

SENSEON

Sensory AI for cyber defence

CUSTOMER CASE STUDY: NOT FOR PROFIT



FAST FACTS

Company

- bpha

Size

- 400+ employees

Industry

- Not-for-profit housing association

Challenges

- Wanted to utilise the latest in AI threat detection and response technology
- Keen to manage their own security solutions
- Looking to increase visibility across digital estate to match growth
- False positives from existing tools proving problematic

Outcomes

- AI augments the role of the IT team
- Intuitive interface helps the team understand the threat environment
- Increased accuracy of threat detection
- Context-rich alerts raised for attention of team

“Senseon’s ability to adapt and learn strengthens my confidence that we will stay ahead of tomorrow’s cyber threats.”

**Graeme Hope, Infrastructure
Technical Architect, bpha**

The not-for-profit threat landscape

Large not-for-profits (NFPs) may hold the personal identification information of thousands of customers, along perhaps with their card details. Such data can either be used to launch further attacks elsewhere, or more likely can be sold in online forums to other criminals. NFPs may not offer such enormous data sets, but generally suffer from restricted security capabilities due to tight budgets, so may offer cyber criminals more efficient returns on their investment. NFPs typically experience data theft, financial theft, or even ransomware impacting their business.

“GDPR, continuing high levels of cyber criminality, and growing use of online business practices by NFPs mean investment in cyber security is increasingly imperative for the sector.”

UK’S National Cyber Security Centre

Business background

bpha is a leading provider and developer of affordable homes - for rent, sheltered living, residential care, and shared ownership. As an NFP, all the money bpha makes is reinvested in its business, enabling it to build new homes, and to deliver new and improved services. With over 18,500 homes and 400 staff under management, securing their digital estate against cyber threats is a big priority.

Value for customers

As an NFP, bpha is devoted to providing great service for its customers, in this case, those who live in their managed properties. This focus on the customer, and the company belief in getting things right the first time, extends to bpha’s innovative IT department. bpha’s IT team were looking to utilise an AI-led technology to increase visibility, decrease false positives, and free up their security team’s time for investigating genuine threats. With this in mind, they began a Senseon Value Assessment.

“We were keen to utilise new and innovative technology to defend our organisation. We spent a lot of time looking at more conventional solutions, but only Senseon offered the functionality we wanted at a sensible price point.”

Adrian More, IT Director

Safe as houses

With Senseon installed, bpha immediately began to see the value. Whereas other solutions would have required the expensive hiring of outside parties to help them manage the sheer volume of alerts, Senseon’s intuitive interface was instantly accessible to the entire IT team.

22% of NFPs identified cyber security breaches or attacks in the last 12 months

“I really like that Senseon gives us full visibility across our entire organisation. Accurate alerts help us avoid a backlog, so we can be sure that we stop the threats.

Adrian More, IT Director, bpha

The platform's accurate detection of threats across endpoints and the network meant that not only was their visibility increased, but the number of false positives also dramatically reduced. This allowed the IT team to take more control of the process, saving them time and money.

A unique approach

Senseon combines its multiple 'senses' across endpoints, networks, and Investigator Bots, which look at potential threats from an outside point of view, to maintain visibility across an organisation's entire digital estate. Senseon's ability to converse autonomously through AI allows for the accurate detection of threats anywhere in the company. This blending of senses - a process known as 'AI Triangulation' - provides the context and clarity needed to ensure that Senseon can detect and isolate even the most advanced and subtle threats.

“Senseon's ability to adapt and learn strengthens my confidence that we will stay ahead of tomorrow's cyber threats.”

Graeme Hope, Infrastructure Technical Architect

Once deployed in an environment, Senseon builds up a pattern of behaviour specific to the devices and users. This self-learning approach constantly adapts to distinguish between unusual behaviour and malicious threats. Senseon's unparalleled visibility across their entire digital estate, combined with its use of AI Triangulation and its ability to provide context, results in genuine threats being escalated for the attention of the IT team.

Augmenting the analyst

Senseon's unique 'AI Triangulation' technology observes threats from multiple perspectives, pauses for thought, and learns from experience. The platform automatically gathers context, carries out investigations, and provides highly accurate alerts. This automation reduces the burden of manual detection and investigation for the security team, enabling them to focus their efforts where they matter most: dealing with genuine threats.

Complex threats, simple solutions

Senseon's unique user interface, with its intuitive design, usability, and adaptability, was welcomed by the bpha team. The platform detects threats across an organisation's entire digital estate and prioritises them according to their importance. Each threat has its own dedicated 'Case' automatically created by Senseon.

Looking to the future

As a housing association, bpha is used to planning years in advance. bpha's investments have to be justifiable for decades, and their cyber security is no exception. Senseon was designed to be flexible and scalable so that it could grow in parallel with its customers' needs and stay ahead of the changing cyber threat landscape. bpha look forward to working together with Senseon to continue protecting their digital estate now and into the future.

About Senseon

Senseon is the next phase of AI for cyber defence, moving beyond rules-based systems that are too rigid to keep pace with emerging cyber-attacks or ineffective AI systems that cannot differentiate between unusual behaviour and malicious threats. Unique to Senseon, 'AI Triangulation' understands and correlates threats across an organisation's entire digital estate, providing much needed context and clarity in an increasingly noisy landscape. Founded in 2017, Senseon brings together cyber security experts, former government cyber operatives, and applied machine learning specialists. Headquartered in London, UK and Chicago, USA, Senseon also has a presence in the Middle East and Australia.

Contact Us

✉ info@senseon.io
☎ +44 (0) 20 7692 5178
🌐 senseon.io
🐦 @SenseonTech
📍 100 Pall Mall, London, SW1Y 5NQ