Network Monitoring and Defense

THE SECRET WEAPON THE BAD GUYS WANT YOU TO IGNORE

Understanding and defending your network has never been easy. Massive amounts of traffic, BYOD policies, growing deployments of OT/IoT devices, and the rapid move to hybrid cloud environments have all made network visibility and defense a daunting task. The issues have lead IT and security practitioners at all but the largest organizations to focus on deploying firewall and endpoint defensive tools, actions that have created opportunities for the adversaries.

It used to be that hiding in the massive amounts of network traffic was easy, as no human could accurately watch and understand the data. The advent of artificial intelligence (AI) has changed the nature of monitoring network traffic creating new opportunities for effective defense.

Artificial Intelligence & the Cloud

A new generation of AI driven network detection and response (NDR) tools hit the market about four years ago, bringing this technology to large, well-resourced organizations. Complex, expensive, and requiring extra manpower to operate, these tools were never designed for medium and small enterprises.

Within the last few years, the advent of Software as a Service (SaaS), has enabled security vendors like CyGlass to take this once complex capability and deliver it securely from the cloud to organizations of all sizes. The advantages of a SaaS delivered solution includes:

- No need to deploy and manage on premise appliances, agents, hardware or software
- No need to increase workload or hire hard to find resources as required activities are handled in the service or through automation.
- Lower total cost of ownership as solution upgrades, new features and capabilities are includes in the service.

Why Network Defense is Foundational

It goes without saying that your organization's operations, production and services rely on your network, but that also means that for adversaries, your network is critical to their attack success. Regardless of if the attack is ransomware, data theft, denial or destruction of services, or financial theft, the deeper the adversary penetrates your network, the more successful the attack will be. The opposite is also true with network defense.

If the attacker can only penetrate a single laptop, server or workstation and move no further without detection, the chances of accessing critical data or services, opening backdoors or leaving hidden malware drop to zero. The basic fact is that network activity make up a majority of the MITRE ATT&CK® stages. The adversaries rely on your network for their success as much as you do and therefore defending it is foundational.

NETWORK RELATED MITRE ATT&CK® stages

RECON → WEAPONIZE → DELIVER → EXPLOIT → CONTROL → EXECUTE → MAINTAIN

PRE-ATTACK

- Technical Information Gathering
- Weakness Identification
- Adversary OpSec
- Test Capabilities

ATTACK

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control

Understand Network Normal, Surface Risks

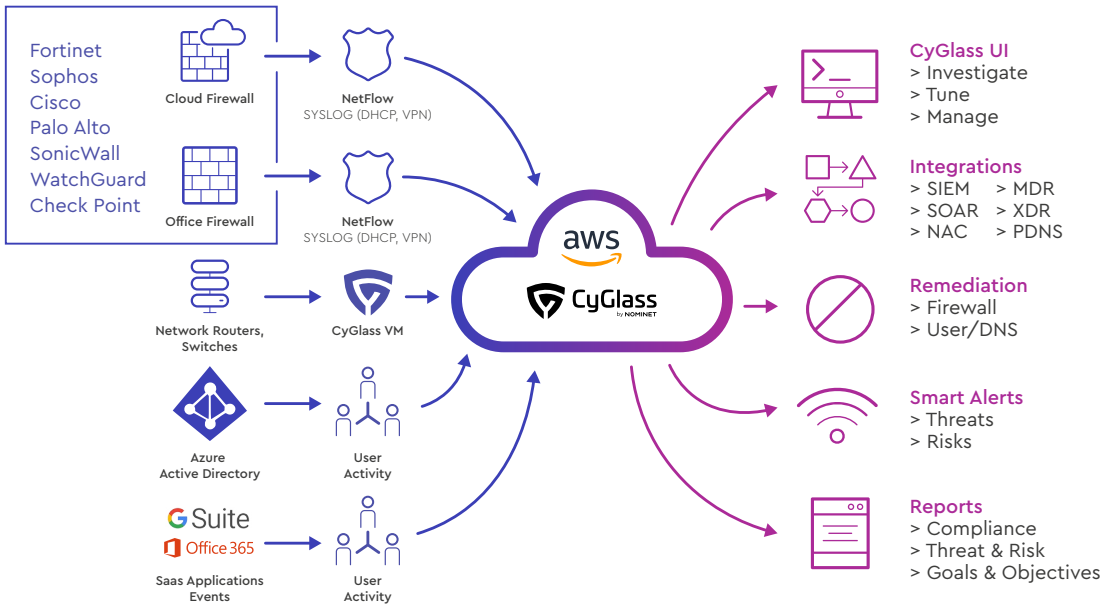
To defend the network, IT and security managers must first understand what devices are on the network and where the organization's most valuable data resides on the network. With a SaaS based network defense system, IT gains visibility to abnormal risky network activities including coverage of remote workers and hybrid cloud environments. Managers can quickly identify rogue devices, unprotected devices, risks to IoT devices and backup system failures without overburdening the IT team.

Threat Detection and Remediation

SaaS network defense enables automated continuous monitoring for threats across networks, cloud, and VPNs. Utilizing a unique combination of cyber attack tactics, techniques and procedures (TTP) policies, threat intelligence and layered AI, CyGlass delivers a short, prioritized list of smart alerts and investigation reports covering the greatest and immediate threats facing the organization. This 24X7 threat detection includes multiple paths for automated remediation to quickly contain infected systems and prevent further spread. Malware eradication must be complete and the network monitored for any potential reattack, because if the adversary maintains even a small foothold, reinfection will send the security team back to square one. Accurate network visibility and an understanding of "normal business," AI driven by threat intelligence and TTP driven policies, and 24X7 monitoring are critical to effective defense, and all are core capabilities of SaaS network defense.

Compliance is part of network defense

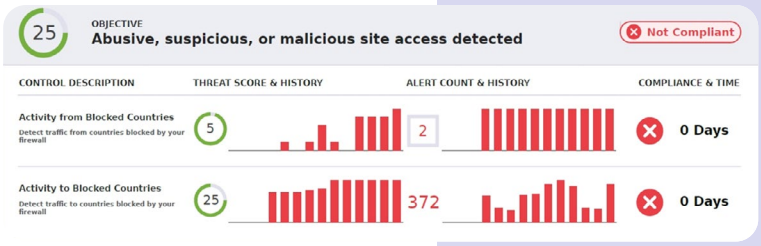
From NIST standards like CSF, 800–53, and 800–171(DFARS/CMMC) to regulatory frameworks like HIPAA, FFIEC, PSS, and NIAC, all regulatory standards and frameworks include significant network monitoring, asset discovery and threat protection requirements. As a small security team, adding additional headcount or software tools is not an option. The "services" part of a network defense offering includes compliance reporting driven by policy frameworks for applicable regulations. Security teams will save both time and money with prebuilt compliance policies and reporting while easing the burden of proving effective processes.



Is SaaS network defense for me?

NDR tools have long been deployed by large enterprises with sophisticated security operations centers (SOCs). But companies that maintain a SOC, and the myriad of software tools and numbers of analysts required to run them are limited. Small and most mid-sized enterprises cannot afford them. SaaS network defense is a powerful alternative to resource constrained organizations. If the answer to any of these questions is true for your organization, then network defense delivered as a service is a real option.

1. My organization does not have a SOC, or the ability to run a 24X7 monitoring operation.
2. We do not have a SIEM deployed, or are challenged to properly or fully operate the SIEM we have deployed.
3. Our primary defensive tools are firewalls, VPNs, and endpoint protection.
4. My industry relies heavily on traditional or hybrid network for our business operations.



"Many mid-sized enterprises and organizations in manufacturing, healthcare, education, banking, state government, and local government have successfully deployed network defense as a service solutions with exceptional results."

No SIEM, No SOC, No Problem

For organizations with small IT security teams missing 24X7 automated network monitoring, asset discovery, threat detection, and response, CyGlass offers a cloud-based, AI-driven, lightweight, and easy-to-deployed Network Defense as a Service (NDaaS) offering that delivers all of these capabilities.

Our successful customers are the small and medium enterprises that struggle to find success with the vast array of complex and costly security tools. CyGlass focuses on simplicity and operational success, delivering an amazingly affordable and effective network defense solution.