



DARK THREAT DETECTION

BEHAVIORAL ANOMALY DETECTION

THREAT HUNTING

THREAT RESPONSE

AI-BASED LEARNING

WHY CYGLASS

CyGlass has unparalleled experience in delivering dark threat anomaly detection solutions for strategic cyber defense operations.

THE CHALLENGE

We are fighting an asymmetric war against motivated and creative cyber threat actors. Their attacks are never a single event. They are a well-defined and orchestrated series of tactics, techniques and procedures designed to use your network against you. At the same time, the cost to engage in these sophisticated attacks is decreasing.

We can no longer protect ourselves with reactive technology. End point detection and response systems can be subverted. SIEM technology provides event notifications and alerts after the fact. Our firewalls, anti-virus, intrusion detection systems and data loss prevention systems depend on existing signatures and rules. They can only prevent known threats and are static by nature.

The security paradigm has shifted and we are now mandated to anticipate, and proactively defend against unknown dark threats before they evolve.

CYGLASS DARK THREAT DETECTION

CyGlass uncovers in real time how advanced threats are evolving within your network and helps you stop them before they turn into attacks.

Using an ensemble of artificial intelligence, machine learning, and deep learning techniques, CyGlass correlates the sequences of network traffic, log data, asset metadata and federated intelligence to provide context to the behaviors in your network and pinpoint the exact threat.

CyGlass is driven by the principle that intimate knowledge of your network is your greatest advantage against cyber threat actors. By understanding the behaviors of your network in relationship to the value of your assets, and the context of emerging threats, you can now regain the upper hand.

QUICK FACTS

- Hackers can break in to your network in less than 12 hours
- 50% of all attacks on corporate networks are unknown
- It takes more than 200 days to discover complex attacks

STEP 1: DISCOVERS AND LEARNS

Virtual or hardware based collectors are deployed as a SPAN or TAP to ingest network traffic, log data, asset and user metadata in addition to sources of federated intelligence. CyGlass Analytics begins to learn the behaviors of your network while identifying and classifying the value of your critical assets.

STEP 3: PINPOINTS AND MITIGATES

Visualization mapping provides a time based narration of how a threat is evolving in your network and permits you to drill down into the details of the threat. Integration with security orchestration and incident management tools provide semi-automatic or fully automatic response and remediation.

Federated intelligence from 3rd party sources can be leveraged to enrich the data sets and provide enhanced capabilities in pinpointing threats.

OPERATIONAL INFORMATION

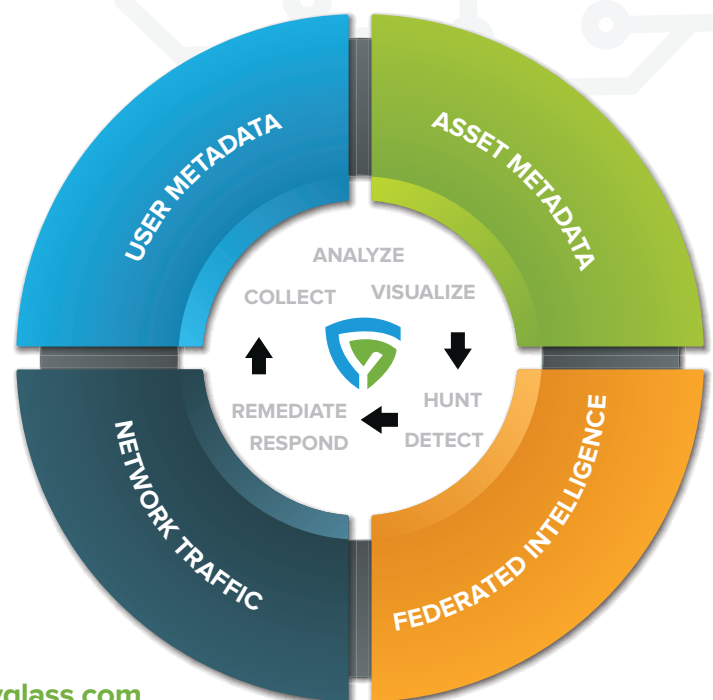
CyGlass Analytics can be deployed either in a SaaS model through our AWS offering or can be deployed in your own private cloud or on premise. Collectors can be deployed either as hardware or virtual appliances.

STEP 2: PREDICTS AND PRIORITIZES

Anomalous behaviors are uncovered and prioritized through an ensemble of machine learning and deep learning algorithms and are pinpointed into areas of concern. Areas of concern provide an in-depth understanding of the context of the threat and its evolution in relationship to the critical assets involved.

SURFACES THREATS

- Web and DNS Activities
- Masqueraders
- Credential Compromise
- Rogue behaviors
- Low Slow | Low Fast Behaviors
- Insider Threats
- Lateral Movement
- Exfiltration (Dark Nets)



For more information, please contact sales@cyglass.com