VECTRA
SECURITY THAT THINKS.®

INDUSTRY REPORT

2020 Spotlight Report on Office 365

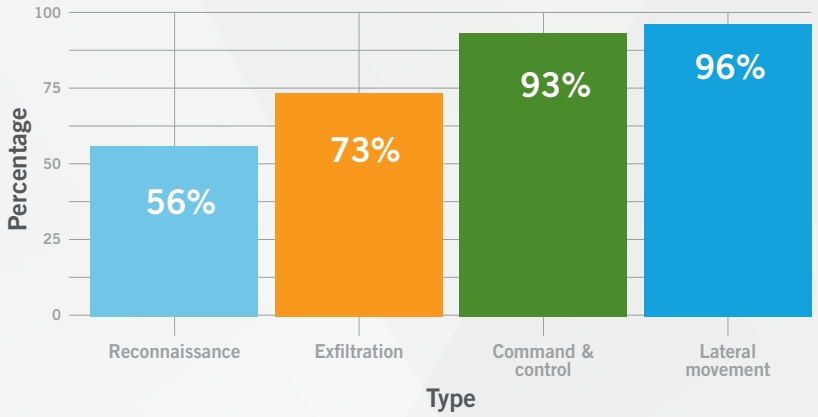
Executive summary

Microsoft continues to grow as the world's most adopted SaaS application provider with over 258 million Office 365 and 75 million Teams users, according to the company's third-quarter earnings call in 2020. As a result, it has become a rich repository for critical business data and a tantalizing target for cyberattackers.

Cognito® Detect for Office 365 from Vectra® automatically detects and responds to hidden cyberattacker behaviors, accelerates incident investigations, and enables proactive threat hunting. In its first 90 days of availability in 2020, Cognito Detect for Office 365 was deployed and protected over 4 million Office 365 accounts.

The Vectra 2020 Spotlight Report contains analysis and findings from Cognito Detect for Office 365 deployments and highlights how cybercriminals use legitimate Office 365 services to launch attacks. Key findings include:

- Multifactor authentication (MFA) controls are being bypassed using malicious OAuth federated authentication applications.
- Microsoft Power Automate workflow services are used to create and automate command-and-control and data exfiltration attack behaviors in Office 365.
- 96% of customers sampled exhibited lateral movement behaviors, and 93% exhibited command and control behaviors.



Frequency of suspicious behavior categories observed in Vectra NDR Office 365 deployments

Read the spotlight report to learn how cybercriminals use legitimate Office 365 services to launch attacks, and how Cognito Detect for Office 365 identified and stopped attackers from reaching their goals.

Get the full report

Email info@vectra.ai vectra.ai