Monitoring in the cloud: Office 365

Microsoft Office 365 has become the most widely used cloud application suite in the world with over 100 million monthly active users. This increase in usage along with the ever-growing amount of personal and business critical data being processed through the platform has led to increased levels of attack behavior against Office 365 users. As such, the need to monitor for this activity and potential vulnerabilities has also increased. This document explores what activities all businesses using Office 365 should be monitoring and some of the insights that can be seen through this data.

What to monitor	What to look for	What it means
Access *User and Administrator account access*	• Successful Logins • Failed Logins • Login Time • Login Location • Indicative Patterns: Successful login after failed login(s)	Repeated failed logins, especially from the same account or source can indicate brute-force attacks. Unusual login times and locations can be indicators of compromised user credentials.
Administration *Administrator level activities*	• User Creation/Removal • User permissions/role changes • Changes to logging and audits • Backup schedule changes • Whitelist/Blacklist updates	Activities such as these, when unplanned, are often an indication of attackers setting up future/persistent access to target systems.
Documents *OneDrive and SharePoint*	• User file access • File restoration/deletion • Large file transfers • Updates to groups • Access for external users	Whilst external attackers may be looking to move data out of the target system, this also takes place when an insider threat is involved. Using this data, it is possible to see abnormal activity with files.
Policies *Rules and Filtering*	Changes to policies including • Exchange (e.g. Malware Policies, SPAM Filtering Policies) • Data Leakage Protection Policy • Other configured policies	It may be possible to detect an attack in the early stages should changes to policies be required in order for the attacker to perform their target actions.
Third Parties *Azure, Active Directory, Applications*	• Changes in AD policies • Authorisation of third party application(s)	If systems are configured to allow users to connect to third party applications, it is essential that these third parties are known and all settings are in line with security internal policies

Pervade Software

As you will have seen in the information above, the key to monitoring in the cloud is utilising the available data to find patterns of behaviour or changes that indicate malicious activity or vulnerabilities. **Pervade** Software's unique suite of products and award-winning database allows for this data to be collected in a single place. Customisable correlation rules and dashboards can then be used to ensure you have the most relevant, actionable intelligence in near real-time in the way your teams can use it best.