VECTRA
SECURITY THAT THINKS®

INDUSTRY INSIGHTS

Top Threat Detections Across the Education Sector

Clarity for Education Providers' Expanding Cloud

This past year accelerated the adoption of new technologies in order to keep people safe, connected and productive. Education was certainly no exception as students and educators made the switch to distance learning, which in many cases meant extending the use of familiar applications while also adopting new ones. With the need to quickly spin up new tools and solutions, IT teams started reaching further into the cloud for help supporting the need to connect and collaborate with researchers, teachers and students. And while this pace of change was forced by COVID-19, security priorities often got put aside as the dash to maintain access to education was rationally prioritized.

Fast forward a year through the pandemic with cloud usage in colleges and universities at an all-time high, there's still one area that might seem a bit foggy—the security of these applications. This is because the cloud continues to change everything we know about security, leaving the legacy approach to protecting users and assets obsolete. And while it might seem like quite a chore for an already swamped IT staff to sort out how to defend their new cloud assets—AI can make all the difference. The last thing any institution

While it might seem like quite a chore for an already swamped IT staff to sort out how to defend their new cloud assets—AI can make all the difference.

KEY HIGHLIGHTS

- **Top Threat Detections**: Detections detailing abnormal or unsafe activity in Microsoft Azure AD and Office 365 across the education sector.
- **Suspicious and Risky Activity**: A high level of email forwarding and file sharing detections could mean your institution's proprietary information is at risk.
- **Closing the Gap**: Artificial intelligence provides the vision and visibility required to truly know what's going on in your cloud accounts.

needs is its tech team spending valuable cycles on benign alerts, but they do need to accurately detect what is truly going on in their environment.

This industry report discusses the top threat detections across Vectra's education customer base that help ratify attacks in Microsoft Azure AD and Office 365. The information in this report is part of Vectra's 2021 Q2 Spotlight Report titled, Vision and Visibility: Top 10 Threat Detections Across Microsoft Azure AD and Office 365.

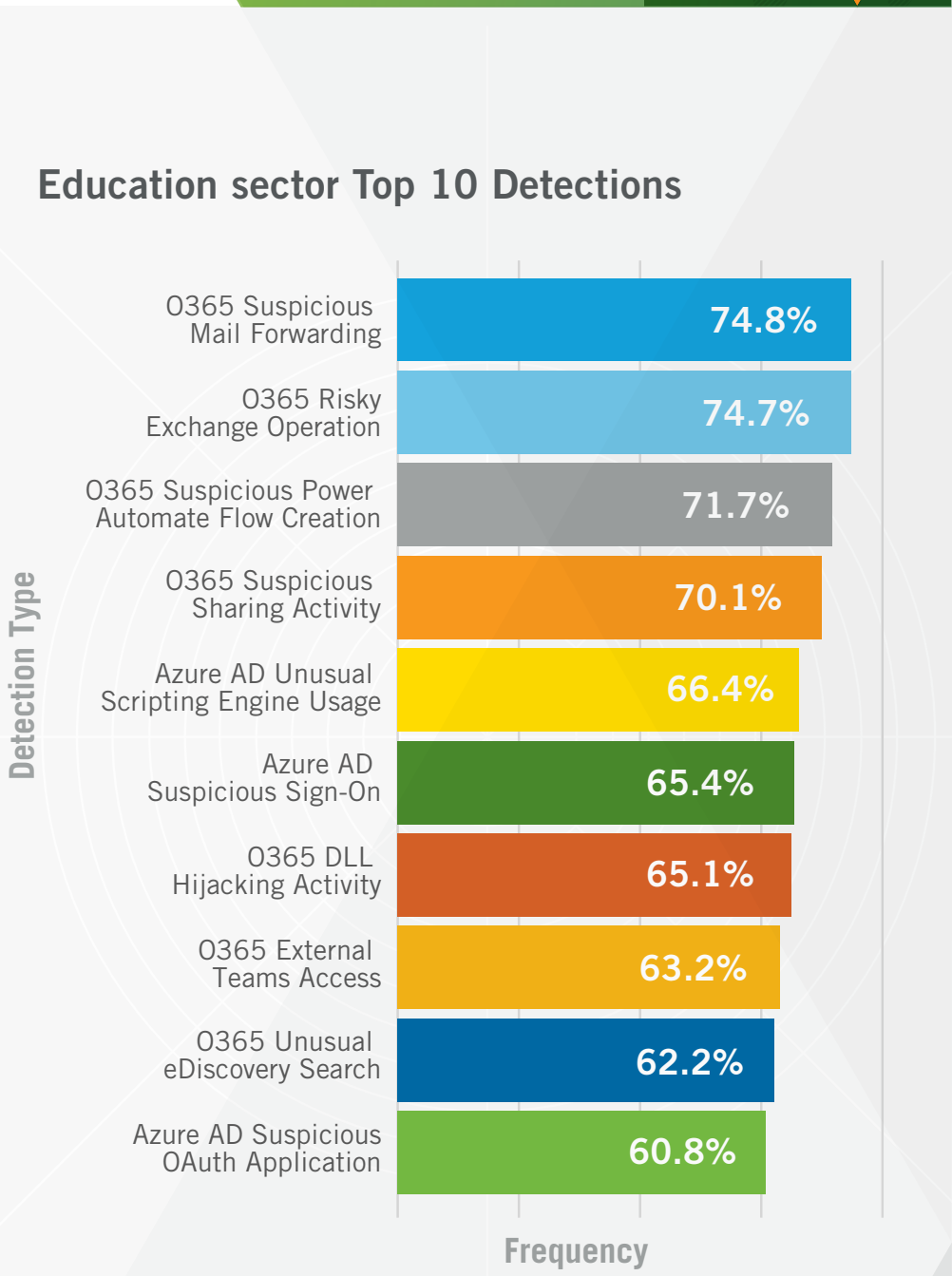
Top Threat Detections Across Education

While these insights focus on the top detections spanning across the Vectra EDU customer base, it's important to keep in mind that threat detection and response is easiest when adversaries take actions that are obviously malicious. This makes it critical that modern network defenders understand the intersection that may exist between the types of actions an adversary would need to take to progress towards their objectives and the behaviors routinely taken by authorized users across the enterprise. Many of the detections discussed in this report represent anomalous behavior and not all of these detections are due to malicious activity. Let's see what detections are frequently being trigged in this environment.

Files on the Move

Result: The high relative frequency of O365 Suspicious Email Forwarding, O365 Risky Exchange Operations, O365 Suspicious Power Automate Flow Creation and O365 Suspicious Sharing Activity relate to email, automated workflow and sharing activity.

Analysis: It's no surprise that email and sharing activity are triggering detections, especially in higher education institutions with the highly mobile and diverse user population. These detections also highlight the challenges that institutions face protecting PII or proprietary research information. While



pervasive information sharing enables learning and collaboration, it adds a level of difficulty to spotting malicious data leakage.

Additionally, the education sector had a high prevalence of Azure AD Suspicious Sign-On detections compared to other verticals. This could be due to the mix of on-campus and remote learning, which has led to a wide range of unmanaged devices and mobile users—highlighting an attack surface that other verticals are able to control more readily. Outside of education, it is common to see a tightly controlled enforcement for what devices are allowed to access within the cloud environment, including apps.

The education sector had a high prevalence of Azure AD Suspicious Sign-On detections compared to other verticals.

Also worth noting is the O365 Suspicious Power Automate Flow Creation detection. Power Automate helps automate mundane tasks like saving email attachments to OneDrive, recording form responses in SharePoint and all types of other convenient uses, however, it's on by default in Office 365 and comes standard with hundreds of connectors. Power Automate is a powerful tool that is appealing to attackers because of the access it would provide for them to live off the land even with basic, unprivileged Office 365 access. Institutions using Power Automate should rationalize access only for users who require it and closely monitor account manipulation that can lead to elevation of privileges and theft of information.

Knowing "Your" Account Behavior

Education certainly isn't the only industry that had to make massive changes to its tech solutions, now it's just a matter of what security tools are used to counter any opportunities left open for actors to exploit. The difference between attacker behavior and privileged account usage can be a blurry area without being able to collect the right data that's aligned with vision and visibility—so you know what authorized use looks like in order to understand the behaviors adversaries are willing to take.

Meaningful AI can help close the gap in your Office 365 and Azure AD accounts, so you have the right data to detect when something out of the ordinary happens. Are you aware when a suspicious attachment gets downloaded, forwarded or shared? It probably wouldn't hurt to know.

Meaningful AI can help close the gap in your Office 365 and Azure AD accounts, so you have the right data to detect when something out of the ordinary happens.

For more information please contact us at info@vectra.ai.

Email info@vectra.ai vectra.ai

Get the full report

Cognito® Detect for Office 365 from Vectra® automatically detects and responds to hidden cyberattacker behaviors, accelerates incident investigations, and enables proactive threat hunting.

About Vectra

Vectra® is the leader in threat detection and response—from cloud and data center workloads to user and IoT devices. Its Cognito® platform accelerates threat detection and investigation using AI to enrich network metadata it collects and stores with the right context to detect, hunt and investigate known and unknown threats in real time. Vectra offers four applications on the Cognito platform to address high-priority use cases. Cognito Stream™ sends security-enriched metadata to data lakes and SIEMs. Cognito Recall™ is a cloud-based application to store and investigate threats in enriched metadata. Cognito Detect™ uses AI to reveal and prioritize hidden and unknown attackers at speed. And Cognito Detect for Office365 and Azure AD™ finds and stops attacks in enterprise SaaS applications and the Microsoft 365 ecosystem. For more information, visit vectra.ai.