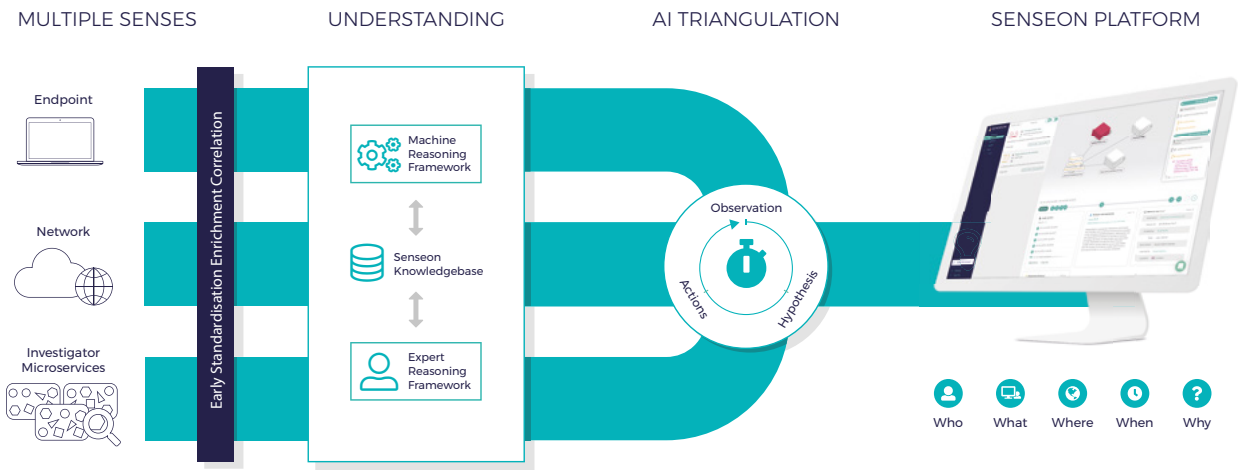
Technology overview

Senseon's unique 'AI Triangulation' technology emulates how a human security analyst thinks and acts to automate the process of threat detection, investigation and response. By looking at the behaviours of users and devices from multiple perspectives, pausing for thought and learning from experience, Senseon provides accurate and context-rich alerts. These automated capabilities free security teams from the burden of exhaustive analysis, alert fatigue and false positives.



The Senseon technology architecture

Whilst being very complex under the hood, the Senseon architecture was designed to allow for the simple deployment of Senseon's technological innovations. Performing the job of multiple tools in one platform, Senseon's broad approach uses various methods to allow for the automation of threat detection, investigation and response. These innovations give security teams the best chance of identifying and remediating cyber threats, no matter where in the organisation they occur.

1. Multiple senses

By gathering data from multiple perspectives, Senseon is able to help organisations build an accurate picture of their environment. As well as providing unparalleled visibility, looking at behaviour from multiple perspectives means that the accuracy of alerting is increased with greater context and understanding. In turn, this allows for the reduction of false positive alerts.

The Network

The Senseon network appliance is typically installed in the core of a network, taking a TAP or SPAN from the core switch. From here, the passive and in parallel network appliance ingests raw traffic network. The breadth, visibility and rich source of data provided here is crucial for allowing Senseon to build a baseline of the environment and its behaviours for later anomaly detection.

Endpoint devices

Senseon's lightweight endpoint agent is installed on corporate devices such as laptops, desktops and servers, and runs on various operating systems such as Windows, Mac and Linux. From this data Senseon can observe and understand the processes that are running on each endpoint. The information of these processes is then mapped to network connections and other data points. This is one of the advantages of having visibility across both endpoint and network data.

Investigator microservices

Investigator microservices are cloud-hosted microservices that perform 'just-in-time' intelligence gathering to allow Senseon to further-qualify activity. For example, if Senseon identified an unusual outbound connection, the network appliance might reach out to the Investigator Bot to ask for some more information about that domain - when was it registered, is it a known malicious domain, etc.

2. Understanding

Once the data has been ingested and enriched, Senseon can then store and analyse it. Two reasoning frameworks allow for a combination of automated detection methods before the output of Observations are further analysed by Senson's AI Triangulation.

Senseon knowledge base

The knowledge base stores all of the raw data collected from Senseon's multiple senses. This is also where models of user, device and business behaviours are stored for later recall.

Machine reasoning framework

The machine reasoning framework consists of both unsupervised and supervised machine learning approaches.

Unsupervised machine learning is used to conduct data driven detections for identifying exploits or new and novel techniques that can't be described in Senseon's range of other detection approaches. Features extracted from the endpoint and network are fed into these approaches to either look for anomalies in raw data such as connection, process or DNS data etc, or anomalies in user, device and network behaviour in order to detect new and novel attacker techniques.

Supervised learning is used to help make the output of the anomaly detection more understandable for human analysts, helping them to investigate and remediate threats quickly.

Find out more about Senseon's enhanced anomaly detection using a Supervised/Unsupervised cross-over method in this abstract here.

Expert reasoning framework

The Expert Reasoning Framework contains analytics built by Senseon's expert analysts. These custom analytics flag behaviours or events that are of interest to organisations and security teams. The analytics are often low confidence indicators and will only become alerts when further activity is added to the 'Case' and Senseon is confident that the activity is malicious or interesting.

3. AI Triangulation

Unique to Senseon, AI Triangulation automates investigation. It brings together the outputs from both reasoning frameworks as Observations, compares them to real-world hypothesis, and then takes a series of automated actions to confirm or deny the hypothesis and the presence of malicious activity.

Observations

Observations are the output of both reasoning frameworks. They are effectively unique and independent events seen within your organisation. Related Observations are later combined into Cases. By associating related Observations analysts and IT are able to understand and deal with threats quickly.

Hypothesis

The AI Triangulation creates real-world hypotheses to explain what each Observation may be. For example, Senseon witnesses a large volume of data leaving the corporate network. Here the hypothesis could be 'potential data exfiltration'.

Actions

To AI Triangulation performs actions to prove or disprove each hypothesis. Actions include the combination of understanding user and device behaviour, intelligence from previously seen attacks, and analytics from the Human reasoning framework.

Case timer

The Case timer is a simple yet powerful innovation that can only be enabled by the high telemetry nature of Senseon. It allows the system to 'pause for thought', unlike other tools that would jump to conclusions and fire off several alerts without understanding the nature and context of an anomaly. Instead, Senseon waits to receive further passive Observations relating to the Case. This allows time for AI Triangulation to confirm or deny the hypothesis.

In the event of a high velocity, high impact attack (such as ransomware), the Case Timer would be bypassed and an alert would immediately be raised. When dealing with attacks like these it's better to be early and wrong, than late and right.

4. Senseon user interface

Once the hypothesis from the AI Triangulation has confirmed interesting or malicious activity, the Case is escalated and prioritised in the Senseon interface for further investigation by a human analyst.

Investigate

The Investigate View simplifies the process of investigation and prioritises genuine threat Cases for the attention of security teams. Its step-by-step narrative interface breaks down individual Observations, allowing analysts to quickly ascertain the sequence of events.

Hunt

The Hunt View provides analysts and more experienced users with a collection of tools to undertake their own manual threat hunting and analysis. The raw data, enriched by Senseon, is collected from endpoints devices and the network and available for analysts to run SQL queries.

Experience

The Experience View provides access to the underlying data of all Observations and Cases. Unlike a black box solution, the Experience View exposes the output and reasoning of Senseon's AI Triangulation to help organisations understand how and why decisions have been made.

Dashboard

The Dashboard View provides a high-level overview of your organisation and helps CISOs and security professionals to understand and manage the risks facing their business. Gathering intelligence from the richest sources of data, Senseon is able to show interesting insights and trends at an organisational level.

Deploying Senseon

Senseon deploys across your organisation and gathers intelligence from the richest sources of data. Below is an example of a basic, on-prem Senseon deployment. If your environment is more complex or if you would like to know more about Senseon cloud deployments, a member of the team will be happy to discuss this with you.

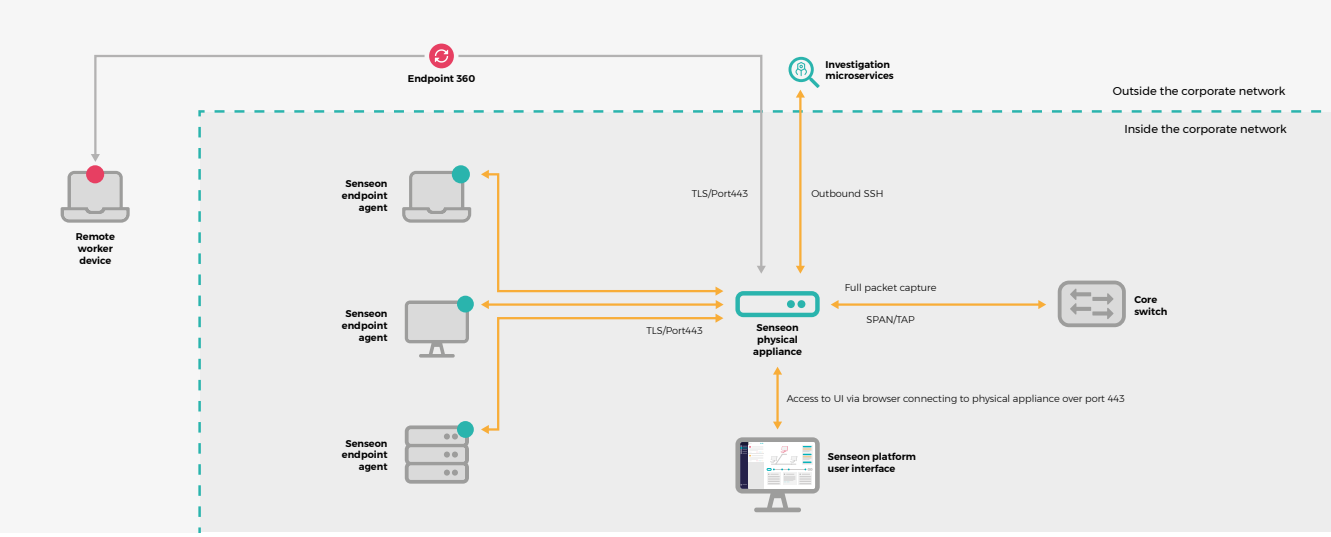


Illustration of a basic Senseon deployment

Network appliance

The Senseon network appliance is very simple to install and is designed to be plug and play. It comes pre-configured and built to meet the requirements of your organisation. The appliance can be installed on-prem or within your data centre and is configured to receive network traffic via a SPAN or TAP, typically from your core switch. The network appliance is the heart of a basic Senseon deployment. It is through the appliance that all data is gathered and processed and where users access the Senseon interface.

Endpoint agents

Senseon's lightweight endpoint agents are easily deployed across endpoint devices such as laptops, desktops and servers. The endpoints are available for Windows, Mac and Linux systems.

Endpoint 360

Endpoint 360 protects your employees and devices 24/7 both within and outside of the corporate network. This optional service requires no further deployment than the standard endpoint roll-out.

Investigator microservices

Investigator microservices are hosted by Senseon. There are no requirements for you to deploy or host these.

Senseon platform user interface

The user interface can be accessed using any machine via any browser (we recommend Chrome) that connects to the Senseon physical appliance.

About Senseon

Senseon's unique 'AI Triangulation' technology emulates how a human security analyst thinks and acts to automate the process of threat detection, investigation and response. Capable of looking at the behaviours of users and devices from multiple perspectives, pausing for thought and learning from experience, Senseon provides accurate and context-rich alerts. These automated capabilities free security teams from the burden of exhaustive analysis, alert fatigue and false positives. Founded in 2017, Senseon brings together cyber security experts, former government cyber operatives and applied machine learning specialists.

Contact Us

info@senseon.io
+44 (0) 20 3994 1069
senseon.io
@SenseonTech
100 Pall Mall, London, SW1Y 5NQ