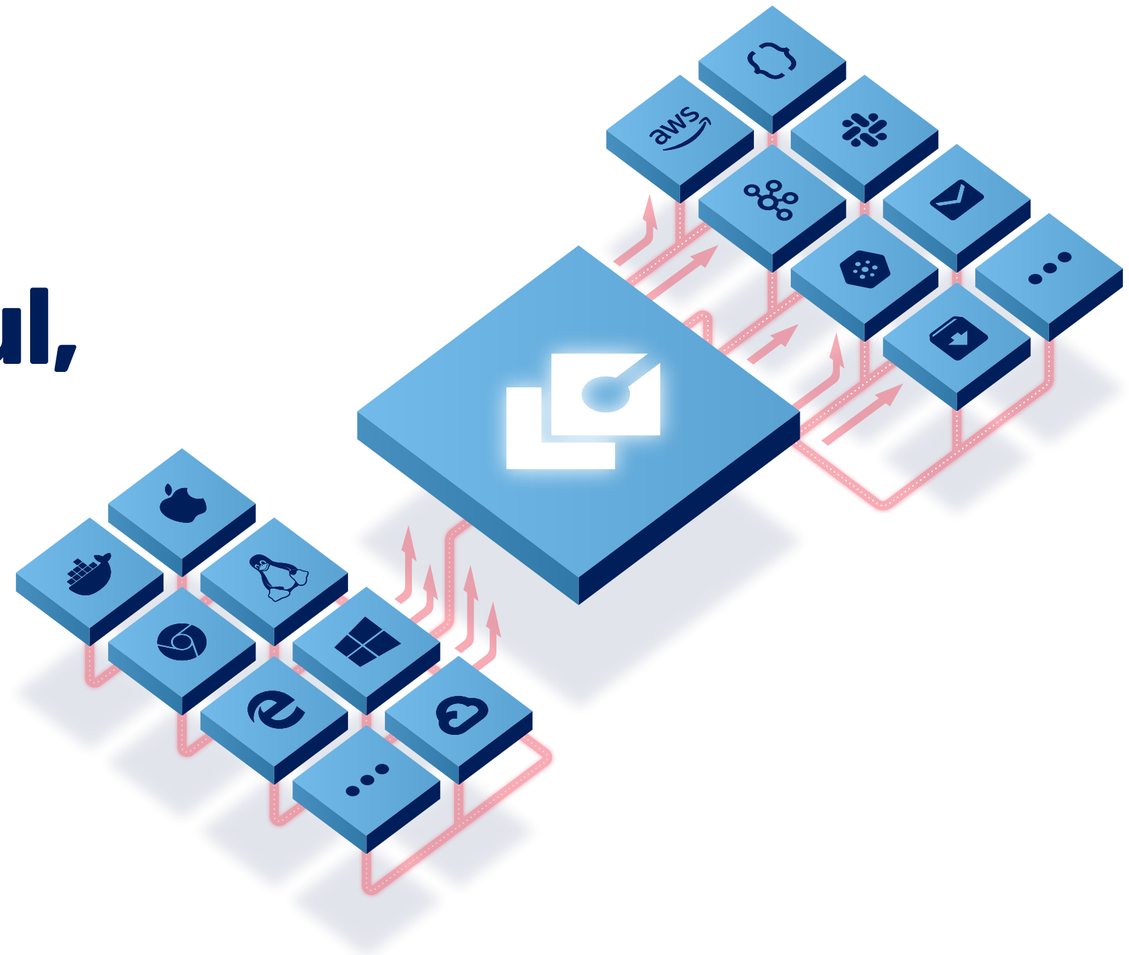
LimaCharlie™

CASE STUDY

# MSSP finds a powerful, flexible EDR solution in LimaCharlie



# BACKGROUND

Soteria is a cybersecurity firm that provides MDR, IR, security assessments, and security advisory and consulting services. The company works with a broad range of clients: pre-Series A startups looking to build robust cybersecurity programs, state and local governments, and publicly-traded multinational companies.

Today, MDR is a key part of Soteria's business. But that wasn't always the case. In 2019, the company was getting ready to launch a new MDR offering, and was searching for an EDR solution that would meet its needs.

Company Profile

**Company:** Soteria

**Founded:** 2014

**Headquarters:** Charleston, South Carolina

**Services:** MDR, IR, security assessment and advisory services, penetration testing, vulnerability assessments, training services
Sectors: Healthcare, government, transportation, finance, manufacturing, technology, insurance, legal, private equity

# Challenges

Soteria knew that it needed an EDR tool powerful enough to help it compete with established players in the MDR space. But it also wanted a solution that would be customizable enough to leverage the company's high level of technical expertise. Soteria was founded by former members of the National Security Agency and cybersecurity experts from different industries. Clearly, this significant competitive advantage could not be ignored, and had to be factored into the eventual decision. This need for flexibility immediately ruled out many off-the-shelf EDR solutions.

After some initial discussion, Soteria's leadership identified three main criteria for the EDR tool. It had to:

- Allow for extensive customization, especially when it came to writing custom detection and response (D&R) rulesets
- Be quick to deploy, so that Soteria could take rapid action when handling new IR requests
- Offer a cost-effective way to store and access telemetry, so that the company could review historical data if needed

## Challenges

- Find an EDR solution powerful enough to compete with better-established MDR providers, but flexible enough to allow for extensive customization
- Develop a true rapid response capability to serve clients with IR requests
- Secure cost-effective access to historical telemetry data

# Solution

Soteria found that LimaCharlie's EDR solution checked all of those boxes and then some.

LimaCharlie provides a range of cybersecurity tools and supporting infrastructure: EDR, software defined networking, artifact ingestion, and a wide range of adjacent capabilities. The company takes an AWS-like approach to cybersecurity called "security infrastructure as a service" (SIaaS). Unlike other cybersecurity vendors, LimaCharlie offers everything to users via an open API, and on a self-serve, on-demand basis.

Particularly attractive to Soteria was the fact that LimaCharlie's tools are designed with developers in mind. While these tools can certainly be implemented as turnkey solutions, LimaCharlie is also flexible enough that advanced users can use the platform to build their own products and capabilities.

That, of course, was exactly what Soteria was looking for. With LimaCharlie's EDR tool, they would be able to author their own D&R rules, retaining ultimate control over the data produced by the platform. As Cofounder and Managing Principal Paul Ihme noted, this promised a great degree of operational flexibility: "With LimaCharlie, we would be able to build our own custom rules to be as broad or as targeted as we wanted, and easily deploy them to all customers or to a single environment".

"We can deploy EDR sensors in minutes and adjust licensing on the fly, without having to jump over hurdles. This is a massive advantage over the other EDR players out there."

**Glenn Starkman,**
CEO

LimaCharlie's on-demand, self-service model helped to meet Soteria's second major requirement for an EDR tool: speed. With LimaCharlie, procurement and configuration could be streamlined, especially when taking on new customers. As CEO Glenn Starkman put it, "The process is extremely efficient. We can deploy EDR sensors in minutes, and adjust licensing on the fly without having to jump over hurdles." In his view, this offers "a massive advantage over the other EDR players out there."

The final piece of the puzzle for Soteria — cost-effective telemetry storage — was provided by LimaCharlie's unusual approach to pricing. The company does not require contracts or fixed minimums as most other vendors do. Pricing is meant to be as simple, transparent, and predictable as possible.

For EDR users, there are two basic pricing options: set up a pure usage-based billing plan, or pay a flat rate per endpoint per month. Because LimaCharlie's flat-rate EDR pricing includes full telemetry storage for one year, Soteria would have an easy and economical way to ensure access to historical data. The company considered this to be an important advantage. In Starkman's words, "The ability to store telemetry for one year without incurring massive costs is hugely beneficial".

> "The ability to store telemetry for one year without incurring massive costs is hugely beneficial."
>
> **Glenn Starkman,**
> CEO

## Solution

- LimaCharlie's open API and infrastructure-first approach allow for nearly unlimited customization
- LimaCharlie's on-demand, self-service model provides superior speed of deployment, provisioning, and configuration
- LimaCharlie includes one year of telemetry data storage as part of its flat-rate EDR pricing

# Results

For the past two years, Soteria's MDR business has continued to grow, supported by LimaCharlie's EDR solution.

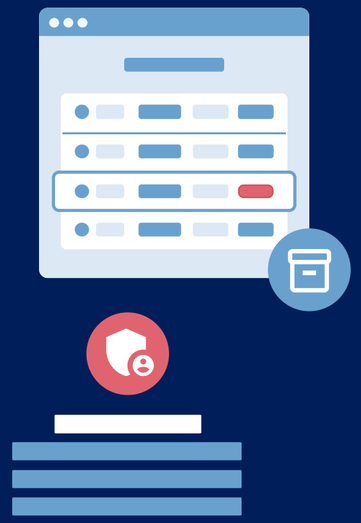
As Soteria predicted, their engineers were able to leverage LimaCharlie's flexibility to good effect, delivering optimized solutions for their MDR clients. For example, Soteria often writes custom data exfiltration rules for EDR agents to better suit the environment in which they are deployed. As Ihme notes, this allows the company to tailor its sensors to capture the required data with minimal impact on performance and bandwidth — especially when they are being used in sensitive systems. From a purely business perspective, he adds, this is a powerful differentiator for Soteria: "Our customers sincerely appreciate our ability and willingness to customize our efforts to address their unique needs".

> "We can automate a significant portion of the tasks needed to operate the platform on a day-to-day basis, in a way that is scalable, repeatable, and self-documenting, using LimaCharlie's APIs to do the heavy lifting."
>
> **Paul Ihme,**
> Cofounder and Managing Principal

In addition to customer satisfaction, LimaCharlie's flexibility has also provided substantial operational advantages for Soteria. Ihme reports that the company's engineers are able to automate "a significant portion of the tasks needed to operate the platform on a day-to-day basis". Perhaps even more importantly, they are able to do this in a way that is "scalable, repeatable, and self-documenting, using LimaCharlie's APIs to do the heavy lifting".

The fact that LimaCharlie can be deployed quickly has also helped Soteria to strengthen its relationships with customers. The company finds that it is able to respond to new incidents seamlessly, configuring new environments and deploying sensors in a matter of minutes. This, Ihme explains, "creates a great deal of confidence for our customers".

Soteria's choice of an EDR tool that would offer access to telemetry data also proved to be a sound decision. In the aftermath of the 2020 SolarWinds supply chain attack, when enterprises around the world were scrambling to figure out if they'd been compromised, Soteria says that it was able to analyze the historical data stored by the LimaCharlie platform and provide its clients with definitive answers as to whether or not they had been affected.



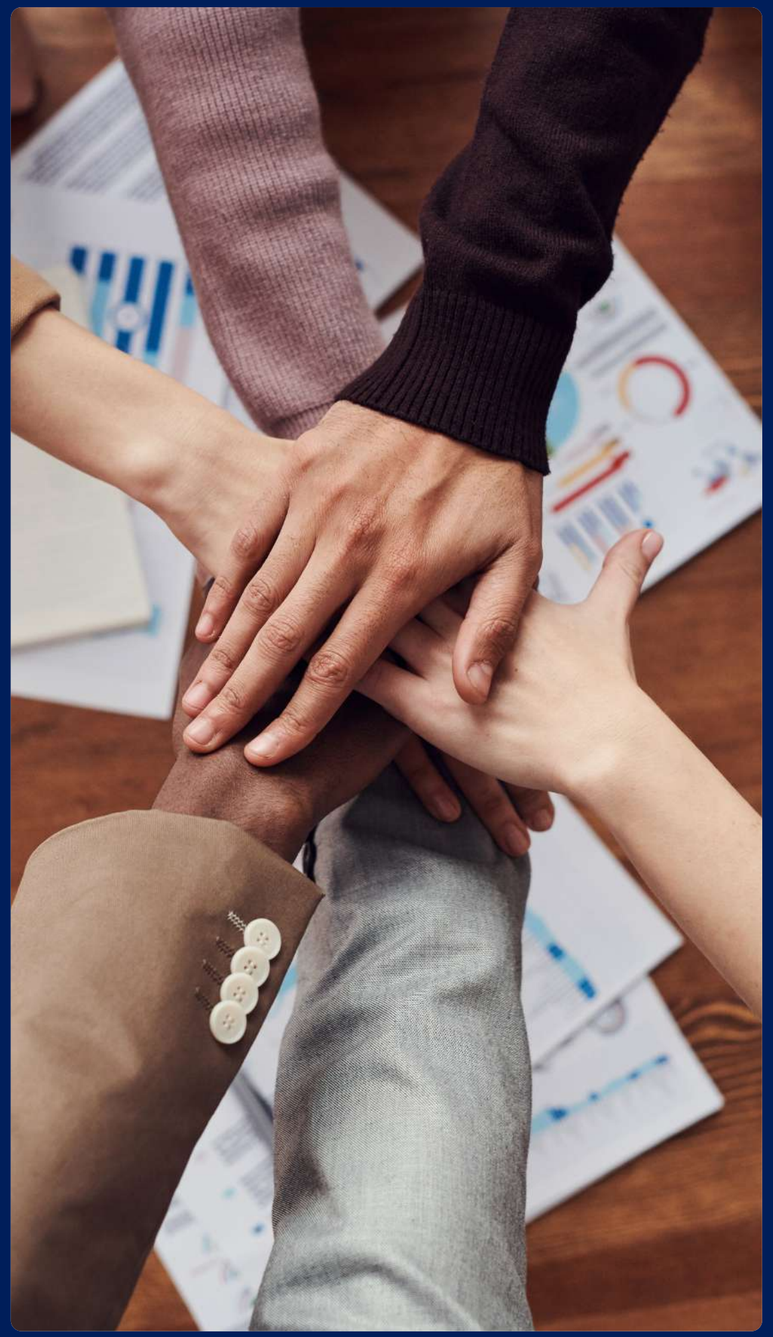
# Outlook

Soteria has been extremely satisfied with LimaCharlie's EDR solution — and with the company itself. As company CEO Glenn Starkman puts it: "LimaCharlie has been an amazing partner to Soteria. They are incredibly responsive when we need support or guidance on how to best leverage their platform".

As Soteria looks ahead, they expect that the relationship will grow and evolve. LimaCharlie is constantly developing and expanding its vision of SIaaS, and regularly adding new capabilities to its platform. Soteria says that they take advantage of newly deployed components when possible — and that they routinely bring ideas for new features to LimaCharlie's engineers.

Here too, LimaCharlie has proved exceptionally responsive, according to Starkman: "In some situations, new features or tweaks are added within hours to help us better serve our customers. In other cases, our suggestions are placed onto the longer-term roadmap. In either case, we feel that we have a true partnership that provides a ton of value in both directions".

Whatever the future brings, Soteria and LimaCharlie's relationship will continue to be marked by collaboration and mutual respect, driven by both companies' intense focus on development. As Starkman says, this partnership between two technically innovative teams has a very human element at its heart: "We truly feel like LimaCharlie is an extension of our own team. The tech is great — but the relationship is easily the best part."



**To learn more about LimaCharlie,**
**try it out for free or book a demo today.**

Book a Demo: calendly.com/demo-lc/20-min-call
Sign Up: app.limacharlie.io/signup

> “We truly feel like LimaCharlie is an extension of our own team. The tech is great — but the relationship is easily the best part.”
>
> **Glenn Starkman,**
> CEO