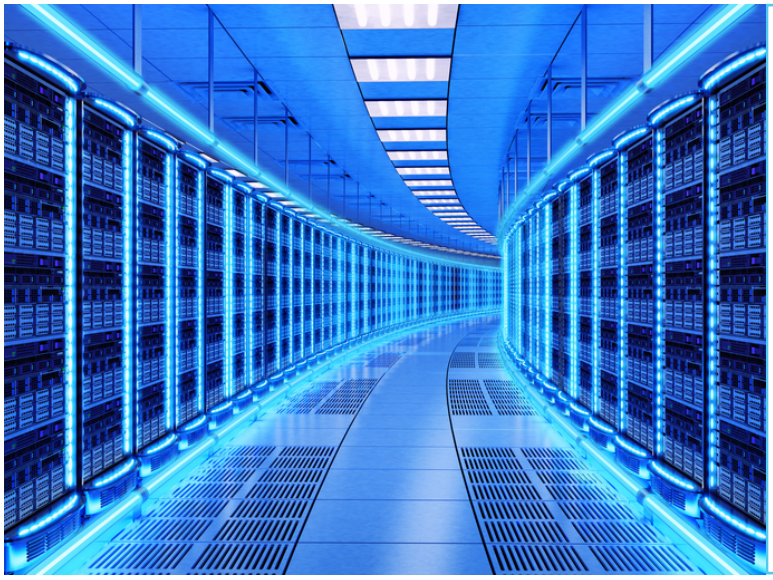
# How Security Coverage utilizes Enterprise Secondary DNS for added DNS Resilience

## Learn How from Security Coverage



> The Secondary DNS services provided by CloudFloorDNS gives us the additional insurance against a major DNS outage. We learned our lesson when the Dyn outage happened in 2016 and immediately put a plan in place to add a Secondary DNS platform to the mix. It was an easy decision when we compared it to the extraordinary cost of DNS downtime"
>
> *Eric Christoffersen, Security Coverage*

## WHO IS SECURITY COVERAGE?

Security Coverage offers customized software and support solutions to hundreds of internet service providers and retailers across the United States, Canada and Caribbean.

*DNS IS THE FOUNDATION OF ONLINE OPERATIONS AND WHEN IT GOES DOWN, ONLINE OPERATIONS COME TO A HALT*

For any online business, authoritative DNS is the most critical component next to having a domain name registered. DNS makes everything else online work and Eric and his team at Security Coverage know that. Back in the early days of the company, Security Coverage moved their authoritative DNS away from their domain registrar for better reliability, flexibility and performance. They selected long time DNS provider TZO and eventually ended up at Dyn managed DNS after they acquired TZO in late 2012.

## DNS OUTAGES ARE COSTLY

Their DNS had always been rock solid until the massive DDoS attack on Dyn in October 2016. This direct attack on the Dyn infrastructure caused outages and DNS degradation and affected both small and large online business including Netflix, Twitter, Amazon, Zappos and many more. Although hard to put an exact figure on the damage, it's likely that this DNS outage cost many millions of dollars in damages.

It's not just DDoS attacks that can cause outages on DNS platforms, human error, software bugs, network outages and exploits can also take down a DNS provider. By spreading your DNS across multiple providers it minimizes the risk, especially if the DNS providers have a different network and software. By selecting a secondary DNS provider that uses a different software platform, you are minimizing the risk of software exploits that could affect both providers running the same version of BIND or other popular open source DNS platform.

CloudFloorDNS™
AN EVERBRIDGE SOLUTION

VISIT CLOUDFLOORDNS.COM
CALL +1.781.819.5189

# Q&A with Eric Christoffersen, VP of IT and Development at Security Coverage

SecurityCoverage®

### *WHY DID SECURITY COVERAGE SELECT CLOUDFLOORDNS AS YOUR SECONDARY DNS?*

Secondary DNS wasn't on the top of our list for many years since TZO and Dyn were so reliable. The DDoS attack on Dyn really opened our eyes to the possibility of a DNS outage and the astronomical costs associated with a total DNS outage. We reviewed our options and liked that CloudFloorDNS had almost two decades of experience in DNS and that we worked with them in the past when they ran TZO DNS before Dyn bought them. CloudFloor also had step-by-step guides on setting up secondary DNS with Dyn and other major providers. Another huge plus was the fact that CloudFloor uses a proprietary DNS software platform that's not based on BIND (Berkeley Internet Name Domain). BIND is what Dyn's DNS platform is built on and we wanted to avoid a BIND exploit possibility and felt that it was important to have both network and software diversity when selecting our secondary DNS provider.

### *WHY IS DNS INFRASTRUCTURE IS SO IMPORTANT TO SECURITY COVERAGE?*

DNS is the lifeblood of any online business and in our case we absolutely have to be available 24x7x365 for our customers. With the massive increase in online threats such as DDoS attacks, Malware and other exploits, we wanted additional protection to avoid a DNS outage. Weighing the costs between downtime and adding a secondary DNS was easy – downtime was much more expensive and much more disruptive to our operations.

### *HOW HARD WAS THE SECONDARY DNS TO SETUP AND GET DELEGATED?*

It was amazingly easy and the whole process took less than 15 minutes to get going. The guys at CloudFloor also were very hands-on and helped us setup a free trial so we could synch zones and see a proof of concept before we delegated live.

### *HAS THE SECONDARY DNS CHANGED YOUR PROCESS AT ALL FOR DNS EDITS & UPDATES?*

Not one bit. We still make changes at Dyn when editing the zone files and with the NOTIFY command CloudFloorDNS automatically synchs the records once we save and publish the DNS changes at Dyn. Adding CloudFloorDNS as a secondary provider lowered our costs with Dyn since our query level has dropped. CloudFloorDNS takes a little less than half of our queries since we have them in the delegation. Overall it has had minimal impact on our day-to-day and we really like having the extra DNS protection at a minimal cost.

## About CloudFloorDNS and Everbridge

CloudFloorDNS is a global Anycast DNS provider offering both Enterprise and SMB DNS platforms, Domain Registration for over 180 TLDs and a lineup of advanced DNS services that help companies of all sizes provide faster, smarter and more reliable websites, applications & mission critical services. CloudFloor advanced DNS services include GEO DNS, Global Server Monitoring & DNS Failover. CloudFloorDNS is a wholly owned subsidiary of Everbridge

Everbridge, Inc. (NASDAQ: EVBG), is a global software company that provides critical communications and enterprise safety applications that enable customers to automate and accelerate the process of keeping people safe and businesses running during critical events. Everbridge is based in Boston and Los Angeles with additional offices in San Francisco, Beijing and London.

*For a full product description please visit the CloudFloorDNS website at https://CloudFloorDNS.com.*

CloudFloorDNS™
AN EVERBRIDGE SOLUTION



VISIT CLOUDFLOORDNS.COM
CALL +1.781.819.5189