**Darktrace Antigena Q&A**

**NOTE FOR SALESPEOPLE:**

Darktrace Antigena should not be introduced into new sales opportunities. It is for existing Darktrace customers only.

Darktrace Antigena is not as simple to install as core Darktrace.

***Do not let it get in the way of first POVs.***

Table of Contents

[What is Darktrace Antigena and how does it work? 2](#_Toc444720790)

[Why would companies need Darktrace Antigena? 2](#_Toc444720791)

[Why is Darktrace Antigena different? 2](#_Toc444720792)

[Won’t people get annoyed if their business operations are disrupted? 2](#_Toc444720793)

[What type of actions can Antigena take? 3](#_Toc444720794)

[Machines taking actions sounds scary. How do I trust it? 3](#_Toc444720795)

[When you talk about cyber defense at machine speeds, are you referring to botnets? 3](#_Toc444720796)

[How does Antigena compare with products like LastLine (or other legacy vendors)? I’ve heard that LastLine detects, decides and defends against evasive threats across web, email, content and mobile. 3](#_Toc444720797)

[I have already Bluecoat / Websense / [other] deployed. 4](#_Toc444720798)

[How are you different to DLP? 4](#_Toc444720799)

[What’s the Internet Module? 4](#_Toc444720800)

[What’s the Network module? 4](#_Toc444720801)

[What’s the Communication module? 4](#_Toc444720802)

[Would it help detect ransomware? 5](#_Toc444720803)

[Does Antigena integrate with anti-virus, etc? 5](#_Toc444720804)

[What triggers Antigena to generate a response? 5](#_Toc444720805)

[What does ‘measured response’ mean? 5](#_Toc444720806)

[Can you give me an example of Antigena in action? 5](#_Toc444720807)

[How is Antigena deployed? 6](#_Toc444720808)

[Is Antigena in use now by customers? 6](#_Toc444720809)

[Is Antigena generally available? How is it licensed? How much does it cost? 6](#_Toc444720810)

[I am interested in deploying some of these modules. What are the next steps? 6](#_Toc444720811)

[Can I do an Antigena POV? 6](#_Toc444720812)

# What is Darktrace Antigena and how does it work?

*Darktrace* *Antigena is a new product, which extends the capability of Darktrace’s Enterprise Immune System. It is a significant development because – for the first time – it allows machines to automatically fight back and actively self-defend.*

*Antigena produces digital antibodies, deployed by the immune system to take measured, defensive action related to live threats, without impacting the business.*

*Because Darktrace has a unique understanding of an organization’s ‘pattern of life’, Antigena can use this to enforce that pattern – without disrupting normal behaviors. Antigena simply takes over the defense, slowing threats for long enough to allow humans to arrive and take action. As attacks are so fast today, Antigena can react to slow or stop the attack, until the humans arrive on scene.*

*For example, if the immune system finds an employee acting abnormally – perhaps he has started accessing a file share more often than usual or at abnormal times of day, Antigena may decide to slow, or prevent, access to that specific location – while humans can investigate further. In the meantime, Antigena would permit the user to access areas that are part of his normal pattern of life.*

# Why would companies need Darktrace Antigena?

*We are living through a new era of threat – and the reality is that no security team, no matter how large, can respond effectively to continually evolving threats. Humans are simply too slow.*

*So, where a human response is too slow to protect you, Antigena takes automatic action to stop threats in their tracks, without disrupting day-to-day activity.*

*Because we understand what a real threat is, we can take* ***better*** *and* ***faster*** *action.*

*Any organization would benefit from using Antigena. The larger the network, the harder it is too keep up. While large companies may have more tools, those tools are not taking actions in a measured way. Smaller organizations have fewer security professionals on their teams, which makes it difficult to keep abreast of fast-moving threats.*

# Why is Darktrace Antigena different?

*It comes down to our machine learning and mathematics approach to detection. Darktrace is unique in its ability to automatically learn what is ‘normal’ inside a network – without using rules or signatures.*

*We are the first that have machine learning that is proven to work at scale, to detect unknown threats.*

*We call this approach the Enterprise Immune System.*

*So, Antigena is different, because it knows, through Darktrace, what ‘pattern of life’ should be enforced, and what is not part of the ‘pattern of life’.*

*Ultimately, this means that we can automatically defend networks and information – and do this far faster than any human can possibly do. Irrespective of the type of threat it is.*

*In contrast, traditional automated response tools have been too aggressive –they are extremely blunt tools that repeatedly shutting down network functionality and disrupting business operations. This is because they are based on arbitrarily-defined rules.*

# Won’t people get annoyed if their business operations are disrupted?

*The power of Darktrace is the accurate detection of genuine threats. Darktrace Antigena is so effective because the actions that it takes are* ***targeted*** *and* ***proportionate****.*

*Antigena will allow normal day-to-day activity to continue, whilst taking measured actions to curb threat where it has been detected, and in accordance with severity.*

*For example, a user that is behaving abnormally may have certain web connections slowed, or prevented, while continuing to interact normally with other web connections or IP addresses. If we see that the user is persistently acting abnormally, Antigena can also adapt its response appropriately.*

*Antigena is also fully configurable – you can choose how automated you want Antigena to be. Our experience is that organizations want to authorize the immune system to take certain automatic actions in instances where people would be too slow to act, and threats would otherwise get out of hand.*

# What type of actions can Antigena take?

*There are a number of actions that Antigena can take. It all depends on what is appropriate, based on what we understand about the threat.*

*For example, Antigena may slow, disrupt or even prevent activity – buying your security time, and stopping threats in their tracks.*

*There are three active modules:*

* *Antigena Internet – regulates user and machine access to the internet*
* *Antigena Communication – regulates email, chat and other messaging protocols*
* *Antigena Network – regulates machine and network connectivity and user access permissions*

*We will work with you to decide which module you require, based on your requirements.*

# Machines taking actions sounds scary. How do I trust it?

*Today we are living in a new era, where threats are outpacing humans routinely. Your security team is never going to be fast enough, particularly as we move to a phase of machine-on-machine attacks. Darktrace Antigena helps you regain the advantage.*

*Darktrace Antigena is entirely configurable. So you can choose to review and confirm Antigena’s suggested response, to start with. That way, you gain confidence in the actions Antigena suggests, and you still save time responding. Our expectation is that customers will choose to automate beyond this, in order to enable real-time response.*

# When you talk about cyber defense at machine speeds, are you referring to botnets?

*While botnet owners are trying to mimic legitimate cyber behavior to fly under the radar, what Darktrace has detected is very sophisticated attackers using machine learning to LEARN what normal behavior is for an employee. This is very difficult for a human to detect and will likely escalate into machine-versus-machine cyber warfare.*

# How does Antigena compare with products like LastLine (or other legacy vendors)? I’ve heard that LastLine detects, decides and defends against evasive threats across web, email, content and mobile.

*It’s very different.*

*LastLine is a system emulator approach that aims to prevent breaches by detecting malware. It uses sandbox technology to replay threats in a closed environment.*

*This can be evaded, by looking for clues that the computer is a ‘fake’ and waiting.*

*The major limitation of this legacy approach is that it can only ever spot known threats. It’s certainly not going to spot an insider like Edward Snowden.*

*In comparison, Darktrace Antigena knows what normal is, based on its mathematical understanding of the ‘pattern of life’ of the organization. It enforces this ‘pattern of life’ by keeping out abnormal behaviors, while maintaining normal activity.*

# I have already Bluecoat / Websense / [other] deployed.

*Not a problem. We would sit alongside Bluecoat. The challenge you have is that threats routinely get past Bluecoat. And it doesn’t address insider threat either.*

# How are you different to DLP?

*We are not looking at data. We are interested in ‘pattern of life’ which is constantly evolving. It’s a different approach.*

# What’s the Internet Module?

*This is about securing data within your trusted network, and protecting the network at large.*

*The internet module sits on the edge of your trusted network. Typically, you’ll have proxy tools here too (e.g. Bluecoat), which work on rules. The problem with those standard proxy tools is that they rely on rules. So you have to wait 3 weeks for your rules to be updated so that they restrict access to particular IPs, or websites that are known to contain malware. Administratively, it is a nightmare. And these tools are always out of date, and always changing.*

*For example, an individual sending ICS backup data and configurations to his home broadband would be missed by a proxy tool (such as Bluecoat) because that behavior doesn’t correspond to a known signature.*

*Darktrace Antigena – using the internet module – is different. We’d recognize activity as unusual, based on what we understand about the user and devices in question – and we’d decide to either slow the connection down, and maybe stop it.*

*The ability to do this in a measured way is critical – it gives you more time to solve the problem, while mitigating the risk.*

# What’s the Network module?

*This one sits inside your network. It can also work with your internet service providers*. *It can take targeted action within the network.*

*For example, Sue Smith is in HR, and has started to access the Operations network in the U.S. Darktrace has also noticed other unsual factors – the time she has attempted to access it, as well as data transfers. Here, Antigena may decide to take action, and temporarily revoke her user access privileges from this specific subnet. But we will not stop her doing her everyday job, because we allow her normal pattern of life to continue, uninterrupted.*

# What’s the Communication module?

*This is a bit different to the others. It’s mainly about email.*

*Email goes over same network channel. So you don’t get fine control from network point of view. This module understands the communication protocol, so more nuanced responses are possible. It gives you access and control over communication channels.*

*For example – we see questionable email activity related to Peter’s account. As a first step, we may decide to immediately stop Peter sending work email to his personal Gmail account, while we investigate. However, Peter will still be able to email all his colleagues, as normal.*

*At the network level, you can’t act with that same degree of subtlety.*

# Would it help detect ransomware?

*Yes – in fact, Darktrace already detects ransomware all the time. This is a good example of why humans are often too slow.*

*The problem with ransomware is that, once you’ve been infected, it will immediately start encrypting people’s data. By the time that the human has noticed, it’s too late.*

*Darktrace detects the* ***change*** *implicit in ransomware – either at the point of infection, or as executables are downloaded. With Antigena complementing Darktrace, we can stop that behavior as soon as we see it. The vast majority of the data can be protected.*

*Also, these digital antibodies don’t need to have seen ransomware threats before, to be protected from them.*

# Does Antigena integrate with anti-virus, etc.?

*Yes, we can work with your infrastructure. For the internet module, we’d work with tools on the border, such as Open Flow or Cisco, where we are able to take measured responses. For the network module, we would likely interface with Microsoft Active Directory.*

# What triggers Antigena to generate a response?

*Darktrace assesses threats constantly, and makes a judgement – which is manifested in Antigena’s response.*

*You can have a user to confirm Antigena’s preferred action, however, to give your team further control. When you are comfortable with Antigena’s responses, we’d anticipate that you would decide to fully automate certain functions. So you have total control over Antigena.*

# What does ‘measured response’ mean?

*Antigena can take action that is in proportion to the severity of the threat. It is a dynamic product, that is constantly evaluating and re-judging threats. Antigena‘s feedback loop means that it learns dynamically from a machine or user’s response to its action – and adapts its continued response accordingly.*

# Can you give me an example of Antigena in action?

*Let’s say Darktrace detected anomalous behavior, which uncovers that a bored employee has started browsing around and stumbles across back-up emails on a drive. You don’t want to fire that person, but you do want to take some action. Antigena may decide to slow down the user’s connections.*

*If that user starts waiting and doing it again – then Antigena will learn that the user is not just casually browsing. They are persistent. Antigena may then prevent the employee from seeing those PSTs. He gets blocked from the file share.*

*If that user continues by trying to gain access via other machines, Antigena knows that they are a threat.*

*Antigena may go through several cycles of response and feedback, before a human intervenes – it gets there faster, and mitigates risk before a security analyst can give it their attention.*

# 

# How is Antigena deployed?

*It is deployed as a physical appliance, in addition to your core Darktrace appliance(s), and can be installed easily and quickly. The right place in the network needs to be identified.*

*It is a separate appliance to the core Darktrace appliance. Darktrace sits passively in the network, whereas Darktrace Antigena sits in-line, in order to take action.*

*[The Antigena appliances don’t displace other tools. If it blows up, it will ‘fail open’. So it won’t bring down your network]*

# Is Antigena in use now by customers?

*We have deployed Antigena with selected early adopters. Selected organizations include a hedge fund, media company, and genetics company.*

# Is Antigena generally available? How is it licensed? How much does it cost?

*We are initially rolling out our Internet Module as part of our early adopters program. Antigena will be licensed on a subscription basis. Please speak to your manager to discuss specific pricing.*

# I am interested in deploying some of these modules. What are the next steps?

*That’s great. We are working with early adopters at the moment. I’d be happy to set up a meeting to discuss your interests, and if you’d like to join the early adopter program.*

*[Speak to Jack Stockdale first, before setting up customer calls about Antigena]*

# Can I do an Antigena POV?

*We don’t offer POVs for Antigena. Darktrace POVs are designed to demonstrate the value of Darktrace – the core of our Enterprise Immune System approach. Antigena is an extension of that approach, and can be purchased as an add-on.*