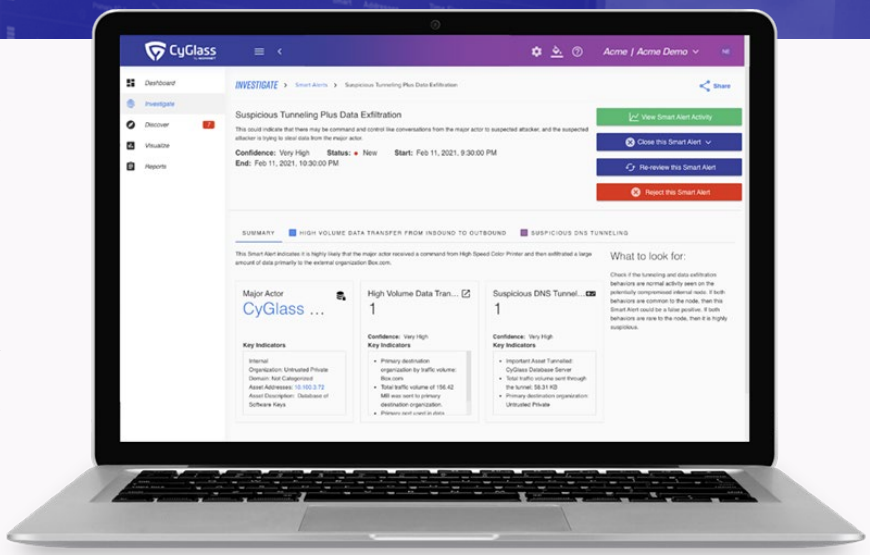
CyGlass eXtended Cloud Security

Network and Cloud Security Made Simple



CyGlass eXtended Cloud Security is a Cloud platform that delivers a cost effective detection, response, and compliance solution for cyber security teams that have distributed, hybrid networks but do not have the resources to operate a SIEM or 24X7 security operations center.

Utilizing AI driven security policies, CyGlass eXtended Cloud Security reduces the massive volume of network and Cloud traffic into prioritized smart alerts, investigative views, and compliance reports. CyGlass enables any security team to **See Risks Across Their Network, Stop Threats, and Prove Compliance.**

See Risks Across Your Hybrid Network

Network & Cloud Operations Managers gain visibility to abnormal risky activities that occur across remote workers, on-premise, and Cloud environments. Managers can quickly identify unprotected or rogue devices, threats to IoT devices, misconfigured ports, risky traffic, and backup system failures without overburdening IT teams.

Stop Threats

CyGlass enables automated continuous monitoring for threats across networks, cloud, and VPNs. Utilizing a unique combination of cyber TTP policies, threat intelligence and AI, CyGlass delivers a short, prioritized list of smart alerts and investigative reports. Cyber and IT managers utilize CyGlass to quickly investigate and remediate cyber-attacks 24x7.

Prove Compliance

Prebuilt, automated compliance policies and reports are activated with the push of a button using CyGlass Goals and Objectives. Prove compliance through prebuilt reporting including control effectiveness, SLA tracking, and compliance objective metrics. Compliance policies include multiple aggregated rules, AI models, control objectives, and assurance reports for ISO 27001, NIST 800-53, Cyber Essentials, FFIEC, NIAC, CMMC, and more.

Built for Small IT Security Teams

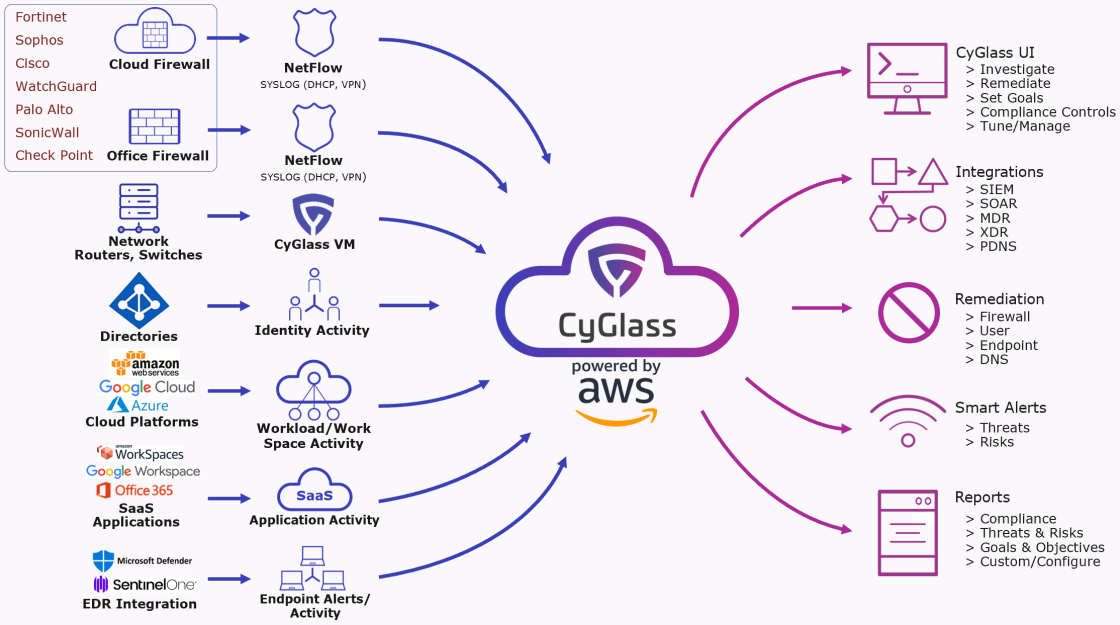
CyGlass' unique Cloud-native delivery model provides enterprise class cyber security at a fraction of the cost of traditional NDR or SIEM tools. Deployed in just hours, CyGlass is designed for operational success in any environment, delivering:

- No IT overhead: 100% SaaS solution with no appliance, no agents, no new on-premises software or hardware, utilizing existing firewalls, VPNs, AD, and SaaS applications.
- Increasing ROI: Policy by objective with advanced AI and automation reduce overhead, increase effectiveness and use case coverage over time. CyGlass replaces legacy network traffic analyzers, NDR, marginal SIEM deployments, and legacy DLP tools.
- Low TCO: Advanced AI drives automation, reduce overhead and manpower requirements while increasing operational effectiveness and threat detection from devices anywhere, anytime. CyGlass operates at 1/3 of the cost of traditional security tools.

CyGlass Threat Coverage

- Ransomware
- Supply Chain
- VPN Threats
- Command & Control C2
- Man-in-the-Middle
- Unauthorized web & DNS activities
- Masqueraders (tunneling)
- Credential compromise
- Rogue behaviors
- Insider threats
- Lateral movement
- Data exfiltration

CyGlass Cloud Architecture



CyGlass collects NetFlow, Syslog, VPC, and other logs via a data collector layer which ingests data, parses it into relevant formats, and transmits it to our Cloud AI engine via a secure SSH channel.

The CyGlass AI engine utilizes unsupervised machine learning in a big data architecture with integrated policy engine. The policy engine harmonizes AI models and enables the fast deployment of operational, threat, and compliance objectives and controls which drive the relevant analytics.

Outputs include data flows to security tools, smart alerts, reports, and an investigative UI.

Continuous Visibility, Automated Compliance Reporting

CyGlass objective-driven alerts and reports enable security teams to focus on what is important, why, and what remediation action is needed.

Prebuilt policy objectives for leading regulatory and IT control frameworks enable teams to activate and report on controls with a click of a button. Control models include:

- ISO 27001
- NIST 800-53
- Cyber Essentials
- NIST 171/DFARS
- FFIEC
- NIAC,
- CMMC
- MPAA

Control models are easily configured and new models added. Security teams save both time and money actionable, easy to understand automated reports.