

Fortinet and Cyglass Integrated Security Solution

Security without Compromise with Artificial Intelligence Driven Network Behavior Anomaly Detection

Challenges

Over the last three years, more than 50% of breaches were a result of “advanced cyberthreats”. The failure of existing security technologies to stop unknown attacks, and the continued dependency on security analysts to sift through an overwhelming volume of logs and alerts has resulted in 70% of “advanced threats” going unfound. With breaches occurring daily, relying on signatures or rule-based security products is ineffective, leaving organizations more exposed and inundating the Security Operations Center (SOC) with false positives. Organizations’ organically developed or “accidental” network architectures are especially vulnerable to exploit. The key to effective cybersecurity lies in focusing on the most critical threats. Organizations today are leveraging Artificial Intelligence (AI) to provide enhanced visibility, improved productivity and greater precision in defending their networks from cyber-attacks. Without automating security responses and comprehensively applying artificial intelligence with self-learning technologies, networks will continue to be breached. In order to survive the modern, sophisticated attacker, companies need AI to create actionable intelligence. Only then will organizations be able to keep their critical IT assets secure.

Joint Solution Description

The Fortinet and CyGlass solution integrates battle hardened AI technology to the industry leading Fortinet Security Fabric. The Fortinet Security Fabric is designed around a series of open APIs, Open Authentication Technology, and standardized telemetry data to enable organizations to integrate existing security technologies via open interfaces and provide end-to-end security without compromise.

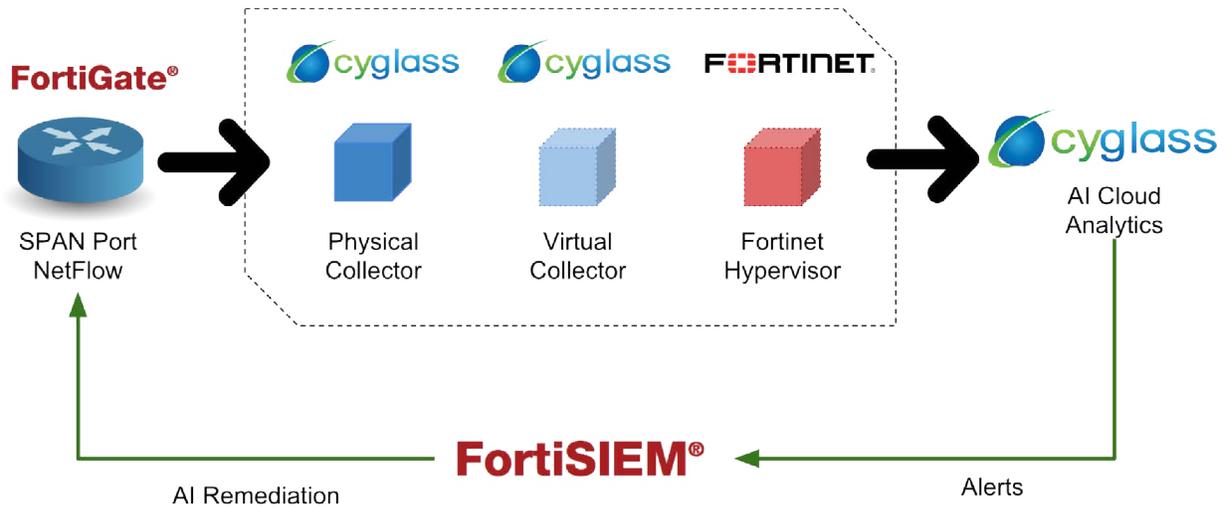
As part of the Fabric-Ready partnership between Fortinet and CyGlass, network traffic information flowing into FortiGate and FortiSwitch is shared with the CyGlass physical or virtual collector. The PCAP (packet capture) Header or Netflow data flows through an encrypted channel to CyGlass’s analytics engine in the cloud. CyGlass applies machine learning and machine reasoning to baseline normal behaviors, and correlate events and behaviors across networks. This promptly detects anomalous behaviors and potential threats. CyGlass charts out the emergence of threats to provide greater insight into the major actors involved, and the behaviors causing the suspicious activities. As it learns from customer feedback, it becomes more precise and allows analysts to focus on the most serious threats. CyGlass AI sends detailed alerts to FortiSIEM, enabling efficient and effective investigations and remediation.

FortiSIEM also provides rapid time to value with out-of-the-box compliance reporting and analytics tools. Pre-built reports are standard and help to manage a wide range of compliance needs, including PCI – DSS, HIPAA, ISO 27001, FISMA, SOX, NERC, COBIT, ITIL, SOX, GLBA, GPG13, and SANS best practices. These reports can be customized to suit unique needs.

Solution Benefits

- Enhanced threat detection and behavioral analysis capability
- Greater visibility and protection against advanced cyber-threats
- Identification and classification of rouge assets not covered by endpoint agents
- Anomaly spotting without prior knowledge or human intervention
- Security focused network monitoring and customizable reporting

**Fabric-Ready**



Caption: Fortinet - Cyglass Integration

Cyglass

CyGlass is a network behavior anomaly detection solution, which uses artificial intelligence to surface and prioritize unknown threats within your network. Regardless of whether on-premise, in your virtualized environment, or your cloud, CyGlass provides visibility and understanding of your network behavior as well as the behavior of your critical assets. Based on unsupervised and supervised machine learning, CyGlass uniquely leverages a layered algorithmic approach to analyze network traffic and build an illustrated story of how a threat has emerged over time. Areas of concern are prioritized by confidence levels and threat scores to save your security operations critical time in mitigating a surfaced threat.

FortiGate Enterprise Firewall

The Fortinet FortiGate Network Security Platform provides high performance, layered security services and granular visibility for end-to-end protection across the entire enterprise network. Innovative security processor (SPU) technology delivers

high-performance application layer security services (NGFW, SSL inspection, and threat protection), coupled with the industry's fastest SSL inspection engine to help protect against malware hiding in SSL/ TLS encrypted traffic. The platform also leverages global threat intelligence to protect individual customers, by using Fortinet's FortiGuard Security Subscription Services to enable visibility and control for next-generation protection against advanced threats, including zero-day attacks.

About Cyglass

CyGlass is a leading provider of network centric threat detection solutions using artificial intelligence that allow you to uncover, pinpoint, and respond to non-signature based cyber threats that have evaded traditional security controls. Incubated over the last decade in the most rigorous environments, CyGlass has unparalleled experience delivering solutions based on artificial intelligence, machine learning and deep learning for mission critical cyber defense operations? Learn more at www.cyglass.com