

Q: What is Senrio Insight?

A: Senrio Insight finds and categorizes devices on the network, telling you not only what devices you have but what they are doing, and when they are doing. Insight provides both technical and non-technical users with context-rich analytics based on device-specific behavior and adaptive learning. Insight alerts you when devices behave abnormally, enabling you to implement your safety or security protocols.

---

Q: Is it software or an appliance?

A: Insight is software. You can install it on your own commodity hardware running Linux, or a commodity wireless access point (we support over 700 different makes/models).

---

Q: How big is the Insight executable?

A: The Insight executable is about 1MB. It's small enough that some customers actually embed it into their own security appliances.

---

Q: You said Insight looks at devices. I heard you mention a "sensor." Is it an endpoint protection solution? Does it use "agents?"

A: No. Insight works at the network, session, and transport layers.

---

Q: What kind of data does Insight look at?

A: In short, packet headers. It does not perform deep packet inspection. This allows us to operate in highly regulated environments because we do not see data that might violate user privacy such as PCI or HIPAA.

---

Q: How much of a strain on bandwidth will Insight put on my network?

A: Nominal. Insight collects and processes packet header information. It does not do deep packet inspection. This allows us to deal with large volumes of traffic without having a noticeable impact on throughput. Additionally, Insight is design to track IoT devices and ignore non-IoT devices (laptops, desktops, and servers). Generally speaking IoT devices have a much smaller network utilization rate, which means the traffic captured by Insight is smaller than the equivalent number of non-IoT systems.

---

Q: How well does Insight scale?

A: Insight does its analytical heavy lifting in the cloud. Data collected by your Insight network sensor is pushed to your own dedicated instance on AWS. Our scalability tests have shown an ability to handle 50,000 connections (connections - not packets) / second.

---

Q: Does Insight collection personally identifiable/health information?

A: No. Insight only captures IP and TCP/UDP headers along with other network meta-data (currently DNS and DHCP, more in the works). This is used to help fingerprint and track device behavior.

---

Q: Our enterprise includes X facilities in Y states and Z countries. How would we deploy Insight?

A: Every location would need a system running Insight to capture data locally. That data would be sent to your own dedicated instance in the cloud, at which point you would be able to access the data through our user interface. Alternately, you could have local traffic collected and sent to a central location (e.g. your NOC or SOC) for ingest into your existing SIEM. Insight has an API, and exports data in STIX, TAXII, CSV and other formats.

---

Q: How do you define "IoT?" In my environment a laptop or tablet might be connected to, or be the user interface to, an IoT device (e.g. medical device).

A: In the context of Insight we divide devices into two camps: user and non-user. A user-based system would be any commodity IT device that has a person sitting behind it using productivity or some other common software (e.g. administration, billing, etc.). Non-user devices include what most people define as an IoT device (drug pumps, programmable logic controllers, cameras, etc.). You can classify any

and all devices using tags, so in the case of a nurse or doctor using a tablet to interface with medical devices, you could tag that tablet in whatever fashion makes the most sense.

---

Q: Can you manage multiple Insight deployments through a single UI?

A: Yes, but. If you're an MSP/MSSP and want to talk about this sort of use case, please drop us a line and we'll have a more in-depth conversation.

---

Q: Does Insight only work with AWS? I need to use <another cloud provider> or an on-premise solution.

A: No, but. Insight was built to take advantage of a range of features AWS provides. Retooling things to work with another cloud provider is entirely do-able, but probably not trivial (easier to transition to AWS GovCloud than, say, Azure). The same goes for an on-premise approach. If Insight seems like the right solution for you, let's talk about what might be required to make it work for you.

---

Q: How does Tagging work?

A: We have a number of pre-built tags that will automatically populate a device entry based on information we've already collected from the same make/model device, or from data the device gives up in packets. You can also create your own tags based on specific use cases or needs, and you can create meta-tags, which 'bundle' other tags to help you further refine how you describe devices.

---

Q: Do you have an API?

A: Yes, we have a RESTful API.

---

Q: What other security or visualization tools do you integrate with?

A: We export data in .csv, JSON, and other formats. We have a Splunk app, and we are a RSA certified technology partner.