IDENTITY SECURITY ASSESSMENT

Powered by Managed ITDR

For Quantum Shield Solutions

08-15-2025

In Partnership with

Understanding Your Identity Landscape

104
Total Identities

Billable Breakdown

68
Billable Identities

36
Non-Billable Identities

What are Billable Identities

A **billable identity** is typically "human controlled" and with an assigned Microsoft 365 license, that Huntress actively monitors and protects. While all identities within a tenant are protected, billing only applies to these specific, licensed user accounts, excluding shared mailboxes or unlicensed admin accounts.

License Distribution

- O365_BUSINESS_PR... - 100
- DEVELOPERPACK_E5 - 15
- AAD_PREMIUM_P2 - 96
- MCOCAP - 3
- SPB - 23
- 2 Others - #

A single identity can have multiple Microsoft licenses assigned to it, which is why the total license count will not equal the total number of identities

Usage Location:

United States

Canada

If an identity logs in from a Usage Location that matches their licensed locations, Huntress will allow it and won't send an incident report. This ensures users can always access their accounts from approved countries.

About this Assessment

The Identity Security Assessment provides a summary of your Microsoft 365 Identity Threat landscape. It offers a snapshot of key insights, including license types, application visibility, and potential malicious inbox rules or suspicious logins.

This assessment highlights suspicious activity detected within your environment. If no such activity is found, it shows you the key security areas we constantly watch and what type of threats we look for, including relevant examples.

This is a one-time snapshot of your tenant's current environment.

Prevent Unauthorized Login Attempts with Unwanted Access

Suspicious Login Incidents: 3

We have detected 3 suspicious login attempts in your tenant. Huntress has already alerted you about these incidents.

Showing 1 of 3 incidents

View all Incidents >

Incident Type: Credential Theft Critical

2025-06-17 12:21:27 UTC

What Happened?

Evidence suggests [REDACTED] at 2025-07-02 00:33:58 UTC authenticated from the public IP 1.1.1.1 with the following anomalous behavior indicative of credential theft and malicious account takeover:

- The anomalous authentication attempt(s) occurred from two unmanaged devices, i.e. devices that are not controlled or monitored by an organization's IT policies and security tools.
- The authentication attempts were made without using multi-factor authentication, which is considered anomalous.
- An anomalous authentication from a VPN PIA_VPN
- An anomalous authentication attempt was detected using both Chrome and Other browsers...

Remediations

Disable Identity Huntress Containment Remediation

What is Unwanted Access?

Unwanted Access is a security capability to detect attempts by attackers to infiltrate your Identity Provider account or organization without permission. These efforts commonly involve the theft of login details (like your username and password) or the compromise of active sessions that bypass password requirements. This includes detecting unauthorized VPN access, logins from unusual or unauthorized locations, Adversary-in-the-Middle (AiTM) attacks, token theft, and session theft.

Detect Hidden Inbox Attacks with Shadow Workflows

Malicious Inbox Rule Incidents: 3

We have detected 3 malicious inbox rules in your tenant. Huntress has already alerted you about these incidents.

View all Incidents >

Incident Type: Credential Theft Critical

2025-06-17 12:21:27 UTC

What Happened?

Evidence suggests that at 2025-06-17 12:21:27 we detected an inbox rule named '.', created for the user [REDACTED] to move emails sent from [REDACTED] to the 'Conversation History' folder. Threat actors create or manipulate email inbox rules for malicious purposes, such as forwarding sensitive emails to a threat actor-controlled environment, deleting important messages, or redirecting emails to hide malicious activity.

Threat Descriptions:

Malicious Email Inbox Rules: Threat actors create or manipulate email inbox rules for malicious purposes, such as forwarding sensitive emails to a threat actor-controlled environment, deletin…

Remediations

Disable Identity Huntress Containment Remediation

Disable Inbox Rule Huntress Containment Remediation

Delete Inbox Rule Huntress Containment Remediation

What are Shadow Workflows?

Shadow Workflows is a security capability focused on the most common post-compromise attacker tradecraft. This includes identifying malicious inbox rules, outbound phishing campaigns, and data exfiltration attempts.

Uncover Rogue Applications

Rogue Application Incidents: 0

Great news! **We didn't find any rogue applications in your tenant.** While **12.3%** of all Huntress-protected tenants had a Rogue App detection in the last 10 months, **you can rest easy knowing we're here to catch them if you ever become one.**

Known Traitorware Applications

This is a list of known traitorware applications—a type of rogue application we detect—that Huntress has identified and actively monitors for in various environments.

eM Client

A robust email client often leveraged by attackers due to its extensive capabilities.

PerfectData Software

An application that can export mailboxes for backup purposes.

Newsletter Software Supermailer

Software used for email mass mailing, often abused to send phishing emails.

rclone

Rclone is a command-line program to manage files on cloud storage.

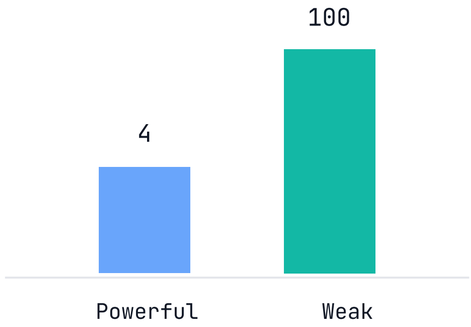
CloudSponge

CloudSponge allows you to export all contacts from and inbox.

68

Total Applications

Application Permissions



Powerful permissions provide broad or administrative access to organizational data, users, or system-wide settings, and can pose a significant security risk if misused. Applications with **weak permissions** have limited access, while those with **"none"** permissions are excluded from this graph. Applications with no permissions often include Microsoft Service Principals that don't require them, or apps from inactive tenants.

What are Rogue Applications?

Rogue Applications is a security capability to detect malicious or abused software within your enterprise environment that attackers use to gain unauthorized access or control. This includes two primary types: Traitorware and Stealthware.

Traitorware is when trusted, legitimate applications are exploited by cybercriminals to perform harmful actions, enabling attacks and data theft.

Stealthware is where attackers create custom OAuth apps for persistence, data theft, and stealthy long-term access.