



CyGlass
a WatchGuard brand

FIREWALL + CYGLASS =

TURBO CHARGE POWER

*TURN YOUR FIREWALL INTO
AN AI POWERED THREAT
DETECTION MACHINE*

Gartner: “Through 2025, policy misconfigurations, not firewall flaws, will remain the cause of 99% of firewall breaches and bypasses.” **

Firewalls are one of the core cybersecurity defensive tools with 95% of IT pros regarding their deployed firewalls as critical infrastructure.* As critical as they are, firewalls are dependent on the rules that activate their defensive capabilities and they provide a limited, but very important set of defensive capabilities, but must be complimented with other cybersecurity tools to truly protect an organization.

95%
**OF IT PROS VIEW
 FIREWALLS AS CRITICAL
 INFRASTRUCTURE.**

Complexity - The Enemy of Cyber Defense

As the Gartner quote calls out – rule configuration is the major cause of firewall failures during an attack. It is not surprising when one realizes that even a small company can run more than 10 firewalls, a mid-size company more than 50 and large company numbers running from 100 to over 1000. Often, the firewalls are from different vendors with different user interfaces and rules engines. To make matters worse, the rapid increase in multiple hybrid cloud deployments only exacerbates the difficulty of managing firewall rules in terms of both complexity and number of rules.

The challenge, as rules are not properly designed, or not kept up, due to the policy enforcement nature of firewalls, gaps open up that are quickly and easily exploited by attackers. The problem for IT and security teams – understanding what risks are created by weaknesses or failures in firewall rules and what rules need to be fixed or updated.

What's Really Wrong With Firewalls?

The difficulties respondents had with their firewalls ranged from deployment to obtaining budgets, implementing changes and verifying them. Here's a look at how they described these challenges.



Initial deployment and tuning

67% say initial deployment and tuning of firewalls is extremely to somewhat challenging



Implementing changes

67% say implementing changes in firewalls is extremely to somewhat challenging



Verifying changes

61% say verifying changes within firewalls is extremely to somewhat challenging

* <https://www.eweek.com/security/94-percent-of-organizations-see-firewalls-as-critical-infrastructure/>

**Control Network Security Complexity, Inefficiencies and Security Failures by Minimizing Firewall Diversity. Published 27 March 2020 – ID G00466951, By Adam Hills, Rajpreet Kaur
 Graph from <https://www.illumio.com>

Firewalls

Powerful

Firewalls play a limited but critical defensive role controlling internet access into your organization. Firewalls provide multiple security features to help protect an organizations network including:

- Packet Inspection to understand the details of each inbound communications protecting against unauthorized traffic and controlling legitimate traffic. The firewall also captures critical information and counts of connections, total connection rates, amount of data received and sent, and where communications are flowing to and from.
- Authentication Proxy, enforce granular per-user authentication and access control policies based on the risk and sensitivity of the website, sub-net or devices being accessed.
- Application Mapping, Define TCP or UDP ports numbers to specific network services or applications and control any non-standard Application Layer protocols data flows.
- Access Control where policies are used to control or block access between outside websites or machines and the internal network and control access by users or machines inside the network or to cloud services.
- Zone Trust Policy definition and enforcement which defines authentication and access control policies to specific subnets and devices on the network.
- Intrusion Prevention, signature based detection to identify and block known external threats.



Limited

Even with all these powerful and valuable capabilities, Firewalls are not a panacea, not even for network security. They have some significant shortfalls, first and foremost being the complexity of policies and the risk created when policies are poorly defined or become out of date. Other weaknesses include:

- Inability to defend from an attack within, including a social engineering based attack when an employee unknowingly granted access to an adversary letting on malware or an insider attack.
- Inability to see or stops traffic that does not pass through the Firewall as the traffic moves into or around the network.
- Firewall Rule permitted traffic that is malicious, commonly email traffic where rules are permissive. Firewalls cannot detect embedded malware in the traffic or detect that malware as it operates inside the network.
- Lack of AI and the ability to monitor network traffic for anomalies, risks, or unknown to signature based threats. Firewalls primarily enforce policies, they do not watch the network or the devices on the network to look for risk or threats.



FIREWALL + CYGLASS

- EMPOWERING YOUR FIREWALL, PROTECTING YOUR NETWORK

30 MINUTES

CyGlass Network Defense is a powerful, inexpensive and easy to operation addon to your WatchGuard on-premise or cloud firewall.

CyGlass transforms your firewalls into AI driven, monitoring, risk, threat detection and remediation machines. A true addon, cloud-native solution, CyGlass connects to most firewalls in under 30 minutes, and requires no on-premise hardware.

Overcoming Firewall Limitations enhancing Firewall Powers

CyGlass turbo charges your firewall with advanced AI combined with a security policy engine and threat intelligence to see risks across your network, detect cyberattacks like ransomware, and automatically remediate attacks 24X7. CyGlass AI utilizes rich Firewall captured Netflow data to deliver:

- Rich visibility to network devices including unknown and rogue devices.
- Firewall policy and network risk scoring reports including traffic to risky/improper sites or locations, risky activity on unsecured ports, risky/improper endpoint NetBIOS traffic, and many more.
- 24X7 continuous cyber threat monitoring across networks, cloud, and VPNs. Utilizing artificial intelligence, cyber TTP policies, and threat intelligence, CyGlass delivers a short, prioritized list of critical cyber threat alerts and supports firewall policy updates and remediation.
- Threat visibility inside permitted traffic and in outbound traffic including coverage for reconnaissance, command and control, Man-in-the-Middle, Unauthorized web & DNS activities, masqueraders (tunneling), insider threats, lateral movement, and data staging and exfiltration.



Threat Assessment for CyGlass, Inc.

Report generated on May 21, 2019

Analysis based on 90 days of retained data from February 20, 2019 to May 21, 2019

Your threat score is

C 725

Target* threat score is

B 767

* Based on threat scores from CyGlass users

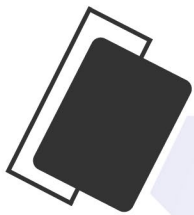
Continued use of CyGlass is aimed at improving your threat score and securing your critical IT assets. CyGlass identifies, detects, and responds to threats to your network without requiring any additional hardware, software or people. The CyGlass Cloud continuously analyzes the billions of conversations happening on your network, learns what is normal, and alerts when suspicious behaviors that risk the security of your critical IT assets are detected.





Firewall + CYGLASS

- EMPOWERING YOUR FIREWALL, PROTECTING YOUR NETWORK



CYGLASS



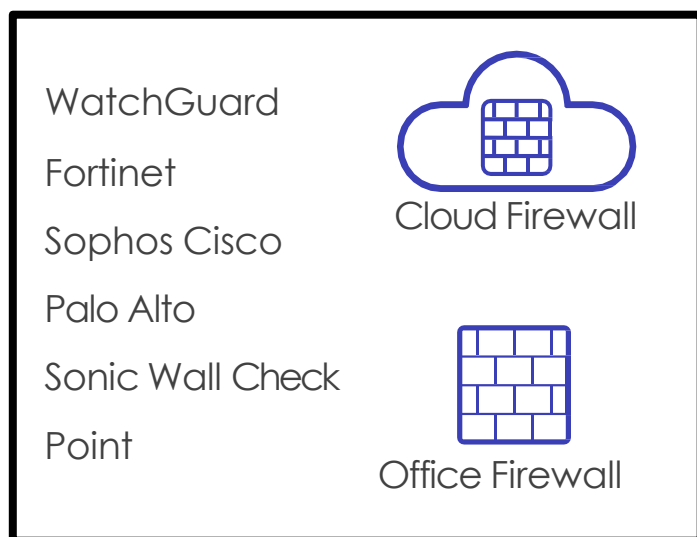
Firewall

- Global hybrid network visibility
- Real-time asset inventory and tagging
- Detection of rogue devices and network blind spots
- Continuous network monitoring and threat scoring
- Network threat detection and response
- Firewall and Azure remediation and black listing
- Priority threat and risk smart threat alerts
- Scorecard and compliance reporting
- Zero trust security zones

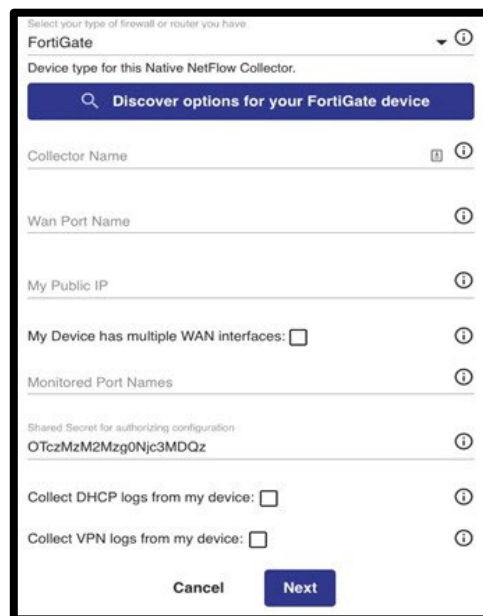
- Perimeter traffic control
- Network traffic control
- IP address blocking
- Port blocking

Rapid Time to Value

Plugs into most leading Firewalls



Point-and-Click Installation



Select your type of firewall or router you have
FortiGate

Device type for this Native NetFlow Collector.

Discover options for your FortiGate device

Collector Name

Wan Port Name

My Public IP

My Device has multiple WAN interfaces: ☐

Monitored Port Names

Shared Secret for authorizing configuration:
OTczMzMzMzg0Njc3MDQz

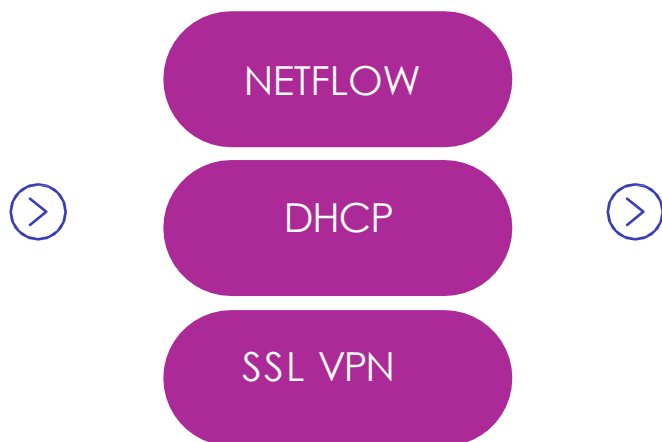
Collect DHCP logs from my device: ☐

Collect VPN logs from my device: ☐

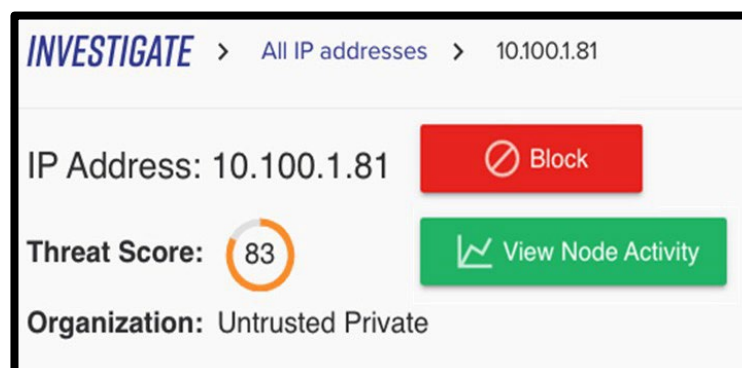
Cancel Next

The screenshot shows a web-based configuration interface for a FortiGate device. It includes fields for Collector Name, Wan Port Name, My Public IP, and a checkbox for multiple WAN interfaces. There are also fields for Monitored Port Names and a Shared Secret. At the bottom, there are checkboxes for collecting DHCP and VPN logs, and 'Cancel' and 'Next' buttons.

Firewall Log Ingestion



Automated Remediation



CyGlass Network Defense

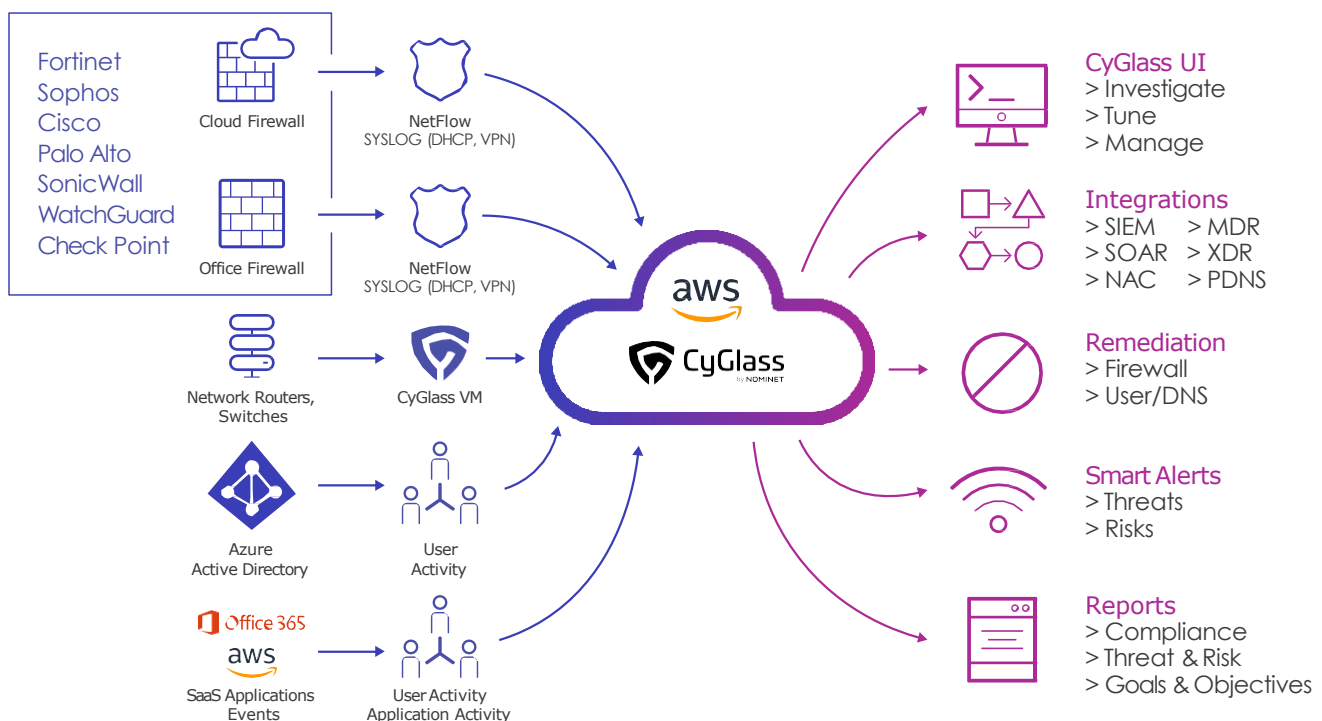
CyGlass collects NetFlow, Syslog, and other logs via a data collector layer which ingests data, parses it into relevant formats, and transmits it to the CyGlass AI engine via a secure SSH channel.

The AI engine utilizes unsupervised machine learning in a big data architecture with integrated policy engine. Collecting millions of data flows, CyGlass AI defines and builds normal working models for thousands of different device, application, user, and communications parameters.

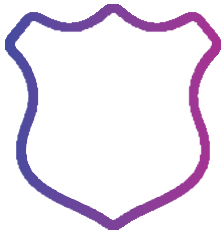
The policy engine enables the fast deployment of operational, threat, and compliance objectives and controls which drive the relevant analytics. CyGlass's unique AI/policy engine integration reduces alerts and false positives down to a truly manageable amount of smart alerts. On average, a 30,000 user deployment will see 3 smart alerts per day. Outputs include data flows to security tools, smart alerts, reporting, and an investigative UI.

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



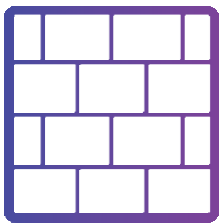
Empowering Small & Medium Organizations



CyGlass is specifically designed to be successfully deployed and operated by the resource limited IT and security teams of small and medium enterprises and organizations.



CyGlass is a cloud-native solution that removes IT overhead by requiring no on-premise hardware, software or agents.



It works with your organizations existing firewalls, VPNs and SaaS applications including AWS, Microsoft Azure and M365.



As an easy to use, SaaS based solution it offers a low total cost of ownership with constantly increasing operations effectiveness as backend patching, system management, policy updates, new report delivery, and new AI models are all included.



As a highly effective cyber defense tool, CyGlass offers a strongly positive ROI, replacing costly legacy systems like NDR, NTA, network DLP, and can be deployed as significantly less expensive SIEM alternative.

Best SME Security Solution



Finalist Best Behavior Analytics/
Enterprise Threat Detection

