CatchBefore

Product Information

CatchBefore

www.catchbefore.com.au

Introduction

The drive to the cloud has made your data more accessible. Gone are the days where access was limited to a physical office location. It is not uncommon to have team members working from home, from a different city, interstate, or even overseas. The cloud makes this accessibility possible, however it also accessible for unauthorised access attempts from every corner of the globe. The configuration that you receive with your tenancy is designed to make it easy for you to use. It is not configured for optimal security. It is common to find misconfiguration, or suboptimal security configuration. How confident are you with the technical security skills of the people that setup and configured your tenancy? Have you had it recently re-assessed? Do you know which users have access? Have you checked for unauthorised access lately?

CatchBefore was created to provide enhanced ongoing protection for organisations using 365. Security is never permanently addressed, it requires an ongoing system of Monitoring, Reviewing, and Reporting. Standards are continuously changing, and with the global threat levels showing no signs of receding we beleieve that security enhancement is critical.

Monitor

At the heart of CatchBefore is the monitoring service. Your tenancy is online, exposed to the Internet 24/7. Accessible to your staff, and potentially also to the rest of the world! Utilise our monitoring to help detect and provide early warning for configuration and tenancy health issues. Alerting for security issues, licensing, quotas and usage problems enable an early warning mechanism that is critical for every organisation. Without this service you run the risk of having your tenancy exploited, and potentially finding out many months or years later. Early action is the key to minimising damage.

Review

The review service is undertaken by a CatchBefore technician on a monthly basis. This is to provide your tenancy an extra set of 'eyes' on the configuration and usage. CatchBefore technicians run through a dynamic list of additional checks, with the focus on reviewing areas that the Monitoring system does not currently provide coverage on. Our technicians may also provide general advice regarding your tenancy.

Report

CatchBefore provides a regular, easy to read report. The reports are suitable for both technical and non-technical managers. A wide range of information is covered, from core information about the tenancy, your current "Secure Score", user lists, license usage, quota usage, hardening, multi-factor authentication, login attempts, to Microsoft Alerts.

Support and Consulting

CatchBefore is a valuable security & monitoring system. It is important that you have an in-house IT person or IT service provider to help you with your general IT needs and to work on alerts generated by Catchbefore monitoring system. However at any stage, if you need help enhancing your tenancy configuration, investigating an alert, or general 365 help then our support and consulting team can assist. Please contact sales for latest pricing on support and consulting.

List of monitoring checks

#	Check	Description
1	On Premises Sync Status	This alert is triggered when the Microsoft 365 Active Directory tool has not completed a synchronisation with the cloud services within a set period of time. This may happen for a variety of reasons, and is normally related to the failure of the synchronisation software itself, or the systems that run the synchronisation software.
2	Overseas Successful Login	This alert is triggered when a login is detected from a suspected overseas location. If it is from overseas, and you do not have any staff members overseas, then it may be an indication of an account breach (intrusion).
3	Overseas MFA Failure	This alert is triggered when a username and password is accepted by 365, however the Multi-Factor Authentication step fails and the location of attemp is overseas. If it is from overseas, and you do not have any staff members overseas, then it may be an indication of an account breach (intrusion) - or a near account breach, with the username and password being compromised.
4	New 365 Alerts	This alert is triggered when the Microsoft 365 system creates an 'alert' for your attention. The alerts vary on impact and importance. This is Microsofts way to send you information, and it is important that a suitably qualified technician reviews each one.
5	Login Success Percent	This alert is triggered when the total number of successful logins to your tenancy falls below a pre-set percentage. This may be due to your team members failing to authenticate in a non-malicious manner, or it could also be an attempt from an external party to gain unauthorised access. If your authentication and authorisation settings are weak, then un-authorised access may be possible.
6	Secure Score Percent	This alert is triggered when the the secure score of your tenancy goes below a pre-set percentage. This may be due to Microsoft releasing additional security enhancements that have not been enabled. If your security settings are too weak you may be at higher risk of compromise. It is important to keep your Secure Score to a sufficient level.
7	MailBox Quota	This alert is triggered when a user's account email box is close to the quota alert limit. If usage continues to increase, the ability to send, and then receive email will gradually be disabled in line with Microsoft policy.
8	OneDrive Quota	This alert is triggered when a user's OneDrive is close to the quota alert limit. If the storage usage continues to increase to the quota limit then the user will no longer be able to add content to the impacted drive.
9	SharePoint Quota	This alert is triggered when the total available storage is close to the quota alert limit. If usage continues to increase then all sharepoint sites on the tennacy will no longer be able to add new content once the quota is reached.

#	Check	Description
10	Email Rule containing a forward	This alert is triggered when a forward option is located in a standard email rule. If it was inserted maliciously, then all emails could be 'copied' to an external address, resulting in a data breach.
11	Email Rule containing a delete	This alert is triggered when a delete command is detected in an email rule. If it was inserted maliciously, then it may be being used to hide inbound emails, or related bounces.
12	Company and Global Administrator count	This alert is triggered when there are too many or too few Company or Global Administrators in the tenancy. If there are too few, then it may be difficult to manage the tenancy. Too many is considered a security risk.
13	Administrator with Licenses attached	This alert is triggered when an account with a license also has an Administrative role. An administrative account used for normal activities is at higher risk in the event of a compromise.
14	Possible Under Utilised Licenses	This alert is triggered when the number of assigned licenses is less than the activated license count (potentially indicating under utilisation). If there is an actual under utilisation, it may be an indication of licenses that can be reduced.
15	Inactive Mailbox	This alert is triggered when a user has not accessed the mailbox for the specified period. There may be an old account that can be archived, or a user that requires assistance.
16	Inactive OneDrive	This alert is triggered when a user has not accessed OneDrive for the specified period. There may be an old account that can be archived, or a user that requires assistance.
17	Inactive SharePoint	This alert is triggered when a user has not accessed Sharepoint for the specified period. There may be an old account that can be archived, or a user that requires assistance.
18	Inactive Teams	This alert is triggered when a user has not accessed Teams for the specified period. There may be an old account that can be archived, or a user that requires assistance.
19	Directory Quota	This alert is triggered when the space (capacity) availabile on the Directory goes below a specific level. If capacity is reached it may not be possible to to add new users or groups (amongst other potential issues).
20	Tenant Country	This alert is triggered when your tenancy is not in the default country list. There may be performance issues if your tenancy is overseas. There may also be legal requirements for your data to be within a specific country.
21	Verified Domains	This alert is triggered when one of your domain name(s) is not listed as verified by Microsoft. You may not be able to send email on behalf of this domain (or otherwise use the domain inside your environment).

#	Check	Description
22	Domains Health	Alerts when a client domain fails one of a number of checks. Checks include: • Domain has Name Servers with IPs that resolve. • Name Servers are responding. • Name Servers output is matching. • Name Servers SOA is matching • Root name servers have matching entries for Name Servers (matching with the assigned NameSevers output) • Name Servers have no private IP addresses • Name Servers have no private IP addresses in SOA • Name Servers are spread out over at least 2 separate /24 networks • Domain has at least 1 MX record • Domain is missing a 3rd party filtering system (ie, direct 365 connection) • If the domain is a 365 direct, it only has the required 365 MX record(s) • The domain has no SPF record • The domain has no DMARC record • The domain is listed in Phishtank All the checks above are designed to detect configuration, reputation, or operational problems revolving around DNS and your domain names in use. The impact of a fault will vary depending on the individual configuration, however it may range from slow performance, intermittent failures, complete outages, enhanced risks, to email deliverability issues.
23	License Health	This alert is triggered when some of your licenses are going to expire, or are suspended. This may stop you using the services, and may result in data-loss.
24	Compromised Account	This alert is triggered when an email addresses from your tenancy is listed as being in a compromised list from a breach on https://haveibeenpwned.com In some situations passwords may be compromised, allowing malicious use of the sites/systems compromised. If common passwords are shared, then it is also possible that related services may be compromised (including your email if you use the same password).
25	Successful login from blacklisted IP address	This alert is triggered when a successful login is detected from a 'black-listed' IP address. This is an indicator of suspicious activity. If it was not one of your team members, then it may be an indication of an account breach (intrusion).
26	New Application detected	This alert is triggered when an new application is granted to the tenancy. If it was not expected it may be an indicator of malicious activity, or 'back-door' access.
27	Application Role Grants	This alert is triggered if a new application is given access to the tenancy by one of the users. If the application that has been granted permission then access to your tenancy may be gained without other ongoing authorisations (such as explicit permission, or MFA). Effectively 'silent' access in the background without you being aware.

#	Check	Description
28	MultiFactor Authentication Status	This alert is triggered if an enabled user is detected as not having MFA enabled, not having MFA setup (even if enabled), and will also alert if MFA is not enforced (even if enabled). Any users that can login should have MFA enabled, setup, and enforced. If they do not then the account (and the data it can access, as well as configuration control) is at a higher risk of access by an un-authorised party.
29	Domain Phishing list lookup	This alert is triggered when our system detects one of your domains in being listed in Phishtank. This may have an negative impact on deliver-ability, and indicate that your domain is implicated in a phishing attempt.
30	Risky Login	This alert is triggered if a login is suspected as being "Risky" (potentially fraudulent, unwanted). This is an indicator of suspicious activity. It might be a compromised account.
31	Targeted Users	This alert is triggered when there is a required (total) volume of failed logins for a specific user, and/or if there are enough failed logins from unique IP addresses for a given user (indicating a wider/broader attack).
32	Legacy Authentication	This alert is triggered when there is a successful authentication event utilising legacy authentication methods. Legacy authentication methods are highly targeted, and are inherently less secure. This may lead to a higher chance of exploitation and un-authorised access.
33	Problematic MFA	This alert is triggered when there is an unhealthy amount of Multi-Factor-Authentication (MFA) login failures. This may be a related to a user(s) that has problems with the MFA process, or, an indication of an account that is otherwise compromised, except for MFA.
34	Access Policy Violation	This alert is triggered when an otherwise successful login (user/password worked) - is blocked by Conditional Access Policy. This could be a sign of a compromised account. If this is the case, the attacker may try to further by-pass the Conditional Access Policies. This may lead to a compromised account.
35	On Premises User Provisioning Errors	This alert is triggered if a user account has provisioning errors during the synchronisation from on-premises systems to 365. This typically indicates a configuration issue that needs to be addressed. The expected user or email configuration may not result in the desired outcome.
36	Ghost Users	Alerts if an active (can be logged into) user account has not been logged in to for an extended time period. This typically indicates a user account that is not being actively used, however is still operational. These accounts are at risk of being forgotten about, and later activated or used without permission.
37	Application Password Expiring	Alerts if an Application, with an applied password, is going to expire shortly. This typically indicates that an Application needs its password renewed.

Report information

A regular PDF summary report covering key aspects of your tenancy. At the time of writing these items are covered:

#	Description
1	Tenant information (Name, Country, Last Sync, Directory quota status)
2	Secure score
3	Domains in use and DNS status
4	Users summary (Active, Total, Possible underlicensed, inactive accounts)
5	Hardening information (MFA Status, CA/GA count, Admin accounts with licenses, Conditional access policies)
6	Quotas and usage (Exchange, OneDrive, Sharepoint)
7	Audit Logs (successful access logs, as a %, MFA failures, suspected overseas logins)
8	365 Alerts that require attention

Review information

The monthly technician review of your tenancy is designed to cross-check some of the ongoing monitoring, address important areas that are not covered by the monitoring, and provide the opportunity for a technician to give suggestions for improvement.

#	Description
1	Manual check of syncronsiation status.
2	MFA Status check.
3	Email forwarding and rule review.
4	Confirm that auditing is enabled.
5	Check of audit logs for suspicious activity.
6	Review mailbox limits.

#	Description
7	Review Anti Malware settings for email.
8	Review Ransomware alerts (email alert).
9	Security Score.
10	Email security improvements (DKIM, SPF, DMARC).
11	Check email alerts email.
12	Advise on enhanced protection (ATP Anti Fishing, ATP Safe Attachments, ATP Safe Links, GeoBlocking).

The results of the review (and any suggestions) are sent to you via email. The review will not typically cover metrics or other reporting (please see the reporting facility separately).

It is important to note that this review is not customisable. The checks and coverage of this review are dynamic, and as such are subject to change without notice. Additional consulting and support services can be purchased if you wish to further expand on the review.

Plan information, and check frequency

Key Features

	Basic	Standard	Enhanced
Essential Daily Checks^	✓	✓	✓
Technicians managing alerts (business hours on weekdays)		✓	✓
Regular Insights Summary Report		✓	✓
Increased frequency of important checks^		✓	✓
Technician managing alerts once a day on weekends			✓
Enhanced Security and reputation checks Includes compromised account checks & Domain involved in phishing attempts			✓
Dedicated Technician time to provide a review and advise on any improvements			✓

Frequency of Daily Checks

	Basic	Standard	Enhanced
Days in which checks are run	Mon-Fri		Mon-Sun
On Premises Sync Status	1x	2x	4x
New 365 Alerts	1x	2x	1x
Login Success Percent	1x	1x	1x
Secure Score Percent	1x	1x	1x
MailBox Quota	1x	1x	1x
OneDrive Quota	1x	1x	1x
SharePoint Quota	1x	1x	1x
Overseas Successful Login	1x	2x	4x
Overseas MFA Failure	1x	2x	4x
Email Rule containing a forward	1x	2x	4x
Email Rule containing a delete	1x	2x	4x
Company and Global Administrator count	1x	2x	4x
Administrator with Licenses attached	1x	2x	1x
Possible Under Utilised Licenses	1x	1x	1x
Directory Quota	1x	1x	1x
Inactive Mailbox	1x	1x	1x
Inactive OneDrive	1x	1x	1x
Inactive SharePoint	1x	1x	1x
Inactive Teams	1x	1x	1x
Tenant Country	1x	1x	1x
Verified Domains	1x	2x	4x
Domains Health	1x	2x	4x

	Basic	Standard	Enhanced
Days in which checks are run	Mon-Fri		Mon-Sun
License Health	1x	2x	4x
New Application detected	1x	2x	4x
Application Role Grants	1x	2x	4x
MultiFactor Authentication Status	1x	2x	4x
Risky Login	1x	2x	4x
Targeted Users	1x	2x	4x
Legacy Authentication	1x	2x	4x
Problematic MFA	1x	2x	4x
Access Policy Violation	1x	2x	4x
On Premises User Provisioning Errors	1x	2x	4x
Ghost Users	1x	2x	4x
Application Password Expiring	1x	2x	4x
Compromised Account	NA	NA	1x
Successful login from blacklisted IP address	NA	NA	4x
Domain Phishing list lookup	NA	NA	4x

Alert Notification workflow

The Basic plan provides notification of alerts via email.
Alerts with the Standard and Enhanced plans are managed via a ticketing system. CatchBefore will create a new ticket on alert, with our technicians reaching out via email with an explanation of the alert.
With all plans: further investigation and remidiation of the source of the issue may need to be undertaken by you or your contracted technician.

Contact Us

We are here to answer your questions and give product information.
Please visit us at **www.catchbefore.com.au**
Reach us on 1300 CATCH1 (1300 228 241) within Australia,
or +61 2 61024550 from overseas.

Considerations

- As part of the monitoring process we may need to submit email addresses from your tenancy to third party databases. This is used to check for known compromised accounts. This is covered in further detail in the Privacy Statement available on our website
- This product is provided based on the number of active users in your tenancy. CatchBefore will stop processing checks once the licensed CatchBefore user limit has been hit. This may result in incomplete or inaccurate checks if you have more active users than licensed with CatchBefore. There are some checks that are required on non-active users. As such, a limit is also required on non-active users. CatchBefore will allow for checks on disabled users to the amount of up to 3 x the licensed users. For example, if you are licensed for 15 users with CatchBefore, then CatchBefore will undertake checks on up to 45 disabled users within the same licensed tenancy as the active users.
- This service does not include consulting or general support for your environment to make changes, setup new systems/access, or to address problems. Advice from monitoring alerts is limited to generic information about the alert. You may need to engage CatchBefore on a support basis (or an external provider) to further assist.
- The reports are non-customisable. The review advice is non-customisable. You may need to engage CatchBefore on a support basis (or an external provider) to further assist.
- Not all checks are available on all plans. Please see the plan listing in this document for further information. This document has not taken your individual requirements in to account. Inclusions and offerings subject to change without notice. Please check our website for the latest information.
- The entry level Microsoft 365 plans do not provide us with sufficient access to all logs and reporting. We suggest the business premium plans as a minimum to enable full functionality.
- At the time of writing, Shared Mailboxes are not identified or managed with the reporting and monitoring systems. Please be aware that there is more than one type of forwarding rule, CatchBefore only detects one sort. In both cases additional manual checks are advised.
- Checks (Monitoring) and reports may produce false positives, please be aware that any investigation in to an alert is at the discretion of the client.