Data sheet

VECTRA®

Cognito Detect for Office 365

Detect and stop the largest attack vector in Office 365

30% of organizations suffer account takeovers every month. Vectra understands attacker behavior and account privilege in SaaS applications, allowing you to put an end to breaches.

Deploy in minutes

Native deployment into Office 365 without agents. Simply link your instance and Vectra will immediately detect attacker behaviors.

Make sense of security telemetry

Overwhelmed by the volume of security logs? Automate triage and enrichment at scale.

Office 365 data breaches are at the forefront. Even with the rising adoption of incremental security approaches like multi-factor authentication, access controls continue to be circumvented. In fact, 30% of organizations continue to suffer from an Office 365 account takeover every month.

As the industry's first network detection and response solution for the cloud, we are proud to announce that we are extending the Vectra Cognito® platform to Microsoft® Office 365®.

The Vectra platform prevents data breaches in the cloud by automatically detecting and prioritizing threats, accelerating investigations, and enabling proactive threat hunting – leaving attackers with nowhere to hide.

By applying the proven methodology that currently protects public clouds, private data centers and enterprise environments to cover SaaS applications. Vectra Cognito melds together security research and artificial intelligence to deliver timely attack visibility and put attack details at your fingertips to empower immediate action or automate response.

Easily deploy into Office 365 natively in minutes. Cognito Detect for Office 365 allows you to seamlessly integrate with your existing install without needing to maintain or install agents. Simply link your instance and Vectra will start detecting attacker behaviors right away.

The Vectra Cognito platform allows you to regain visibility across your entire infrastructure, from cloud to ground. By surfacing advanced cyberattacks in Office 365 from activity logs, we enable security operations teams that are understaffed and under siege to stay ahead of such attacks and respond faster to hidden threats.

Integrate with existing security ecosystem Feed AWS activity into your data lake or SIEM as Zeek-formatted security-enriched network metadata. Monitor and integrate with your existing cloud security tools such as EDR or SOAR solutions.

WHAT TO EXPECT FROM COGNITO DETECT FOR OFFICE 365

Detect malicious behaviors in all attack stages spanning your complete network: from LAN, to IaaS to SaaS

Review and analyze findings with prioritized and actionable alerts

Partnership with the Vectra team and our commitment to evolve our products in order to meet your growing needs

Cognito for Office 365 consumes event logs from Azure AD, SharePoint and OneDrive, like login events, mailbox routing configuration changes, file creation and manipulation and DLP configuration changes, to flag detections across all steps in the Kill Chain.

SaaS KILL CHAIN

Infiltration and elevation	Attackers gaining illicit access to Office365 and manipulating the environment to reach inappropriate resources. Detections in these stages include: Brute force logins, Adding users to groups, New privileges to groups, New roles
Reconnaissance	Attackers finding their bearings in unfamiliar Office 365 environments. Detections in this stage include: List all shares, List all users, List all roles, List all files, Unusual activities, Unusual processing, Elevated number of Searches, Accessing rare files, Accessing abnormal volume of sensitive files
Persistence and evasion	Attackers cementing continued access time and avoid detection. Detections in these stages include: App installations, Authentication changes, Unusual uploads, DLP changes, Mailbox sinks, Audit log settings changed, Policy changes
Exfil and destruction	The ultimate prize: extract critical information or destroy it. Detections in these stages include: Elevated downloads from new IPs and geos, Mail routing changes, Elevated number of deletes, Elevated number of share accesses

Office 365 Data Handling

Cognito uses the Office 365 Management API to retrieve Azure Active Directory, SharePoint and OneDrive event logs by requesting the ActivityFeed.Read and ActivityFeed.ReadDLP privileges.

Role-based Access Control (RBAC) and object anonymization help protect privacy, and customers can choose between multiple data sovereignty regions to meet their compliance requirements. Moreover, the detection environment uses a serverless approach to stay completely current with the latest available patches.

Information about the Microsoft Management API is available here:
https://docs.microsoft.com/en-us/office/office-365-management-api/office-365-management-apis-overview

VECTRA®
Security that thinks.®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai