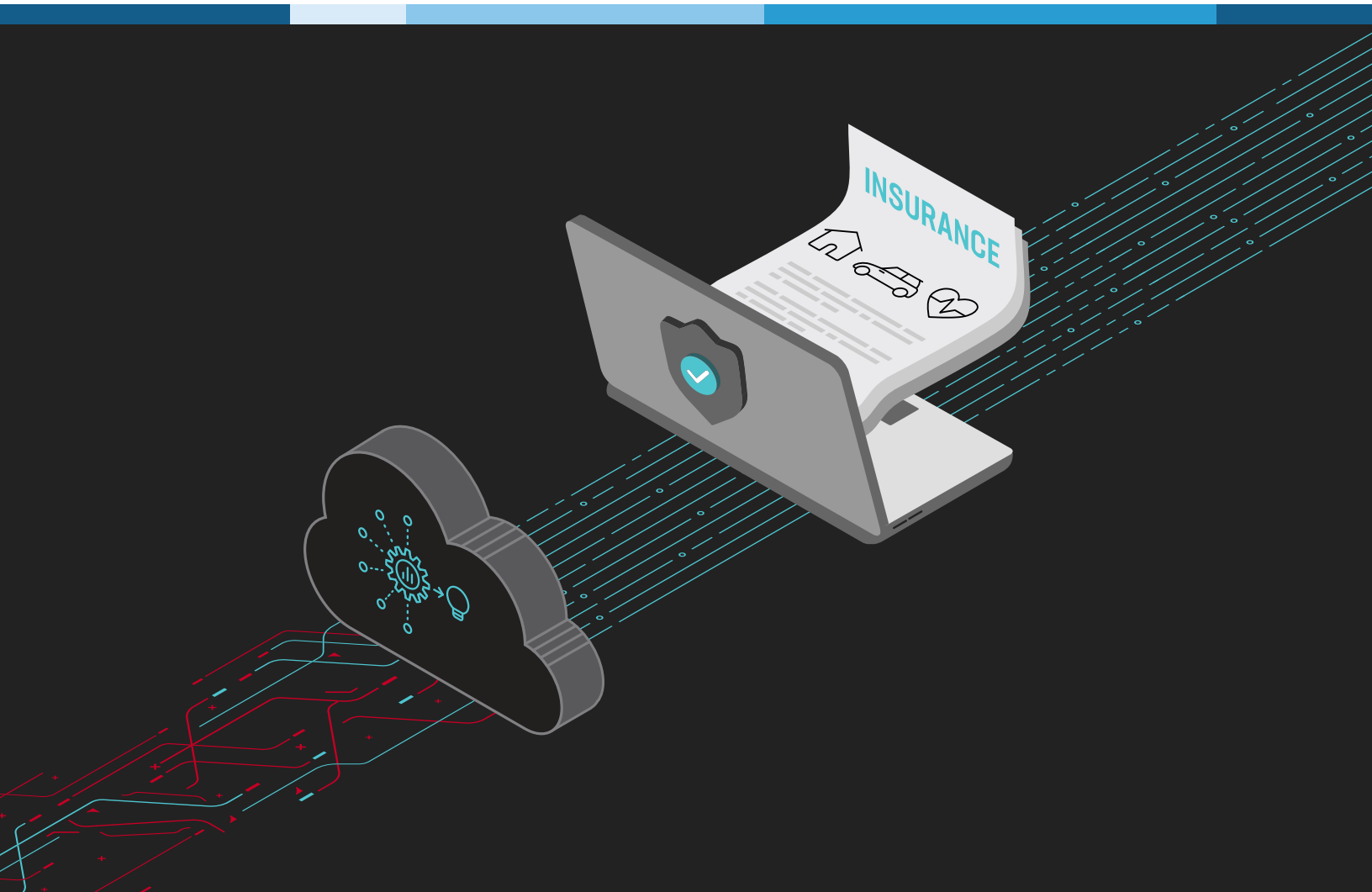
CASE STUDY

Insurer Prevents Losses from Fake Quotes



$300 PER CALL

The cost of each ghost quote follow-up made by an agent.

The Customer: Top P&C Insurer. A top 10 insurance company (“insurer”) with over $10 billion in revenue, focused on automotive and life insurance as well as financial services such as banking and mutual funds.

The Challenge: Detecting Dummy Quotes

The insurer noticed higher than anticipated traffic on its quote generation application and was concerned that the unexpected volume was caused by a surge of automated traffic creating fake insurance quotes.

Besides slowing down the insurer’s website, fake quotes created a financial burden. Insurance agents follow up with a lead once a quote is generated using the application. When quotes were created via automated requests, the agents would attempt to follow up with these “ghost leads” in vain. The insurer calculated that each bogus quote cost $300 per follow-up due to a loss of agent productivity.

The insurer believed there were two parties responsible for these ghost quotes.

AGGREGATORS

Within the insurance industry, there are many tools available by insurance providers and third parties that allow prospective insurance purchasers to compare quotes across various providers from a single location. These aggregating tools rely on automation to visit each insurance company’s quote generation application and then send back the real-time quote provided. The insurer believed that the volume of automated traffic on its quote generation app was exceeding the expected thresholds and thus affecting the accuracy and quality of its data.

COMPETITORS

The insurer suspected that some quotes were coming from competitors looking to determine the company's actuarial formulas. With enough quotes generated, a competitor could, in theory, reverse-engineer the algorithm generating each resulting quote based on the variable inputs. This intellectual property theft would put the insurer at risk of losing its competitive advantage in the market as its rivals would be able to easily under price the insurer and steal away potential customers.

Beyond the dummy quotes, the insurer had concerns that it was a potential target for account takeover attacks on its banking login endpoint.

The Decision

The insurer first attempted to identify and remedy the problem by relying on existing cloud-based web application firewall services. When these tools failed to stop the attack, the insurer decided to evaluate F5® Distributed Cloud Bot Defense to see if it could expose and stop the attacks against the quote generation tool.

OBSERVATION MODE INSIGHTS

Within the first 24 hours of deployment, Distributed Cloud Bot Defense observed that nearly half (48%) of all requests made to the quote generation application were automated. Detailed analysis showed the presence of three possible malicious automation campaigns. The service's intelligence report also showed trends within the campaigns including workflows within the sitemap.

The insurer, quickly able to see the level of detail and insight provided for the quote generation application, decided to move forward with also protecting its banking login endpoint by placing it behind the F5 service.

After collecting two weeks of data in observation mode, the intelligence report identified:

1. Malicious vs. benign human and automated traffic
2. Traffic volume and POSTs for each endpoint
3. Seven distinct unauthorized aggregator or scraper attacks with information including which unique accounts the aggregator attempted to log in to and associated success rate

The snapshot details a single scraper’s activity on the quote generator endpoint spanning the two-week period. Over 65,000 automated requests from 188 IP addresses were made in this campaign ranging across the application’s site map. The insurer, now able to flag and block these requests, was able to ensure agents would no longer waste efforts following up with quotes generated by automation. The insurer was able to prevent spending over $1 million in dummy quote follow-up by identifying that these 4,000 completed quote requests were generated by an automated tool.

The login endpoint was also continuously examined over the two-week period by several aggregators. These campaigns totaled a probe of over 10,000 unique accounts with login success ranging from 85% to 98%. Upon discovery of the nearly 26,000 requests made by aggregators, the insurer’s security team was surprised, stating, “Wait, we don’t allow aggregators, do we?” With F5's solution, the insurer could now see and understand the full extent of the problem it faced.

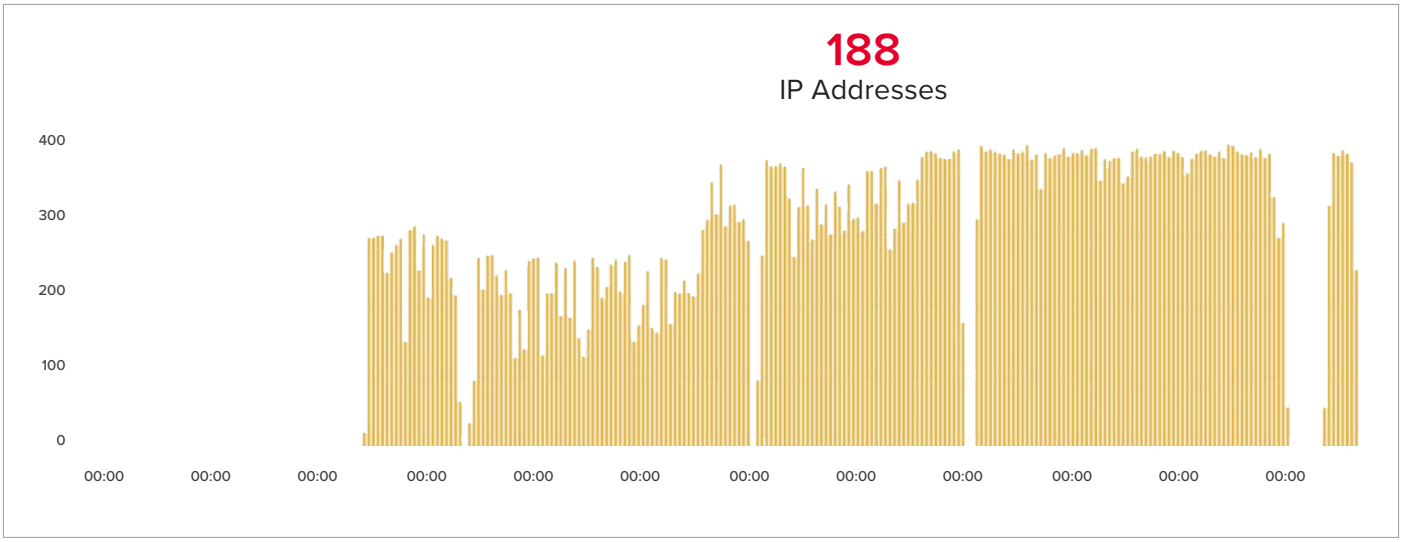


Figure 1: Single scraper campaign at quote generator

THE VALUE TO THE INSURER

- Protected intellectual property
- Reduced number of bogus quotes, protecting revenue
- Reclaimed infrastructure resources from load caused by bots

The Outcome

MITIGATION MODE RESULTS

Impressed by the level of granularity Distributed Cloud Bot Defense was able to deliver on the automated attacks, the insurer was confident the F5 service would not negatively impact legitimate users. Therefore, the insurer was comfortable moving into mitigation mode on its quote generation application and banking login form. With Distributed Cloud Bot Defense, the insurer was able to protect its intellectual property, reduce costs incurred from bogus leads, and remove unwanted aggregators from interacting with its applications.

Summary

F5's campaign analysis and sophisticated technology pleased the insurer so greatly that the company has expanded the scope of the initial deployment of the product from two applications to multiple properties across its online presence. The results were so compelling, in fact, that the insurer encouraged F5 to meet with peer insurance companies in hopes of eliminating automation threats from the industry as a whole.

To learn more, contact your F5 representative, or visit f5.com.