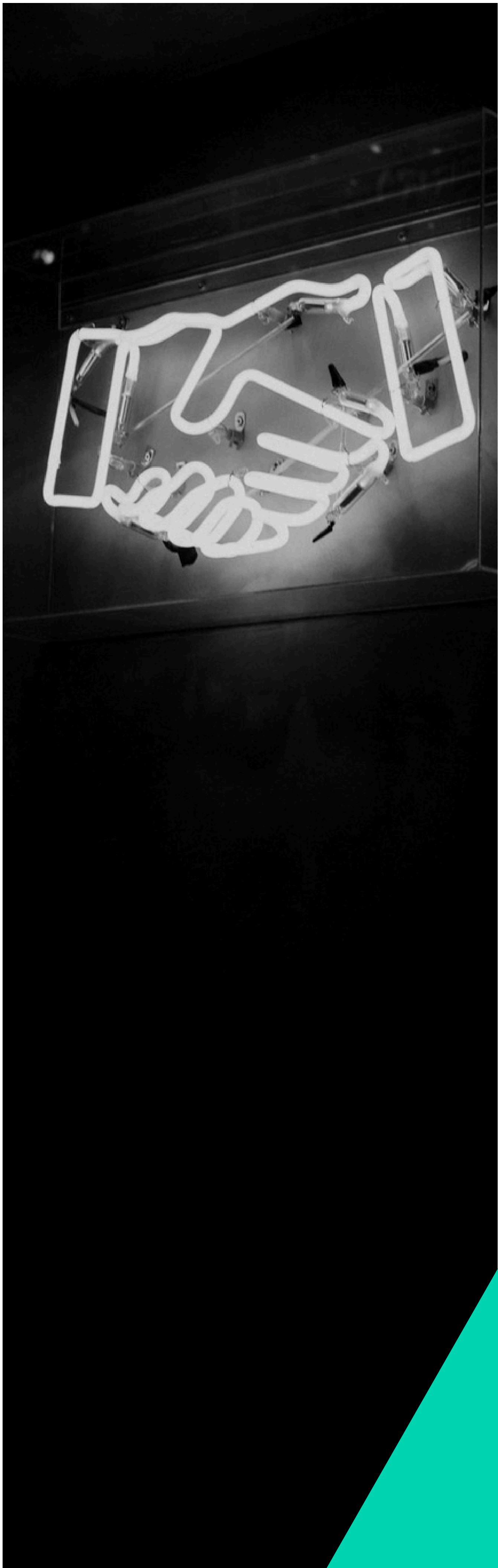
ENTHEC©

Partner Program



kartos©

qondar

Table of contents

The Enthec Partner network is an essential part of our business model.

On the one hand, it increases our commercial reach and customer reach.

On the other hand, due to the characteristics of our product, cyber-surveillance software, it is necessary to have organizations with the resources to initiate remediation processes in our customer service network, mitigation, and protection once the vulnerabilities and breaches of our clients have been detected.

Sometimes the customer has these resources in-house, but in most cases, the person in charge of performing these tasks is a partner that provides managed security services. This creates a symbiotic relationship between Enthec and its partners, who, by incorporating the Enthec product into their managed cybersecurity services, can provide their customers with a complete cyber-surveillance strategy, which allows them to discover and resolve incidents impossible to detect with traditional cyber protection strategies and perform a third-party IT risk assessment and relevant people protection, adding value to the offer.

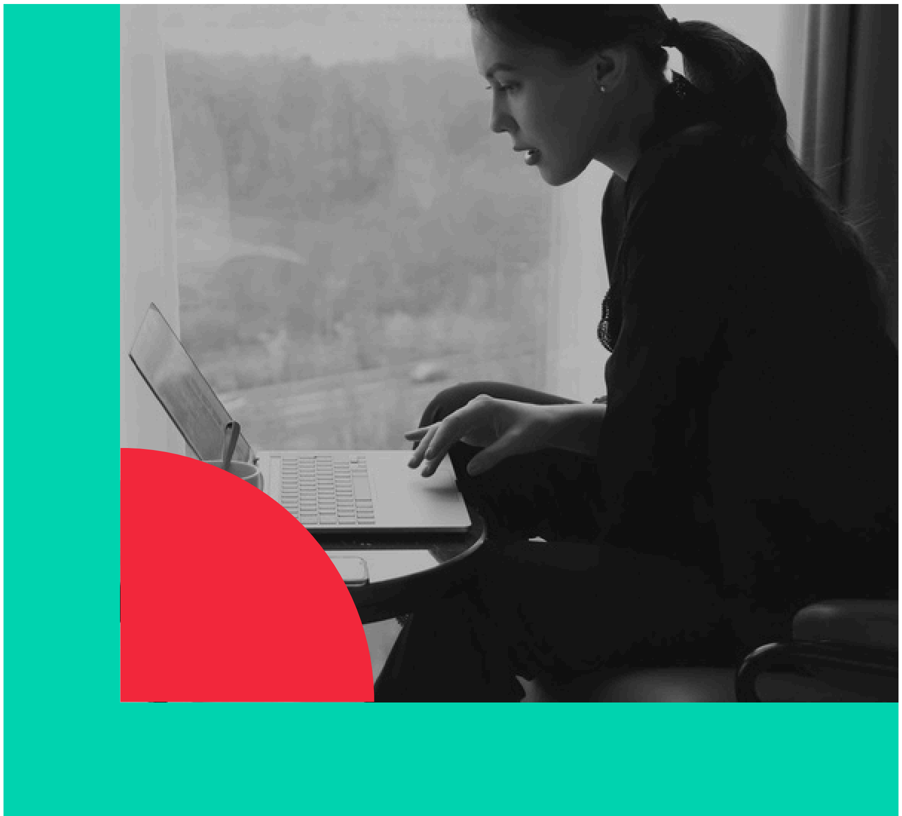
Therefore, within our Partner Program, we have two modalities:

Reseller Partner

Sells our licenses to our customers and can, if desired, provide them on it the services for which it is trained according to his capabilities and infrastructure.

MSSP Partner

Uses our tools to offer its customers the corporate cyber-surveillance and third-party IT risk assessment service and the relevant people online protection service within its portfolio of managed cybersecurity services.



Enthec does not have its own direct sales channels or managed security services. Therefore, Enthec does not act as a competitor of our partners in either of the two modalities. Both the sale of our licenses and the offer of remediation of detected vulnerabilities or assessment of third-party IT risks are made 100% through our partner network.

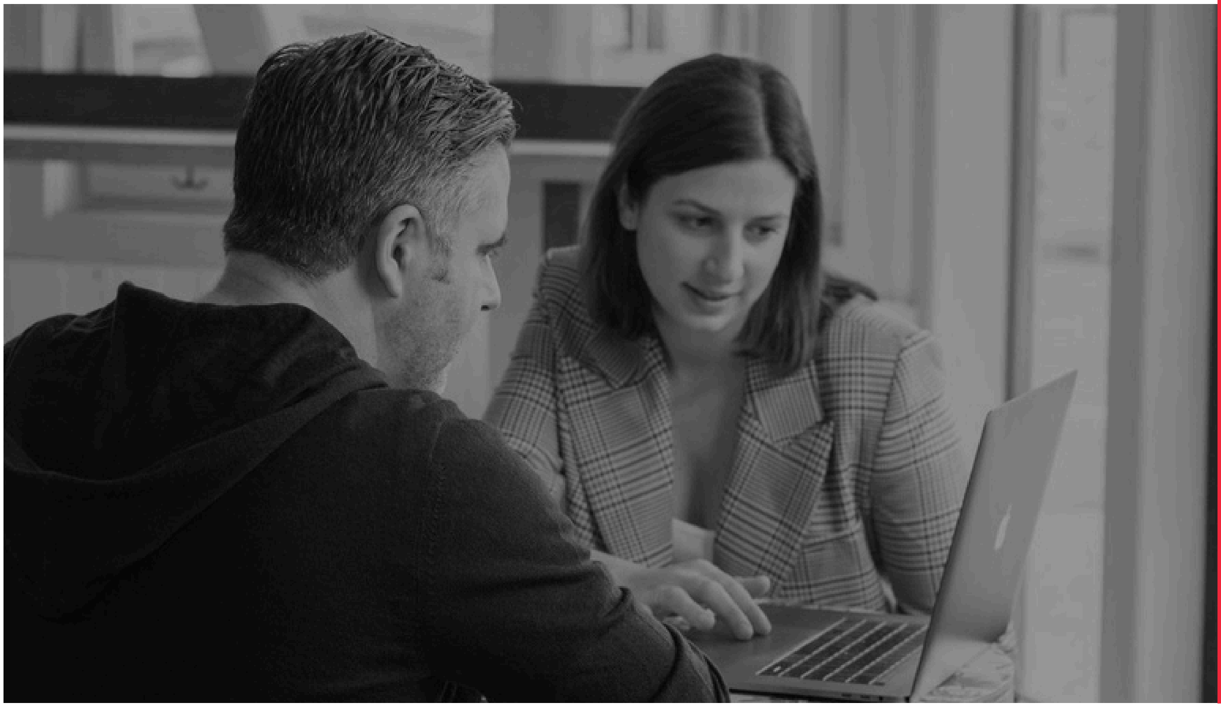
Client Value Proposal

Kartos Corporate Threat Watchbots

Kartos is formed by an army of Watchbots explicitly designed to protect organizations searching Internet, the Deep Web, and the Dark Web for open breaches and exposed vulnerabilities. Kartos works, autonomously, automated and continuously 24x7 monitoring and tracking to find all the filtered and exposed information and assets of the client company and detect the security breaches that have caused the leak. Kartos also assess the TI risk of third parties.

Qondar Personal Threat Watchbots

Qondar is formed by an army of Watchbots explicity designed to provide people with continuous and real-time information about their identity and digital assets and the ongoing activities related to them on Internet, the Deep Web and the Dark Web, so they can control their online security.



kartos©

Capabilities

Cyber-intelligence

To discover latent vulnerabilities

Locates the organization’s open and exposed information and vulnerabilities on the Internet, the Deep web, the Dark web and Social Networks. Phishing, fraud and scam campaigns, CVEs and DNS health. Leaked passwords and credentials, documentation or databases.

Cybersecurity

To keep digital assets safe

Expands cybersecurity strategy beyond the corporate IT perimeter. Brand, Domain and subdomain protection. Corporate email protection. Ransomware protection. Web Security & Takedowns.

Third-Party Risk Assessment

To control others risks that pose a threat

Controls in an automated, continuous and real-time manner the exposed information of a third party or potential third party and the detection of their security breaches, as well as the umpteenth critical ones associated with them.

Compliance

To comply with current regulations

Corporate compliance and third-party compliance based on objective data taken in real time. ISO 27001. PCI

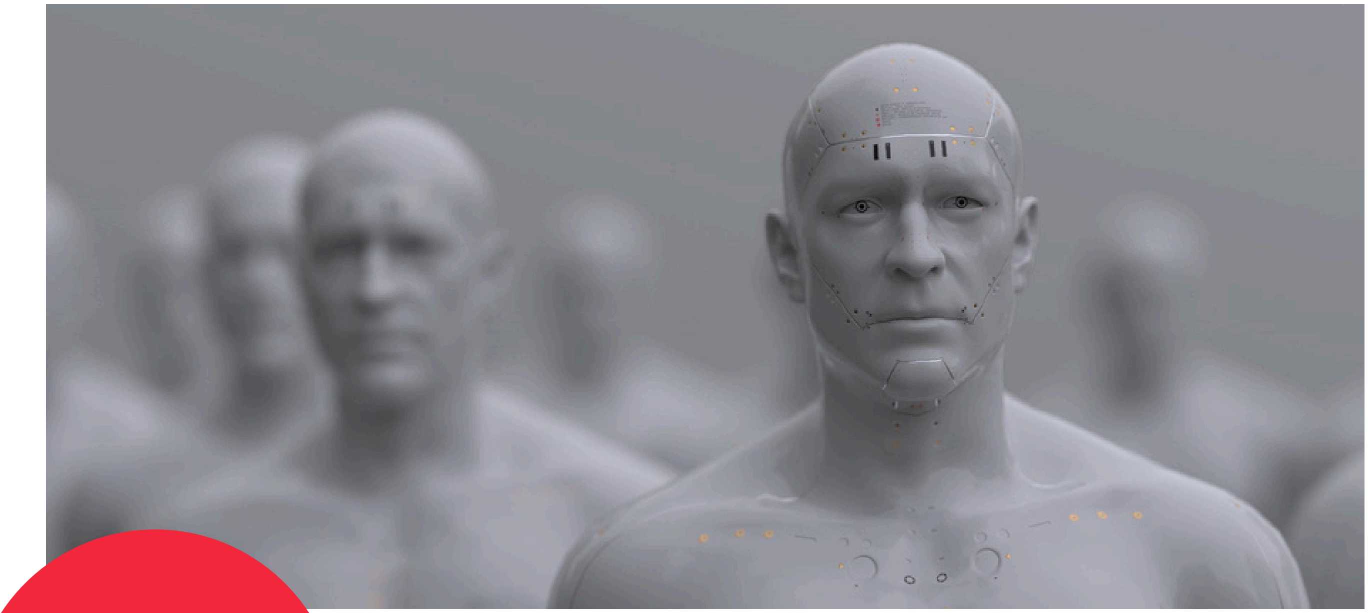
How it works

For the process to begin, you only need to enter the company´ś domain being searched.

The information is organized into 11 vectors from which the organization’s risk indices are built.

The tool administrator can customize authorized users and permission granted.

One of the main differences between Kartos and similar tools is that it not only allows obtaining information that poses a cybersecurity risk. It also allows you to identify thefts and leaks of confidential, critical, or sensitive information that pose a legal or reputational risk or intellectual property that may lead to a loss of competitive advantage or a risk to the business.



Capabilities

- **Protection of personal assets:**

Bank accounts, payment cards, crypto wallets

- **Protection of personal and professional communications:**

Email, phones, social networks

- **Protection of personal reputation.**

Name and surname, nicknames, date of birth

- **Protection against suspicious online activities that deal with personal data:**

ID, health card, passport, driver's license

- **Protection against digital identity theft.**

Name and surname, nicknames, social nicks

- **Protection of the integrity of personal profiles on social networks:**

LinkedIn, Facebook, X, Instagram, Telegram, TikTok

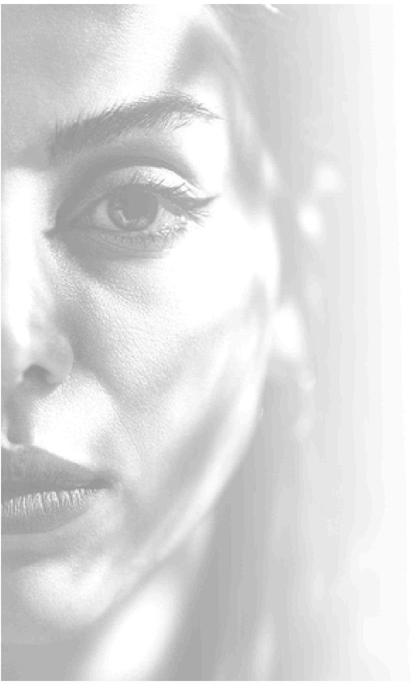
How it works

For the process to begin, you only need to enter the person´s name, data and assests being searched.

The research is carried out on the Internet, the Deep Web and the Dark Web and only on the person who has issued the protection authorization, so its operation and the information obtained strictly comply with the limits imposed by legislation.

The tool administrator can customize authorized users and permission granted.

All technology used by Qondar is developed internally and does not depend on third-party applications for its operation. In this way, the personal data obtained is never diverted to a third party or leaves the platform and is delivered directly to the client.



What is the innovation of our tools against the current almost homogeneous approach of Cybersecurity?

Today, systems and process efforts are focused on ensuring the protection of the internal perimeter and infrastructure and verifying that this protection works. That is, shield the organization with a wall of tools that prevent the assault of cybercrime: a system of dubious effectiveness given the data, which does not take into account the risks of third parties, the organizations relevant people and whose scalability is complicated at the level tools and costs with the entry of new technologies such as the cloud or the IoT.

This internal shielding approach is not enough because it does not include an essential part of any protection strategy: the surveillance of the external perimeter, which allows to anticipate cyberattacks neutralizing the potential advantage that the filtered and exposed information provides to cyber criminals; detecting security breaches in the wall of internal armor tools; assessing the risk of third parties; and minimizing the effects of the human factor, the weakest link in the protection chain.

Our platform´s innovation and value proposition start precisely from the opposite perspective of traditional corporate security, with a much more practical and straightforward vision born of the hacker approach of our solution: we observe the organization and the people from the outside, as a cybercriminal does.

Penetration and brute force attacks are usually easily detected and neutralized by perimeter protection systems. However, the problem of cyberattacks appears when they are designed and carried out using corporate or personal information that is filtered and publicly exposed without the knowledge of the companies and that facilitates the entry or launch of attacks on people. Our tools look for publicly available vulnerabilities to potential cyber attackers and discovers their origin so that appropriate neutralization and remediation measures can be taken.

In an automated continuous and real-time way, our platform provides the corporate security team with the information they otherwise do not have access to, to have a 360º view of the situation and be able to desing a complete and adequate protection and defence strategy

Partner Value Proposition

What value should a technology partner bring?

·Contribute to providing more and/or better billable services to their customers.

·Help to retain existing customers.

·Incorporation into the portfolio that does not involve a large investment either in economic terms or in terms of time, learning curve or training.

· Our platform enables customers or partners to identify corporate or personal vulnerabilities, third-party breaches, and information that companies have not filtered or exposed, which can only be found using our tools. Its uniqueness facilitates both the sale of licenses and the contribution of value to a portfolio of cybersecurity services, allowing the inclusion of remediation, mitigation, protection, and risk assessment services from third parties not previously contemplated, with the consequent increase in turnover.

· Our platform is an automated system that operates continuously, 365 days a year, 24 hours a day, 7 days a week, integrating with the management system to provide immediate alerts every time an incident occurs. Only Kartos, Qondar, and its partners can offer and provide this information in this way and with this frequency.

· Our platform provides information through an interface designed to cater to profiles ranging from those with fundamental knowledge of Cybersecurity to those who can understand the most technical aspects and take the necessary remediation measures to solve problems. In addition, Kartos and Qondar can be integrated through APIs in customer systems, SOCs, and other partner management systems straightforwardly, making production a matter of minutes.

Why be part of the Enthec Partner Program?

For differentiation: The incorporation of Kartos and Qondar into the catalog of Cybersecurity solutions and services provides a compelling competitive advantage and differentiation in the innovation of our partners' offers compared to their competitors.

By scope: Our platform works 24/7 and transfers information on threats in real-time, allowing our partners or their clients to take immediate remediation action when necessary and generating trust.

For simplicity: Our platform is a non-intrusive, automated platform with an attractive design, easy to use and that also provides our Partners or their clients with different types of reports adapted to the level of technical knowledge of each recipient.

For the support: We are always at the side of our Partners through our excellent technical and sales support service, providing them with technical support, marketing and sales materials, training, and permanent assistance.

Benefit	Description
New Revenue Stream	Offer Kartos™/ Qondar™ as White Label or Co-branded services to expand your Security Portfolio
Simple Integration	API based, multi-tenant, compatible with leading SOC/SIEM environments.
Fast Go To Market	2-month pilot program with technical support & marketing materials
High Market Demand	Highly relevant for customers in regulated industries (Finance, Manufacturing, Public Sector).
Partner Support	Technical onboarding, joint marketing, sales enablement & partner margin incentives

Why be part of the Enthec Partner Program?

Partnership Model

1. Pilot Phase (0 2 Months): Free test access for 1 3 end customers, Proof of Value, training & integration
2. Go to Market (3 6 Months): Integration into MSP portfolio, joint marketing, co-branding, case studies, potential exclusivity.

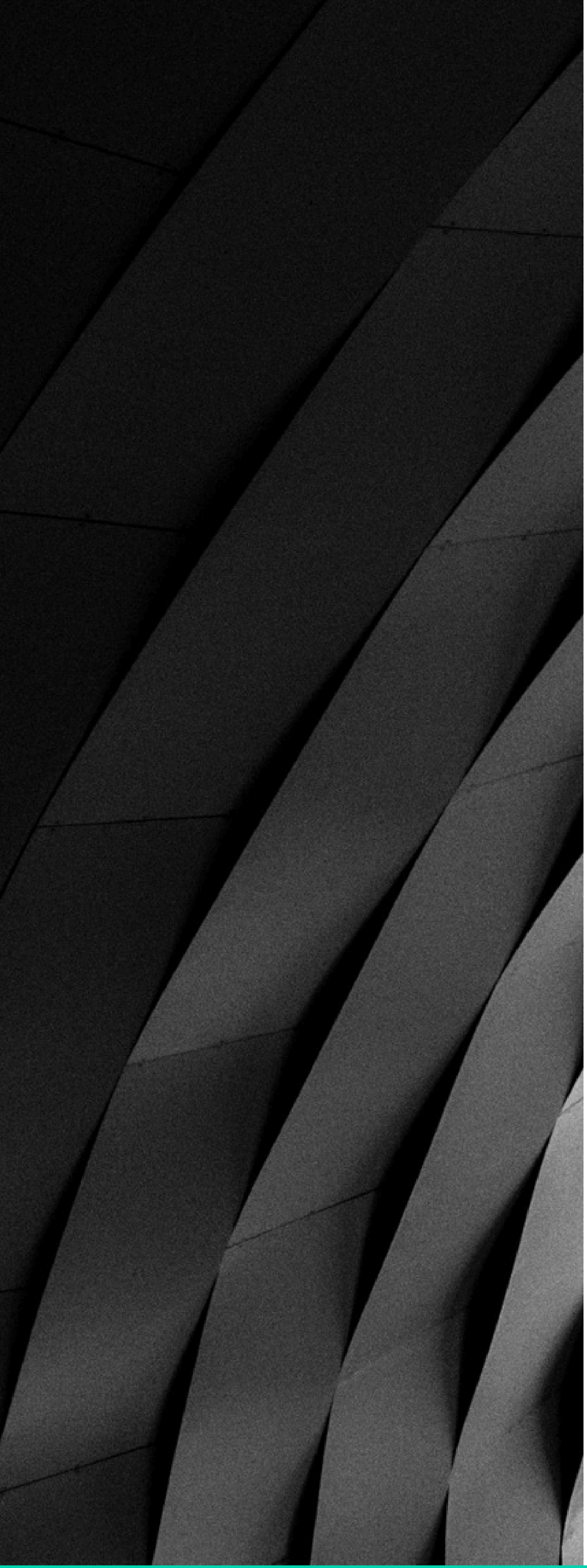
Target Customers

· Mid-sized and large enterprises with critical infrastructure
· Finance, insurance, manufacturing, energy, and the public sector
· Organizations with ISO 27001 / TISAX / BSI compliance requirements

What do we expect from a partner?

- Business development and search for new clients.
- Client relationship and renewal management.
- Training, experience, and resources that enable them to provide the necessary cybersecurity services, so that the client perceives the tool's usefulness and its contribution to reducing the organization's risk and exposure.
- Long-term commitment.

We are looking for technological partners who want to commit to the Enthec project, who help us in the search for clients, and who have the knowledge and technical capabilities in Cybersecurity that allow them to develop the necessary Remediation, Mitigation, and Protection actions, as well as IT risk assessment of third parties, becoming an integral part of our value chain.



Enthec Solutions is a Deep Tech company that develops cybersecurity software to extend organizations' cyber-protection beyond the IT perimeter. Enthec Solutions helps organizations deploy and expand their AI cybersecurity strategy to control any leaked data, exposures, and security breaches on the Internet, the Deep Web, and the Dark Web.

Enthec Solutions has consolidated itself as one of the deep techs with more innovative and effective external perimeter Cyber-Surveillance solutions through the success of its **Kartos Corporate Threat WatchBots** Platform, which provides organizations with Cybersecurity, Cyber-Intelligence, Compliance, and Third-Party Risk Assessment capabilities, and its latest innovative product, **Qondar Personal Threat Watchbots** Platform, Cyber-Surveillance software for the protection of people's online information and digital assets.

www.enthec.com

If you want to learn more about our Partner Program or try our Kartos Corporate Threat Watchbots or Qondar Personal Threat Watchbots in a demo and discover how they can protect your customers and the competitive advantages they brings to your Cybersecurity solutions and services, you can contact us through this email address:

hello@enthec.com

Thank you!