ACME

Powered By CyGlass

Threat Assessment for Acme

Report generated on November 13, 2019

Analysis based on 19 days of retained data from October 25, 2019 to November 13, 2019

Your threat score is

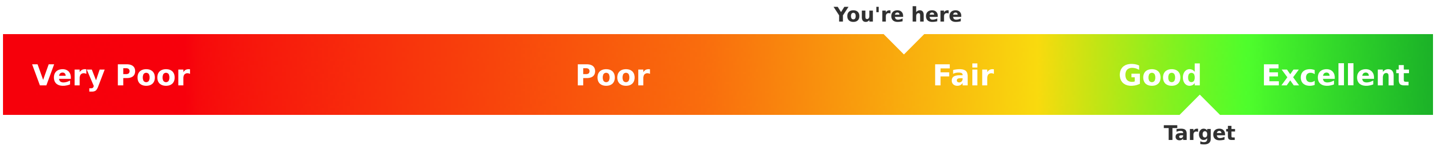
D 650

Target* threat score is

B 763

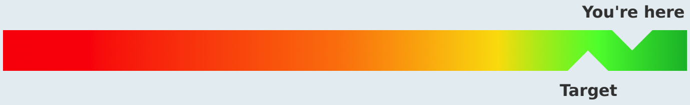
* Based on threat scores from CyGlass users

Continued use of CyGlass is aimed at improving your threat score and securing your critical IT assets. 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 assets are detected.

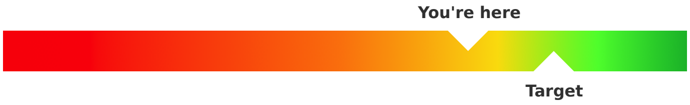


THREAT DETECTION

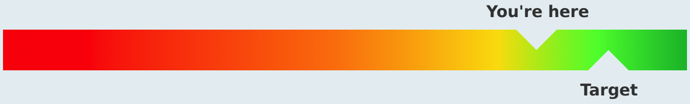
A **Open Smart Alerts**
3 Currently open



D **Average Time to Close Smart Alerts**
3.2 Days, (Using a trailing 7-day average)

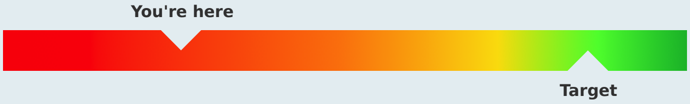


C **Manual Effort Saved**
1.8 Person Days per Week

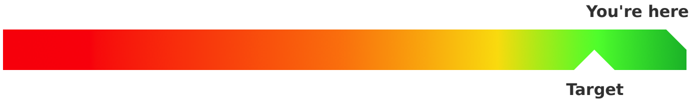


NETWORK VISIBILITY

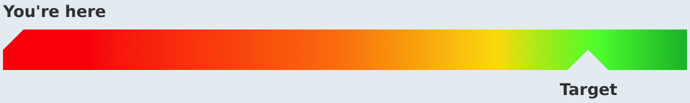
F **Unidentified Assets**
68.2%



A **High Risk Assets**
0.0%

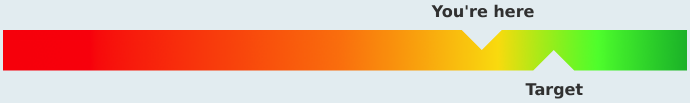


F **Unidentified Subnets or IP Ranges**
100.0%



POLICY ASSURANCE

C **Policy Alerts**
3.0 Per day (Average of past 7 days)



This report has been prepared for Acme. It is for illustrative purposes only and CyGlass is not responsible for any decisions or actions taken based on this information.

ACME

Powered By CyGlass

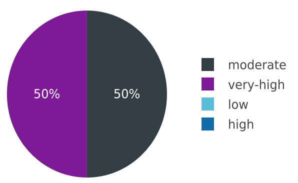
Threat Detection

A

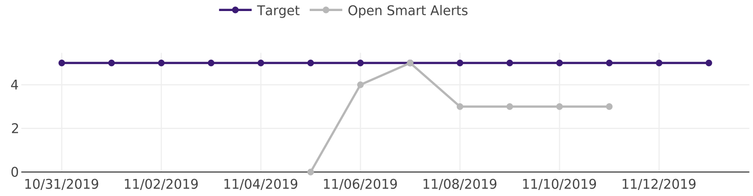
Open Smart Alerts

3 Currently open

Smart Alerts by AI Confidence



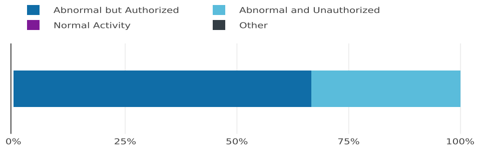
Having Less than 5 open alerts at any given time is a good indicator that you are addressing detected threats in a timely manner.



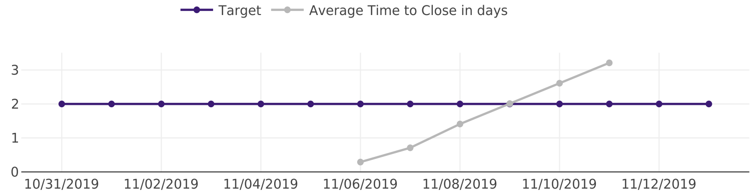
D

Average Time to Close Smart Alerts

3.2 Days, (Using a trailing 7-day average)



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



C

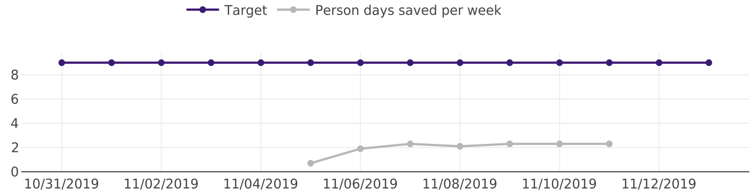
Manual Effort Saved

1.8 Person Days per Week

Occurrences over past 1 week

Policy Alerts	21
New Smart Alerts	3
Orphaned Behaviors	15
Unconfirmed Smart Alerts	0

In networks of 100 to 200 unique internal IPs, you should see a savings of 5 work days per week. Larger networks should see more. Your target time saved is proportional to the size of your network.



Smart Alert Summary

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

Smart Alert Type	Status	# Major Actors	Time First Seen	Time Last Triggered
Suspicious Activity On an Asset	🔴	1	11/07/2019 04:00:00 UTC	11/07/2019 05:00:00 UTC
Suspicious Tunneling Plus Data Exfiltration	🟡	1	11/07/2019 10:30:00 UTC	11/08/2019 10:42:09 UTC
Internal to External Probing or Reconnaissance Activity	🟢			
Probing or Reconnaissance Activity	🟢			
Suspicious Activity On an Untrusted Private IP	🟢			

🔴 - High Threat 🟡 - Medium Threat 🟢 - Low Threat

This report has been prepared for Acme. It is for illustrative purposes only and CyGlass is not responsible for any decisions or actions taken based on this information.

ACME

Powered By CyGlass

Network Visibility

Your Network over the previous 7 days

Internal IPs		External IPs	Network Flows	Traffic in Bytes
Trusted: 96	Untrusted: 94	16,879	577,458	16,112,333,568

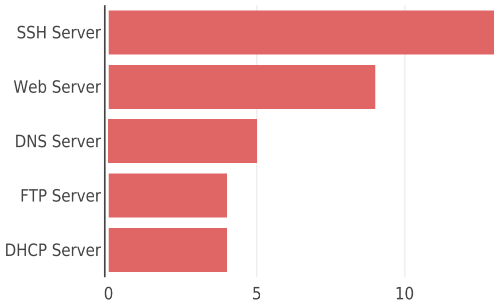
F

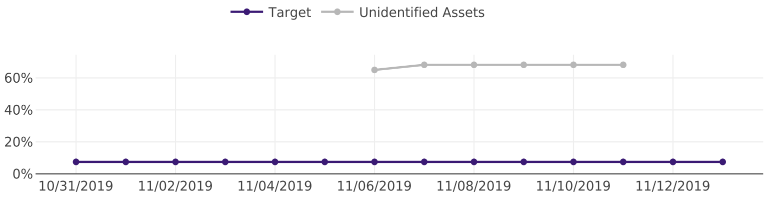
Unidentified Assets

68.2%

Unidentified Assets are those that CyGlass sees that you have not labeled and rated. By applying labels and importance ratings, you provide important context to CyGlass in better understanding what threats are most critical to you.

Optimally, there should be no unidentified assets on your network. You may, however, have an assets or 2 pop up that needs to be identified. Address them quickly by labeling them or remediating any rouge assets. Don't let them accumulate.





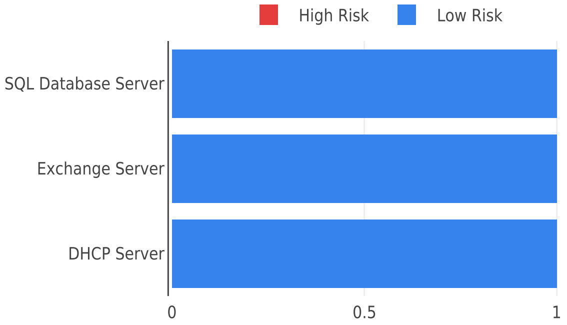
A

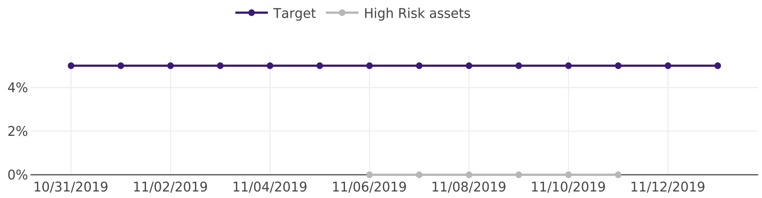
High Risk Assets

0.0%

You know which assets are important to your business. CyGlass knows which assets are most likely the target of threatening behavior. That’s how we rate risk.

Work to reduce the number of high risk assets to no more than a few. Do this by addressing Smart Alerts promptly and protecting your systems against attack.



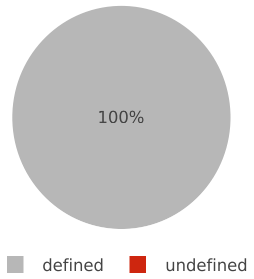


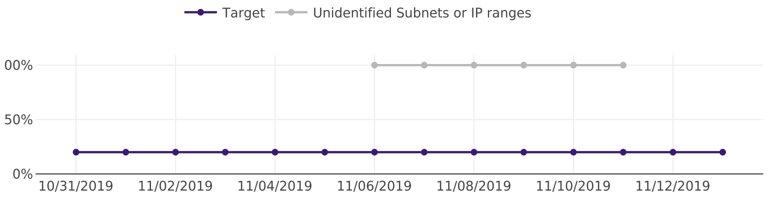
F

Unidentified Subnets or IP Ranges

100.0%

Unidentified Subnets are those that CyGlass sees that you have not labeled. By applying labels, you provide important context to CyGlass in better understanding what threats are most critical to you.





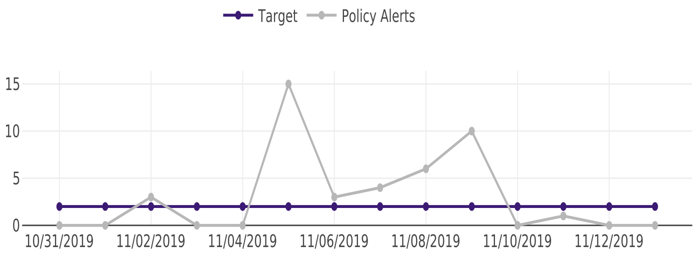
This report has been prepared for Acme. It is for illustrative purposes only and CyGlass is not responsible for any decisions or actions taken based on this information.

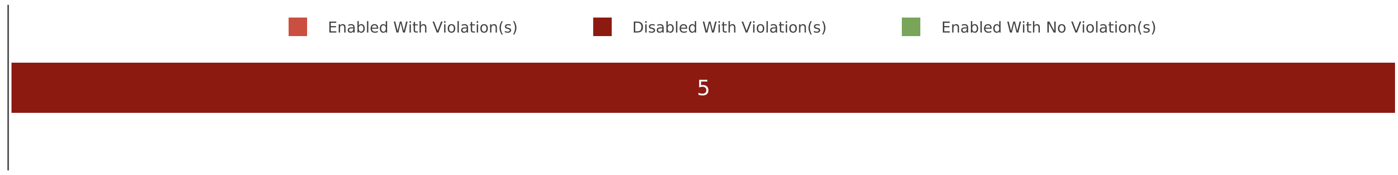
Policy Assurance

C

Policy Alerts

3.0 Per day (Average of past 7 days)

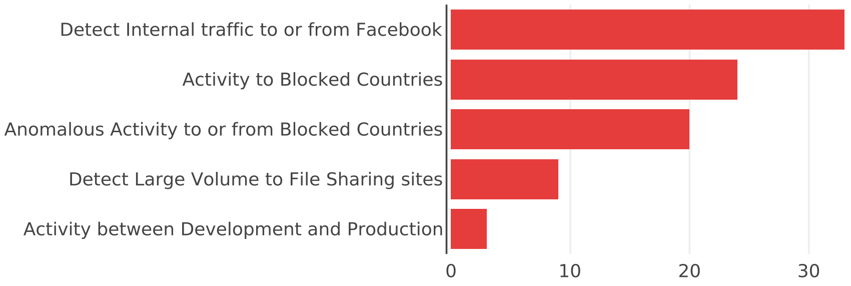




Top 5 Most Common Policy Types

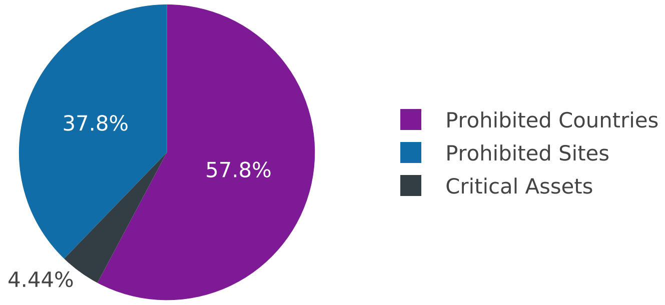
CyGlass monitors your network for violations of activity policies that are important to you.

This chart shows the number of alerts generated for these policies that were active over the previous 19 days.



Policy Alerts by Category

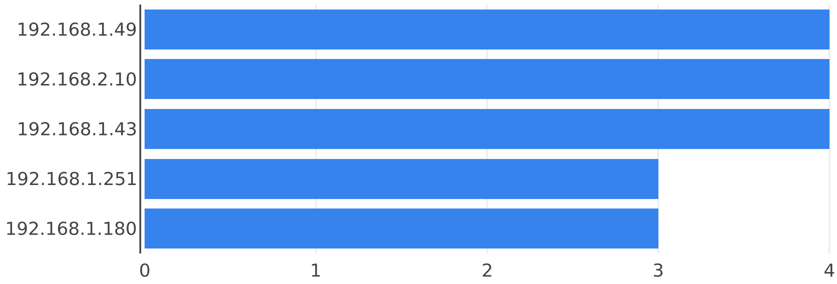
This chart shows the most common categories of alerts generated over the previous 19 days.



Policy Alerts by Asset or IP

These are the assets in your network that were most frequently involved in policy violations.

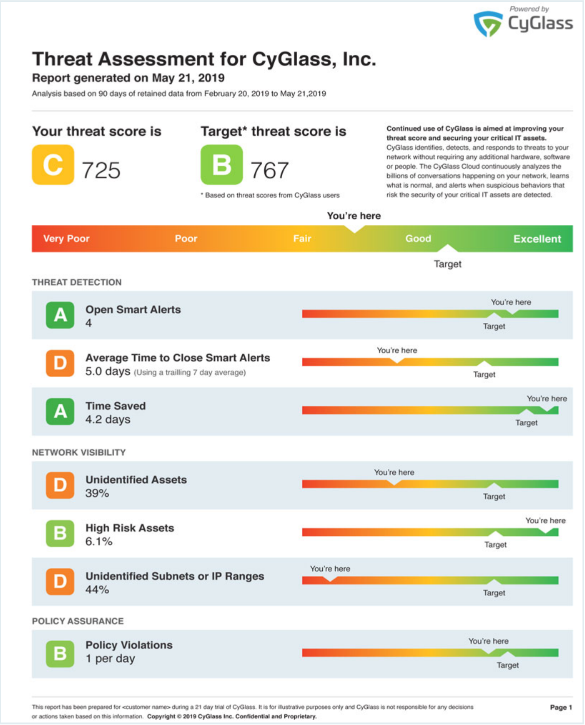
This chart shows the number of alerts generated for these assets over the previous 19 days.



This report has been prepared for Acme. It is for illustrative purposes only and CyGlass is not responsible for any decisions or actions taken based on this information.

How to Use this Report

Whether you are evaluating CyGlass for use or actively protecting your network with it, this report provides you with a quick and easy assessment of your network, enabling you to see where key threats and vulnerabilities are.



Threat Assessment for CyGlass, Inc.

Report generated on May 21, 2019

Analysis based on 90 days of retained data from February 20, 2019 to May 21,2019

Your threat score is C 725

Target* threat score is B 767

* Based on threat scores from CyGlass users

Continued use of CyGlass is aimed at improving your threat score and securing your critical IT assets. 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 risk the security of your critical IT assets are detected.

THREAT DETECTION

A Open Smart Alerts
4

D Average Time to Close Smart Alerts
5.0 days (Using a trailling 7 day average)

A Time Saved
4.2 days

NETWORK VISIBILITY

D Unidentified Assets
39%

B High Risk Assets
6.1%

D Unidentified Subnets or IP Ranges
44%

POLICY ASSURANCE

B Policy Violations
1 per day

This report has been prepared for <customer name> during a 21 day trial of CyGlass. It is for illustrative purposes only and CyGlass is not responsible for any decisions or actions taken based on this information. **Copyright © 2019 CyGlass Inc. Confidential and Proprietary.** Page 1

Threat Score

Your threat score provides you an overall measure of threats and vulnerabilities that CyGlass detects. The score enables you to track your progress over time and compare your network to that of other CyGlass customers.

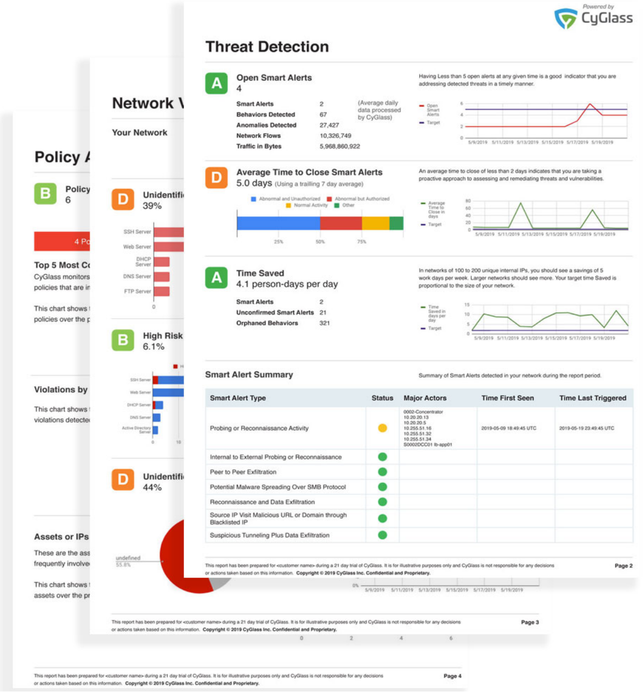
The score is calculated like a credit score, on a scale of 300 to 850. Your letter grade reflects your performance compared to others. Most get a B. But we all strive for an A.

Metrics

CyGlass tracks 7 key metrics across 3 key areas: Network Visibility, Policy Assurance and Threat Detection.

These metrics allow you to see your progress in each area so you can work on increasing your score.

The additional pages of the report provide more detail about each one of these three areas.



Threat Detection

A Open Smart Alerts
4

Smart Alerts	2	(Average daily data processed by CyGlass)
Behaviors Detected	67	
Anomalies Detected	27,427	
Network Flows	10,326,749	
Traffic in Bytes	5,968,860,922	

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

D Average Time to Close Smart Alerts
5.0 days (Using a trailling 7 day average)

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

A Time Saved
4.1 person-days per day

Smart Alerts	2
Unconfirmed Smart Alerts	21
Orphaned Behaviors	321

In networks of 100 to 200 unique internal IPs, you should see a savings of 5 work days per week. Larger networks should see more. Your target time Saved is proportional to the size of your network.

Smart Alert Summary

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

Smart Alert Type	Status	Major Actors	Time First Seen	Time Last Triggered
Probing or Reconnaissance Activity	●	0002-Concentrator 10.20.20.13 10.20.20.5 10.255.51.16 10.255.51.32 10.255.51.34 S0002DCC01 lb-app01	2019-05-09 18:49:45 UTC	2019-05-19 23:49:45 UTC
Internal to External Probing or Reconnaissance	●			
Peer to Peer Exfiltration	●			
Potential Malware Spreading Over SMB Protocol	●			
Reconnaissance and Data Exfiltration	●			
Source IP Visit Malicious URL or Domain through Blacklisted IP	●			
Suspicious Tunneling Plus Data Exfiltration	●			

This report has been prepared for <customer name> during a 21 day trial of CyGlass. It is for illustrative purposes only and CyGlass is not responsible for any decisions or actions taken based on this information. **Copyright © 2019 CyGlass Inc. Confidential and Proprietary.** Page 2

Metric Details

Pages two, three and four provide more details into the key metrics displayed on page one. Each metric includes a fourteen day trend chart showing how the metrics has varied over the preceding 14 days.

It also contains additional charts that show specific information about the metrics.

The Manual Effort Saved metric is Not Applicable when there were no Smart Alerts or Behaviors generated during the reporting period.

The Unidentified Assets metric is Not Applicable when there are no assets defined in the system nor any detected undefined assets.

The High Risk Assets metric is Not Applicable when there are no assets defined in the system.

The Unidentified Subnets or IP Ranges metric is Not Applicable when there are no subnet defined in the system nor any detected undefined subnets.

The Policy Alerts metric is Not Applicable when there are no active policies.

This report has been prepared for Acme. It is for illustrative purposes only and CyGlass is not responsible for any decisions or actions taken based on this information.