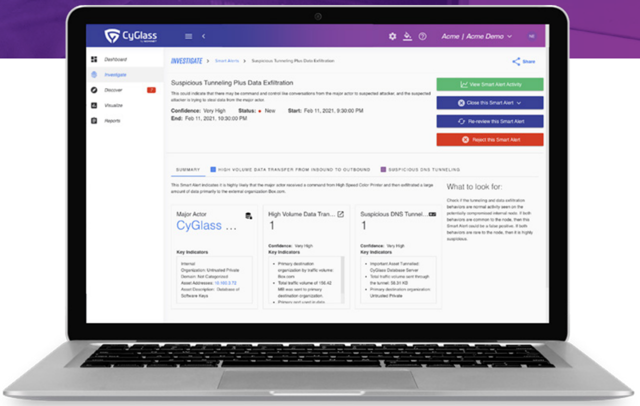
CyGlass
by NOMINET

Network Defense as a Service

NETWORK SECURITY MADE SIMPLE


CyGlass
Acme | Acme Demo
Dashboard
Investigate
Discover
Visualize
Reports
INVESTIGATE > Smart Alerts > Suspicious Tunneling Plus Data Exfiltration
Share
View Smart Alert Activity
Close this Smart Alert
Re-review this Smart Alert
Reject this Smart Alert
SUMMARY
HIGH VOLUME DATA TRANSFER FROM INBOUND TO OUTBOUND
SUSPICIOUS DNS TUNNELING

Suspicious Tunneling Plus Data Exfiltration

This could indicate that there may be command and control like conversations from the major actor to suspected attacker, and the suspected attacker is trying to steal data from the major actor.

Confidence: Very High Status: ● New Start: Feb 11, 2021, 9:30:00 PM
End: Feb 11, 2021, 10:30:00 PM

This Smart Alert indicates it is highly likely that the major actor received a command from High Speed Color Printer and then exfiltrated a large amount of data primarily to the external organization Box.com.

What to look for:

Check if the tunneling and data exfiltration behaviors are normal activity seen on the potentially compromised internal node. If both behaviors are common to the node, then this Smart Alert could be a false positive. If both behaviors are rare to the node, then it is highly suspicious.

Major Actor
CyGlass ...
Key Indicators
Internal
Organization: Untrusted Private
Domain: Not Categorized
Asset Addresses: 10.100.3.72
Asset Description: Database of Software Keys

High Volume Data Tran...
1
Confidence: Very High
Key Indicators
- Primary destination organization by traffic volume: Box.com
- Total traffic volume of 156.42 MB was sent to primary destination organization.
- Primary port used in data

Suspicious DNS Tunnel...
1
Confidence: Very High
Key Indicators
- Important Asset Tunneled: CyGlass Database Server
- Total traffic volume sent through the tunnel: 58.31 KB
- Primary destination organization: Untrusted Private

CyGlass Network Defense as a Service (NDaaS) delivers a cost effective network detection, response, and compliance solution for cyber security teams that have a distributed, hybrid network and do not have the resources to operate a SIEM or 24X7 security operations center.

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

See Risk Across Your Network

Network operations managers gain visibility to abnormal risky network activities including remote workers and hybrid cloud environments. Managers can quickly identify rogue devices, unprotected devices, threats to IoT devices and backup system failures without overburdening your IT team.

Stop Threats

CyGlass NDaaS enables automated continuous monitoring for threats across networks, cloud, and VPNs. Utilizing a unique combination of cyber TTP policies, threat intelligence and layered AI, CyGlass delivers a short, prioritized list of smart alerts and investigation reports covering network, AD, and cloud threat surfaces. Cyber security managers utilize NDaaS to surface and remediate cyber-attacks 24×7.

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

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 NIST, Cyber Essentials, FFIEC, NIAC, CMMC, and more.

Built for Small IT Security Teams

CyGlass' unique NDaaS delivery model provides enterprise class cyber security at a fraction of the cost of traditional NDR tools. 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, and 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. NDaaS replaces legacy network traffic analyzers and NDR, marginal SIEM deployments, and DLP tools

Low TCO: Objective policy packs and advanced AI drive automation, reduce overhead, reduce manpower requirements while increasing operational effectiveness and threat detection and response from devices anywhere, anytime.

CyGlass
by NOMINET

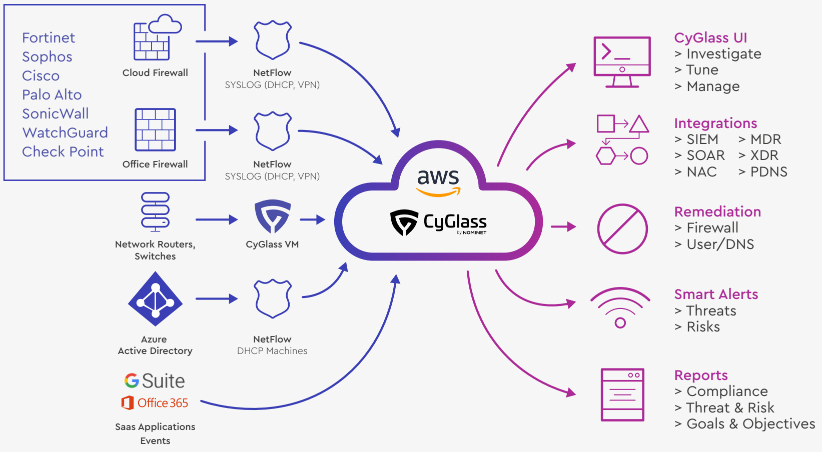
CyGlass NDaaS Delivery Architecture

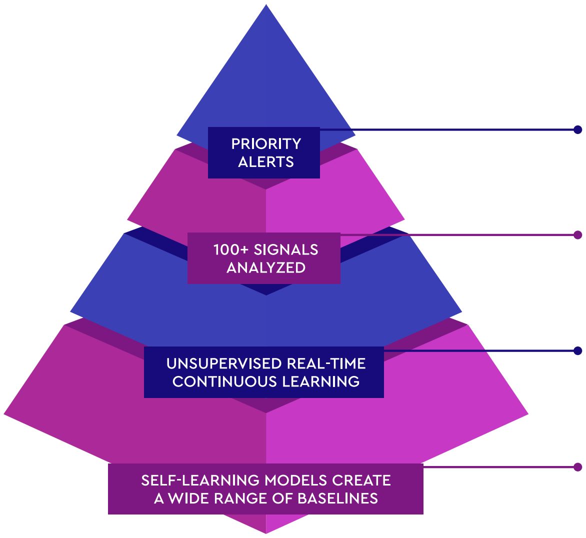
CyGlass collects NetFlow, Syslog, and other log data via a data collector layer which ingests data, parses it into relevant formats, and transmits it to the AI engine via a secure SSH channel.

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.




PRIORITY ALERTS
100+ SIGNALS ANALYZED
UNSUPERVISED REAL-TIME CONTINUOUS LEARNING
SELF-LEARNING MODELS CREATE A WIDE RANGE OF BASELINES

Focus on what is important with Layered AI

Very Few Prioritized Smart Alerts

A very small number of alerts that capture behavioral and event intelligence

Hundreds of Anomalous Behaviors

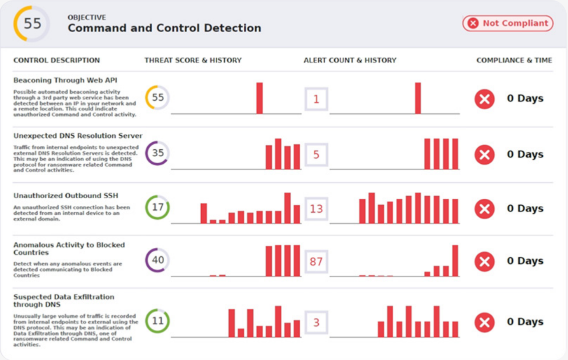
Scans (Lateral Movement), Rogue activities C2, Suspicious Tunneling, Exfiltration

Thousands of Anomalous Events

Asset Discovery, Connection rate, volume, source, target, port etc. anomalies

Millions of Network Conversations

Real-Time Netflow, Real-Time or offline PCAP



55 OBJECTIVE
Command and Control Detection
Not Compliant

CONTROL DESCRIPTION	THREAT SCORE & HISTORY	ALERT COUNT & HISTORY	COMPLIANCE & TIME
Beaconing Through Web API Possible automated beaconing activity through a 3rd party web service has been detected between an IP in your network and a remote location. This could indicate unauthorized Command and Control activity.	55	1	0 Days
Unexpected DNS Resolution Server Traffic from internal endpoints to unexpected external DNS Resolution Servers is detected. This may be an indication of using the DNS protocol for ransomware related Command and Control activities.	35	5	0 Days
Unauthorized Outbound SSH An unauthorized SSH connection has been detected from an internal device to an external domain.	17	13	0 Days
Anomalous Activity to Blocked Countries Detect when any anomalous events are detected communicating to Blocked Countries	40	87	0 Days
Suspected Data Exfiltration through DNS Unusually large volume of traffic is recorded from internal endpoints to external using the DNS protocol. This may be an indication of Data Exfiltration through DNS, one of ransomware related Command and Control activities.	11	3	0 Days

In depth visibility, automated reports

CyGlass objective driven alerts and reports enable security teams to focus on what is important, why, and what remediation action is needed to mitigate the risk or threat. Prebuilt policy objectives mean teams click a button to activate controls, AI models and reports based on organizational needs. Policies cover threats like ransomware defense, risks like rogue device identification, or regulations/frameworks like HIPAA or NIST. Security teams save both time and money with these easy to activate prebuilt policies.