

# Microsoft 365 Defense Goal Report

## Acme Corporation

**Continued use of CyGlass is aimed at improving your threat score 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.

[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

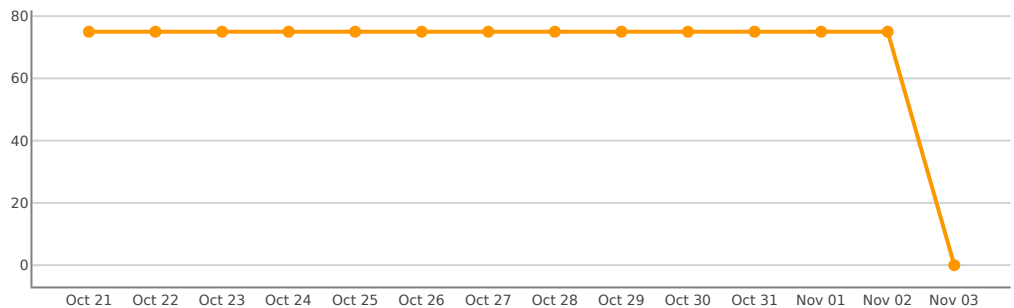


## Network Defense Overview

### Threat Score



### Threat Score History



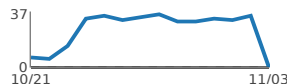

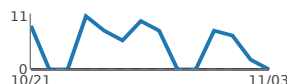



2/3 Objectives are not compliant



3/5 Controls are not compliant



## Top Network Threats

THREAT SCORE	CONTROL DESCRIPTION	REMEDATION	ALERT HISTORY	COMPLIANCE
75	<b>3. Suspicious Login Activity</b> <b>3.1 Possible Brute Force Account Access Attempt</b> 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	<b>1. Exfiltration by an Internal Actor</b> <b>1.2 Suspicious Rate of File Activity</b> 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	<b>1. Exfiltration by an Internal Actor</b> <b>1.1 Internal Files Shared Externally</b> 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


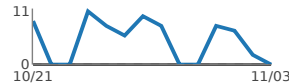
55

#### 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	<b>1.1 Internal Files Shared Externally</b> 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	<b>1.2 Suspicious Rate of File Activity</b> 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



0

#### 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	<b>2.1 Suspicious Access Location</b> 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	<b>2.2 Suspicious Access Time</b> 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


75

#### 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	<b>3.1 Possible Brute Force Account Access Attempt</b> 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

### 1.1 Internal Files Shared Externally

### External file sharing may signal an exfiltration attempt.

## Remediation

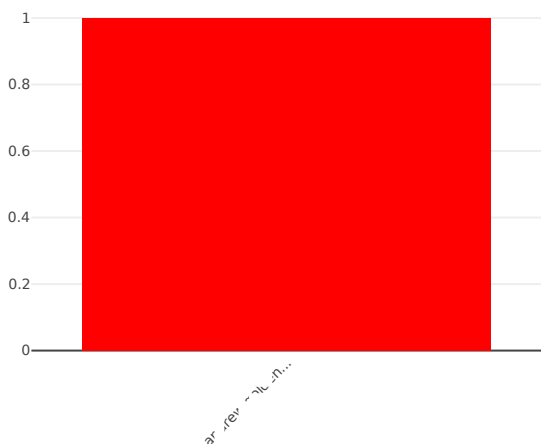
We suggest removing file-sharing permissions from high-value data and documents and following a least-privilege policy across all user accounts. We also suggest investigating this activity to determine if it was legitimate.

### Alert Detail

### Distribution of Policy Alerts by User

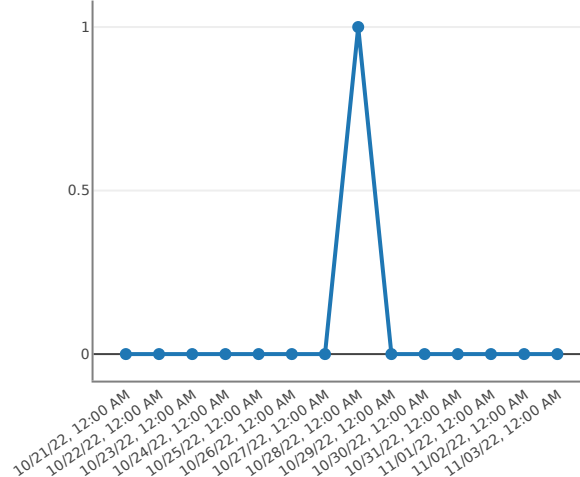
### Distribution of Policy Alerts by User

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



### 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

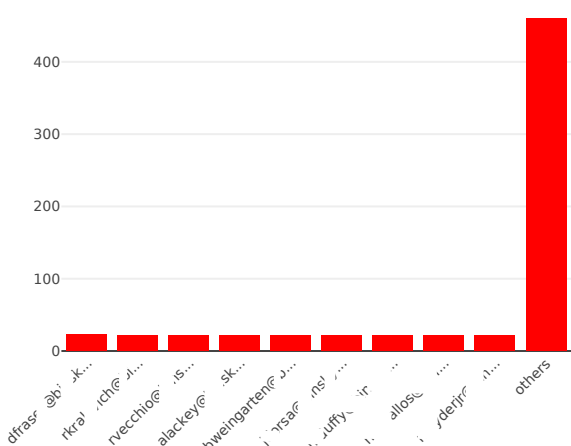
We recommend enabling multi-factor authentication and enforcing a password complexity policy. We also suggest investigating these access attempts for unusual login time or location. If you are concerned this access is not legitimate, we recommend contacting this user and forcing a password reset.

### Alert Detail

### Distribution of Policy Alerts by User

### Distribution of Policy Alerts by User

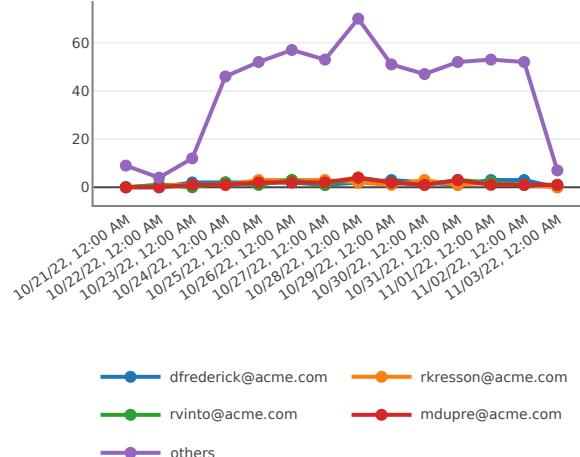
Number of Possible Brute Force Account Access Attempt Policy Alerts, broken down by user



### Distribution of Policy Alerts Associated with User Over Time

### Distribution of Policy Alerts Associated with User Over

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



1.2 Suspicious Rate of File Activity

Control Detail

This policy is based on activity baselining, and triggers when CyGlass' machine learning detects a significant change in file activity. An unusual rate of file activity can indicate exfiltration or ransomware encryption.

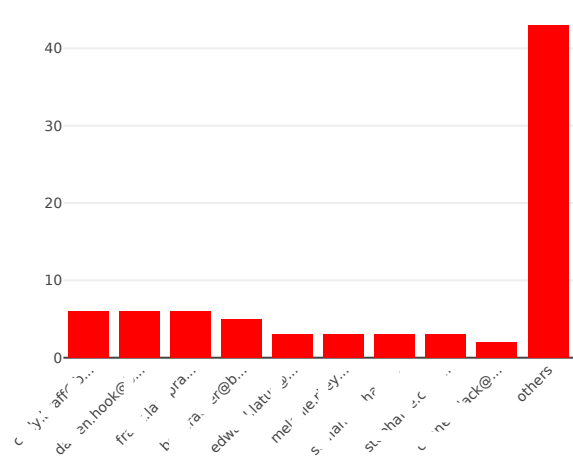
Remediation

We recommend verifying that MFA and password complexity requirements are enabled for involved users and forcing a password reset. We also suggest verifying that this user has not had a recent employment change. To establish whether this alert was generated by attack traffic, we recommend looking for associated suspicious access location, time, or traffic volume alerts and investigating involved files to determine if this activity was legitimate.

Alert Detail

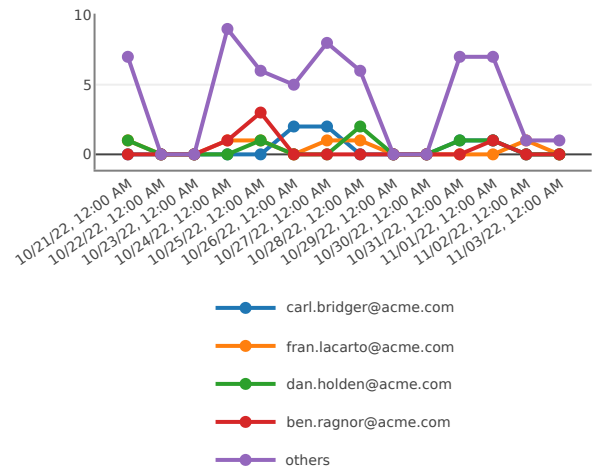
Distribution of Policy Alerts by User

Number of Suspicious Rate of File Activity Policy Alerts, broken down by user



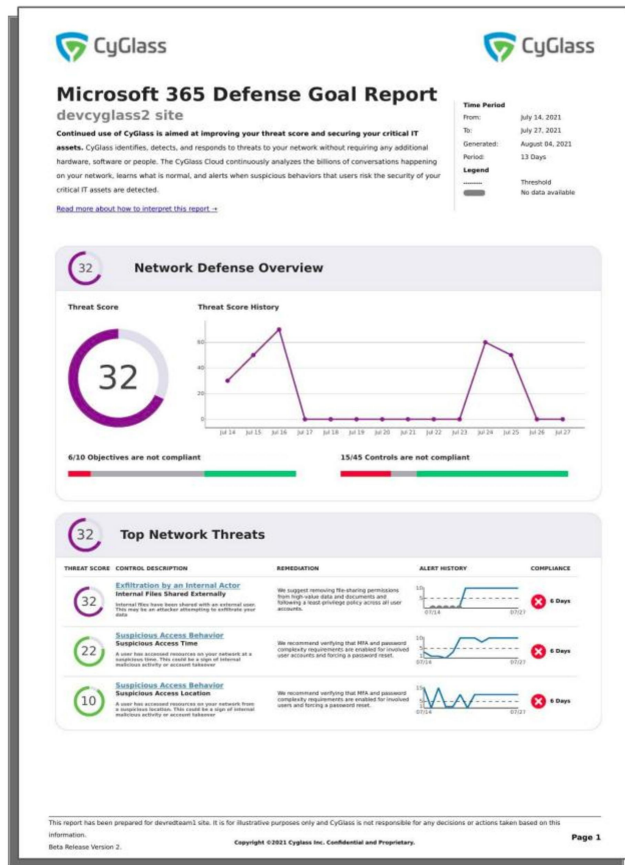
Distribution of Policy Alerts Associated with User Over Time

Number of Suspicious Rate of File Activity Policy Alerts over time



# How to Use this Report

This report is based on M365 security best practices, security features behind the Microsoft 365 E5 paywall, and recommendations from the Cybersecurity & Infrastructure Security Agency (CISA <https://www.cisa.gov/>). This report presents a summary of the controls CyGlass monitors to help you monitor user activity within the Microsoft 365 product suite and identify both exposure and attack behavior.



Page 1 contains a summary of the Microsoft 365 Defense Goal.

## Threat Score History

Your Microsoft 365 Threat Score represents your exposure to cyberattack via the 365 product suite. It is an aggregation of the threat scores for each of the controls that is presented in the report.

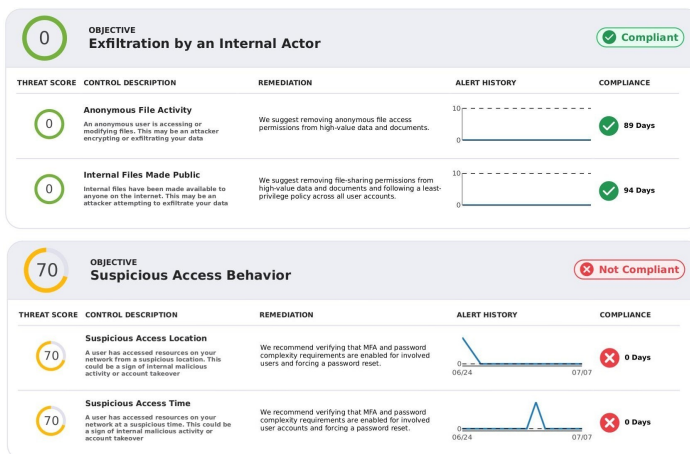
The Microsoft 365 Defense Goal is a collection of Defense Objectives, each organized around a specific prevention area. Each Defense Objective consists of a set of controls that should be enabled and monitored to help prevent attacks via M365 services.

The Threat Score History Chart shows the Defense Goal Threat Score for each day in the report period, and the score on the left shows the highest value recorded in the report period.

The Objective and Control summary charts display the proportion of objectives and controls that are compliant, violated, or which we have insufficient data to evaluate. The stacked bar chart shows green for every objective or control that is compliant, red for those that are violated, and grey for those that we have insufficient data to evaluate.

## Top Network Threats

The Top Network Threats section lists the three highest-risk controls covered in this report. These controls will still be listed in the corresponding Objective section.



## Objective and Control Detail

The remainder of the report contains additional detail for each of the Defense Objectives included in the Defense Goal.

Each section identifies the name of a Defense Objective, its Compliance Status, and the Controls configured to be included in the Objective.

Each Control entry describes the purpose of that control, the threat score associated with violations of this control, a short remediation recommendation, and a line chart with an alert history count.

Finally, each control summary tells you the number of days that the control has been Compliant.

The top Defense Objective in the image to the left is Compliant. We consider a control "compliant" when it is associated with an alert count equal to or less than the configured alert count and threat score thresholds. The lower Defense Objective is not compliant. In this example, all the controls are in violation. A Defense Objective is considered non-compliant if any of the controls associated with it are violated.

### Control Violation Detail and Remediation

For controls that have been violated within the report period, we include a detailed description of both the control and our remediation suggestions.

This policy is based on activity baselining, and triggers when CyGlass' machine learning detects a login far from any previous activity. An unusual access location may be a sign that an account is compromised. It can also indicate a user logging in during off-hours to exfiltrate files.

We recommend verifying that MFA and password complexity requirements are enabled for involved users and forcing a password reset. We also suggest verifying that this user has not had a recent employment change. To establish whether this alert was generated by attack traffic, we recommend looking for associated suspicious access time or traffic volume alerts.

**Distribution of Policy Alerts by User**      **Distribution of Policy Alerts Associated with User Over Time**  
 Number of Possible Brute Force Account Access Attempt Policy Alerts, broken down by user      Number of Possible Brute Force Account Access Attempt Policy Alerts over time

