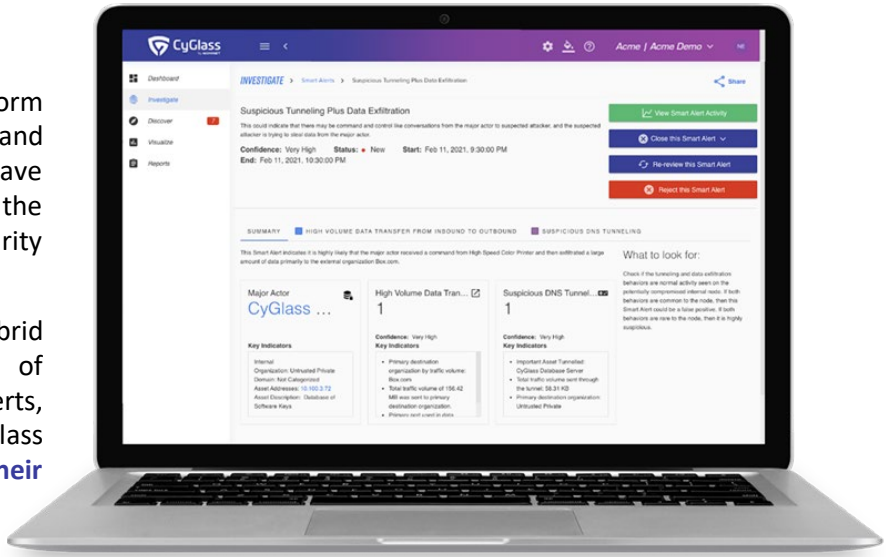
CyGlass

CyGlass Network Defence Risk and Compliance Reports

1 (978) 665-0280 www.cyglass.com info@cyglass.com

CyGlass Hybrid Network Defense

Network and Cloud Security Made Simple



CyGlass Hybrid Network Defense is a Cloud platform that delivers a cost effective detection, response, and compliance solution for cyber security teams that have distributed, hybrid networks but do not have the resources to operate a SIEM or 24X7 security operations center.

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

See Risks Across Your Hybrid Network

Network Operations Managers gain visibility to abnormal risky activities that occur across remote workers, on-premise, and Cloud environments. Managers can quickly identify unprotected or rogue devices, threats to IoT devices, misconfigured ports, risky traffic, and backup system failures without overburdening IT teams.

Stop Threats

CyGlass enables automated continuous monitoring for threats across networks, cloud, and VPNs. Utilizing a unique combination of cyber TTP policies, threat intelligence and AI, CyGlass delivers a short, prioritized list of smart alerts and investigative reports. Cyber and IT managers utilize CyGlass to quickly investigate and remediate cyber-attacks 24x7.

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 ISO 27001, NIST 800-53, Cyber Essentials, FFIEC, NIAC, CMMC, and more.

Built for Small IT Security Teams

CyGlass' unique Cloud-native delivery model provides enterprise class cyber security at a fraction of the cost of traditional NDR or SIEM tools. Deployed in just hours, 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, 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. CyGlass replaces legacy network traffic analyzers, NDR, marginal SIEM deployments, and legacy DLP tools.
- Low TCO: Advanced AI drives automation, reduce overhead and manpower requirements while increasing operational effectiveness and threat detection from devices anywhere, anytime. CyGlass operates at 1/3 of the cost of traditional security tools.

CyGlass Threat Coverage

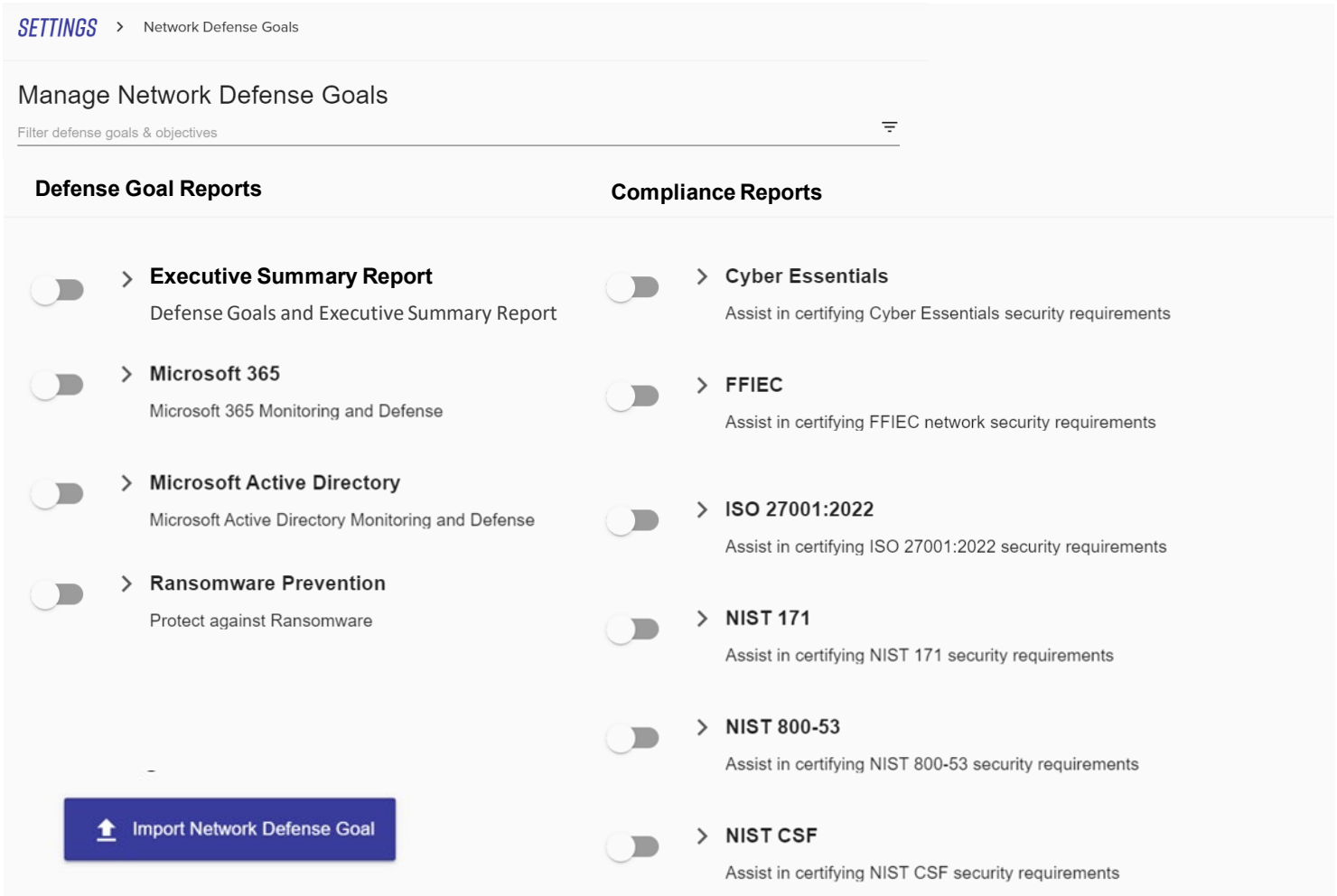
- Ransomware
- Supply Chain
- VPN Threats
- Command & Control C2
- Man-in-the-Middle
- Unauthorized web & DNS activities
- Masqueraders (tunneling)
- Credential compromise
- Rogue behaviors
- Insider threats
- Lateral movement
- Data exfiltration

CyGlass

CyGlass Network Defence Risk and Compliance Reports

SET DEFENCE GOALS, SHOW COMPLIANCE SUCCESS

- Defense goals activate prebuilt policies and AI driven controls
- Reports are generated automatically
- No extra overhead, Reduce Manual Activities



1 (978) 665-0280 www.cyglass.com info@cyglass.com

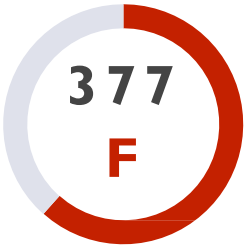
CyGlass

Executive Summary CyberScore Report

Report generated on November 03, 2022

Read more about how to interpret this report →

Cyber Score



A cyber score of 612 or higher is your target based on other CyGlass users.

Continued use of CyGlass is aimed at improving your CyberScore and securing your critical IT devices. 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 users risk the security of your critical IT devices are detected.

Time Period

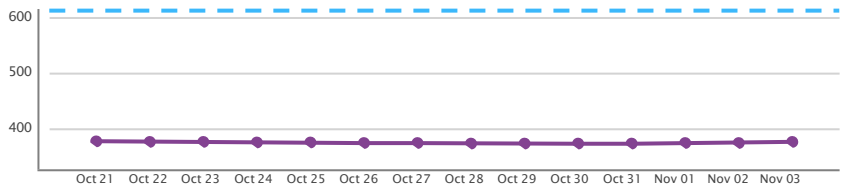
From:	October 21, 2022
To:	November 03, 2022
Generated:	November 03, 2022
Period:	14 Days

Legend

Target Cyber Score

No data available

Cyber Score History



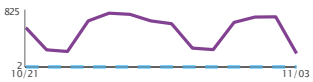
Threat Detection Summary

CYBER SCORE	SUMMARY	DESCRIPTION	14 DAY HISTORY
A	**Open Smart Alerts** 0 currently open	Smart Alerts are CyGlass' highest – priority alerts. They highlight potential active attack behavior.	
A	**Average Time to Close Smart Alerts** 0.0 Days (Using a trailing 7-day average)	Smart Alerts represent possible active attacks, investigating and closing them promptly is an important part of your organization's security process.	
A	**Detected Smart Alerts** 0 Smart Alerts	Smart Alerts represent possible active attacks. As CyGlass learns and vulnerabilities are addressed, you should see the total volume of smart alerts decrease. This metric counts the number of smart alerts were created or updated each day.	
B	**Log Collection Uptime** 96%	CyGlass is only able to protect your network when collectors are receiving logs. Gaps in collection are a vulnerability.	

Network Visibility Summary

CYBER SCORE	SUMMARY	DESCRIPTION	14 DAY HISTORY
F	**Unidentified Devices** 75.0%	Unidentified Devices have not yet been labeled and rated in CyGlass. Labels and importance ratings help CyGlass highlight the threats that are most critical to you.	
A	**High Risk Devices** 0.0%	CyGlass identifies devices that are most likely to be the target of threatening behavior.	
A	**Unidentified Subnets or IP Ranges** 0.0%	Unidentified Subnets have not yet been labeled in CyGlass. Labels help CyGlass highlight known networks and identify new or rogue networks.	

Policy Assurance Summary

CYBER SCORE	SUMMARY	DESCRIPTION	14 DAY HISTORY
F	**Policy Alerts** 1152.1 Per day (Average of past 7 days)	Policy Alerts allow you to detect violations of your enterprise access policies, selected from pre-built policy definitions or custom-built by you.	

Threat Detection Detail

A

Open Smart Alerts

0 currently open.

Having less than 5 open alerts at any given time is a good indicator that you are addressing detected threats in a timely manner.

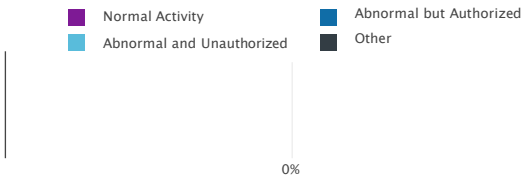
Smart Alerts by AI Confidence

A

Average Time to Close Smart Alerts

0.0 Days (Using a trailing 7-day average)

An average time to close of less than 2 days indicatesthat you are taking a proactive approach to assessing and remediating threats and vulnerabilities.



A

Detected Smart Alerts

Summary of Smart Alerts detected in your network during this report period.

SMART ALERT TYPE	COUNT	MAJOR ACTORS	TIME LAST TRIGGERED
Internal to External Probing or Reconnaissance Activity	0	No threats of this type detected in your network	
Peer to Peer Exfiltration	0	No threats of this type detected in your network	
Probing or Reconnaissance Activity	0	No threats of this type detected in your network	
RDP Tunneling Activity	0	No threats of this type detected in your network	
Suspicious Activity On an Asset	0	No threats of this type detected in your network	
Suspicious Activity On an Untrusted Private IP	0	No threats of this type detected in your network	
Suspicious Tunneling Plus Data Exfiltration	0	No threats of this type detected in your network	
Suspicious Tunneling Plus Port Scan	0	No threats of this type detected in your network	

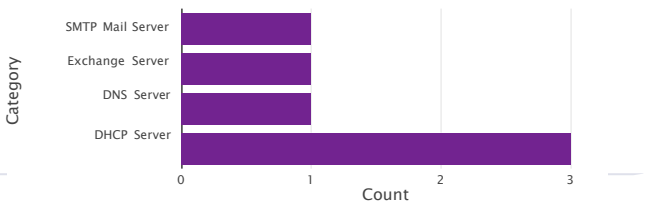
Network Visibility Detail

F

Unidentified Devices

75.0%

Unidentified devices are those that CyGlass sees that you have not labeled and rated. By applying labels and importance ratings, you provide important context for CyGlass in better understanding what threats are most critical. Optimally, there should be no unidentified devices on your network, however, when they are present, you should label them quickly or remediate any rogue ones. Don't let them accumulate. This chart reflects your network at the time of report generation, November 03, 2022.

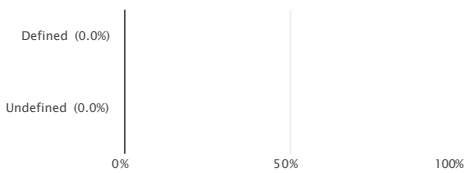


A

Unidentified Subnets or IP Ranges

0.0%

Unidentified subnets are those that have not been labeled in CyGlass. By applying labels, you provide important context to CyGlass in better understanding what threats are most critical to your organization. This chart reflects your network at the time of report generation, November 03, 2022.



IP START RANGE	ACTIVE IPs	LAST UPDATED
No Unidentified Subnets or IP ranges Available		

A

High Risk Devices

0 Devices with a Threat Score above 70

You know which devices are important to your business. CyGlass knows which devices are most likely the target of threatening behavior. That's how we rate risk. Work to reduce the number of high risk devices to no more than a few by addressing Smart Alerts promptly and protecting your systems against attack. This chart reflects your network at the time of report generation, November 03, 2022.

HIGH RISK DEVICES	THREAT SCORE	ALERT COUNT	ROLE	IP ADDRESS
No High Risk Devices Available				

CyGlass

Microsoft 365 Defense Goal Report

Read more about how to interpret this report ⇢

Time Period

From:	October 21, 2022
To:	November 03, 2022
Generated:	November 03, 2022
Period:	14 Days

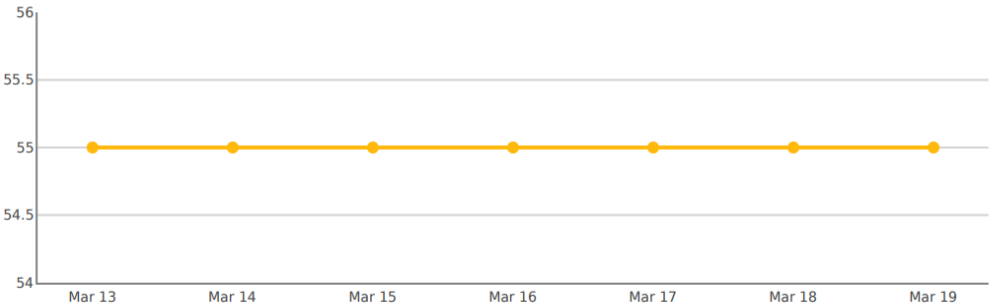
Legend

.....	Threshold
	No data available

55 Network Defense Overview

Threat Score

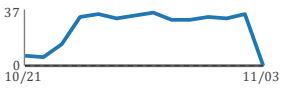
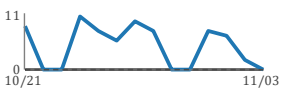
Threat Score History



2/3 Objectives are not compliant

3/7 Controls are not compliant

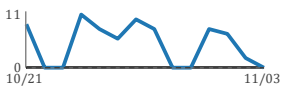
75 Top Network Threats

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
75	3. Suspicious Login Activity 1. Possible Brute Force Account Access Attempt Detect a user has attempted and failed to log into resources on your network multiple times	We recommend enabling multi-factor authentication and enforcing password complexity requirements. We also suggest forcing a password reset on involved user accounts.		0 Days
55	1. Exfiltration by an Internal Actor 1.2 Suspicious Rate of File Activity A suspicious rate of file creation, deletion, or modification has been detected. This may be an attacker encrypting your files with ransomware or exfiltrating your files.	We recommend verifying that MFA and password complexity requirements are enabled for involved user accounts and forcing a password reset. We also recommend investigating the involved files to determine if this activity was legitimate.		0 Days
50	1. Exfiltration by an Internal Actor 1. Internal Files Shared Externally Internal files have been shared with an external user. This may be an attacker attempting to exfiltrate your data	We suggest removing file-sharing permissions from high-value data and documents and following a least-privilege policy across all user accounts.		0 Days

55 OBJECTIVE 1. Exfiltration by an Internal Actor

Detect anomalous file modification and sharing consistent with file exfiltration

Not Compliant

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
50	1.1 Internal Files Shared Externally Internal files have been shared with an external user. This may be an attacker attempting to exfiltrate your data	We suggest removing file-sharing permissions from high-value data and documents and following a least-privilege policy across all user accounts.		0 Days
55	1.2 Suspicious Rate of File Activity A suspicious rate of file creation, deletion, or modification has been detected. This may be an attacker encrypting your files with ransomware or exfiltrating your files.	We recommend verifying that MFA and password complexity requirements are enabled for involved user accounts and forcing a password reset. We also recommend investigating the involved files to determine if this activity was legitimate.		0 Days

OBJECTIVE

2. Suspicious Access Behavior

Detect anomalous access behavior that may indicate a compromised account or an account takeover attempt

Compliant

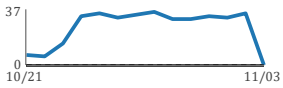
THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
0	**2.1 Suspicious Access Location** A user has accessed resources on your network from a suspicious location. This could be a sign of internal malicious activity or account takeover	We recommend verifying that MFA and password complexity requirements are enabled for involved users and forcing a password reset.		22 Days
0	**2.2 Suspicious Access Time** A user has accessed resources on your network at a suspicious time. This could be a sign of internal malicious activity or account takeover	We recommend verifying that MFA and password complexity requirements are enabled for involved user accounts and forcing a password reset.		38 Days

OBJECTIVE

3. Suspicious Login Activity

Detect anomalous login behavior that may indicate a compromised account or an account takeover attempt

Not Compliant

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
75	**3.1 Possible Brute Force Account Access Attempt** Detect a user has attempted and failed to log into resources on your network multiple times	We recommend enabling multi-factor authentication and enforcing password complexity requirements. We also suggest forcing a password reset on involved user accounts.		0 Days

Control Violation Detail and Remediation

1.1 Internal Files Shared Externally

Control Detail

External file sharing may signal an exfiltration attempt.

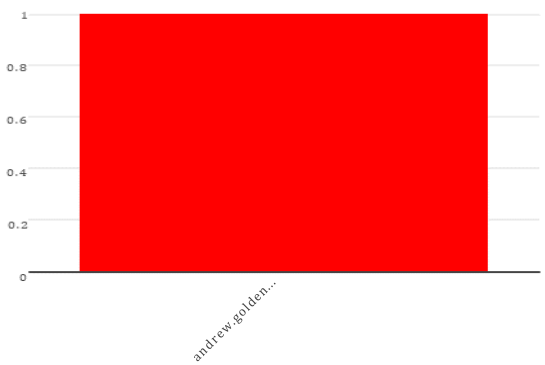
Remediation

We suggest removing file-sharing permissions from high-value data and documents and following a least-privilege policy across all user accounts. We also suggest investigating this activity to determine if it was legitimate.

Alert Detail

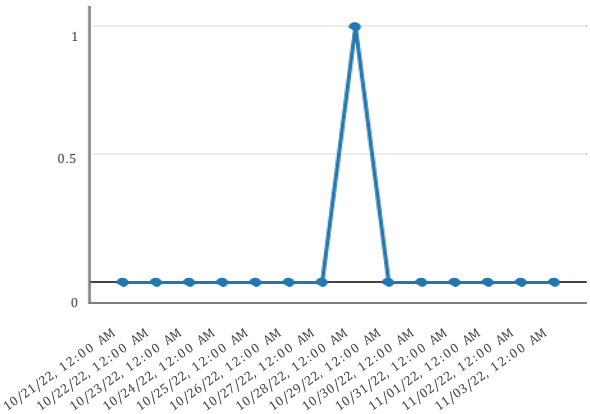
Distribution of Policy Alerts by User

Number of Internal Files Shared Externally Policy Alerts, broken down by user



Distribution of Policy Alerts Associated with User Over Time

Number of Internal Files Shared Externally Policy Alerts over time



3.1 Possible Brute Force Account Access Attempt

Control Detail

An unusual number of failed logins can indicate that an attacker is trying to gain access to your network by iteratively trying common or published passwords.

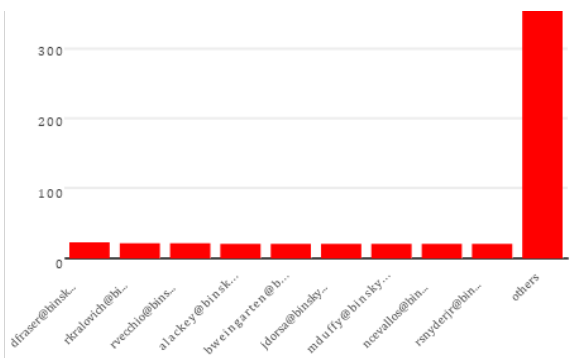
Remediation

We recommend enabling multi-factor authentication and enforcing a password complexity policy. We also suggest investigating these access attempts for unusual login time or location. If you are concerned this access is not legitimate, we recommend contacting this user and forcing a password reset.

Alert Detail

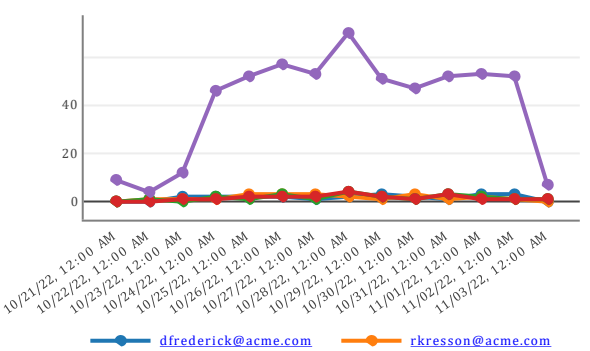
Distribution of Policy Alerts by User

Number of Possible Brute Force Account Access Attempt Policy Alerts, broken down by user



Distribution of Policy Alerts Associated with User Over Time

Number of Possible Brute Force Account Access Attempt Policy Alerts over time



Ransomware Prevention Defense Goal Report

Read more about how to interpret this report →

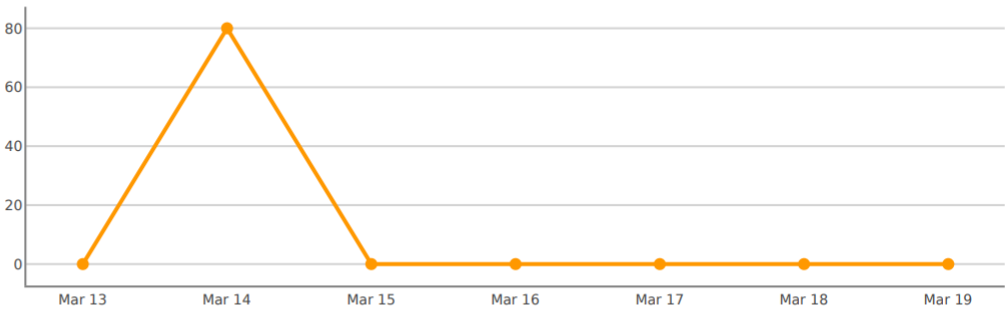
Time Period

From:	October 21, 2022
To:	November 03, 2022
Generated:	November 03, 2022
Period:	14 Days

80 Network Defense Overview

Threat Score

Threat Score History



4/8 Objectives are not compliant

13/23 Controls are not compliant

75 Top Network Threats

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
75	1. Abusive, suspicious, or malicious site access detected 1.2 Activity to Blocked Countries Detect traffic to countries blocked by your firewall	We recommend configuring your firewalls to block all traffic with IPs registered in Russia, China, Iran, North Korea, Cuba, Syria, Libya, South Yemen, and Sudan.		0 Days
70	7. Unnecessary or Unexpected Port Activity 7.5 Traffic on High Ports Crossing Network Boundary High port to high port traffic - a possible indicator of peer-to-peer activity - is detected across network boundary. Unless specifically needed in your network, this is Unnecessary or Unexpected Port Activity, and blocking it is part of preventing ransomware attacks.	We recommend investigating what ports the triggering traffic was running on. If these ports are not associated with applications you expect to see in your network, we recommend blocking them at the firewall.		0 Days
50	3. Command and Control Detection 3.4 Unauthorized Outbound SSH An unauthorized SSH connection has been detected from an internal device to an external domain.	We recommend routing all legitimate external SSH connections through a VPN and blocking all incoming activity on ports 3389 and 22.		0 Days

75 OBJECTIVE
1. Abusive, suspicious, or malicious site access detected

Detect any activity to Internet sites identified as abusive, suspicious, or malicious.

Not Compliant

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
0	1.1 Activity from Blocked Countries Detect traffic from countries blocked by your firewall	We recommend configuring your firewalls to block all traffic with IPs registered in Russia, China, Iran, North Korea, Cuba, Syria, Libya, South Yemen, and Sudan.		38 Days
75	1.2 Activity to Blocked Countries Detect traffic to countries blocked by your firewall	We recommend configuring your firewalls to block all traffic with IPs registered in Russia, China, Iran, North Korea, Cuba, Syria, Libya, South Yemen, and Sudan.		0 Days

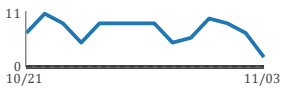
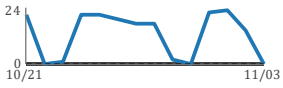
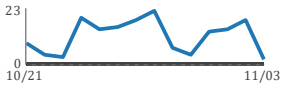
40

OBJECTIVE

2. Activity on Unsecured Ports

Block network activity on application protocols that are encrypted.

Not Compliant

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
0	**2.1 Unsecured Inbound FTP/TFTP Traffic** FTP/TFTP Traffic is detected from external to internal endpoints. This Activity on Unsecure Ports indicates vulnerabilities against ransomware attacks.	We suggest using SFTP in place of FTP/TFTP to ensure that your data is secured during transfer and blocking ports UDP/137, UDP/138, and TCP/139 at perimeter firewall in both directions		38 Days
0	**2.2 Unsecured Inbound IRC Traffic** IRC Traffic is detected from external to internal endpoints. This Activity on Unsecure Ports indicates vulnerabilities against ransomware attacks.	We suggest closing TCP ports 194 and 6667 on all your high-value devices and blocking traffic on these ports from your perimeter firewalls.		38 Days
0	**2.3 Unsecured Inbound SNMP Traffic** SNMP Traffic is detected from external to internal endpoints. This Activity on Unsecure Ports indicates vulnerabilities against ransomware attacks.	We suggest disabling SNMP on all high-value devices in your network and blocking ports 161 and 162 on your perimeter firewalls. If you require SNMP, we suggest upgrading to SNMP3, which is encrypted.		38 Days
0	**2.4 Unsecured Inbound Telnet Traffic** Telnet Traffic - port 23 TCP - is detected from external to internal endpoints. This Activity on Unsecure Ports indicates vulnerabilities against ransomware attacks.	We suggest disabling telnet on all your high-value devices and blocking port 23 on your perimeter firewalls.		38 Days
23	**2.5 Unsecured Inbound Web Server Activity** Unsecure web server traffic - port 80 TCP - is detected from external to internal endpoints. This Activity on Unsecure Ports indicates vulnerabilities against ransomware attacks.	We suggest using HTTPS to serve any publicly-facing content. If this alert was generated for a high-value device, we suggest investigating the source, destination, and traffic volume.		0 Days
28	**2.6 Unsecured Internal FTP/TFTP Traffic** FTP/TFTP Traffic is detected between internal endpoints. This Activity on Unsecure Ports indicates vulnerabilities against ransomware attacks.	We suggest using SFTP in place of FTP/TFTP to ensure that your data is secured during transfer.		0 Days
40	**2.7 Unsecured Internal IRC Traffic** IRC Traffic is detected between internal endpoints. This Activity on Unsecure Ports indicates vulnerabilities against ransomware attacks.	We suggest closing TCP ports 194 and 6667 on all your high-value devices and blocking traffic on these ports from your perimeter firewalls.		0 Days
0	**2.8 Unsecured Internal Telnet Traffic** Telnet Traffic - port 23 TCP - is detected between internal endpoints. This Activity on Unsecure Ports indicates vulnerabilities against ransomware attacks.	We suggest disabling telnet on all your high-value devices and blocking port 23 on your perimeter firewalls.		38 Days
23	**2.9 Unsecured Internal Web Server Activity** Unsecure web server traffic - port 80 TCP - is detected between internal endpoints. This Activity on Unsecure Ports indicates vulnerabilities against ransomware attacks.	We suggest using HTTPS to serve any publicly-facing content. If this alert was generated for a high-value device, we suggest investigating the source, destination, and traffic volume.		0 Days

0

OBJECTIVE

4. Disruption in Scheduled Backups

Identify any disruptions or suspicious variations to scheduled backup services.

Compliant

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
0	**4.1 External Backup Server Disruption** Regular backups to an external server from internal devices was discontinued. Stopping or changing backups is a common part of ransomware attacks.	We recommend re-running any interrupted or stopped backup processes and investigating the cause of the disruption to your periodic backup.		318 Days

0

OBJECTIVE

5. SMB Leakage

Block any outbound traffic on Windows SMB protocols.

Compliant

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
0	**5.1 Outbound NetBIOS Traffic** NetBIOS traffic from internal endpoints to public IPs is detected. This is an indicator of possible SMB Leakage, and blocking such activity is part of preventing ransomware attacks.	We suggest blocking ports UDP/137, UDP/138, and TCP/139 at the perimeter firewall in both directions and disabling NetBIOS-NS on all of your Windows devices.		38 Days

ISO 27001:2022 Network Defense Goal Report

Read more about how to interpret this report →

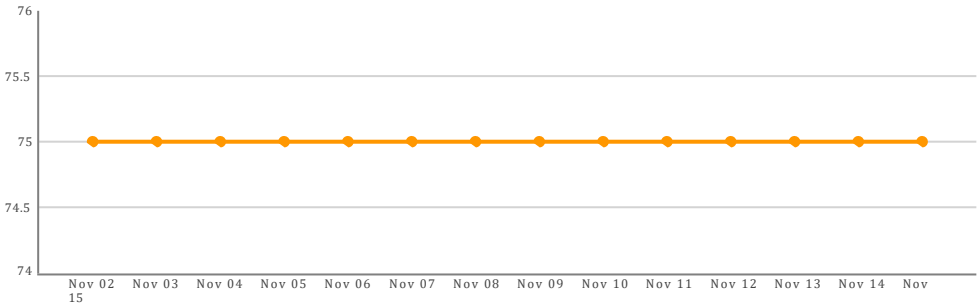
Time Period

From:	November 02, 2022
To:	November 15, 2022
Generated:	November 15, 2022
Period:	14 Days

75 Network Defense Overview

Threat Score

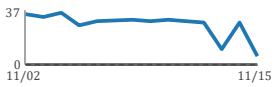
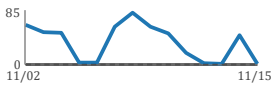
Threat Score History



7/8 Objectives are not compliant

27/58 Controls are not compliant

75 Top Network Threats

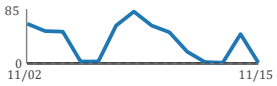
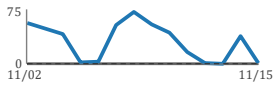
THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
75	1. A.5.15: Access Control 1.3 Activity to Blocked Countries Detect traffic to countries blocked by your firewall	We recommend configuring your firewalls to block all traffic with IPs registered in Russia, China, Iran, North Korea, Cuba, Syria, Libya, South Yemen, and Sudan.		0 Days
75	8. A.8.5 Secure authentication 1. Possible Brute Force Account Access Attempt Detect a user has attempted and failed to log into resources on your network multiple times	We recommend enabling multi-factor authentication and enforcing password complexity requirements. We also suggest forcing a password reset on involved user accounts.		0 Days
70	1. A.5.15: Access Control 1.4 Activity to Social Media Sites Detect when anyone communicates with a prohibited social media site	Block social media access to protect from data loss or phishing attacks, as well as to increase productivity. Use exclusions to not alert on sites that are authorized or groups of users that may access social media for their jobs.		0 Days

65 OBJECTIVE 1. A.5.15: Access Control

The Controls in this Objective address ISO 27001:2022 requirements for Section A.5.15: Access Control with the Objective: To limit access to information and information processing facilities.

Not Compliant

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
0	1.1 Activity between Development and Production Detect when unauthorized development systems are communicating with Production systems	We suggest investigating this traffic and, if you suspect this may have been attack activity, running antivirus on the involved machines.		22 Days
0	1.2 Activity from Blocked Countries Detect traffic from countries blocked by your firewall	We recommend configuring your firewalls to block all traffic with IPs registered in Russia, China, Iran, North Korea, Cuba, Syria, Libya, South Yemen, and Sudan.		22 Days

0	**1.2 Activity from Blocked Countries** Detect traffic from countries blocked by your firewall	We recommend configuring your firewalls to block all traffic with IPs registered in Russia, China, Iran, North Korea, Cuba, Syria, Libya, South Yemen, and Sudan.		22 Days	
75	**1.3 Activity to Blocked Countries** Detect traffic to countries blocked by your firewall	We recommend configuring your firewalls to block all traffic with IPs registered in Russia, China, Iran, North Korea, Cuba, Syria, Libya, South Yemen, and Sudan.		0 Days	
70	**1.4 Activity to Social Media Sites** Detect when anyone communicates with a prohibited social media site	Block social media access to protect from data loss or phishing attacks, as well as to increase productivity. Use exclusions to not alert on sites that are authorized or groups of users that may access social media for their jobs.		0 Days	
0	**1.5 Connection From New External Domain to Internal** A remote Domain has connected to a device in your network for the first time. It may be unusual for connections to be initiated from external domain, especially those that have not connected in the past.	We recommend investigating the traffic that triggered this alert and either blocking the involved external IPs at the firewall or updating the zones associated with this policy to prevent future alerts.		22 Days	
0	**1.6 Connection To New Domain from Critical Device** A Critical Device in your network has connected to a domain for the first time. It may be unusual for a critical device to interact with an external domain that it has never communicated with before.	We suggest investigating this traffic and, if you suspect this may have been attack activity, running anti-virus on your critical device.		22 Days	
0	**1.7 Critical Device to or from Facebook** Detect when a critical device is communicating with Facebook	We suggest blocking traffic between high-value devices and Facebook.		22 Days	
70	**1.8 Detect Internal traffic to or from Facebook** Detect when anyone is communicating with Facebook	Block access to Facebook to reduce the risk of data loss or to increase productivity.		0 Days	
70	**1.9 Detect Large Volume to File Sharing sites** Detect when sending more than 40K bytes to a public file sharing site	Identify the User sending more than 40K bytes. Consider that this could be an indicator of account take-over.		0 Days	

OBJECTIVE

5. A.8.19 Installation of software on operational systems

The Controls in this Objective address ISO 27001:2022 requirements for Section A.8.19 Installation of software on operational systems ewith the Objective: To ensure the integrity of operational systems.

Compliant

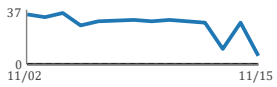
THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
0	**5.1 WUDO Traffic Crossing Network Boundary** Detects Windows Update Delivery Optimization (WUDO) traffic between devices within your network and the public internet.	Identify the devices communicating on WUDO port 7680 and scan the machines with antivirus and investigate the destination domains are allowed in your network.		22 Days

OBJECTIVE

8. A.8.5 Secure authentication

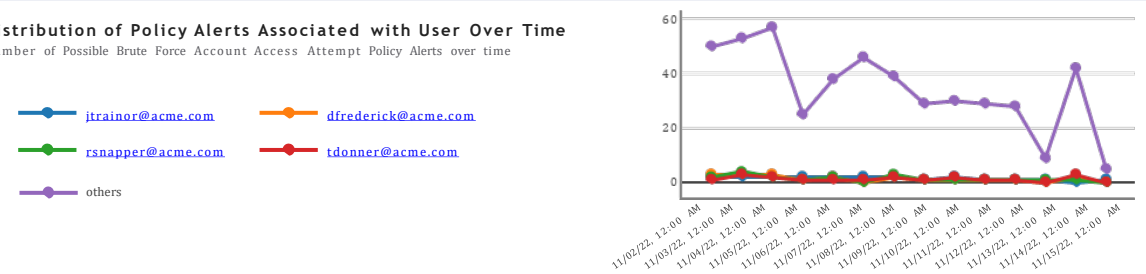
The Controls in this Objective address ISO 27001:2022 requirements for Section A.8.5 Secure authentication with the Objective: To prevent unauthorized access to systems and applications.

Not Compliant

THREAT SCORE	CONTROL DESCRIPTION	REMEDIATION	ALERT HISTORY	COMPLIANCE
75	**8.1 Possible Brute Force Account Access Attempt** Detect a user has attempted and failed to log into resources on your network multiple times	We recommend enabling multi-factor authentication and enforcing password complexity requirements. We also suggest forcing a password reset on involved user accounts.		0 Days

Distribution of Policy Alerts Associated with User Over Time

Number of Possible Brute Force Account Access Attempt Policy Alerts over time



CyGlass

Continuous Visibility, Automated Compliance Reporting

CyGlass objective-driven controls 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 based on NIST and ISO control standards mean teams click a button to activate required controls, and AI-driven models validate control effectiveness. Automated report creation delivers needed reports on demand. Security teams save time and money with these easy-to-activate prebuilt policies and reports. Control models are easily configured, and new models are added. CyGlass compliance controls and reporting eliminate manual control assessments, validation, and report creation, saving hundreds of manual hours of labor.

Executive Summary Report

The Executive Summary Report (ESR) provides a top-level view of the risks, threats, and vulnerabilities that CyGlass detects. The report provides an overall threat score for your network and a set of more detailed metrics to understand where opportunities for improvement can be found. The ESR provides a comprehensive threat score calculated like a credit score and an overall grade. The ESR allows IT and security teams to determine how well their cyber defense program operates over time and provides objective scoring to support continuous improvement.

Risk and Threat Reports

> **Ransomware Prevention**
The Ransomware Prevention Defense Report is an objective and control effectiveness report built around CISA ransomware defense best practices. This report provides an instant view of the risk, threats, and vulnerabilities for ten objectives and forty-three controls automatically implemented in the CyGlass deployment.

> **Microsoft 365 Monitoring and Defense**
The Microsoft 365 threat detection and response report contains three objectives and ten controls to monitor for risks, threats, and vulnerabilities across M365 applications and users.

> **Microsoft Active Directory Monitoring and Defense**
Microsoft Active Directory Monitoring and Defense contains one objective and eight controls covering risks and threats to your AD domain, admins, and users.

Compliance Reports

> **Cyber Essentials**
The Cyber Essentials control sets cover four objectives and sixty controls across the network, DMZ traffic, malware protection, secure configuration, and security update management standards.

> **ISO 27001**
The ISO 27001 control set covers 2013 and 2022 across eight objectives and fifty-eight controls covering network, identity, and application security to support ISO compliance.

> **NIST 800-53**
The NIST 800-53 control set and report include seven objectives and eighty-eight network, identity, and cloud controls to support compliance programs.

> **NIST 171**
The NIST 171 control set and report include seven objectives and eighty-seven network and cloud controls to support compliance programs for 171, CMMC 2.0, and DFARS.

> **MPA**
Beyond standard frameworks, it is simple to configure control sets to meet specialized supply chain and compliance rules. The Motion Picture Association content security program defense goal report protects the intellectual property of movies, electronic games, and other productions, including three objectives and forty-four controls.

> **Configure your own**
With over one hundred prebuilt controls (and more being added monthly), and an easy-to-configure policy and reporting engine, CyGlass eliminates hundreds of manual control and reporting tasks with a few button clicks. Configurable controls and control reports are easily created for NIST CSF, FFIEC, and many more.