OVERVIEW

You know hackers operate in the dark. That's what keeps you up at night. We shine a spotlight on all areas of your network, even places where others can't. With Vigilant, you can be confident there is no threat.

KEY FEATURE AND DIFFERENTIATORS

Vigilant serves as an extension of your existing security team, notifying you only about legitimate security events in near real time. We then provide clear, easy to understand Recommended Courses of Action (RCAs) so you can address the issue quickly and get back to running your business. We help your team reduce the average incident detection time from months and years, down to minutes and hours, thus significantly reducing breach impact and incident response costs.

The Vigilant team works to bolster your in-house team with:

- Unlimited incident response, meaning that we won't set an arbitrary incident maximum beyond which we'll start charging you. We will respond to all incidents on your network as part of your protection.
- Zero false positive guarantee so we don't waste your team's time with security threats or incidents that are anything less than legitimate.
- 24/7 expert monitoring of your networks, scan for threats and alert you only about legitimate threats. Our Hunt Team has years of experience in protecting all types of organizations, from Fortune 500 companies to small businesses.

Additionally, because our technology is 100% passive, we are able to conceal our

LOCATIONS

Vigilant is headquartered in Cincinnati, Ohio.

We have offices in Ohio, Tennessee, Iowa and Washington.

We do not have any offices outside the U.S.

SERVICE OFFERINGS

SECAAS
Vigilant is a privately owned and operated cybersecurity firm, headquartered in Cincinnati, Ohio.

Trusted by hundreds of top enterprise organizations across multiple industries; Vigilant has been providing exclusive, patented and fully managed visibility detection, prevention and response services since 2009.

With our zero false positive guarantee, unlimited incident response and the fastest detection and resolution times in the industry, Vigilant protects over 450 million identities every day and over 100 billion in customer assets globally.

Allied
communication

identity in your infrastructure (attackers don't now we are watching) and we can independently confirm the efficacy of any existing NexGen security product. And, because our software is not available to purchase off-the-shelf, hackers can't get their hands on it. In the case of many of our competitors, hackers can purchase the exact same software you can – and adapt their technology accordingly to steal your data.

IDEAL CUSTOMER PROFILE

From government to manufacturing and healthcare to financial institutions, Vigilant provides comprehensive security protection for all industries. In addition, our team has years of experience in protecting all types of organizations, from Fortune 500 companies to small businesses.

Our ideal customer profile includes any organization:

- Without the resources or expertise to house a team of elite analysts to proactively monitor network traffic for potential threats
- Interested in elevating their cybersecurity stance with holistic solutions that together cover all the stages in the cybersecurity lifecycle (detection, protection and response) as well as all seven communication layers within an organization.

CUSTOMER TESTIMONIALS

"I have been a Vigilant customer for over a year. I have been extremely happy with the services they provide because I can sleep at night knowing I am not getting to get breached. I know the Vigilant staff is truly best in the business and are looking out for my business' best interests. They truly have been an extension of my organization that is irreplaceable and have made things easier to grow the organization."

- Leading Healthcare Technology Firm

Allied communication

(i) QUALIFYING QUESTIONS

General Questions to open discussion:
- What are you currently doing for security?
- How is that working for you?
- Do you know if you had any attackers in your environment right now?
- Do you know if you have had any attackers in your environment ever? -
* If no to the above two, you need to consider a no cost Proof of Vigilance with Vigilant regardless of what you have in place for security now.

Other prequalifying questions:
- Are any of your defenses and protection commodotized?
- Do your defenses primarily use/rely on detection algorithms or AI?
- Are you relying on public intel?
- Are traditional pen tests and vulberability tests part of your security strategy?
*If "Yes" to one or more of the following questions, your client's risk is high.