

CyGlass Network Defense as a Service

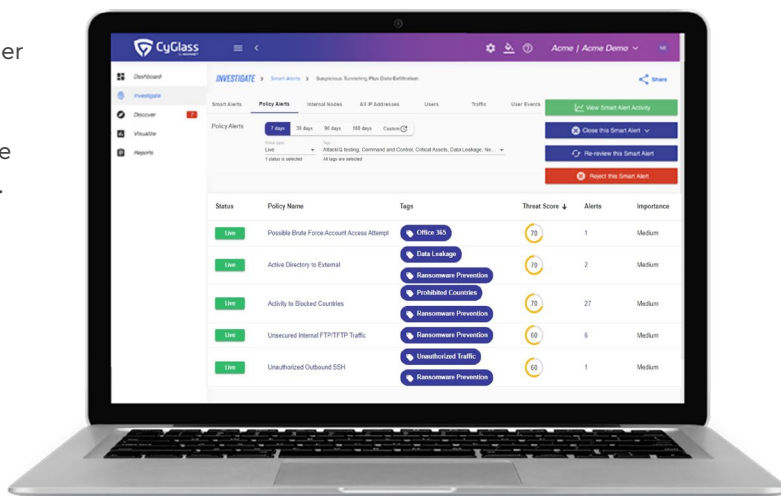


EMPOWER YOUR FIREWALL WITH AI RISK AND THREAT DETECTION

Adding CyGlass Network Defense as a Service to your on-premise or cloud firewall transforms this critical border guard into an AI driven risk and threat detection and remediation machine. The CyGlass NDaaS firewall add-on connects in under 30 minutes, requires no on-premise hardware, and costs as low as \$4.99 per user per month.

Together, your firewall plus CyGlass NDaaS allows your IT team to see risks across your network, detect cyberattacks like ransomware, and automatically remediate attacks 24X7 without the need for a SIEM.

CyGlass NDaaS utilizes advanced AI combined with a security policy engine to reduce the alerts and false positives down to a truly manageable amount of smart alerts. On average, a 30,000 user deployment will see 3 smart alerts per day.



See Risk Across Your Network

Network operations managers gain visibility to abnormal risky network activities including rogue devices, unprotected devices, threats to IoT devices and backup system failures without overburdening your IT team.

Detect Threats

CyGlass NDaaS enables automated continuous monitoring for threats across networks, cloud, and VPNs. Utilizing a unique combination of artificial intelligence, cyber TTP policies, and threat intelligence, CyGlass delivers a short, prioritized list of critical alerts, network risk scorecards with goals and objectives, and threat reports for cyber threats including ransomware.

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

24X7 Automated Remediation

CyGlass NDaaS enables automated continuous remediation. Remediation policies are built within the NDaaS policy engine and as high risk threats are detected, firewall integration automatically updates firewall blacklist or blocks IP addresses. Use case coverage include automated non-working hour remediation.

Built for Small IT & Security Teams

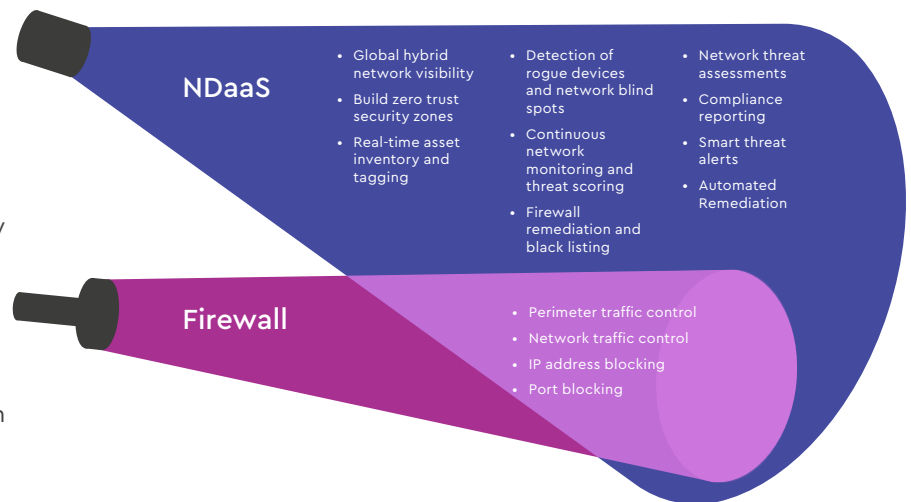
CyGlass' unique NDaaS delivery model provides enterprise class cyber security at a fraction of the cost and overhead of traditional NDR tools. CyGlass delivers:

- 100% cloud-native SaaS solution with no appliance, no agents, no new on-premises software or hardware, utilizing existing firewalls.
- Network Risk Scorecard reporting based on security goals and objectives allows teams to set risk reduction goals and report on progress.
- Low operational costs through reduction of manpower offset by automation and simplicity of operations. Elimination of system maintenance and management costs through software as a service.

Firewall + NDaaS = Enhance Visibility

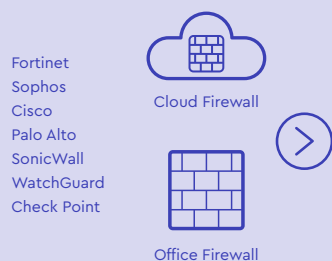
For most companies, firewalls and endpoint protection remain critical components of their cybersecurity defenses. But, as cyber attackers have become more sophisticated, these tools have lost effectiveness. Modern ransomware attacks, for example, often bypass firewall and endpoint tools. At the same time, AI based network monitoring and threat detection has only been deployed in larger organizations. Costly and complex, AI based NDR tools are rarely deployed by medium and small organizations leaving these companies vulnerable to attack.

CyGlass NDaaS plugs into your firewall in less than 30 minutes, creating a powerful, SaaS network defense and monitoring solution in just minutes.

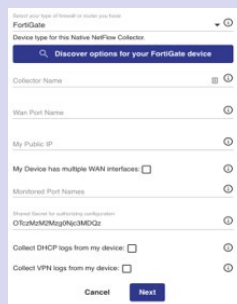


A Simple Affordable Firewall Add-on

Plugs into most leading Firewalls



Point-and-Click Installation



Discover options for your FortiGate device

Collector Name

WAN Port Name

My Public IP

My Device has multiple WAN interfaces

Monitored Port Names

Default Server for authenticating configuration: `0F0C0A0M0A0P0A0M0G0A`

Collect DHCP logs from my device

Collect VPN logs from my device

Cancel Next

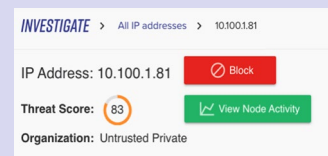
Firewall Log Ingestion

NetFlow

DHCP

SSL VPN

Automated Remediation

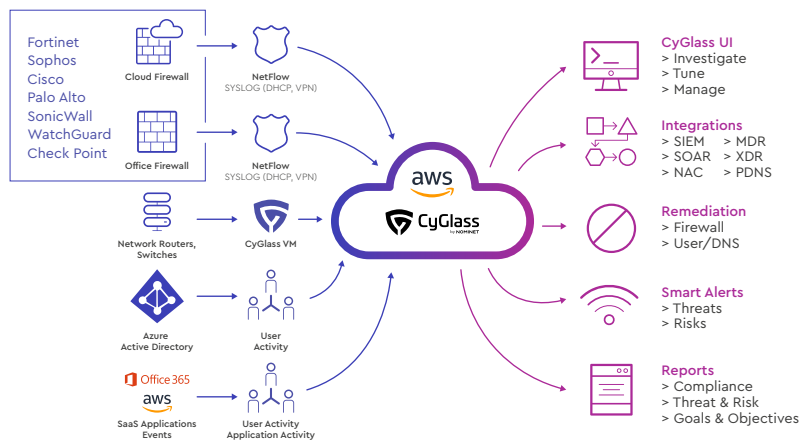


INVESTIGATE > All IP addresses > 10.100.1.81

IP Address: 10.100.1.81 [Block]

Threat Score: 83 [View Node Activity]

Organization: Untrusted Private



CyGlass NDaaS Delivery Architecture

CyGlass collects NetFlow, Syslog, and other logs via a data collector layer which ingests data, parses it into relevant formats, and transmits it to the 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 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, reporting, and an investigative UI.