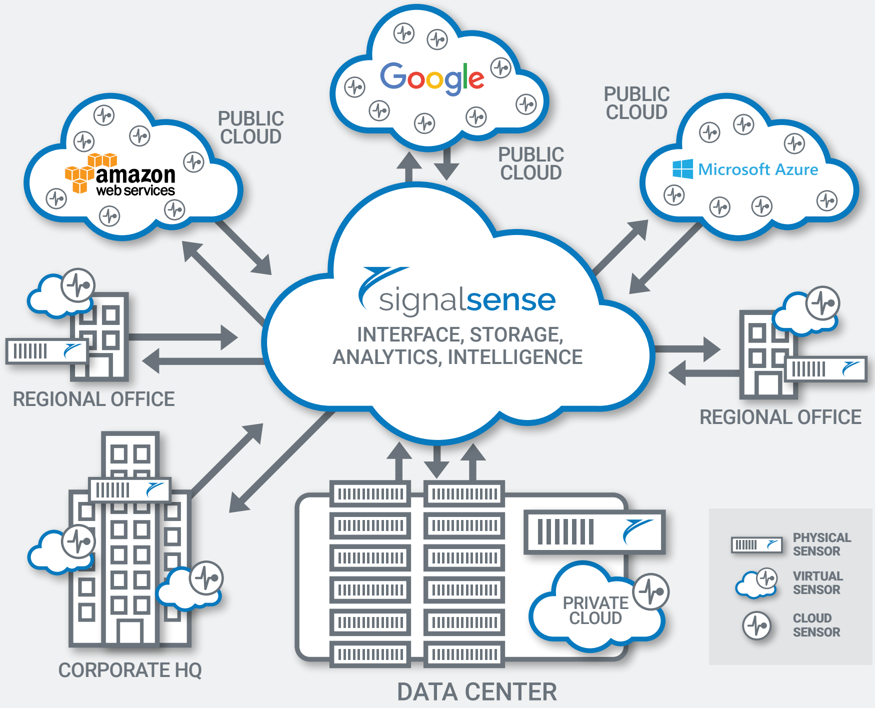
signalsense

PRODUCT BRIEF

ACTIVE BREACH DETECTION

A next-generation, network-centric platform for automatically discovering more compromises—and more elusive compromises—inside your environment.



- » **Get a deep, hyperaccurate view of your environment**-both how it should behave and how it's actually behaving.
- » **Detect compromises in real time**—even the most elusive ones, with our powerful context and next-generation machine-learning threat detection models.
- » **Make better decisions faster.** Dramatically reduce alerts so your security team can act on active breaches with confidence.

Security operations teams are drowning in alerts. The typical enterprise SOC gets 17,000 alerts per week. Less than 20% of those are considered reliable, and only 4% get investigated by scarce and valuable human operators. With the many threats that do get through, average dwell times now exceed 200 days.

Hackers are releasing new malware every 200 milliseconds, and cybersecurity veterans know that we're beyond the ability of humans to keep up. Machine learning is the only way to close the gap—but it's not enough by itself.

You also need context. Context is a complete picture of what's been detected and why—and it's created by the near-human cognition of machine learning combined with a deep understanding of an environment's unique behavior.

SignalSense creates context.

SignalSense is an active breach detection platform that uses context to quickly and automatically identify real-time compromises inside your environment.

We don’t just reduce time to detection. 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.

Acquire and enrich traffic

Your network is the definitive source of truth for compromises inside your environment. We map your entire environment—automatically discovering and classifying everything up to the application level. Then we map all critical traffic on your network, both lateral east-west traffic and north-south flows. This is the first step to proactively seeking out compromises anywhere in your environment.

Create and leverage context

Post-mortems on costly breaches often reveal multiple alerts fired across many systems-but when a SOC is saturated with alerts, it’s extremely difficult to differentiate between false alarms and severe incidents. The key is context. We partner with clients to develop behavioral models that create a deep understanding of their environment—and then we combine that with our patent-protected machine-learning detection modules for massive insight.

Identify and analyze incidents

Our context engine identifies the footprints of actual compromises, not just threats. We treat traditional threat intelligence (TI) as just another data feed, while our context effectively generates its own custom TI, specific to that particular environment. Our analysis looks both forward and back: adding context in real time while a compromise is in progress, and checking back through metadata to find previous occurrences.

Surface incidents at scale, in real time

We push alerts to the SIEM only on actual breaches, and our clear, concise declaration format helps you drill down and navigate details in our UI. By greatly reducing “noise” in the SIEM, we help teams make better decisions faster.