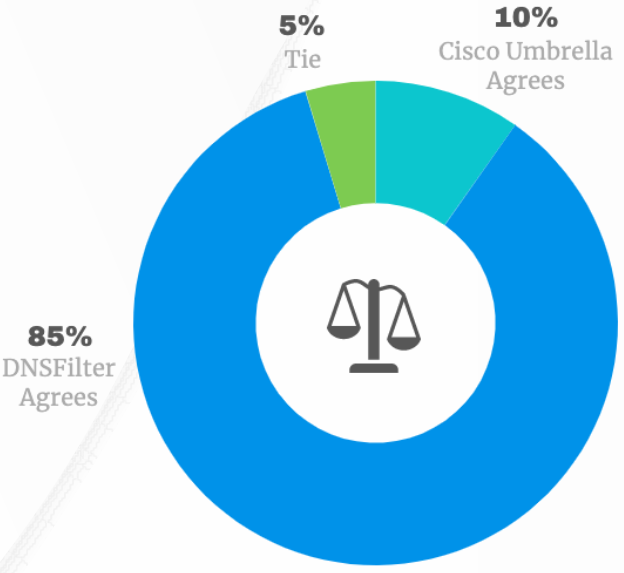
The **results**

We decided to turn to VirusTotal once again to check the validity of all of the threats categorized by both DNSFilter and Cisco Umbrella.

When we checked all of these domains, we confirmed that DNSFilter agreed with VirusTotal 85% of the time, while Cisco Umbrella only agreed with VirusTotal 10% of the time.

After this experiment, we concluded that a majority of Cisco Umbrella's blocked sites are actually false positives (wrongly categorized as "threats") when compared to VirusTotal. We also determined that Cisco Umbrella is likely not blocking 50% of zero-day* malware and phishing sites, putting customers at serious risk.

Meanwhile, because of its unique AI, DNSFilter was able to categorize and block new threats in real-time with great accuracy.



VirusTotal Results

Happily ever after

After our experiment, this F500 company decided to make the switch from Cisco Umbrella to DNSFilter as their official DNS threat protection software.

A zero-day attack (or zero-day exploit) is a cyber attack that occurs on the same day a weakness is discovered