VECTRA
SECURITY THAT THINKS.®

DATA SHEET

Cognito Detect for Office 365

Member of
Microsoft Intelligent
Security Association
Microsoft

Microsoft Office 365 is a high-value target for attackers, as it serves as not only an organization's email, but also a repository for OneDrive and SharePoint documents and sensitive data. Prevention tools and tactics have proven insufficient: 30% of organizations suffer from account takeovers every month despite email security intended to stop phishing, and rising adoption of strict password policies and multifactor authentication to protect accounts.

By taking a cloud-native approach, Cognito Detect for Office 365 detects and stops known and unknown attacks before they lead to breaches, without relying on preventative security.

With preventative security falling short, organizations are investing in detection and response solutions that allow them to find and stop attackers in their environments before they spread or cause harm.

As the industry's first network detection and response solution for the cloud, Vectra Cognito Detect for Office 365 extends the proven platform that currently protects public clouds, private data centers, and enterprise environments to Microsoft Office 365. The award-winning approach leverages security research combined with data science to create an AI that understands real attacker behaviors and account privilege abuse in Office 365. By taking a cloud-native approach, Cognito Detect for Office 365 detects and stops known and unknown attacks before they lead to breaches, without relying on preventative security.

30%

30% of organizations suffer from account takeovers every month despite email security

HIGHLIGHTS

DETECT AND STOP ATTACKERS IN OFFICE 365:

Vectra Cognito offers broad coverage across O365 attack vectors by leveraging AI that understands attacker behavior and account privilege — allowing teams to put an end to breaches.

DEPLOY IN MINUTES:

Vectra deploys natively into Office 365 without agents. A Cloud-native approach will immediately start to monitor and detect attacks.

REGAIN FULL SECURITY COVERAGE:

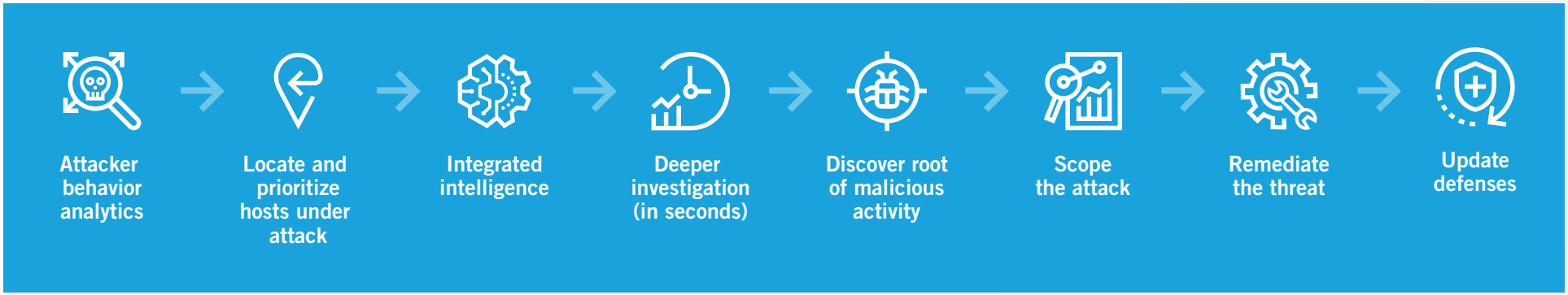
Attackers don't operate in silos; your security solution shouldn't either. Vectra tracks and stops attacks as they progress and move between O365 and your local networks.

Once an attacker has gained access to an Office 365 account, they can move around easily. New phishing attacks originating from the internal company domain, or shared files with malicious code have high success rates and lead to rapid spread in both Office 365 and onto endpoints. The Vectra Cognito platforms' enterprise-wide coverage allows organizations to regain visibility across their entire infrastructure, from cloud to ground. As attacks progress and move between endpoints and Office 365, Vectra enables security operations teams to stay ahead and respond faster with a full context of the threats.

By automatically detecting and prioritizing attacker behaviors, accelerating investigations, and enabling proactive threat hunting, Vectra Cognito for Office 365 takes back control of Microsoft Office 365 security.

Broad coverage across the entire Attacker Kill Chain in Office 365

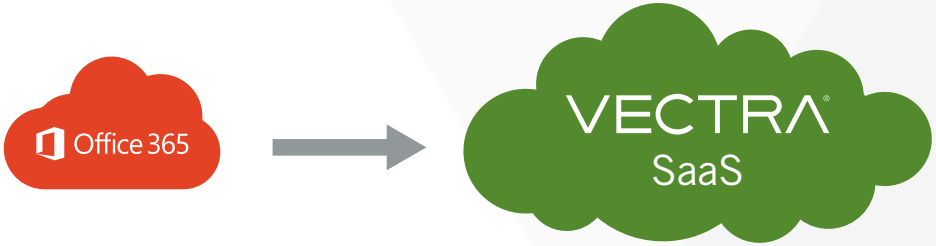
Vectra Cognito for Office 365 ingests activity logs from multiple services like O365, Azure AD, SharePoint/OneDrive, Teams, and Exchange. The Vectra Cognito AI has a deep understanding of Office 365 application semantics and leverages supervised and unsup ervised Machine Learning models. By analyzing events like logins, file creation/manipulation, DLP configuration, and mailbox routing configuration & automation changes, it accurately finds attacker behavior patterns across the entire Attacker Kill Chain. The result is high precision actionable detections instead of anomaly alerts that accurately expose even novel and never before seen attackers with high confidence. The detections are correlated to all accounts devices involved which provides the security team the prioritization and narrative to act quickly.

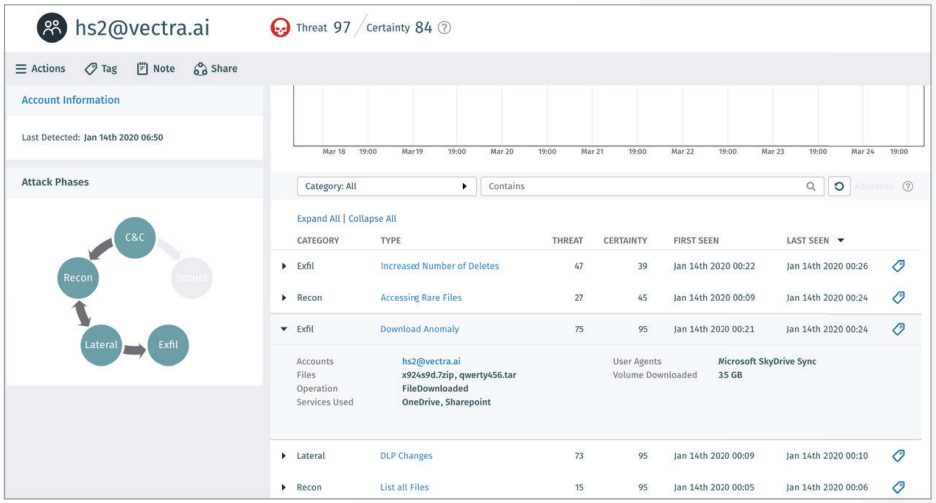


The Vectra Cognito AI has a deep understanding of Office 365 application semantics and leverages supervised and unsupervised Machine Learning models

Cognito Detect for Office 365 covers the entire attacker kill chain

Tactic	Cognito Detect coverage examples
Access	Brute-forcing (including legacy protocols), suspicious logins, adding users to groups
Persistence	Creating Power Automate flows, adding new accounts, installing malicious applications
Privilege escalation	Adding users to groups
Defense Evasion	Disabling security monitoring and logging, bypassing DLP
Discovery	Compliance / eDiscovery searching, email search, file enumeration
Lateral Movement	Internal phishing, watering hole / file poisoning, endpoint takeover via malicious mail rules
Collection	Compliance / eDiscovery searching, email search, file enumeration
Exfilltration	High-risk downloads, mail forwarding rules, employee downloading data before termination
Impact	Encrypting files for ransom





For more information please contact a service representative at info@vectra.ai.

Email info@vectra.ai vectra.ai