Chaser

How DiscrimiNAT augments apree health's Zero Trust security strategy while saving DevOps time

CASE STUDY –

50+

teams self-servicing through DiscrimiNAT

400+

unique FQDNs filtered over 150 applications

160+

DevOps hours saved each month

"DiscrimiNAT allowed us to pay down our tech debt, set up egress filtering to have long-standing metadata information in each of the rules, and ultimately, improve our security posture."

Cat Schwan,
SecOps team lead, apree health

apree health combines data-driven personalization, a coordinated care model, and aligned incentives to unlock value and make life better for those it serves.

Challenges

- Complying with HIPAA regulations
- Preventing data exfiltration via egress filtering
- Earning HITRUST without accruing technical debt

Solution

- Terraform to deploy DiscimiNAT into GCP
- Non-blocking 'See-Thru' mode to discover FQDNs before enforcement
- Self-service to boost operational efficiency

Results

- 50+ teams self-servicing through DiscrimiNAT
- 400+ unique FQDNs filtered over 150 applications
- 160+ DevOps hours saved each month

Challenges

Protecting PHI & Other Sensitive Data

For Donovan Ellison, Cloud Security Engineer at apree health, nothing is more important than protecting sensitive customer data. He knows exactly how much is at stake.

> **"We deal with healthcare and patient data—really sensitive information," he explains. "If that information leaks, even from negligence, it's a HIPAA violation. There would be serious fines. But more importantly, we have contractual obligations with customers to meet certain requirements and compliance standards. Securing our systems is really important."**

To demonstrate its commitment to customer privacy, apree health holds critical certifications like HITRUST and SOC 2.

But there's a problem. In the process of shoring up its data, apree health had accrued massive technical debt.

For example, they'd adopted an egress filtering solution for their data center—a great decision, because it helps prevent data exfiltration. But it wasn't a viable long-term solution because:

- Adding FQDNs to allowlists required an official request and a manual review process that often took days.
- The system lacked a way to account for FQDNs and clearly understand which ones they were using.
- Only the networks team had visibility into how firewall rules were set up, resulting in operational inefficiencies for developers, the IaC team, and the security team.
- The system wasn't scalable; apree health would need a cloud-compatible solution in the future.

Cat Schwan, SecOps team lead, elaborates:

> “Our organization had accumulated about a decade’s worth of tech debt in our traditional data center deployment. We had a tangled web of firewall rules, but we lacked a sound way to track them or understand what they related to.”

When apree health decided to migrate to the Google Cloud Platform, it was time for a change.

> **“It is so important for our organization to have tight visibility on our egress controls because we work with PHI and we’re HITRUST and SOC 2 certified.”**

Solution

Filtering egress by FQDNs in a Shared VPC

After weighing all possible options, apree health partnered with Chaser Systems to solve its egress filtering needs. Their solution, DiscrimiNAT, makes this control frictionless and provides a path for migration. Additionally, Chaser Systems is familiar with HIPAA and PCI DSS requirements.

> **"We needed an egress filtering process that works in GCP and DiscrimiNAT solves that problem. I looked around for alternatives, but I didn't find any other solutions that focus on URL and FQDN filtering when IPs are not static," Donovan says.**

It was time to pay down tech debt and future proof systems. Because DiscrimiNAT is a transparent, proxy-less, and maintenance-free Cloud NAT alternative, it was the perfect fit.

> **"When we had the opportunity to make a change and make our systems much more secure and organized with Chaser Systems and DiscrimiNAT, our organization jumped on it. This was high stakes, not only for the security of our systems, but also from a developer agility standpoint," Cat says.**

A key differentiator was Terraform integration. Chaser Systems provided apree health with Terraform modules for deploying DiscrimiNAT into Google Cloud Platform, which made it easy to roll out to new environments as needed.

Implementation was a cross-functional effort across teams, including apree health's security team, which led the project, the networks team, which wrote the Terraform rules, and the IaC team, which deployed apree health's Terraform code throughout GCP.

> **"One of the things that's nice about Chaser Systems is that they provide a Terraform module for deploying DiscrimiNAT into GCP. Even though we have a lot of VPCs that we have to deploy to, the deployment process has been smooth," Donovan says.**

> **"The fact that DiscrimiNAT had such a wonderful Terraform integration that we were able to tailor to our organization made it a really amazing solution for us," Cat agrees.**

Increased security, visibility, and control

One of the biggest concerns prior to implementation was that DiscrimiNAT would disrupt normal business operations. DevOps teams were worried about having to figure out which FQDNs to allowlist, and how much downtime they risked if they missed something before turning it on.

DiscrimiNAT solves the problem via 'See-Thru' mode, which allows you to see if an FQDN has been allowlisted in **discovery mode** before you action that change in **preventative mode**. Using 'See-Thru' mode, apree health was able to proactively monitor the impact of changes in a low-stakes environment before committing to them.

> **"'See-Thru' mode allowed us to quantify and understand what calls are being made outbound and what calls are required. We are able to hone in on change management and see what FQDNs we need to allow so that there isn't a disruption throughout our organization," Cat says.**

'See-Thru' mode also results in more clarity and transparency around which specific FQDNs have been allowlisted and why specific ones are disallowed. For example, when apree health was having trouble with a specific FQDN, they could see that it was because the FQDN was using an old cipher suite for their encryption that DiscrimiNAT considered insecure.

> **"DiscrimiNAT is wonderful because it allows you to choose your own adventure with FQDN filtering. The way that our deployment is now structured is so clear. Any outside auditor can come in and know exactly what each firewall rule is for and the related ticket, which is critical for us and our controls," Donovan says.**

Self-service boosts operational efficiency

Another major perk of switching to DiscrimiNAT is the self-service feature that enables apree health's developers to discover and manage least-privilege allowlists for network egress controls without waiting for lengthy approvals.

> “DiscrimiNAT and Chaser Systems gives developers the tools to self-service. If an FQDN doesn’t work, they can figure out why. They don’t have to navigate a siloed system with different teams across different time zones. It has really increased our ability to bring features to market quickly in our cloud environment,” Cat says.

At the same time, DiscrimiNAT gives apree health the ability to apply controls at a more granular level. It facilitates microsegmentation versus applying shared rules to all apps which expose organizations to increased risk. In other words, apree health gained both increased security and more flexibility than they had ever had before.

> “DiscrimiNAT gives organizations flexibility. Our initial deployment looks so much different than our final deployment. You are able to tailor the solution to your organization’s needs,” Cat says.

“DiscrimiNAT gave us the flexibility to deploy in a way that did not negatively impact developers while also applying needed security to our systems.”

Results

Securing cloud outbound traffic in minutes

With Chaser Systems, apree health has made a major push toward enforcing HTTPS traffic and eliminating insecure protocols. It's a major HITRUST requirement—and a big differentiator in an industry where data privacy is everything.

> "DiscrimiNAT allowed us to pay down our tech debt, set up egress filtering to have long-standing metadata information in each of the rules, and ultimately, improve our security posture," Cat says.

> "For our customers, deploying DiscrimiNAT ultimately results in a more secure app and they can feel confident that their PHI is safe with us," Donovan adds.

Importantly, DiscrimiNAT augments apree health's journey toward Zero Trust, without sacrificing usability.

Now, more than 50 teams are self-servicing through DiscrimiNAT. Every team has more transparency into egress filtering than ever before and more flexibility too. Previously cumbersome processes have been streamlined, **saving up to 160 hours each month.**

> "If we're talking on a rule-by-rule basis, I think we're saving four hours of FTE work per rule on the low end. On the high end, if a ticket is sitting stale or we're at a communication impasse, we might be saving weeks. It has really increased our operational efficiency," Cat says.

With DiscrimiNAT deployed into the company's Google Cloud Platform estate, apree health is now able to filter roughly 400 FQDNs across 12 environments over 150 applications. And as the company grows and they need to expand across new environments, DiscrimiNAT scales alongside them.

> "Every time we've had a question or a problem, we get a quick and timely response that is also very informative. The support we receive from Chaser Systems is incredible. The support alone saves me 5–10 hours on troubleshooting and debugging each month," Donovan says.

> “With Chaser Systems’ DiscrimiNAT, we were able to filter 400 FQDNs over 150 applications. Making changes to the allowlist used to take hours or days—now it takes minutes.”

CHASER

More flexibility for your DevOps. More security for your customers.

Learn how Chaser Systems and DiscrimiNAT can help you secure your cloud outbound traffic.

Get a Demo