VECTRA
SECURITY THAT THINKS.®

THE CLOUD IS GOOD FOR BUSINESS – AND ATTACKERS

Rapid growth in cloud-based technology adoption

>115M users
Teams is Microsoft's fastest growing business app ever[3]

667% growth
Zoom: Growth since COVID-19 lockdown began

1 in 3 organizations
around the world use Amazon Web Services

70%
of companies are having employees work remote[1]
In many cases, remote work will be either permanent, or optional for employees[2]

Extended workforce now contains contractors, partners, resellers etc., all with access to your data.

8
On average, an employee uses eight SaaS applications.[4]

> " Vectra gives us much better visibility into threat behaviors across our entire deployment. We now have a greater degree of confidence that we can detect and stop credential abuse that has become common in Office 365."
>
> – Kevin Orritt,
> ICT security manager
> Greater Manchester Mental Health

8% decline in IT spending

75% of respondents want cloud first

While Gartner says IT spending will decline 8%, a recent PwC survey shows 75% of respondents want cloud first[5]

Rise of credential attacks vs malware attacks[6]

Account takeover most common vector, even with MFA enabled.

ATTACKS FROM THE CLOUDS

APT33 / Holmium Campaign started in the cloud:
- **Initial Access** gained by compromising O365 accounts
- Created malicious O365 mailbox configurations that forced remote code execution

Famous Breach:
the Capital One breach started in the cloud and cost them 100 million credit card applications and accounts

A note about Virtual machines: If you are digitizing, attackers are sometimes unaware if machine is on-prem or in cloud, making progression seamless between the two.

Vectra analyzed 4 million Office 365 accounts over 90 days[7] (what we found was shocking)

93%
93% of organizations exhibited C2 behaviors

71%
of organizations exhibited suspicious Office 365 Power Automate behaviors

56%
of organizations displayed suspicious Office 365 eDiscovery behaviors

WHAT YOU CAN DO ABOUT IT

1. Monitor for malicious apps connecting to Azure AD with network detection and response for Office 365
2. Turn off capabilities you are not using, including eDiscovery and Power Automate
3. Monitor for malicious account usage (insider threat)

Learn more at: vectra.ai/cloud

VECTRA
SECURITY THAT THINKS.®

[1] https://venturebeat.com/2020/10/27/microsoft-earnings-q1-2021/
[2] https://www.nytimes.com/2020/10/13/technology/offices-reopening-delay-coronavirus.html
[3] https://www.zdnet.com/article/whats-next-for-teams-microsofts-fastest-growing-business-app-in-company-history/
[4] https://www.blissfully.com/saas-trends/2019-annual/
[5] https://www.pwc.com/us/en/industries/tmt/library/covid19-cloud-infrastructure.html
[6] https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf
[7] https://www.vectra.ai/download/spotlight-report-office365