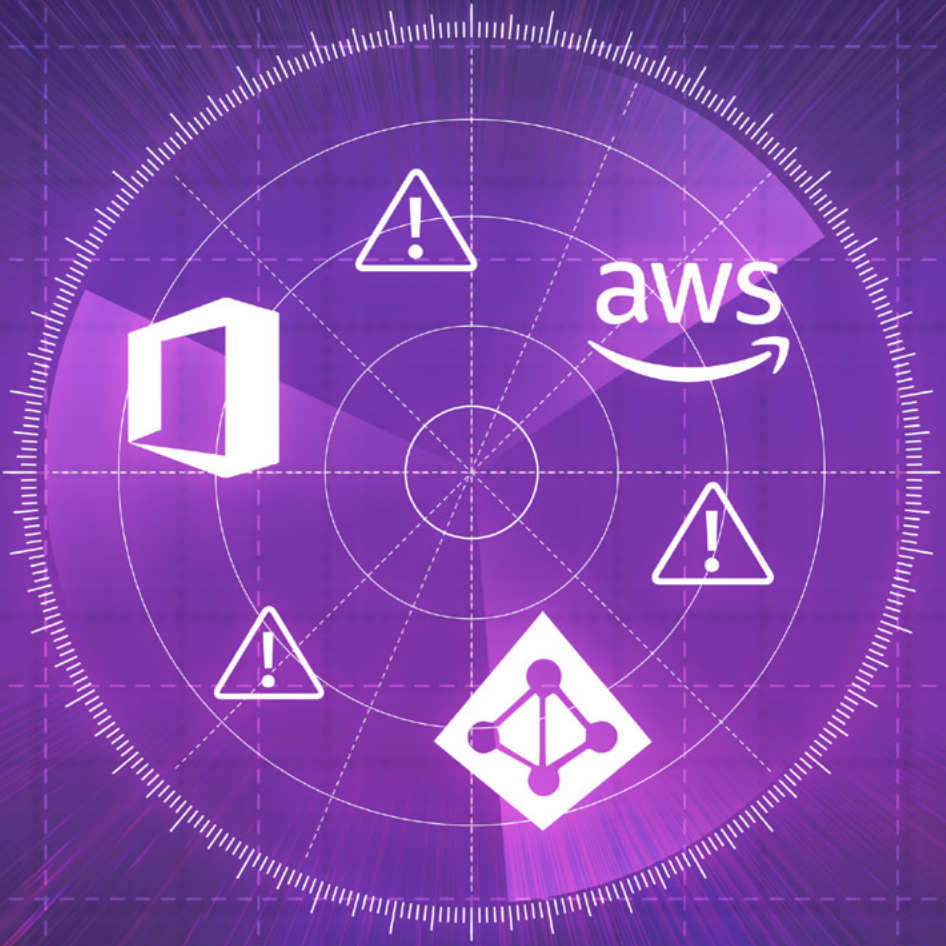
CyGlass
by NOMINET



Expanding Network Detection and Response to the Cloud

WITH CYGLASS NETWORK DEFENSE AS A SERVICE

HOW CYGLASS SECURES MICROSOFT AZURE, O365 AND AWS CLOUD ENVIRONMENTS

The Traditional Network Has Changed Forever

Move over traditional data centers. Step aside fixed office locations. The steady movement to the cloud by organizations of all sizes, accelerated by line of business's enthusiasm for quickly connecting to cloud services from vendors like Microsoft and Amazon, and rapidly hastened by COVID 19's historic shift to remote working, has changed the traditional network forever.

The dramatic move to the cloud has created risk and complexity that IT and security teams must understand and manage. Services like M365 and Azure AD that combine identity authentication and access to a growing variety of cloud-based applications and data storage pose even more significant challenges since they bypass existing defensive protections and access policies. It is true that M365 licenses offer additional security protections, but they are expensive, difficult to understand, and complex to manage.

In many cases, the rush to deploy cloud services to meet business needs has led to serious security gaps and vulnerabilities. In the worst cases, IT and security teams do not have any visibility into who or what has access to which services or how critical data is moving into, across, and out of the cloud.

Even with all the hype about the cloud, IT and security managers know these environments rarely stand alone. Most organizations still maintain traditional mission-critical networks, either because the cloud environments do not support the legacy systems they run on or the cost associated with moving to the cloud offers no advantages.

The defensive tools and processes needed to protect legacy systems remain critical to the organization. This fact adds even greater complexity since user identities must be managed both on premise and in the cloud. Access management also becomes more challenging because legacy applications run on the network while productivity, storage, and collaboration services run from the cloud with critical data often moving across each, typically with few good controls in place.

CyGlass by NOMINET

In this hybrid environment, cyber attackers can now compromise an application, service, or account inside the network or in the cloud. Worse, attackers can compromise an Azure administer account and gain easy access to sensitive data across the entire environment. The combination of legacy networks and cloud means IT and security managers need to monitor and manage:

- User authentication across hybrid (Azure AD, on premise) processes
- User access and privileged access to cloud applications and storage
- Data movement, especially sensitive data moving from inside the network to the cloud
- Cloud application usage and detection of rogue application installations
- Network activity, device IP address, and user account data from the cloud to the network
- Rogue devices that can access both network and cloud applications and services

These are no small undertakings. It is difficult merely to find a starting point from which to build a hybrid cloud security program. One security strategy finding favor with smaller teams that have limited resources involves building a program that starts with and expands from existing network-centric security tools and processes. The model supports cloud security migration strategies defined by the Cloud Security Alliance[1] and supports Zero Trust Strategies.[2] Perhaps most importantly, it helps mitigate the many dangers of cloud migration's so-called "lift and shift" strategy.[3]

Critical to building a network expansion security strategy is the use of vendor tools that support the change. Many legacy cybersecurity tools in the DLP, NTA, and NDR spaces cannot cover cloud migrations. But the good news is, many are capable. Cloud and Web Application Firewalls, Identity and Access Management, Strong Authentication, Secure Web Gateways, and a few best-in-class Network Detection and Response tools all support the leading cloud environments, including AWS and M365/Azure. CyGlass Network Defense as a Service is a best-in-class Network Detection and Response tool that supports cloud migration.

1 https://cloudsecurityalliance.org/blog/2020/02/18/cloud-security-challenges-in-2020
2 https://securityboulevard.com/2021/05/protecting-the-hybrid-cloud-with-zero-trust
3 https://www.itpro.co.uk/cloud/354568/why-lift-and-shift-is-an-outdated-approach

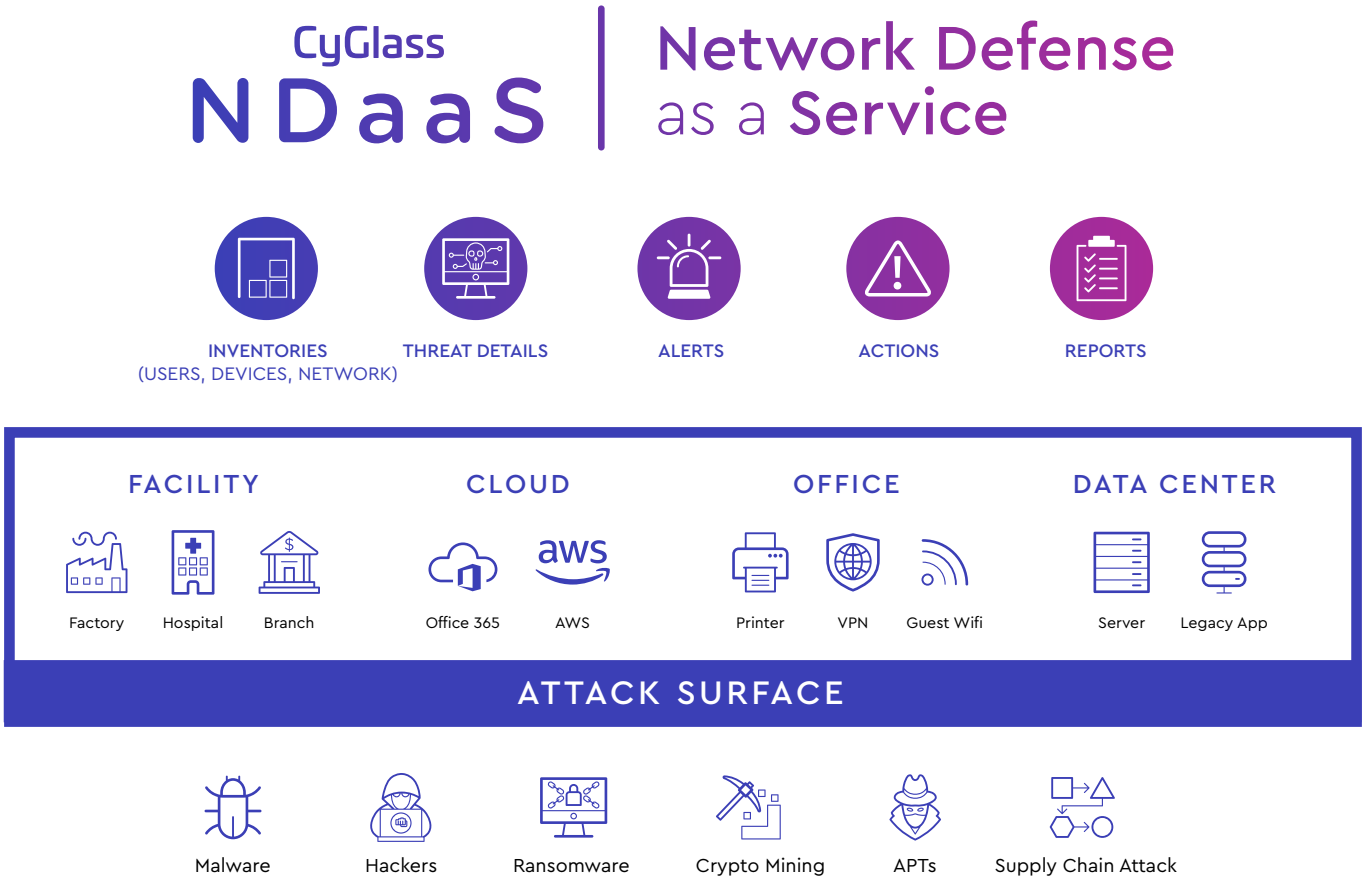


Fig. 1 The Cloud Native CyGlass NDaaS Platform covers a variety of cloud and traditional attack surfaces.

CyGlass NDaaS

CyGlass Network Defense as a Service (NDaaS) delivers cost-effective visibility, defense, and compliance solution for cybersecurity teams working to protect distributed hybrid cloud networks. CyGlass NDaaS is designed for smaller security teams that do not have the resources to operate a 24X7 security operations center.

The cloud-native NDaaS platform utilizes AI to learn and analyze user, service, and device behavior wherever they emerge: the Cloud, Active Directory, VPNs, firewalls, and network traffic. Advanced threat detection and response capabilities surface and remediate potential cyber-attacks across both on premise and among cloud users, devices, and services. With CyGlass NDaaS, IT and security managers can see risk, stop threats, and prove compliance, helping security protect their hybrid network environments.

CyGlass
by NOMINET

CyGlass Hybrid Cloud Coverage

- Users – VPN, Active Directory (AD), and cloud AD-Azure
- Devices – network devices (servers, laptops, IoT, Windows Hosts), Amazon, Azure, and vCenter/ESXi VMs
- Services – network, remote, and cloud services (O365, Azure, AWS, SMB, DHCP, DNS, RDP, FTP, SSH, SD-Wan)

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.

Powerful capabilities like correlating threat and risk level with user account and IP address enable IT and security managers to assess a threat quickly, understand its context, as well as the devices and users involved, and effectively remediate the attack before damage occurs. Security managers can automatically activate remediation policies, including; blocking IP addresses via firewall integration, DNS-based blocking, or user account blocking via AD integration.

How CyGlass works

CyGlass NDaaS addresses risk and threat coverage, including AD/AD-Azure users, O365 applications, and AWS services, by collecting relevant network and cloud logs. This data is sent to the CyGlass AI engine for correlation and analysis. Normal baselines of operations for users, devices, services, and applications are defined within the engine, and anomalous activity surfaced and analyzed.

Across literally billions of pieces of data, NDaaS can determine events that are anomalous or related to potential threats, surface them, and prioritize their risk level. Critically, the NDaaS platform can detect various risks and threats and identify the users and devices involved.

CyGlass by NOMINET

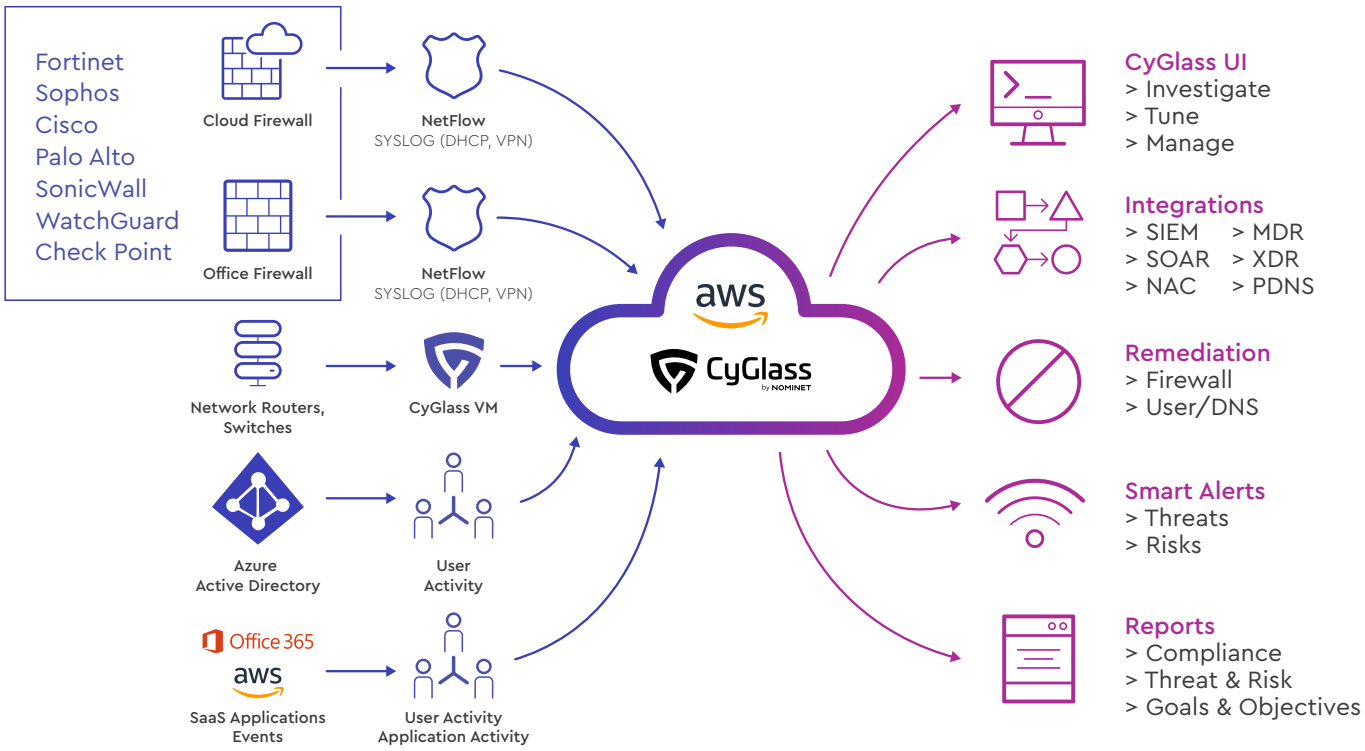


Fig. 2 The CyGlass NDaaS visibility, threat detection, and remediation process with the CyGlass AI engine operating within an AWS Cloud.

Logs ingested: NetFlow, Syslog, VPC Logs, AD Logs, VPN Logs, DNS Logs, DHCP Logs, and Web server logs.

The CyGlass AI engine utilizes unsupervised machine learning in a big data architecture and includes a fully integrated policy engine, and threat intelligence feeds. The policy engine and threat feeds enable AI-surfaced anomalous events from across network and cloud environments to be further defined in terms of known IOCs or threat activities. The policy engine also allows the rapid deployment of operational, threat, and compliance objectives and controls, driving the relevant analytics with even greater accuracy and actionable reporting for security risk mitigation and compliance adherence.

With hundreds of prebuilt monitoring controls and integration to CyGlass's reporting engine, security teams can quickly deploy defenses and report on control effectiveness, including risk and threat, ransomware, and cloud security reports, and more.

CyGlass outputs critical threat alerts and information via Smart Alert emails with links directly to the investigative UI. CyGlass can also deliver threat intelligence to other security tools, including SIEM, SOAR, and MDR systems, although, unlike legacy NDR tools, CyGlass does not require these tools to be deployed.

CyGlass by NOMINET

CyGlass Reporting

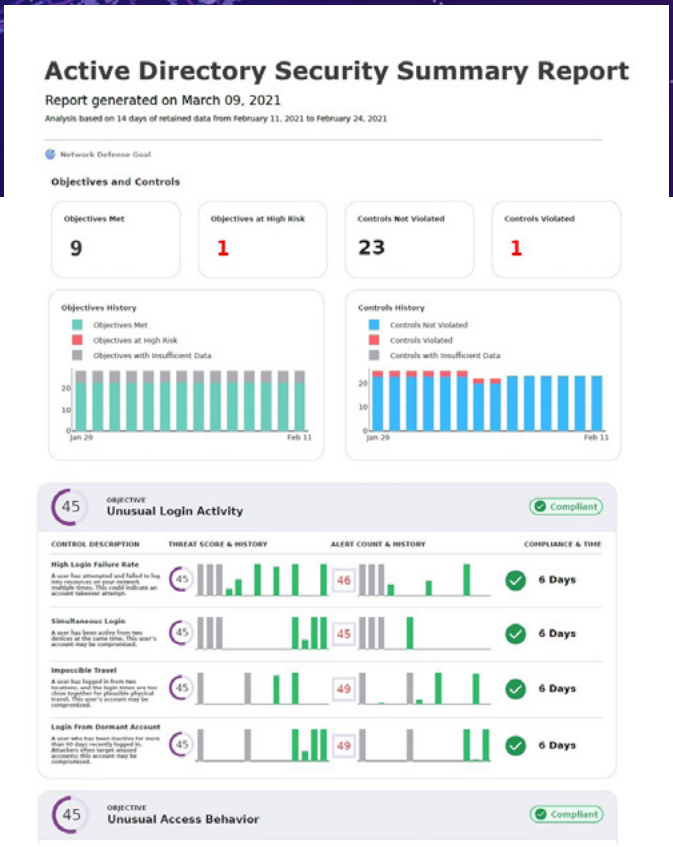


Fig. 3 CyGlass Active Directory Security Reports covers both on premise AD and AD/AZURE, and includes multiple user authentication and access risks and threats.

For all security teams, actionable reporting is an essential communications path for security awareness to the lines of business, executive team, and regulators. For midsized companies with smaller security teams, it is even more critical. Clearly communicating security effectiveness, potential risks and threats, and regulatory compliance efficacy are must-haves, particularly when the team does not have dedicated reporting tools or staff. In most cases, the security and IT teams must create the reports required without any additional resources, and therefore, the solution's reporting capabilities are essential.

CyGlass NDaaS includes a full reporting engine and prebuilt policy objectives to automatically update reports across topics like network risk reports, cybersecurity threat reports, multiple compliance reports, and user risk reports. CyGlass reports are easily configured, updated, and exported. Reports include an overall risk picture and detailed reporting around individual control effectiveness, rogue or risky device discovery, and highest risk user accounts. Most importantly, all CyGlass reporting is included in the software as a service license.

CyGlass by NOMINET

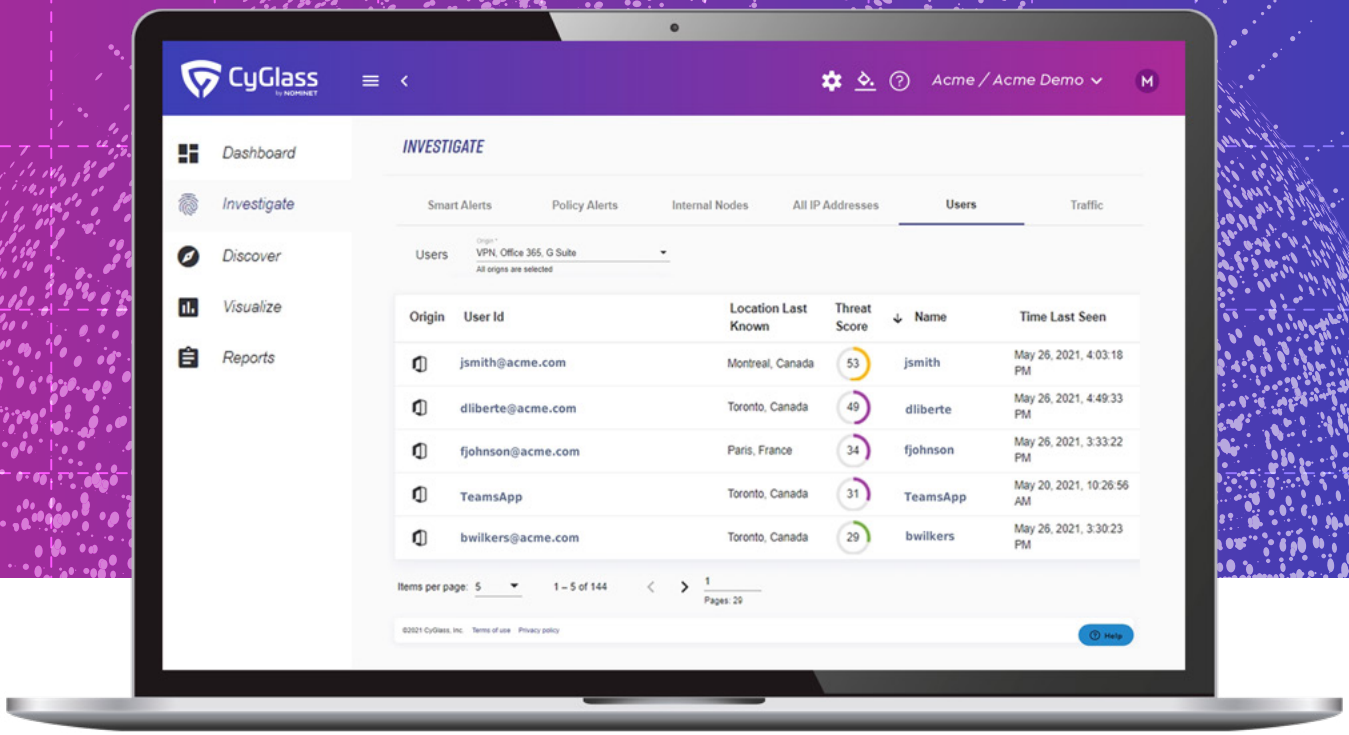


Fig. 4 User risk from VPN, AD, and Cloud platforms is easily correlated with network services and devices.

Risk and Threat Coverage

The CyGlass AI engine uses multiple unsupervised machine learning methods to determine normal baselines of activities for all devices and users on the network and in the cloud. CyGlass AI monitors for risky and threatening behavior across five critical categories:

- Indications of cyberattacks
- Risky human behavior
- Network risk
- Hybrid cloud risk
- Network health

Each category includes multiple AI models and overlying policies to surface and prioritize risks and threats while minimizing false positives. CyGlass threat detection policies can further enrich AI results by identifying common attack stages, for example, determining that a series of anomalous behaviors between the cloud and network align to "known bad activities" tied to a ransomware attack. CyGlass policies can also be used as specific risk-mitigating controls for regulatory compliance.

CyGlass by NOMINET

Indications of Cyber Attacks

CyGlass analytics surface events linked to likely attack stages, score the events by threat level, and explain the event in terms of actions, network traffic, devices, and users, whether the event develops in the cloud, in AD, or the network. Threat coverage includes Ransomware, Command & Control C2, Man-in-the-Middle, Network Account takeover, AD Azure Account Compromise, Unauthorized web & DNS activities, Masqueraders (tunneling), Credentials compromise, O365 data theft, and AWS services attacks.

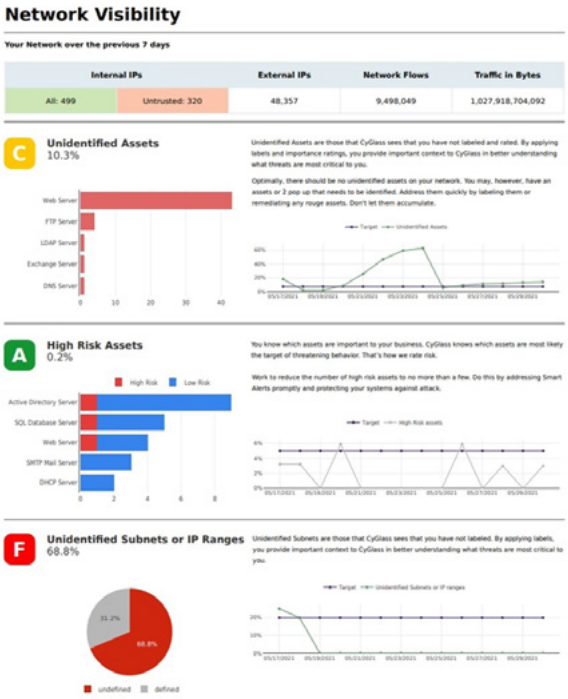


Fig. 5 Network visibility reports identifying unknown or risky assets helps maintaint a healthy network

Risky User Behavior

AD and AD/Azure events related to risky user behavior are surfaced and correlated to IP address and risky events. Alerts can indicate an insider threat or an internal or external compromise. Threat coverage includes rogue behaviors, insider threat, lateral movement, and data exfiltration.

Network Risk

Network risk analytics and network protection policies combine to monitor for evidence of improper or lack of network protection best practices. These can include unprotected ports, backup systems that have turned off, endpoint security protection that is not working or updating, communications with blacklisted or improper locations, and IoT device risk.

Cloud Risk

Cloud risk analytics and protection policies monitor for risky activity related to accounts and data movement from the network to the cloud and in the cloud environment. Particular emphasis is given to administrative account protection. Risk coverage includes authentication failure anomalies, unusual access time and location, anomalous remote access location or IP, AD unusual logging time or location, and multiple failed AD authentication requests, anonymous file activity, internal file or folder share with the public, and file or folder shared with an external user.

Network Health

Network health analytics define the normal devices, segmentation, and traffic on a network and look for changes from normal, which increases the risk of an attack on the network. Coverage includes detecting new devices and rogue devices, improper traffic to IoT devices, and the ability to define and tag all subnets and devices and define and monitor zero trust security zones for any control violations or risky events.

CyGlass by NOMINET

The power of user and device visibility

In expanding to cover cloud applications and identity directories, CyGlass can correlate threats in the context of involved devices and user accounts, both local and in the cloud. One feature usually available only with a full SIEM deployment is the ability to understand a network-detected threat like command and control calls in terms of users and devices involved. This means security managers can quickly understand the extent of the attack and narrow down the attack stage. Further, by understanding risky device and user behavior and matching those to anomalous network traffic, response and remediation actions become far more effective even for evasive advanced attacks.

Figure 6 provides views within the CyGlass NDaaS UI that show unsupervised machine learning models for user risk. These include monitoring file and folder activity, authentication failures, user access and remote access by IP, location and time.

The lower portion shows a detailed event view that reflects the correlation capabilities of the CyGlass AI engine, indicating a machine learning risky event with the related risk score, variation, location, user account and specific IP address. Security teams have immediate access to the critical data needed to remediate an event properly.

CyGlass delivers enterprise-class capabilities for a fraction of the cost of SIEM and legacy NDR tools.

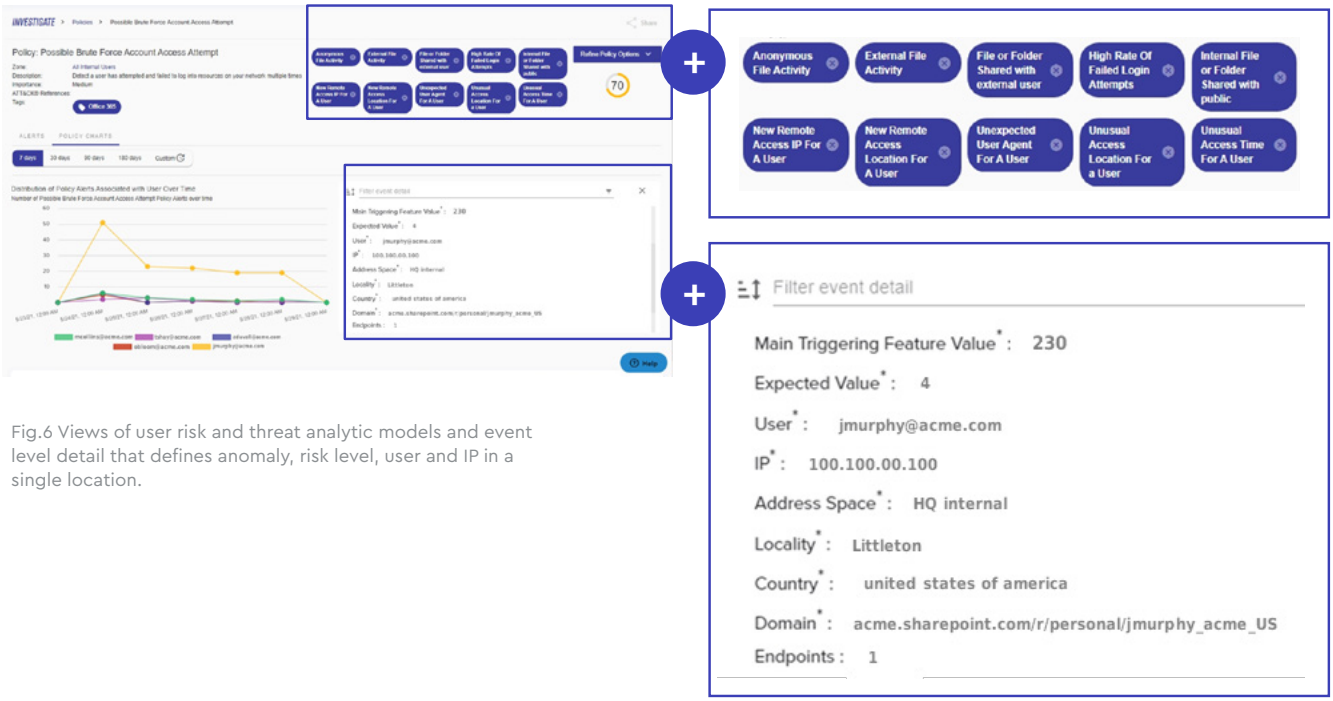


Fig.6 Views of user risk and threat analytic models and event level detail that defines anomaly, risk level, user and IP in a single location.

CyGlass by NOMINET

Summary

In the new reality that is a hybrid cloud and network environment, cyber attackers can now compromise an application, service, or account inside the network or in the cloud to gain access to sensitive systems and data. More alarmingly, attackers can compromise an Azure administer account and gain easy access to sensitive data across the entire environment. The combination of legacy networks with private and public cloud means IT and security managers must monitor and manage:

- User authentication across hybrid (Azure AD, on premise) processes
- User access and privileged access to cloud applications and storage
- Data movement, especially sensitive data moving from inside the network to the cloud
- Cloud application usage and detection of rogue application installations
- Network activity, device IP address, and user account data from the cloud to the network
- Rogue devices that can access both network and cloud applications and services

IT and security teams in medium and small organizations must find affordable solutions that can help manage and monitor hybrid environments. Technologies that support and build on existing security programs and offer monitoring and defenses across both traditional networks and cloud environments will significantly reduce the complexity and staff needed to successfully move and manage identities, devices, and services across both environments. Solutions that cover multiple threat surfaces, offer SaaS models, and are cloud-native (do not require on premise hardware) will minimize total cost of ownership.

CyGlass NDaaS is built explicitly for small security teams. It delivers cost-effective hybrid network visibility, defense, and compliance services, all from a 100% cloud-native platform. Advanced AI and automation means it can operate as a 24X7 continuous monitoring solution watching the organization's users, devices, and services (cloud and network) and supporting immediate remediation of threats when needed. With CyGlass NDaaS, IT and security managers can see risk, stop threats, and prove compliance, helping security protect their hybrid network environments.

CyGlass by NOMINET