Reveal security

Solution Brief

Reveal Security for Microsoft 365

Detect Malicious Activity in Microsoft 365 to Prevent Data Theft

Microsoft 365

Benefits

- **High accuracy:** **P**atented Identity Journey Analytics™ using unsupervised machine learning discovers normal application usage and only alerts on anomalies
- **Early & accurate detection:** Monitors activity across Microsoft 365 and other applications and cloud services, quickly alerting on any suspicious behavior.
- **Full visibility across business processes: Cross-application behavior** sequencing allows the Reveal Security platform to assess risk for business processes that span Microsoft 365 and any other application.
- **Eliminates alert fatigue:** By only alerting on actual anomalous behavior, the Reveal Security platform allows security professionals to focus on incidents that require investigation.
- **Reduces MTTD and MTTR:** Accurate detection and automated investigation significantly reduce mean time to detect and respond.

Overview

As organizations transition from on-prem business applications to SaaS applications, Microsoft 365 has become a valuable target for cyber attackers and insider threats.

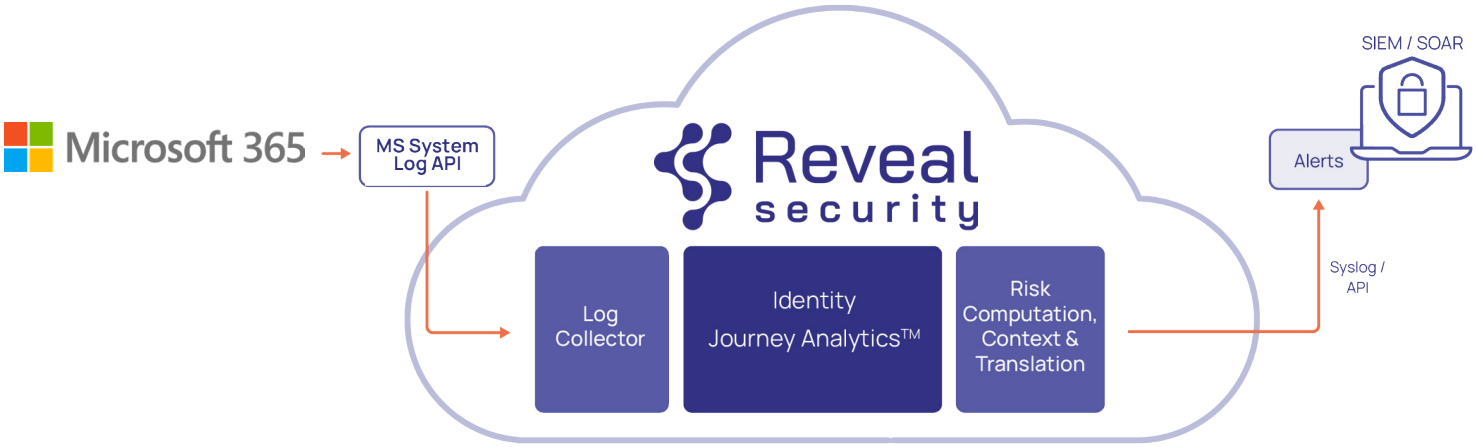
Traditional security controls that protect sensitive data on-prem are often not effective in a SaaS environment. Compromised credentials and insider threats pose a risk that is usually undetected until it is too late. Microsoft 365 has become the de facto platform for information processing in most organizations, hosting vast amounts of sensitive data held in emails, documents, spreadsheets, and presentations. This information is a massive target for cyber attacks. As vendors tighten security and fix vulnerabilities, attackers are shifting more toward gaining access through identities and stolen credentials. This kind of attack is hard to detect with traditional tools as access is achieved with approved credentials and appropriate authentication, which those tools are there to enforce. There are many types of attacks that can be performed in this way, including:

- Account takeover attacks resulting from stolen valid credentials
- Insider threats
- Third-party risk from connected applications and APIs

Reveal Security continuously monitors users and identities (including APIs) inside of applications, including Microsoft 365 - post login - and accurately detects anomalous behavior to identify and remediate potential threats before data exfiltration. The solution is SaaS based, easy to deploy and use. It saves security teams time by eliminating the need to write detection rules or investigate a deluge of alerts and false positives.

Comprehensive Threat Detection for Microsoft 365

The Reveal Security platform addresses the challenges of Microsoft 365 security monitoring by leveraging unsupervised machine learning to help detect both unauthorized and accidental changes as well as anomalous activity that could be an indication of compromised credentials or insider threat. The platform continuously tracks operations performed using the Microsoft 365 web UI and API activity by all identities across all Microsoft 365 services. Unlike UEBA tools or solutions that require the creation of detection rules, Reveal Security's approach significantly reduces the number of false positive alerts allowing security teams to focus on investigating only activity that is cause for concern.



Reveal Security helps detect a broad range of suspicious user and admin activity, including configuration changes, account creation/alteration, and data access either from the Microsoft 365 UI, its clients, or via its APIs.

Detection Use Cases

Reveal Security supports a broad spectrum of detection use cases in Salesforce by monitoring all user and identity behavior for anomalies. The table below highlights suspicious behavior that is automatically detected by the Reveal Security platform without the need for manual rule creation.

Account Takeover Detection

Detect the use of compromised identities (human and machine, workforce, and privileged users) within and across applications and cloud services with continuous monitoring and validation to quickly and accurately detect suspicious behavior.

Third-party Risk

Detect suspicious API behavior in applications to ensure they are not exploited for unauthorized access.

Monitor the behavior of remote vendors, contractors, and business partners.

Insider Threat

Continuously monitor the behavior of users within and across applications and cloud services to detect insider threats before considerable damage occurs.

Privileged User Risk

Reveal Security detects abnormal privileged user behavior across all aspects of Salesforce administration and configuration. The solution identifies activities that require investigation and provides a detailed audit trail of any changes made.

About Reveal Security

Reveal Security quickly and accurately detects insider threats and identity-based attacks in and across SaaS, cloud and on-premises applications. The Reveal Security platform is the only solution in the market based on patented Identity Journey Analytics™ technology that uses unsupervised machine learning to learn the usage patterns or typical "journeys" of human and machine identities in applications and uses it to detect anomalies. This approach delivers a superior level of accuracy and context, reduces alert volumes by orders of magnitude, and enables the business to respond quickly before a material breach can occur.

For more information, visit www.reveal.security