CyGlass NDaaS | Network Defense as a Service

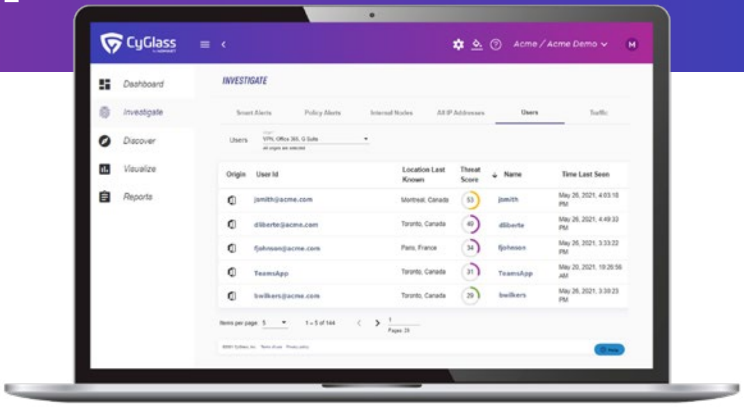
CyGlass by NOMINET

COST-EFFECTIVE HYBRID CLOUD DEFENSE

As traditional networks extend into public and private clouds, their fundamental definition changes as threat surfaces grow and new risks emerge.

CyGlass Network Defense as a Service (NDaaS) is a cost-effective network visibility, defense and compliance solution for cyber security teams with distributed, hybrid networks that lack the resources to operate 24X7 security operations centers.

The NDaaS platform learns and analyzes user and network behaviors wherever they emerge: the cloud, Active Directory, VPNs, firewalls, and network devices. It allows small teams to detect and respond to threats across on premise and cloud users, devices, and both cloud and network services. With CyGlass NDaaS, IT and security managers can see risk, stop threats, and prove compliance across their entire hybrid networks.



INVESTIGATE

Users: VPN, Office 365, G Suite — All origins are selected

Origin	User Id	Location Last Known	Threat Score	Name	Time Last Seen
	jsmith@acme.com	Montreal, Canada	53	jsmith	May 26, 2021, 4:03:18 PM
	dliberte@acme.com	Toronto, Canada	49	dliberte	May 26, 2021, 4:49:33 PM
	fjohnson@acme.com	Paris, France	34	fjohnson	May 26, 2021, 3:33:22 PM
	TeamsApp	Toronto, Canada	31	TeamsApp	May 20, 2021, 10:26:56 AM
	bwilkers@acme.com	Toronto, Canada	29	bwilkers	May 26, 2021, 3:30:23 PM

Items per page: 5 — 1 – 5 of 144 — 1 — Pages: 29

©2021 CyGlass, Inc. Terms of use Privacy policy — Help

CyGlass uniquely correlates user, IP address, event, and risk level for network and cloud threats

Combining AI, machine learning, threat intelligence and layered security policies, CyGlass NDaaS reduces the massive volume of network traffic into easy to understand risk-based smart alerts, investigative views, and threat and compliance reports.

NETWORK DEVICE VISIBILITY

Servers, laptops, IoT, Windows Hosts

USER VISIBILITY

Active Directory (AD), cloud AD-Azure, VPN

SERVICES VISIBILITY

Network, remote, and cloud services (O365, AWS, SMB, DHCP, DNS, RDP, FTP, SSH)

NETWORK DEFENSE AS A SERVICE

INVENTORIES (USERS, DEVICES, NETWORK) — THREAT DETAILS — ALERTS — ACTIONS — REPORTS

FACILITY: Factory, Hospital, Branch

CLOUD: Office 365, AWS

OFFICE: Printer, VPN, Guest Wifi

DATA CENTER: Server, Legacy App

ATTACK SURFACE

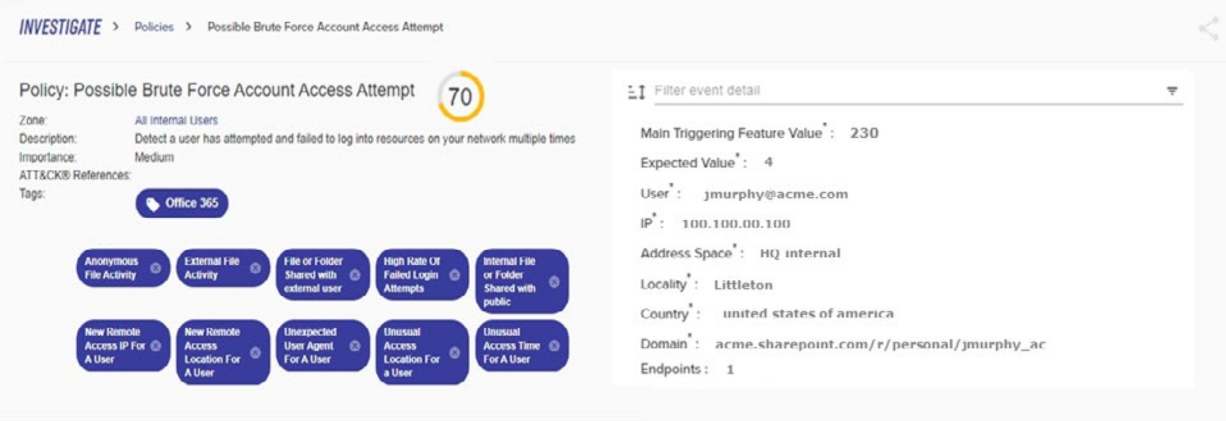
Malware — Hackers — Ransomware — Crypto Mining — APTs — Supply Chain Attack

CYGLASS THREAT COVERAGE

- Ransomware
- Command & Control C2
- Man-in-the-Middle
- Account takeover
- AD Azure Account Compromise
- Unauthorized web & DNS activities
- Masqueraders (tunneling)
- Credential compromise
- Rogue behaviors
- Insider threats
- Lateral movement
- Data exfiltration
- O365 data theft
- AWS services compromise

CyGlass is the only network defense as a service that is affordable, easy to operate and cover both on premise network and cloud environments.

NDaaS Cost-Effectively Correlates Threat, IP and User Account



INVESTIGATE > Policies > Possible Brute Force Account Access Attempt

Policy: Possible Brute Force Account Access Attempt 70

Zone: All Internal Users
Description: Detect a user has attempted and failed to log into resources on your network multiple times
Importance: Medium
ATT&CK® References:
Tags: Office 365

Anonymous File Activity · External File Activity · File or Folder Shared with external user · High Rate Of Failed Login Attempts · Internal File or Folder Shared with public · New Remote Access IP For A User · New Remote Access Location For A User · Unexpected User Agent For A User · Unusual Access Location For a User · Unusual Access Time For A User

Main Triggering Feature Value*: 230
Expected Value*: 4
User*: jmurphy@acme.com
IP*: 100.100.00.100
Address Space*: HQ internal
Locality*: Littleton
Country*: united states of america
Domain*: acme.sharepoint.com/r/personal/jmurphy_ac
Endpoints: 1

User event models include anomalous authentication, access, file usage, and file sharing in O365 environments

As a SaaS solution, CyGlass delivers enterprise-class capabilities such as the ability to correlate threat and risk level with user account and IP address for a fraction of the cost. The result is IT and security managers can quickly assess a threat, understand threat context and the devices and users involved, and effectively remediate an attack before damage is done. Remediation can include automatic blocking of IP addresses via firewall integration or user account blocking via AD integration.

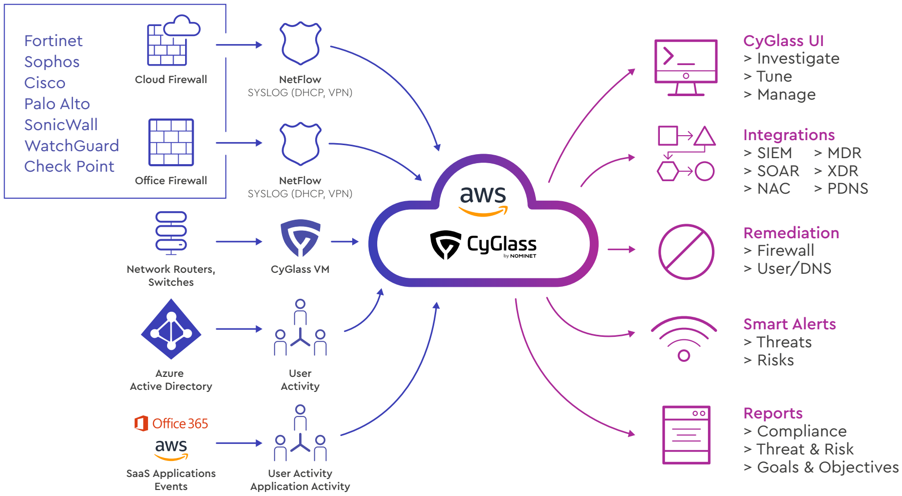
WHAT IS NEW

CyGlass NDaaS risk and threat coverage now includes AD/AD-Azure users and O365 applications and AWS logs. Defenders can identify anomalous activities by device accessing and using AWS services, and correlate risk and threats across users, devices, and services.

CyGlass NDaaS Delivery Architecture: Complete Hybrid Cloud Visibility

CyGlass collects NetFlow, Syslog, AD Logs, and more via a data collector layer which ingests, parses, enriches, and correlates data into relevant formats and transmits it to the CyGlass AI engine via a secure SSH channel.

The CyGlass AI engine operates in an AWS Cloud and uses a mix of unsupervised machine learning and self-learning AI in a big data architecture complete with an integrated policy engine. This enables fast deployment of operational, threat, and compliance objectives and controls, which drive relevant analytics. AI models learn from the continuous flow of data mixed with human feedback.



Fortinet
Sophos
Cisco
Palo Alto
SonicWall
WatchGuard
Check Point

Cloud Firewall
Office Firewall
NetFlow SYSLOG (DHCP, VPN)
NetFlow SYSLOG (DHCP, VPN)
Network Routers, Switches
CyGlass VM
Azure Active Directory
User Activity
Office 365
aws
SaaS Applications Events
User Activity Application Activity

aws
CyGlass by NOMINET

CyGlass UI
> Investigate
> Tune
> Manage

Integrations
> SIEM > MDR
> SOAR > XDR
> NAC > PDNS

Remediation
> Firewall
> User/DNS

Smart Alerts
> Threats
> Risks

Reports
> Compliance
> Threat & Risk
> Goals & Objectives

Outputs include data flows to security tools and MDR services, smart alerts, an investigative UI and complete set of automatically built threat, network visibility and compliance reports. Automated remediation is delivered through IP address identification via firewall integration and user account identification integration via Active Directory.