TrackerIQ Protects against Microsoft 365 Misuse

Introduction

In the transition from on-prem business applications to SaaS applications, many security controls organizations have in place for on-premises protection are not effective at protecting SaaS applications. In addition, enterprises have poor visibility of employee activities across and within applications, as well as their ability to detect threats across those applications, including data exfiltration by both insider and external attackers, compromised accounts used by external attackers, and unapproved or risky security changes.

Microsoft 365 is widely used by many organizations to help drive collaboration and productivity. While Microsoft 365 enables businesses to be more efficient, it is also a high-value target and expansion of the attack surface for attackers. Monitoring Microsoft 365 users and administrators is important to obtain visibility and to track suspicious activities that lead to security breaches.

As applications move to the cloud and SaaS, organizations increasingly lack the visibility and control over user behavior necessary to protect their applications and data.

Microsoft 365 establishes an enormous attack surface, exposes many new types of vulnerabilities, and hinders effective cybersecurity practices.

Rules-based solutions like UEBA are cumbersome to maintain and create far too many false positive alerts. They miss many cybersecurity threats to applications in the cloud.

TrackerIQ allows for the accurate detection of anomalous sessions in Microsoft 365 without requiring rules.

User Journey Analytics, the unique technology embedded in TrackerIQ, enables organizations to monitor user activities (outsiders and insiders) using MS audit logs. It slashes false positives to a highly manageable and effective quantity, and detects actual threats before they do damage.

Solving Microsoft 365 security challenges with TrackerIQ

Microsoft 365 generates extensive audit logs that register activities performed by admins and users. Many organizations gather these logs into their SIEMs and log repositories, such as Splunk and Snowflake, mostly for compliance and regulatory purposes. But they are unable to examine the cumbersome logs to detect suspicious activities that may lead to actual security breaches.

RevealSecurity's TrackerIQ is the only technology that can adequately solve many common Microsoft 365 cyber threats. Examining the audit logs, TrackerIQ learns and establishes normal "user journeys", patterns of application behavior per individual and role.

It then scrutinizes the logs to accurately detect aberrant, suspicious behaviors by external threat actors as well as insiders, eliminating false positives and focusing attention on threats that matter.

Below, we present numerous common Microsoft 365 security problems and show how TrackerIQ uniquely solves them.

Case 1

Impersonation / Account takeover

Authenticating users is vital to any security regime. But even the most effective combination of single sign-on and multi-factor authentication can leave the organization open to a breach, for example, when an employee is cooperating with an attacker, or when an attacker successfully installs a malicious app on an employee's smartphone that steals the one-time password (OTP) that is sent via SMS to the phone. The malicious attacker is authenticated and the organization is wide open to attack.

Via the audit logs, TrackerIQ monitors each user's activities in Microsoft 365 applications. It learns and constructs all the typical journeys ("profiles") that constitute proper behavior for each user. It then uses the audit logs to detect anomalous activities, identifying attackers during recon, before they have a chance to establish persistence or exfiltrate data.

Detecting an attack by what the attacker does

TrackerIQ detects suspicious login events and password-related attacks. It monitors all the login activities and detects abnormalities, for example, due to a sequence of failed logins or a sequence of failed and then successful login operations.

Enterprising hackers can use a variety of techniques beyond the login to gain access. TrackerIQ uses the Microsoft 365 audit logs to detect these as well:

Account takeover and business email compromise (BEC) due to account impersonation by a human hacker or malware.

Credential sharing when an insider shares account credentials with an unauthorized user either intentionally (insider threat) or unintentionally as a result of a phishing attack.

Session hijacking where an attacker uses captured, brute force, or reverse-engineered session IDs to seize control of a legitimate user's session while it is in progress.

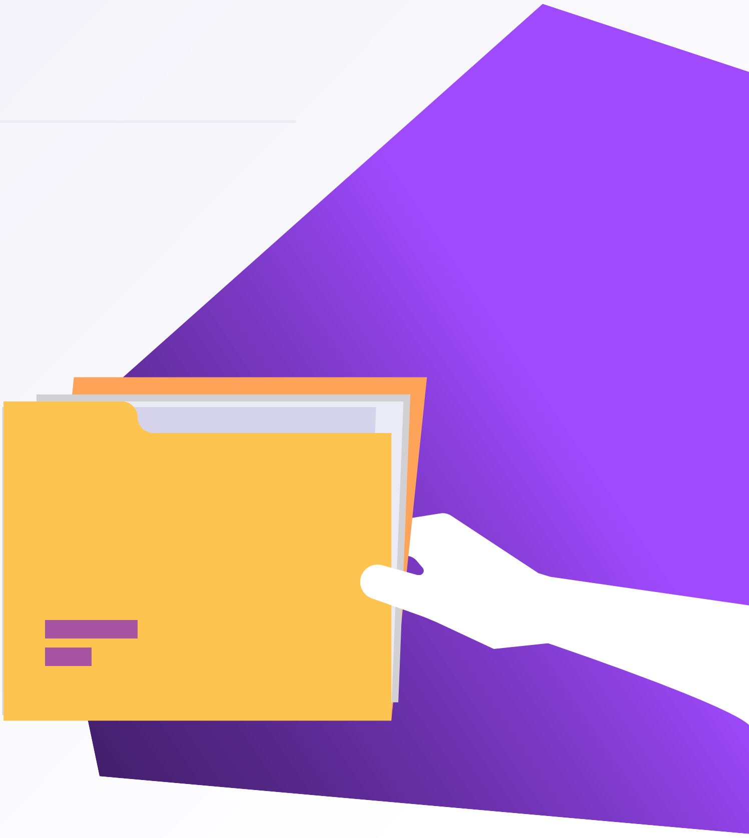
Password enumeration where the attacker exploits credentials exposed in previous breaches or social engineering scams to access other applications where a compromised user may employ the same login information.

During reconnaissance where the hacker tries to collect data about the target system in preparation for future attack.

Case 2

Data leaks due to file sharing and collaboration

File sharing is a standard practice in SaaS applications. Who hasn't shared a spreadsheet or Word document with co-workers? Collaboration is productive and is encouraged by collaboration tools like Microsoft SharePoint and OneDrive, widely used components of Microsoft 365. But collaboration multiples access – even to sensitive resources. Organizations spend a great deal of effort trying to manage the sharing of permissions, but it's impractical in light of such easy collaboration. Non- or misconfiguration can put the organization's vital data at risk. Any authenticated user can – intentionally or unintentionally – share financial files as well as other content with other parties who should not have access to that content.



Detecting data leakage in SharePoint and OneDrive

TrackerIQ monitors all user activities in SharePoint and OneDrive, automatically learning the typical sequences of access and activity within each application per user and role. Armed with its analysis of these proper "journeys", it detects abnormal journeys that may include improper sharing operations of privileged files and folders. With this unique visibility and insights, security teams can quickly determine what files and data a suspicious user has accessed and can put a stop to a leak pronto.

TrackerIQ detects data leakage in SharePoint and OneDrive emanating from suspicious:

File-sharing activities

Anonymous link creation

Resource access using anonymous links

External file sharing

External user file-access activity

Site invitations shared with external users

File downloads and file delete activities by users and applications that were given access rights by authentic users

Case 3

Data leakage via Exchange

There's nothing like email for exfiltrating critical data and inviting exploits. Microsoft Exchange is notorious for sending and receiving attachments that should not enter or leave the organization.

These can take the form of an unauthorized publication or disclosure of a list of email addresses or the simple sending of files containing confidential data. It can come as a result of hacking, mere mishandling of a database or mailing list, or even just attaching a simple spreadsheet.

Detecting leakage in MS Exchange

TrackerIQ monitors all Exchange management operations performed by users and Exchange administrators, including creation and deletion of email accounts, changes of permissions on email folders, rule definitions for email forwarding, and lots more. TrackerIQ focuses on permissions and rule management activities, and spots any abnormal sequence of mailbox management operations. Why wait until a breach happens? TrackerIQ detects prohibited mailbox management activities today that could lead to data leakage in the future, enabling the organization to address the problem proactively.

TrackerIQ detects data leakage threats in Exchange from suspicious:

Mailbox management operations such as

- Mailbox permission changes
- Mailbox rule configurations (e.g., email forwarding rules)

Unusual email operations

TrackerIQ detects abuse and misuse of privileges by administrators due to:

Application management operations, especially when adding applications to Azure Active Directory (AAD)

Suspicious user permission /configuration changes

Suspicious application permission/configuration changes

Website configuration changes

Auditioning configuration changes

Often, employees are granted more or higher privileges than necessary. TrackerIQ detects abuse and misuse of privileges by employees due to.

Suspicious user and /or applications permission changes

Summary

Security teams lose much of their visibility and control when applications move beyond on-prem to the cloud. SaaS apps present a serious threat to the cybersecurity of the organization. Azure-based Microsoft 365, used daily by millions of users, presents a multitude of security threats that often go unnoticed.

Fortunately, Microsoft 365 also produces extensive audit logs. TrackerIQ by RevealSecurity examines these logs to learn, analyze, and determine proper user journeys, and then finds other journeys that deviate from the acceptable. These deviants correlate highly with suspicious behavior that requires the attention of security analysts. Thus, TrackerIQ uniquely detects actual threats in cloud applications with a very high level of fidelity.

TrackerIQ is a new and highly effective technology in the cyber arsenal of organizations who need to monitor the activities across their growing attack surface in the cloud.

Reveal security