Microsoft 365 cyber risk assessment

Business email compromise health check

ASCERIS

londonwidgets.com

About this report

The purpose of this report is to provide you with a view of the environment-level and user-level risk in your Microsoft 365 environment. Rather than a broad analysis aimed at general security compliance, this is a targeted risk assessment using a similar methodology to our investigations of cyber incidents. We analyse patterns of behaviour over time rather than configuration settings alone, and we apply our knowledge of the latest techniques being used by threat actors.

Please note that accounts can be categorised as suspicious even when they have not been compromised, for example because the account owner has travelled frequently or has used anonymising services. Accounts may also have a higher risk rating attached to them if successful logins took place but were subsequently blocked by multi-factor authentication.

Summary of findings

- Your environment is licensed principally for: **Microsoft 365 Business Premium**.
- We found **19** *accounts in your environment*, of which **18** were *active accounts*, **18** were *active user accounts*, **17** were *active accounts with mailboxes*, **17** were *active user accounts with mailboxes*, **17** were *licensed accounts*, and **zero** were *guest users*.[1]
- We found **three** accounts with a **risk rating of high** (15.79% of the total).
- We found **two** accounts with a **risk rating of medium** (10.53% of the total).
- We found **six** active user mailboxes with **a different audit log age limit** to the tenant audit log age limit.
- There were **eight** accounts that did not have an enforced or enabled **multi-factor authentication** status (44% of the total, excluding guest accounts).
- There was **one** active user account with a disabled or undefined **strong password requirement** (7% of the total, excluding guest accounts).
- There were seven active shared or resource mailboxes that **permitted direct sign-ins** (78% of the total).

[1] For detailed definitions, please refer to the Appendices.

Key recommendations

- **Block legacy authentication protocols.** Legacy authentication protocols such as POP3, IMAP and SMTP are older protocols that may be needed to support legacy systems and email clients. Even if multi-factor authentication is enabled on your environment, a threat actor can circumvent it if legacy authentication is permitted (enabling a threat actor to gain unauthorised access with only a username and password). Legacy protocols can also be used by threat actors to create complete copies of mailboxes. Legacy authentication is enabled by default on Microsoft 365, and was enabled for your users. Consider reviewing legacy authentication activity with a goal of blocking it or limiting its use in your environment with user-level settings, security defaults or conditional access policies. To avoid unintended loss of access to legacy services we recommend that you conduct an analysis of legacy connections before fully implementing the policy, potentially including a simulation of the new policy in test mode or for specific groups/departments.
- **Protect against brute force attacks.** Brute force attacks are automated attempts to breach accounts by trying different combinations of usernames and passwords until a correct combination is found. Repeated attempts to compromise accounts using brute force attacks are relatively common, and just one successful attempt is enough to lead to an account takeover. Your environment has undergone periods of sustained attack from frequent failed logins against multiple accounts. Deploy multi-factor authentication so that even successful attempts will not lead to compromise. Also consider applying stricter smart lockout policies to reduce the window of opportunity for threat actors.
- **Control third-party application consent grants.** End users can connect third-party applications to their Microsoft 365 accounts to access additional services. But third-party applications can be leveraged by threat actors to compromise accounts through consent phishing, which relies on the user providing authorisation to a malicious web app. Application consent grants can be used by threat actors to gain access to user data and maintain persistence. Your users can currently consent to applications, including unverified applications, on behalf of the entire organisation. Consider limiting your users so that they can only consent to applications for themselves and only those that have been published by a verified publisher. Also consider enabling the admin consent workflow to manage user application requests.
- **Block direct sign-ins to shared mailboxes**. Shared mailboxes allow multiple users to access the same mailbox. When a shared mailbox is initially set up, an associated account and system-generated password are created. A shared mailbox should be configured to block direct sign-ins to the account which, by default, are permitted. Microsoft also recommends that resource mailboxes such as room, equipment and scheduling mailboxes should block direct logins. During our assessment we identified multiple shared and equipment mailboxes that permitted direct sign-ins. Consider using controls in the Microsoft 365 Admin Center to block direct sign-ins to all shared mailbox accounts in your environment.

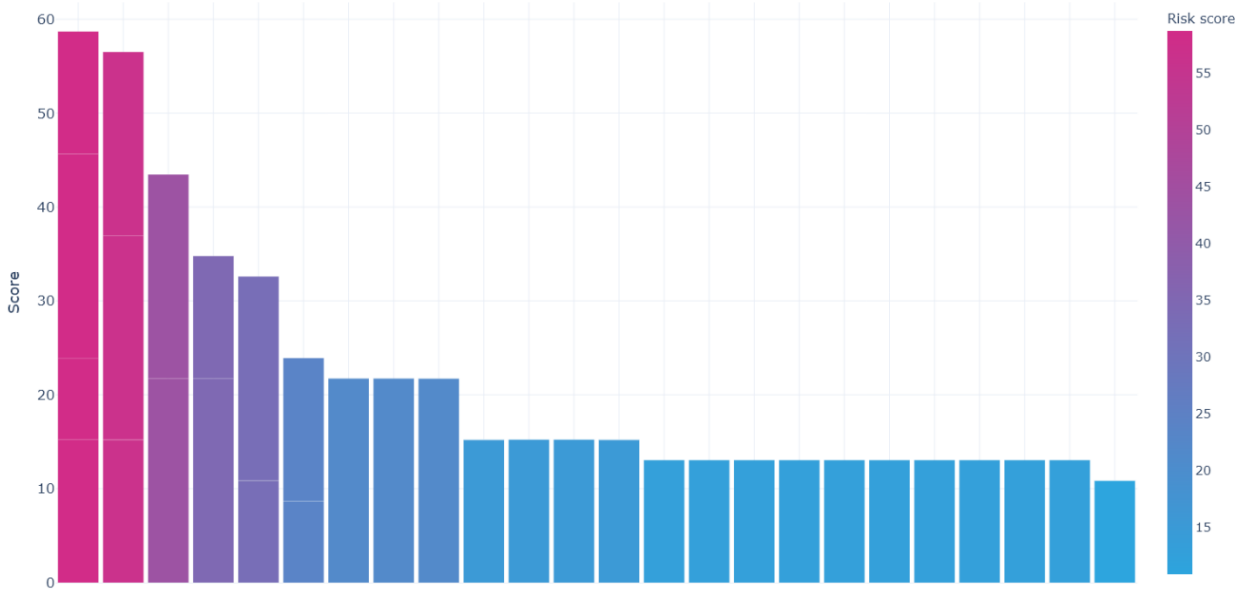
Risk scores and ratings by account

When a cyber incident occurs, it is important to quickly establish what happened and who was affected. By assessing the risk factors exhibited by certain events and accounts, we gain insight into the user accounts at the greatest risk. An understanding of risk factors is also beneficial for proactive risk assessments because it can help to identify suspicious behaviour, higher risk activity, and unexpected user behaviour.

A risk score has been generated for all user accounts observed on your Microsoft 365 environment[2]. The risk score is automatically generated based on the risk factors that are present, using a scale between 0 and 100. An account with a score of 0 has no risk indicators, whereas an account with a score of 100 has triggered all risk indicator groups. Risk indicator groups have different weights, so some groups contribute more to the score than others.

Risk rating	Total	Percentage of total
High risk	3	1.55%
Medium risk	2	1.04%
Low risk	79	40.93%
Very low risk	109	56.48%
Total	193	100.00%

The following chart shows risk scores across your environment. Accounts with a risk score of zero are not displayed.



In context: the chart above shows the distribution of risk scores across all accounts. Accounts with a risk score of zero are not displayed. The average user risk score for your environment is **2.85.**

[2] Every user account that is present in an event log is assigned a risk score, including inactive, internal, system, resource and guest accounts.

The following table shows the accounts that display a higher level of risk in your environment.

Account name	Email address	Risk score	Risk rating
Gemma Tillman	gemma.tillman@londontravelwidgets.com	59.31	High risk
Ralph Walls	ralph.walls@londontravelwidgets.com	58.71	High risk
Magnus Robson	magnus.robson@londontravelwidgets.com	41.22	High risk
Andrew Harris	admin@londontravelwidgets.com	32.86	Medium risk
Carol Maynard	carol.maynard@londontravelwidgets.com	31.61	Medium risk

Risk factors by account

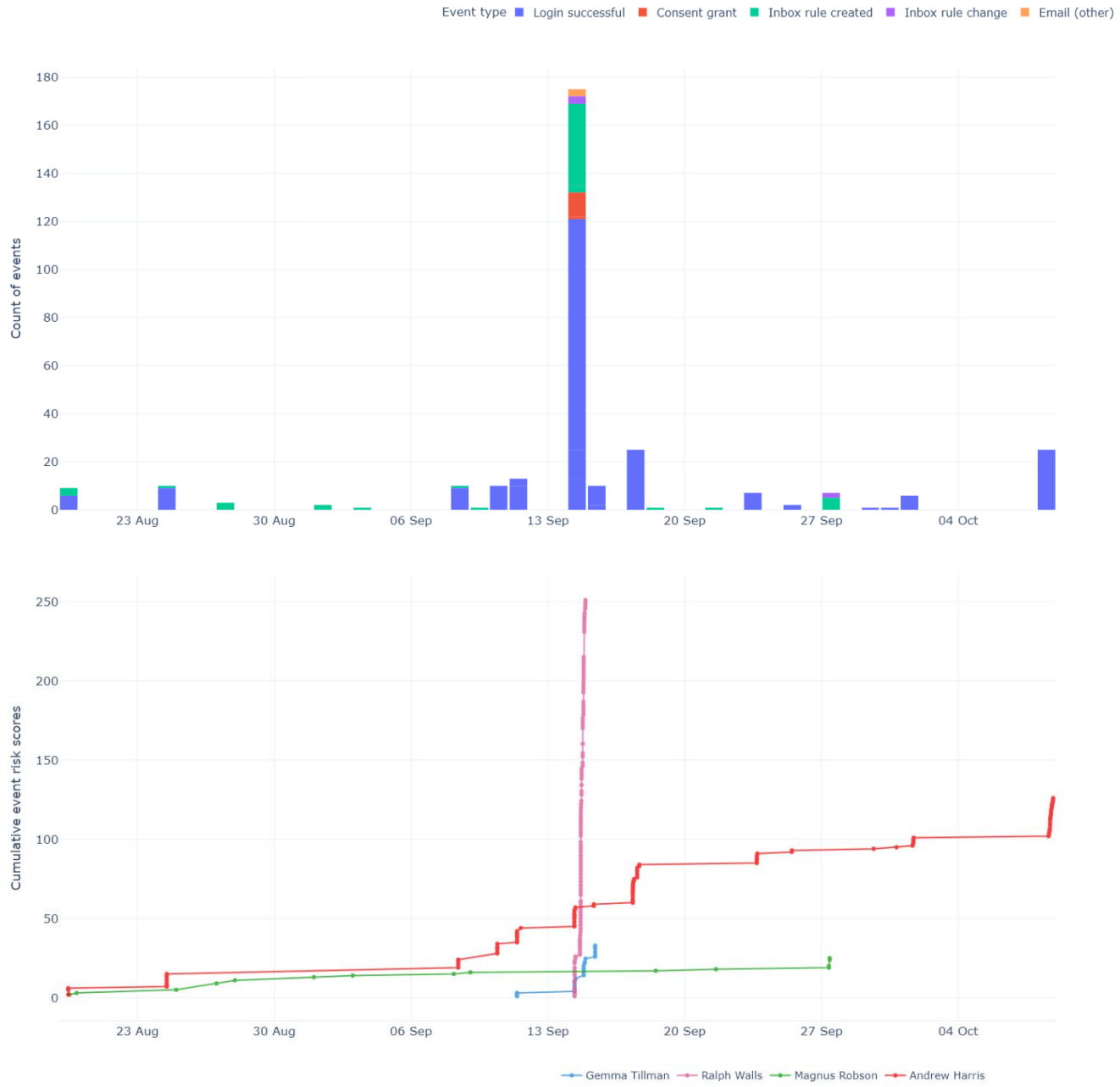
This section provides the risk factors we observed for all accounts with a medium or high risk of compromise. Use these risk factors (which are defined in the Appendices) to understand what contributed to the risk score for each account. When conducting your review of accounts to determine whether they should be investigated, you may need to speak with the account owner (for example, to check whether they were on holiday or travelling on certain dates).

The following table provides the risk factors we observed against accounts with a medium or high risk of compromise.

	HIGH RISK				MEDIUM RISK			LOW RISK		
Account name	Legacy protocols	Unusual countries	Anonymous connections	Mailbox rules	Asceris blacklisted IPs	Recent abusive IPs	Consent grants	Frequent failed logins	New mobile devices	Suspicious speeds
Gemma Tillman	2	4	26	-	-	2	-	-	-	2
Ralph Walls	2	133	156	1	2	5	-	23	-	12
Magnus Robson	-	4	21	-	-	-	-	-	-	-
Andrew Harris	-	-	-	1	-	-	-	20	-	-

Suspicious activity across the environment

We preserve log data from a range of data sources and a variety of event types. Event dates and types can help to identify unusual activity and time periods of interest. We also calculate risk scores for every event we capture at this stage of the investigation. Examining this data side by side can reveal when suspicious activity occurs in specific accounts, and when an environment is under sustained attack against one or more accounts. The charts below show suspicious events by type over time, and the cumulative risk scores over time for accounts with a medium or high risk of compromise.



Individual risk factors

Multi-factor authentication

During our assessment we assess whether multi-factor authentication is active and whether the strong methods of authentication supporting it are registered (e.g. a phone number or an authenticator application). Multi-factor authentication is a secure form of authentication that uses multiple credentials to prove the identity of an individual before they can gain access to a device or service.

Multi-factor authentication can be enabled at the account or environment level. It can be applied by using mailbox configuration, conditional access policies or the security defaults feature. The following sub-sections provide a partial view of the many different ways that multi-factor authentication can be deployed.

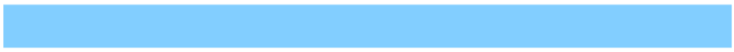
The following chart provides a view of how many user accounts have an enforced or enabled multi-factor authentication status at the account level.

44% of active user accounts have an enforced or enabled multi-factor authentication status in mailbox configuration (excluding guest accounts)

From a total of 193 active user and guest accounts, there are 43 with a multi-factor authentication status of enforced (dark blue), 42 with a status of enabled (blue), 108 with an inactive status (pink), and 0 that are guest accounts (grey)

The following chart provides the total number of enabled user accounts who have at least one registered strong authentication method (irrespective of whether multi-factor authentication is enabled or enforced).

100% of active user accounts have at least one registered method of strong authentication (excluding guest accounts)



From a total of 193 active user and guest accounts, there are 193 with at least one registered method of strong authentication (blue), and 0 with none (pink)

Legacy authentication

One of the reasons that certain legacy authentication protocols such as POP3, IMAP and SMTP are less secure is that they do not support multi-factor authentication. To support older email clients, some organisations decide not to block legacy authentication protocols. However, events linked to legacy authentication protocols could represent an attempt to bypass multi-factor authentication and gain unauthorised access to accounts with only a username and password. Legacy protocols can also be used by threat actors to create complete copies of mailboxes. Note that some protocols such as Exchange Web Services can use either legacy or modern authentication, and are therefore not flagged in this section even if there are events associated with them.

Legacy authentication can be blocked at the account or environment level. These blocks can be applied by using mailbox configuration, authentication policies, conditional access policies, the security defaults feature, or a basic authentication block. The following sub-sections provide a partial view of the many different ways that legacy authentication can be restricted.

Basic authentication block

Microsoft has not applied an automatic Basic Authentication Block to your environment. In the absence of other controls, legacy authentication may be enabled on your accounts.

Legacy authentication blocking using mailbox configuration

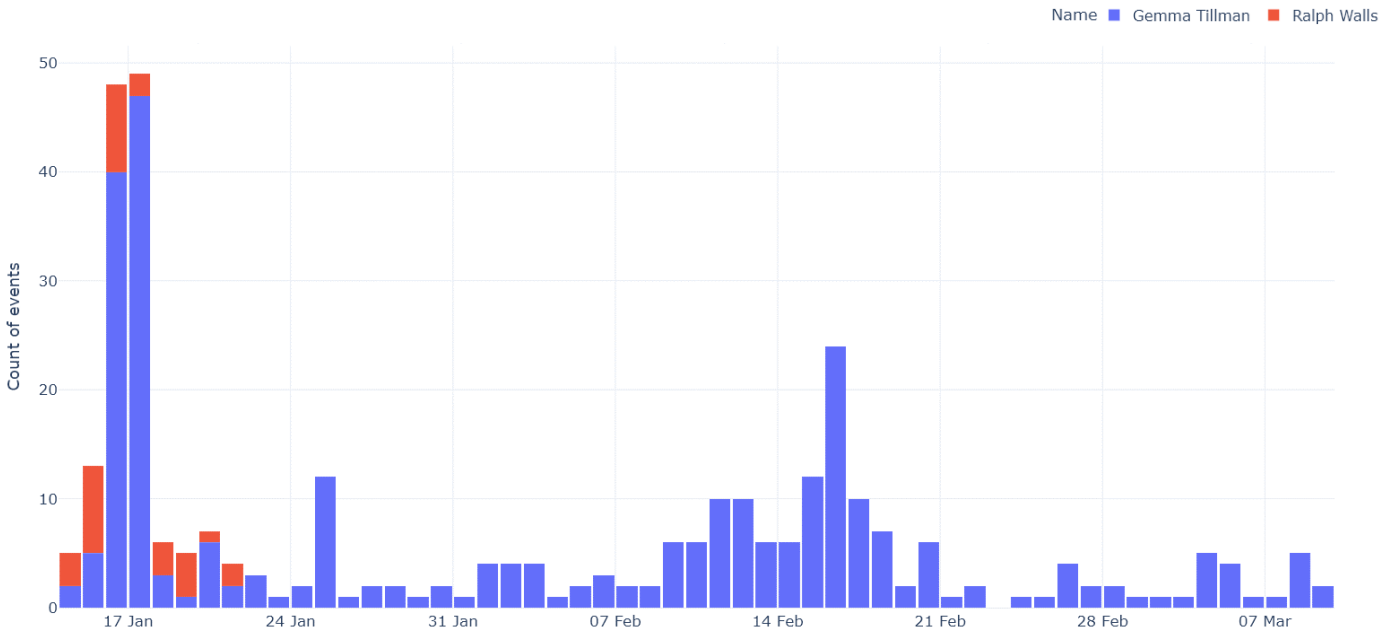
The following chart provides a view of how many accounts have the POP3, IMAP and SMTP Authentication protocols disabled at the user-level.

0% of user accounts have legacy authentication protocols disabled at the user-level

From a total of 63 active mailboxes, there are 0 with disabled legacy authentication (blue), and 63 with at least one legacy protocol set to enabled (pink)

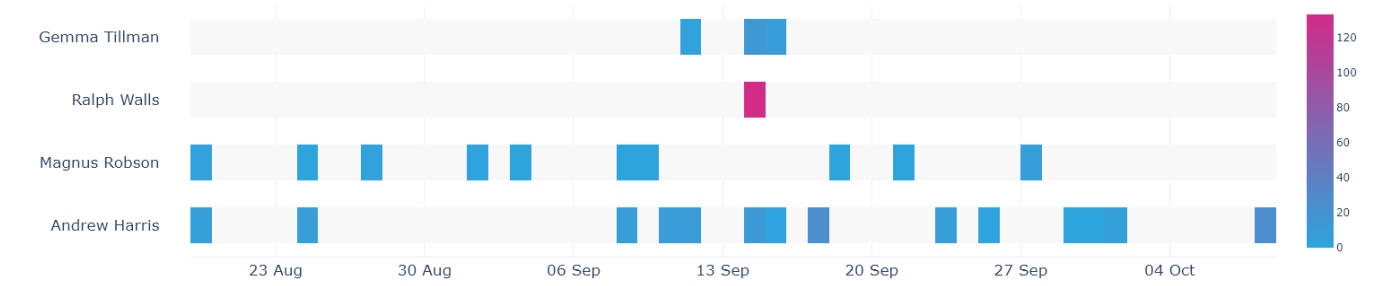
Legacy authentication activity

The following chart shows events linked to legacy authentication protocols. Only successful events are displayed (failed login attempts using these protocols are not).



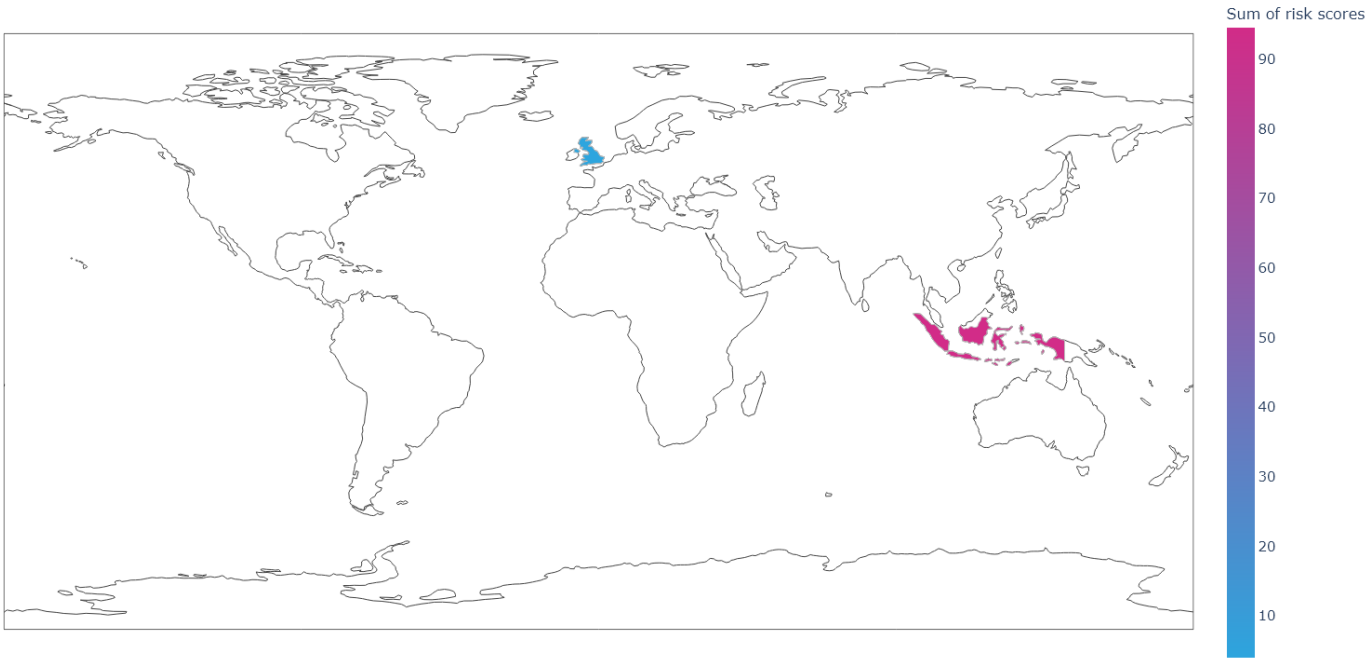
Anonymous connections

The use of VPNs and other anonymising services can disguise the real location of an individual, so they are frequently used for business email compromise attacks. When we link the IP addresses observed on your environment to a physical location, we also identify those that have been anonymised. Comparing an account's pattern of VPN use can help to distinguish normal use against use by a threat actor. However, note that anonymising services can be used for legitimate purposes as well as illicit. The following chart shows the number of events linked to anonymous or TOR networks over the time period under investigation, for each user account that shows some anonymous usage. Failed logins linked to anonymising services are not displayed in the chart.



Unusual countries

Suspicious events from IP addresses that geolocate to locations not typically associated with your organisation can help to identify suspicious activity. Threat actors may select a server in a different country to mount an attack.



Account name	City and country	Continent	Postal code	Organisation	VPN or TOR?	Date range
Gemma Tillman	Colombo, Sri Lanka	Asia	80335	Security Firewall Ltd	Yes	2020-09-14 20:04 to 2020-09-14 20:06
Magnus Robson	Nicosia, Cyprus	Europe	190980	A.b Internet Solutions	Yes	2020-08-24 23:43 to 2020-08-27 23:44
Ralph Walls	São Paulo, Brazil	South America	190980	ExpressVPN	Yes	2020-09-14 15:50 to 2020-09-14 16:50
Ralph Walls	Strasbourg, France	Europe	90012	Host Europe GmbH	Yes	2020-09-14 16:11 to 2020-09-14 19:00
Ralph Walls	Nairobi, Kenya	Africa	10010	Angani	-	2020-09-14 15:23 to 2020-09-14 16:24
Ralph Walls	Colombo, Sri Lanka	Asia	838	Security Firewall Ltd	Yes	2020-09-14 19:57 to 2020-09-14 20:02

Mailbox rules

Mailbox forwarding rules can be used by threat actors to covertly relay messages to external email addresses under their control, and can also be used as an evasion tactic to hide certain messages from the account owner. The following table shows mailbox rules in the environment that have suspicious attributes; for example, they forward or redirect messages to an external email address, delete messages, or move them to infrequently used folders such as RSS Feeds.

Account name	Date created	Event type	City and country	Geolocation organisation	Description
Magnus Robson	2020-08-24 23:43:31	Inbox rule created	Nicosia, Cyprus	A.b Internet Solutions	If the message: the message was received from 'Carol Maynard' Take the following actions: forward the message to 'external_user_ hcadsqzb@protonmail.com' and stop processing more rules on this message

Recent abusive IP addresses

System administrators and cyber security professionals frequently report IP addresses engaging in malicious behaviour to online databases of abusive activity. We cross-reference the IP addresses being used to sign into your environment with one of these databases. The following table sets out all IP addresses that have been reported as malicious in the last 90 days, and which have been linked to medium-risk and high-risk accounts during the time period under investigation. Note that IP addresses can be assigned to new devices over time, so an IP address known with certainty to be malicious could be used by a non-malicious device and account.

IP address	Account name	City and country	Organisation	Connection types	Asceris blacklist?	Confidence score[3]	Date range
148.252.128.189	Ralph Walls	United Kingdom	Vodafone	iPhone	-	11	2020-09-20 22:36:47 to 2020-09-21 02:53:29
85.255.232.57	Magnus Robson	United Kingdom	Vodafone	iPhone	-	24	2020-10-24 21:08:19 to 2020-10-25 09:22:15

[3] This confidence score is the rating (scaled 0 to 100) applied by the online database to describe how confident they are, based on user reports, that an IP address is entirely malicious.

Consent grants

End users can connect third-party applications to their Microsoft 365 accounts to access a range of additional services and capabilities. However, third-party applications can be leveraged by threat actors to compromise accounts through consent phishing, which relies on the user providing authorisation to a malicious third-party web app. If a user grants access to an unusual or suspicious application, it could be a sign that the account has been compromised. The following table sets out all third-party application consent grants by medium-risk and high-risk accounts during the time period under review.

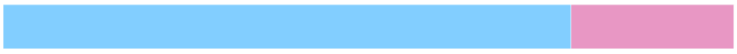
Date and time	Account name	Email address	Application name
2020-09-23 13:59:19	Gemma Tillman	gemma.tillman@londontravelwidgets.com	Zoom
2020-11-09 14:37:23	Ralph Walls	ralph.walls@londontravelwidgets.com	Polly
2020-11-11 11:30:27	Magnus Robson	magnus.robson@londontravelwidgets.com	Office 365 Message Encryption Portal
2020-11-11 16:23:55	Andrew Harris	admin@londontravelwidgets.com	Microsoft Photos
2020-11-16 11:39:41	Carol Maynard	carol.maynard@londontravelwidgets.com	SMART Account

Shared and resource mailboxes

Shared mailboxes allow multiple users to access the same mailbox. When a shared mailbox is initially set up, an associated account and system-generated password are created. A shared mailbox should be configured to block direct sign-ins to the account which, by default, are permitted. Microsoft also recommends that resource mailboxes such as room, equipment and scheduling mailboxes should block direct logins.

The following chart provides the total number of shared and resource mailboxes that block direct logins.

78% of active shared or resource mailboxes block direct sign-ins



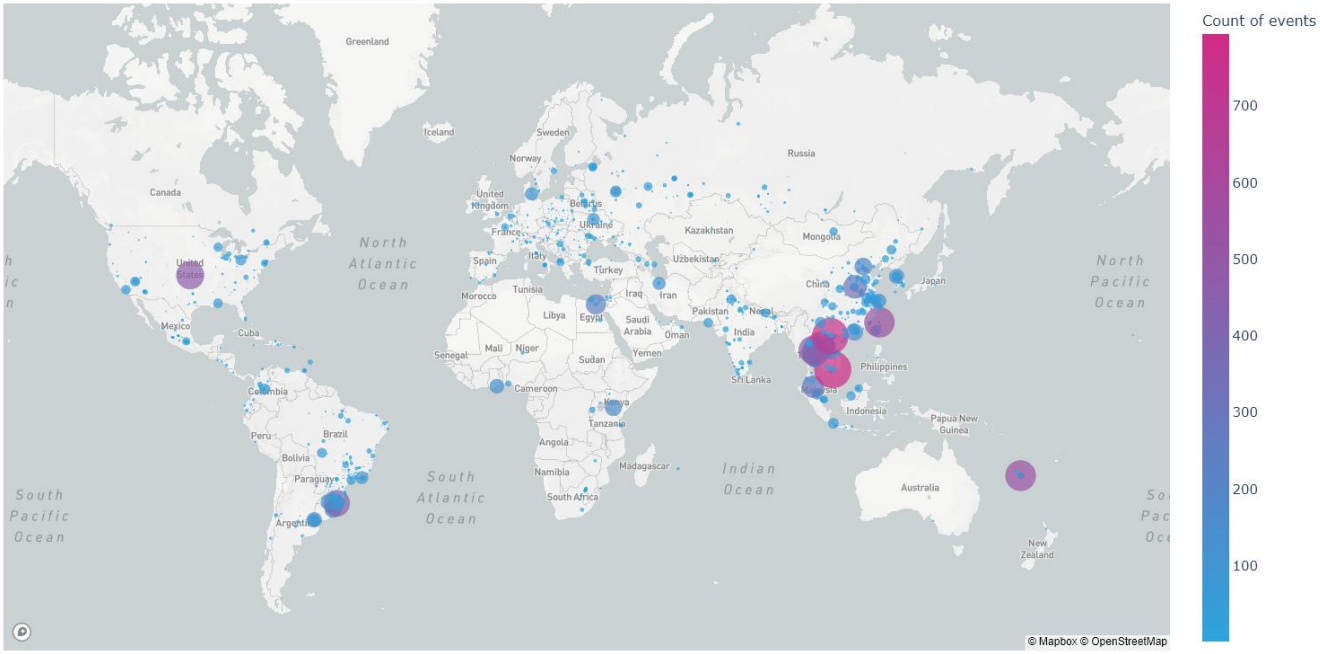
From a total of nine shared or resource mailboxes, there are seven that block direct sign-ins (blue), there are two that do not block direct sign-ins (pink), and there are zero inactive shared or resource mailboxes (grey)

Attempts to compromise accounts

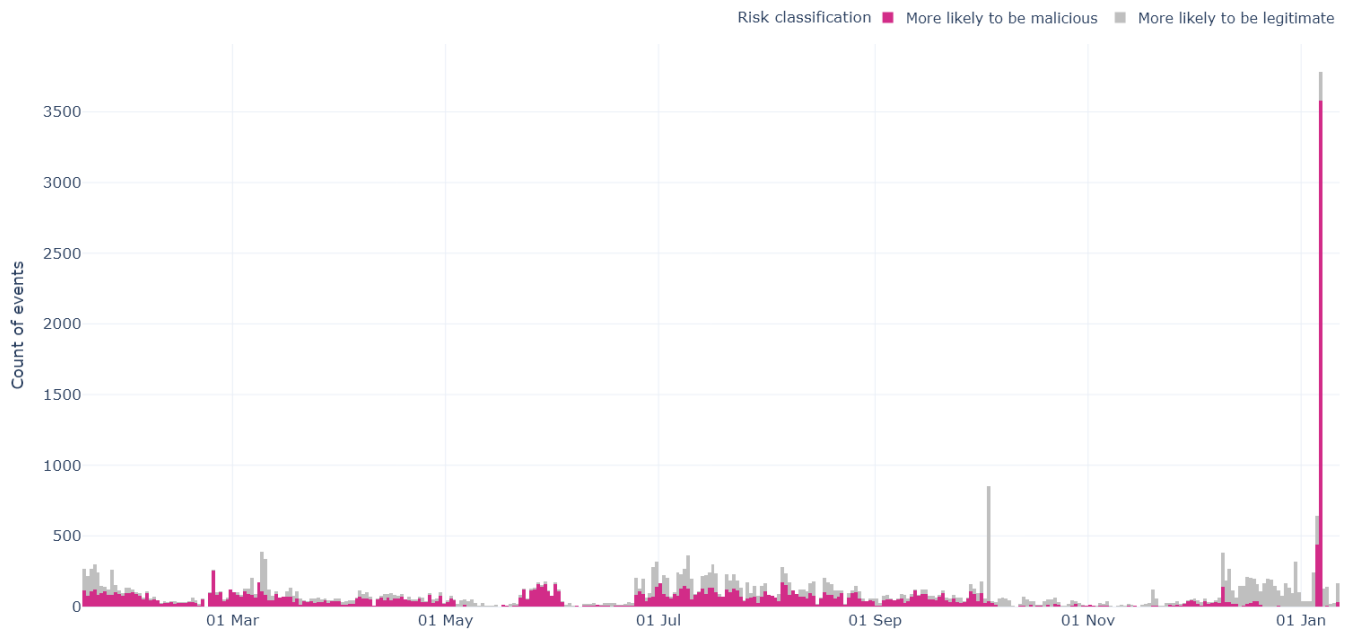
It is common for environments to be targeted regularly and for threat actors to use a range of techniques in their attempts to compromise user accounts. A large number of failed login attempts against multiple accounts can represent brute force attacks and can precede a successful attempt to compromise an account. This section presents details of failed logins, which can show that unauthorised attempts are being made by a threat actor to access an account. Note that failed logins can also occur when a user is unable to log into their account (for example, by entering an incorrect username or password) or when an application with a stored password is unable to authenticate correctly (for example, following a password reset).

Failed logins by location

The following map shows the number and location of failed login events during the period under review.



The following chart shows the number of failed logins over time, classified depending on whether they are more likely to be legitimate or malicious (based on their calculated risk scores).



The following table sets out details of failed logins that are more likely to be malicious (based on their calculated risk scores).

Account name	Organisations	Countries	Connection types	Date range	Count of failed logins
Andrew Harris	Hydra Communications Ltd	United Kingdom	Web browser; BAv2 ROPC	2020-01-04 19:13 to 2021-01-04 19:13	1530
Magnus Robson	Hydra Communications Ltd	United Kingdom	Web browser; BAv2 ROPC	2020-01-26 15:43 to 2021-01-06 10:51	33
Gemma Tillman	Amarutu Technology Ltd; Security Firewall Ltd	Sri Lanka	Web browser	2021-01-08 00:42 to 2021-01-08 00:42	10

Assessment of your logging configuration

The way that your environment is configured and the features available in your product subscription determine the volume and variety of logging data that is captured and available to us. This section identifies environment-level and user-level characteristics.

Environment-level logging configuration

Your configuration has the following characteristics that make monitoring and reporting easier:

- Audit logging is currently enabled
- Audit log ingestion is currently enabled
- Mailbox auditing “on by default” is currently enabled
- Audit logging was activated more than 90 days ago (on 2020-04-22 18:01:59)

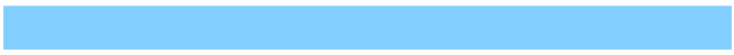
Your configuration has no characteristics that make monitoring and reporting more difficult.

User-level logging configuration

Configuration at the individual user level can override environment-level defaults. This section identifies user-level characteristics that could affect our investigation.

The tenant-level audit log age limit is: **90 days.**

100% of user accounts have active audit logging



From a total of 8 active user mailboxes, there are 8 with audit logging set to enabled (blue), and 0 set to disabled (pink)

31% of user accounts have the same audit log age limit as the environment default

From a total of 8 active user mailboxes, there are 2 with the same audit log age limit as the environment default (blue), and 6 that are different (pink)

Subscription

Your environment is licensed principally for: **Microsoft 365 Business Premium**.

Your licenses are allocated as follows[4]:

- Microsoft 365 Business Standard (54 licenses assigned).
- Microsoft 365 Business Basic (9 licenses assigned).
- Exchange Online (Plan 1) (1 license assigned).

Only certain subscriptions provide access to Microsoft 365's threat protection[5] and premium audit[6] functionality. Most organisations do not have these features, but given their potential value we always assess whether they are available. Some organisations consider adding them to their subscriptions to improve audit and security.

- Advanced auditing does not appear to be available for your subscription.
- Microsoft Defender for Office 365 (previously known as Office 365 Advanced Threat Protection) Plan 1 appears to be available for 17 accounts in your subscription.
- Microsoft Defender for Office 365 (previously known as Office 365 Advanced Threat Protection) Plan 2 does not appear to be available for your subscription.

[4] Note that multiple licenses can be assigned to the same user account, so the total number of licenses may not equal the total number of accounts.

[5] Microsoft Defender for Office 365 provides a range of security features that can be used to prevent and respond to cyber incidents. Microsoft Defender for Office 365 Plan 2 is included in Office 365 E5, Office 365 A5, and Microsoft 365 E5, and in some subscription add-ons. Microsoft Defender for Office 365 Plan 1 is also included in these subscriptions, with Microsoft 365 Business Premium, or as a subscription add-on.

[6] Microsoft Purview Audit (Premium), formerly advanced audit, enables the retention of up to one year of logs for user and admin activities, and records more detailed information on events such as the access of individual email messages. These additional logging capabilities can be useful for monitoring and during forensic investigations following a breach. Microsoft Purview Audit (Premium) is included in accounts with a Microsoft 365 E5/A5/G5 license, an Office 365 E5/A5 license, a Microsoft 365 E3/A3/G3 license with either the Microsoft 365 E5/A5/G5 Compliance add-on or the Microsoft 365 E5/A5/G5 Discovery and Audit add-on, or a Microsoft 365 Frontline F5 Compliance or F5 Security & Compliance add-on. The retention of audit records for ten years is possible with the 10-Year Audit Log Retention add on license.

Appendices

Detailed activity over time

The following table sets out patterns of suspicious activity grouped by account and location, for all accounts with a high or medium risk rating. Please note that suspicious records of every kind are included in this table, including those that attract negligible risk scores and that are potentially false positives.

These records can be a helpful reference when reviewing accounts with an inconclusive risk rating. Consider consulting with the account owner to determine whether the activity shown in the table was legitimate, particularly during periods of time when they appear to have been away from their usual home location.

Account name	City	Country	Organisation	VPN or TOR?	Connection types	IP addresses	Event type	Date range	Suspicious records[7]
Andrew Harris	London	United Kingdom	Clouvider Limited	Yes	Web browser; Zoom	185.169.255.37 (and 1 others)	Log in successful	2020-09-25 11:21 to 2020-10-08 20:27	27
Andrew Harris	London	United Kingdom	Fibergrid	Yes	Web browser	165.231.33.196	Log in successful	2020-09-08 09:58 to 2020-09-11 14:48	29
Andrew Harris	London	United Kingdom	Hydra Communications Ltd	Yes	Web browser; Zoom	185.16.207.49 (and 2 others)	Log in successful	2020-08-19 11:11 to 2020-09-23 17:19	22
Andrew Harris	London	United Kingdom	M247 Ltd	Yes	Web browser; Zoom	141.98.100.180	Log in successful	2020-09-14 08:34 to 2020-09-17 16:17	40
Andrew Harris	London	United Kingdom	UK Dedicated Servers Limited	Yes	Zoom	77.74.197.196	Log in successful	2020-09-29 16:03 to 2020-10-01 17:14	8
Carol Maynard	-	-	-	-	Other	-	Email inbox rule	-	1
Gemma Tillman	-	-	-	-	IMAP	-	Email messages accessed	2020-09-14 21:19 to 2020-09-14 21:19	1
Gemma Tillman	-	-	Amarutu Technology Ltd	Yes	BAv2 ROPC; IMAP	31.220.3.105	Exchange mailbox log; Log in successful	2020-09-14 21:19 to 2020-09-14 22:19	2
Gemma Tillman	Colombo	Sri Lanka	Security Firewall Ltd	Yes	Web browser	45.10.234.71	Log in successful	2020-09-14 20:04 to 2020-09-14 20:06	4
Gemma Tillman	London	United Kingdom	Fibergrid	Yes	Web browser	165.231.33.196	Log in successful	2020-09-11 10:11 to 2020-09-11 10:12	3
Gemma Tillman	London	United Kingdom	M247 Ltd	Yes	Outlook Web Access; Web browser	141.98.100.180	Exchange mailbox log; Log in successful	2020-09-14 08:50 to 2020-09-14 09:53	9
Gemma Tillman	Slough	United Kingdom	UK2.NET	Yes	Web browser	85.203.34.84	Log in successful	2020-09-15 10:05 to 2020-09-15 10:09	8

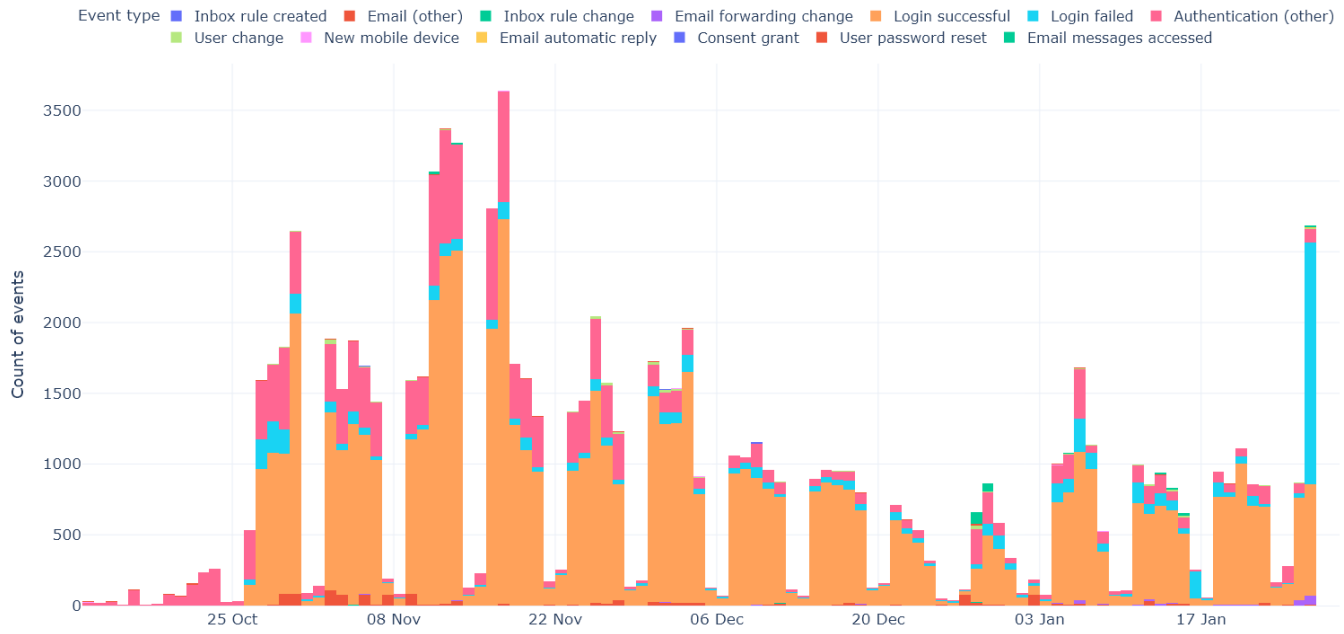
[7] These are suspicious records of any kind, irrespective of the type of risk identified or its degree of significance.

Account name	City	Country	Organisation	VPN or TOR?	Connection types	IP addresses	Event type	Date range	Suspicious records[7]
Magnus Robson	Nicosia	Cyprus	A.b Internet Solutions	Yes	Other	195.47.194.46	Email inbox rule	2020-08-24 23:43 to 2020-08-24 23:43	1
Magnus Robson	Nicosia	Cyprus	A.b Internet Solutions	Yes	Exchange Data Store Objects	195.47.194.46	Exchange mailbox log	2020-08-24 23:43 to 2020-08-27 23:44	4
Magnus Robson	-	United Kingdom	Hydra Communications Ltd	Yes	Exchange ActiveSync	5.226.142.177	Email messages deleted; Exchange mailbox log	2020-09-21 14:30 to 2020-09-27 10:08	8
Magnus Robson	London	United Kingdom	Clouvider Limited	Yes	Exchange ActiveSync; Exchange Data Store Objects	185.169.255.49 (and 2 others)	Exchange mailbox log	2020-08-19 12:52 to 2020-09-18 12:31	9
Ralph Walls	-	-	-	-	IMAP	-	Email messages accessed	2020-09-14 20:59 to 2020-09-14 20:59	1
Ralph Walls	-	-	Foundation for Applied Privacy	Yes	Web browser	109.70.100.39	Log in successful	2020-09-14 21:10 to 2020-09-14 21:10	1
Ralph Walls	-	-	Markus Koch	Yes	BAv2 ROPC; IMAP	185.220.101.207	Exchange mailbox log; Log in successful	2020-09-14 20:58 to 2020-09-14 21:59	2
Ralph Walls	-	-	OVH SAS	Yes	Outlook Web Access	151.80.237.96	Exchange mailbox log	2020-09-14 22:12 to 2020-09-14 22:14	2
Ralph Walls	-	Brazil	Host1Plus	Yes	Exchange RPC; Web browser	191.101.252.70	Email (other); Email messages accessed; Exchange mailbox log; Log in successful	2020-09-14 19:44 to 2020-09-14 20:50	22
Ralph Walls	São Paulo	Brazil	ExpressVPN	Yes	Outlook Web Access; Web browser	45.56.156.20	Exchange mailbox log; Log in successful	2020-09-14 15:50 to 2020-09-14 16:50	3
Ralph Walls	Strasbourg	France	Host Europe GmbH	Yes	Other; Outlook Web Access; REST API; Web browser	92.118.13.65	Email messages deleted; Exchange mailbox log; Log in successful	2020-09-14 16:11 to 2020-09-14 19:00	18
Ralph Walls	Nairobi	Kenya	Angani	-	Outlook Web Access; Web browser	62.12.114.142	Exchange mailbox log; Log in successful	2020-09-14 15:23 to 2020-09-14 16:24	12
Ralph Walls	Colombo	Sri Lanka	Security Firewall Ltd	Yes	Web browser	45.10.234.71	Log in successful	2020-09-14 19:57 to 2020-09-14 20:02	7
Ralph Walls	London	United Kingdom	M247 Ltd	Yes	Outlook Web Access; Web browser	141.98.100.180	Email messages deleted; Exchange mailbox log; Log in successful	2020-09-14 08:51 to 2020-09-14 09:55	26
Ralph Walls	Slough	United Kingdom	UK2.NET	Yes	Exchange RPC	85.203.34.84	Email (other); Email messages accessed; Exchange mailbox log	2020-09-14 20:59 to 2020-09-14 22:13	4
Ralph Walls	Miami	United States	ExpressVPN	Yes	Outlook Web Access; REST API; Web browser	193.36.224.39	Exchange mailbox log; Log in successful	2020-09-14 16:15 to 2020-09-14 19:56	48

Events types in scope

For this assessment, we focus on a subset of specific event types that enable us to identify the most suspicious behaviour on the environment.

The following chart shows the data that has been collected and analysed by event type over time.



Audit logging status

All active user mailboxes have enabled audit logging.

Audit log age limit

All active user mailboxes have the same audit log age limit as the environment default.

Multi-factor authentication status

We found the following active user accounts with an inactive multi-factor authentication status:

- adelev@londonwidgets.onmicrosoft.com
- alex.o'brian@londonwidgets.onmicrosoft.com
- diegos@londonwidgets.onmicrosoft.com
- emma.ohara@londonwidgets.onmicrosoft.com
- gradya@londonwidgets.onmicrosoft.com
- henriettam@londonwidgets.onmicrosoft.com
- isaiahl@londonwidgets.onmicrosoft.com
- johannal@londonwidgets.onmicrosoft.com
- jonis@londonwidgets.onmicrosoft.com
- leeg@londonwidgets.onmicrosoft.com
- lidiao'h@londonwidgets.onmicrosoft.com
- lynner@londonwidgets.onmicrosoft.com

- meganb@londonwidgets.onmicrosoft.com
- miriamg@londonwidgets.onmicrosoft.com
- nestorw@londonwidgets.onmicrosoft.com
- pattif@londonwidgets.onmicrosoft.com
- pradeepg@londonwidgets.onmicrosoft.com
- tammy.ellison@londonwidgets.onmicrosoft.com

Registered methods of strong authentication

We found the following active user accounts with no registered methods of strong authentication:

- adelev@londonwidgets.onmicrosoft.com
- alex.o'brian@londonwidgets.onmicrosoft.com
- diegos@londonwidgets.onmicrosoft.com
- emma.ohara@londonwidgets.onmicrosoft.com
- gradya@londonwidgets.onmicrosoft.com
- henriettam@londonwidgets.onmicrosoft.com
- isaiahl@londonwidgets.onmicrosoft.com
- johannal@londonwidgets.onmicrosoft.com
- jonis@londonwidgets.onmicrosoft.com
- leeg@londonwidgets.onmicrosoft.com
- lidiao'h@londonwidgets.onmicrosoft.com
- lynner@londonwidgets.onmicrosoft.com
- meganb@londonwidgets.onmicrosoft.com
- miriamg@londonwidgets.onmicrosoft.com
- nestorw@londonwidgets.onmicrosoft.com
- pattif@londonwidgets.onmicrosoft.com
- pradeepg@londonwidgets.onmicrosoft.com
- tammy.ellison@londonwidgets.onmicrosoft.com

Legacy authentication protocols

We found the following active mailboxes with legacy authentication protocols enabled at the user-level:

- adelev@londonwidgets.onmicrosoft.com
- alex.o'brian@londonwidgets.onmicrosoft.com
- diegos@londonwidgets.onmicrosoft.com
- emma.ohara@londonwidgets.onmicrosoft.com
- gradya@londonwidgets.onmicrosoft.com
- henriettam@londonwidgets.onmicrosoft.com
- isaiahl@londonwidgets.onmicrosoft.com
- johannal@londonwidgets.onmicrosoft.com
- jonis@londonwidgets.onmicrosoft.com
- leeg@londonwidgets.onmicrosoft.com
- lidiao'h@londonwidgets.onmicrosoft.com
- lynner@londonwidgets.onmicrosoft.com
- meganb@londonwidgets.onmicrosoft.com
- miriamg@londonwidgets.onmicrosoft.com
- nestorw@londonwidgets.onmicrosoft.com
- pattif@londonwidgets.onmicrosoft.com
- pradeepg@londonwidgets.onmicrosoft.com
- tammy.ellison@londonwidgets.onmicrosoft.com

Shared and resource mailboxes

We found the following active shared or resource mailboxes that did not block direct logins:

- billing@londonwidgets.onmicrosoft.com
- finance@londonwidgets.onmicrosoft.com
- sales@londonwidgets.onmicrosoft.com
- room1@londonwidgets.onmicrosoft.com
- room2@londonwidgets.onmicrosoft.com
- boardroom@londonwidgets.onmicrosoft.com
- reception@londonwidgets.onmicrosoft.com

Notices

General notices

- This is an automated report based on your Microsoft 365 audit logs. The results are based on records that were retrieved on the date the report was generated.
- This analysis is based on logs that were preserved from your environment for the purpose of quantifying the level of risk across the environment. Only certain categories of log data are included in the data collection and analysis, so indications of risk levels should not be seen as definitive.
- This automated report does not provide an in-depth review of individual user accounts, so is not guaranteed to identify all potentially malicious activity.
- In some cases, evidence of compromise is not present in logs and is therefore not possible to detect. Examples include: logging was not activated; a service issue with the platform prevented accurate log events from being captured; the compromise took place before the period covered by log data; or the user entered their credentials into a phishing website but the threat actor has yet to utilise them.
- All dates are specified in Greenwich Mean Time (GMT), which is equivalent to Coordinated Universal Time (UTC) with no timezone (UTC+0), unless otherwise stated.

Account definitions

Account types are defined as follows:

- **Accounts in your environment** are accounts that have been registered irrespective of their type or status, including those that are no longer active, guest accounts, and non-user account types such as shared mailboxes.
- **Active accounts** are those that have not been disabled by an administrator and whose credentials have not been blocked by an administrator.
- **Active user accounts** are active accounts with an enabled user mailbox or no mailbox.
- **Active accounts with mailboxes** are active accounts with an enabled Outlook mailbox.
- **Active user accounts with mailboxes** are active user accounts that have been assigned an active Outlook mailbox.
- **Licensed accounts** are accounts of all types, active or otherwise, that have a Microsoft license associated with them in your environment.
- **Guest accounts** are external users from outside your environment who can view documents, chat, and join groups that they are invited to.

Risk factor definitions

Definitions for the risk factors we calculate, and our recommended approach for reviewing them, are set out below.

- **Legacy protocols.** The number of events that use a legacy protocol such POP3 or IMAP. Legacy protocols use basic authentication and can be used by threat actors to access mailboxes and create copies of them. To review legacy protocol use, consult with the account owner to find out whether they use an email client configured for a legacy protocol such as POP3 or IMAP.
- **Unusual countries.** The number of events geolocated to a country that is not typically associated with your organisation. To review unusual countries, consult with the account owner to find out whether they were in the countries specified in the *Unusual countries* section.
- **Anonymous connections.** The number of events associated with an anonymous IP address, such as a virtual private network (VPN) or an anonymous relay (e.g. Tor). To review anonymous connections, consult with the account owner to find out whether they use VPNs regularly, and did so on the relevant dates.
- **Mailbox rules.** The number of email forwarding or inbox rule events that have suspicious attributes; for example, they have suspicious names or descriptions, forward or redirect messages to an external email address, delete messages, or move them to infrequently used folders such as RSS Feeds. Mailbox rules can be used by threat actors to covertly relay messages, for example to external email addresses under their control. To review mailbox rules, manually check all of the listed rules for identified accounts. Consider consulting with the account owners to find out whether they are genuine.
- **Asceris blacklisted IPs.** The number of events associated with IP addresses that have been blacklisted in Asceris' database of known malicious addresses. Note that IP addresses can be assigned to new devices over time, so a blacklisted IP address does not provide conclusive evidence that the account has been compromised. Consider consulting with the account owners to find out whether they initiated the corresponding connections.
- **Recent abusive IPs.** The number of events associated with IP addresses that have been reported as abusive in the last 90 days to a database of malicious activity. Note that IP addresses can be assigned to new devices over time, so a blacklisted IP address does not provide conclusive evidence that the account has been compromised. Consider consulting with the account owners to find out whether they initiated the corresponding connections.
- **Consent grants.** The number of application consent grant events, which occur when the user authorises third-party web applications to access their accounts and data. While this activity can be legitimate, it can also be an indicator of consent phishing, which is a technique used by threat actors to compromise user accounts and maintain persistent access even if multi-factor authentication is enabled. To review consent grants to unfamiliar applications, consider consulting with the account owner to find out whether they granted access on the relevant dates.
- **Frequent failed logins**. Frequent failed logins indicate that attempts may have been made by a threat actor to gain access via a brute force attack. The risk factor table displays the number of frequent failed logins, which

is defined as a minimum of 6 failed logins within a 1 hour period. This risk factor should be considered for information only.

- **New mobile devices.** New mobile device registrations are relatively common, but it is possible for threat actors to use new devices to access user accounts. This risk factor should be considered for information only.
- **Suspicious speeds.** Rapid movement between two locations, as measured by the geolocation of IP addresses between two consecutive events. This risk factor should be considered for information only.

How we describe probability

We use estimative language to give indications of risk levels, which is often based on limited or partial information. The following table describes the language we use and how this maps to real world descriptions and an approximate quantitative scale.

Estimative probability	Description	Quantitative scale
1 – Highly likely	High probability of being true	80% to 100%
2 – Likely	Moderate probability of being true	60% to 80%
3 – Even chance	Equally likely to be true as to be false	40% to 60%
4 – Unlikely	Moderate probability of being false	20% to 40%
5 – Highly unlikely	High probability of being false	0% to 20%

How we rate suspicious activity

At the risk rating stage, we use a simple scale to describe the risk levels for user accounts. The following table describes what we mean by each rating.

Suspicious activity rating	Description
High risk	The level of detected suspicious activity was high, so it is **highly likely** that the account was compromised if there is no legitimate explanation.
Medium risk	The level of detected suspicious activity was medium, so it is **likely** that the account was compromised if there is no legitimate explanation.
Low risk	The level of detected suspicious activity was low, so it is **unlikely** that the account was compromised.
Very low risk	The level of detected suspicious activity was very low or none, so it is **highly unlikely** that the account was compromised.