

# Threat Landscape Assessment

---

## Executive Summary



# What is Threat Landscape Assessment?

It is a comprehensive, complimentary report that provides **5 key insights into the security of your environment**. These are 5 foundational elements of your cybersecurity.

***Know them. Monitor them. Mitigate the threat.***

# About This Executive Summary

You will see 5 sections in this Executive Summary report. Each section is dedicated to each key insight of the security of your environment:

## 01. Sign-In Information

Overview of successful and failed login attempts across the globe.

## 02. Dark Web Scan

The credentials or sensitive information that are sold or exposed.

## 03. Multi-Factor Authentication

Breakdown of MFA enabled and disabled accounts.

## 04. Spoof Protection

Attempts at impersonation targeting your organization.

## 05. Privileged Role Exposure

At-risk accounts with elevated permissions.

# Want More?

Would like to see the full details of the assessment? Want to see the live data? To review the entire assessment, [book a call](#) with a security consultant. Your consultant will walk you through it in detail and answer all your questions.

[Review Your Assessment](#)

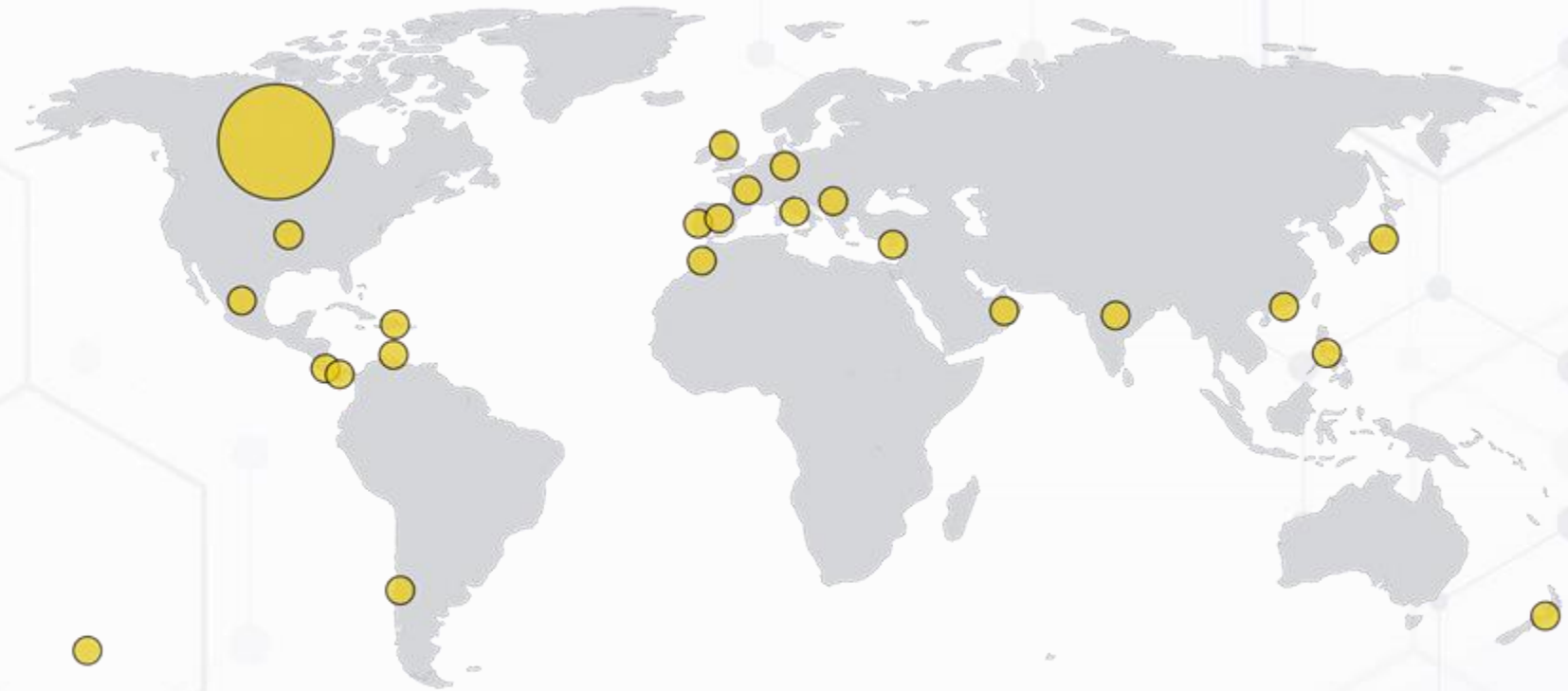
# 01. Sign-In Information





# Successful Login Locations

Shows where users **successfully logged in** to the Microsoft 365 tenant.



Canada	United States	Chile	Oman	United Kingdom	Dominican Republic	Italy	Japan	Hong Kong
136,021	314	68	48	47	14	12	12	9



# Failed Login Locations

Shows where users **failed to log in** to the Microsoft 365 tenant.



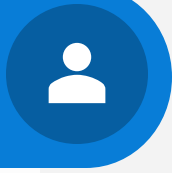
Canada	China	United States	South Korea	India	Russia	United Arab Emirates	Hong Kong
11,590	6,369	2,253	1,848	1,310	1,232	1,132	953

1/11

## 02. Dark Web Scan

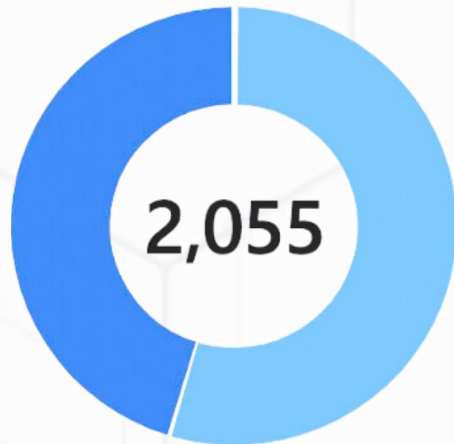






# Number of Compromised Accounts: Internal vs. Guests

Pie chart to show the **total number of internal corporate vs guest accounts** that have had their accounts **found on the dark web**.



Compromised Guests  
**1,120**

Compromised Internal Us...  
**935**

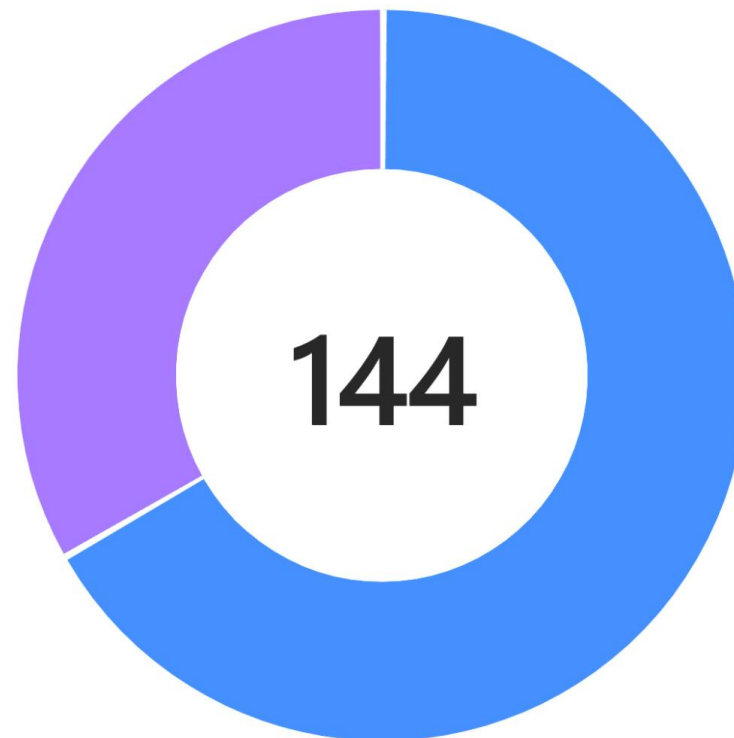
# 03. Multi-Factor Authentication





# Multi-Factor Authentication Status: All Users

Pie chart that displays the number and percentage of MFA enabled and disabled **internal corporate and guest accounts**.



MFA Enabled  
96

MFA Disabled  
48

# 04. Spoof Protection





# Spooof Protection

Displays the **SPF, Microsoft DKIM, DKIM Signing Config Status, and DMARC Records** for all the domains in the Microsoft 365 tenant.

## Spooof Protection

Group	↑↓ LastUpdatedTimeUTC	↑↓ DNSRecord	↑↓ DNSType	↑↓ DomainName	↑↓ itemid	↑↓ Results
▼ me[redacted].com (5)						
	5/21/2024, 1:23:18.870 PM	"v=DMARC1; p=quarantine; sp=quarantine; pct=100; adk...	DMARC	m[redacted].com		⚠ Incomplete
	5/21/2024, 1:23:18.544 PM	"v=spf1 include:spf.protection.outlook.com include:sendg...	SPF	m[redacted].com		✅ Pass
	5/21/2024, 1:23:19.095 PM	FALSE	DKIMSigningConfig	m[redacted].com		❌ Fail
	5/21/2024, 1:23:18.880 PM	No DKIM1 Record Present	MSFTDKIM1	m[redacted].com		❌ Fail
	5/21/2024, 1:23:18.916 PM	No DKIM2 Record Present	MSFTDKIM2	m[redacted].com		❌ Fail
▶ cl[redacted].ca (5)						
▶ cl[redacted].com (5)						
▶ dc[redacted].com (5)						



# Number of Passed, Failed and Incomplete SpooF Protection DNS Records

Tiles to display the total **number of passed/failed/and incomplete DNS records** related to SPF, DKIM, and DMARC.

Total number of domains for **M. ....** is **4**.

Number of Passed, Failed and Incomplete SpooF Protection DNS Records

SPF ✔ Pass 3	SPF ✘ Fail 1	MSFTDKIM1 ✔ Pass 1	MSFTDKIM1 ✘ Fail 3	MSFTDKIM2 ✔ Pass 1	MSFTDKIM2 ✘ Fail 3	DKIMSigningConfig ✘ Fail 4	DMARC ✘ Fail 2	DMARC ⚠ Incomplete 2
--------------------	--------------------	--------------------------	--------------------------	--------------------------	--------------------------	----------------------------------	----------------------	----------------------------

# 05. Privileged Role Exposure





# Number of Active Privileged Accounts in the Microsoft 365 Tenant

Tiles that displays the **total number of privileged accounts** in the Microsoft 365 tenant.

Global Administrator

13

Directory Synchronizati...

3

SharePoint Administrator

3

Teams Communications...

1

Teams Administrator

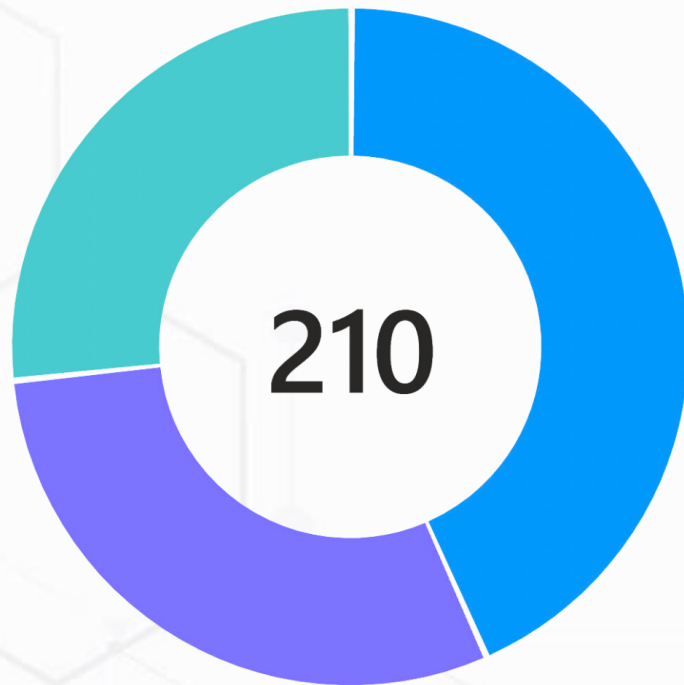
1





# Number of Privileged Accounts with Failed Login Attempts

Pie chart that displays the number of privileged roles that **failed to login**.



# Unlock Your Digital Future



People Matter.



Be Like Gumby.



Do It Right.

Certified



Corporation

## The Right Cybersecurity Starts with the Right Foundations

Contact Us →

From your digital gate to your digital assets, ProServeIT helps provide confidence in your cyber defenses by alerting you when there's a cyber abnormality and **proactively taking action against potential cyber threats** before they become a bigger problem.

There is plenty of evidence of the negative ramifications and negative impact of ignoring or not prioritizing your cybersecurity. Incidents are consistently featured on the news. We want to keep your organization from being another ransomware story.

Let's utilize the right cybersecurity foundations to build the end-to-end safety that your organization, its employees and customers truly deserve.

# Your Microsoft Trusted Partner

As a **Microsoft Solutions Partner**, ProServeIT is relied upon by Microsoft to support and deliver the project needs of organizations using their technology. ProServeIT has won many Microsoft awards and is proud to have our President – Eric Sugar – as a select few, on the Microsoft Security Council in Redmond Washington, helping to shape the future landscape of cybersecurity.

## Microsoft Solution Partner Designations & Specializations

ProServeIT has attained Solutions Partner designations in all six of Microsoft's business solution areas: Business Applications, Data & AI, Digital & App Innovation, Infrastructure, Modern Work, and Security.

As a result of attaining these six solution area designations, ProServeIT has also been awarded a **Solutions Partner for Microsoft Cloud designation**, recognizing broad capabilities across the vast expanse of Microsoft Cloud technologies.



Microsoft  
Solutions Partner  
Microsoft Cloud



Microsoft  
Solutions Partner  
Business Applications




Microsoft  
Solutions Partner  
Modern Work




Microsoft  
Solutions Partner  
Security


Member of  
Microsoft Intelligent  
Security Association



Microsoft  
Solutions Partner  
Data & AI  
Azure



Microsoft  
Solutions Partner  
Digital & App Innovation  
Azure



Microsoft  
Solutions Partner  
Infrastructure  
Azure



# Microsoft Funded Security Workshops

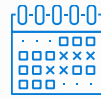
The Microsoft Funded Security Workshops are designed to **assist you with your baseline and advanced security and compliance priorities and initiatives.**



Funded By  
Microsoft



Eligible  
Organizations



Varies

Contact us to check if your organization is eligible for a Microsoft-funded security workshop.

**If you're not eligible**, we'll work with you to explore other options and provide the best possible solutions to enhance your security.

[Check Your Eligibility →](#)



## Threat Protection Workshop

\$11,000 USD or Free for Eligible Organizations

- Strategic plan customized for your organization.
- Gain visibility into immediate threats across email, identity, and data.
- Clarity and support on how to upgrade your security posture for the long term.



## Data Security Workshop

\$11,000 USD or Free for Eligible Organizations

- Understand data security, privacy and compliance risks in your organization.
- Create a safe workplace and protect company assets as well as employee and customer privacy.



## Modern Security Operations

\$10,000 USD or Free for Eligible Organizations

- Gain visibility into threats across email, identity, endpoints, and non-Microsoft data.
- Create a defined deployment roadmap based on your environment and goals.
- Better understand, prioritize, and mitigate potential threat vectors.



## Cybersecurity Assessment

\$2,500 USD or Free for Eligible Organizations

- Cybersecurity maturity level evaluation.
- Discover and address vulnerabilities on clients and servers.
- Understanding risk related to data security and insider threats.
- Recommendations to improve cybersecurity posture and reduce risk exposure.