signalsense

DEPLOYMENT GUIDE

DEPLOYMENT AND IMPLEMENTATION OF THE SIGNALSENSE ALPHA RELEASE

SignalSense is an active breach detection platform that uses context to quickly and automatically identify real-time compromises inside an environment. Our context engine improves detection dramatically, identifying breaches that can't be caught at all by most of today's systems—such as anomalous behavior with valid credentials.

The SignalSense Alpha Program

As we prepare for our initial release, we're working together with a number of partners to test and fine-tune our product. With access to these diverse environments and higher traffic networks, we'll have the real-world engineering feedback to make significant improvements ahead of release.

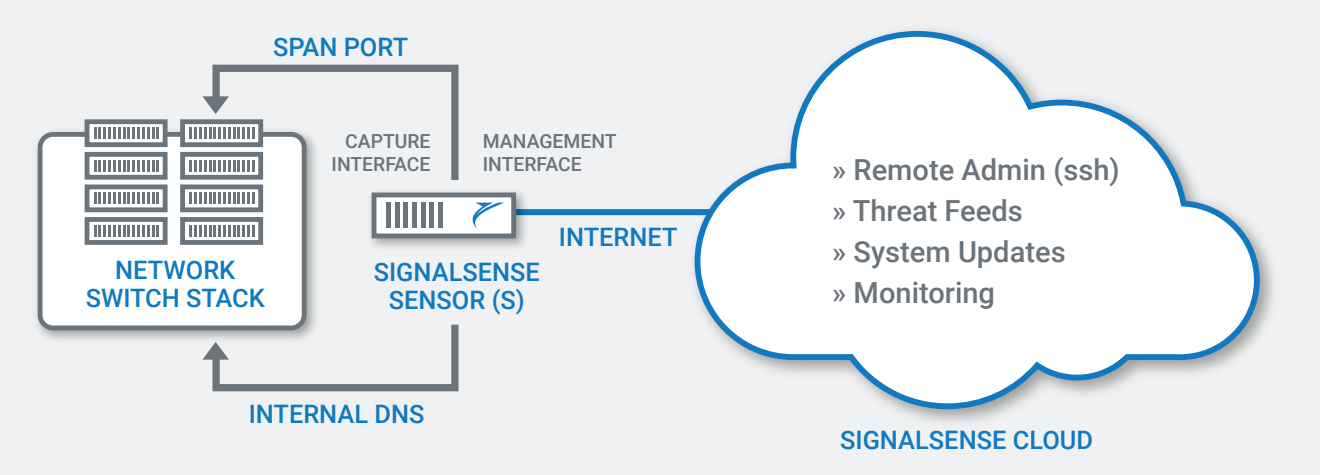
We intend our Alpha Program partnerships to be mutually beneficial: in exchange for access to robust testing environments from our partners, we will be striving throughout the program to provide timely and valuable insight into security threats.

Hardware sensor interface types

All SignalSense hardware sensors come pre-configured with both a capture interface and a management interface.

» **Capture interface:** You should connect the capture interface to a Switch Port Analyzer (SPAN) port on a switch associated with the network segment to be monitored, or to a network Test Access Point (TAP). A sensor can monitor multiple network segments using a network packet broker. By default, an individual sensor can monitor sustained network traffic of up to 5 Gb.

» **Management interface:** You can connect the management interface to the same network segment that's being monitored, or you can isolate it to a separate network segment. In either case, the interface must be accessible by SignalSense through a customer-configured VPN or a reverse SSH tunnel connection. The management interface also needs reachability to your internal DNS for forward/reverse name resolution.



Sensor connections

Once a sensor is deployed and operational, SignalSense will use the management interface to administer, update, monitor, and interact with the sensor. The management interface will also be used to periodically access certain external threat intelligence feeds.

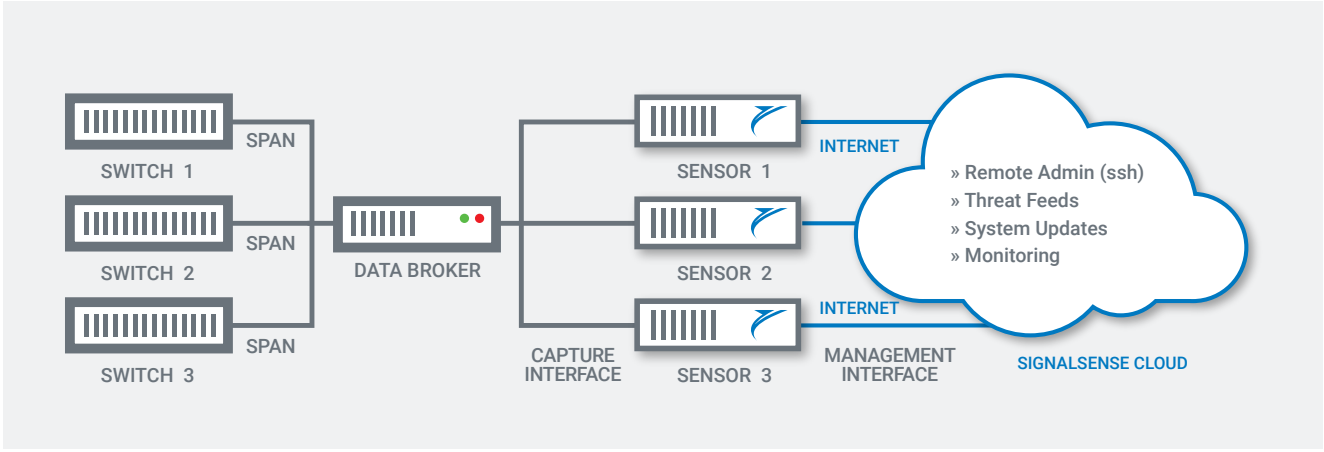
The management interface has an internal firewall and allows connections on ports 22, 9000, and 9099, which correspond to SSH, web UI server, and REST API, respectively.

Outbound, the sensor will open connections from the management interface for the following:

Task	Destination Port	Function
Threat Feeds	80 and 443	Periodic updating of sensor databases from various threat intelligence feeds
System Monitoring	443	Connection to SignalSense cloud services
Sensor Updates	443	Perodic updating of sensor software components from SignalSense cloud repositories
DNS Resolutions	53	Data enrichment for endpoints
Geographic Information	80	Access to mapping data

Sensor configuration and administration

We will pre-configure and remotely administer all sensors for partners in our Alpha Program. If you have more questions about specific sensor configuration and administration details, let us know and we can provide more background.



Questions?

Contact us at 206.495.9780 or info@signalsense.com.

signalsense
217 Pine Street, Suite 1100, Seattle, WA 98101
T: 206.495.9780 www.signalsense.com info@signalsense.com