VECTRA
SECURITY THAT THINKS®

INDUSTRY INSIGHTS

Top Threat Detections Across Financial Services Institutions

Security Clarity in Financial Services' Expanding Cloud

For many industries, this past year sped up the adoption of new technologies in order to keep people safe, connected and productive. Even the heavily regulated financial industry is seeing many of its institutions move towards the cloud to quickly and economically deliver new services to customers. There has also been a focus on enabling flexibility and access, while the use of Single Sign-On (SSO) using Azure Active Directory (AD) and Office 365 has accelerated to the point of being pervasive in Financial Services Institutions (FSI). But what does all of this mean for the attack surface? Eager cybercriminals are curious and already lining up to test new opportunities that such cloud-based services offer.

While it's true that the always-present cyber risk for FSI isn't going away simply because of new technologies being thrown into the fold—the right cloud vision and visibility can keep things on track. A vision for what authorized use should look like alongside the visibility to monitor and measure deviations from that vision to identify known attacker behaviors. As the cloud continues to change everything we know about security, the right data along with meaningful AI can help bring clarity to the cloud.

As the cloud continues to change everything we know about security, the right data along with meaningful AI can help bring clarity to the cloud.

*Insights based on research collected from Vectra's 2021 Q2 Spotlight Report, Vision and Visibility: Top 10 Threat Detections Across Microsoft Azure AD and Office 365

KEY HIGHLIGHTS

- **Top Threat Detections**: Detections detailing abnormal or unsafe activity in Microsoft Azure AD and Office 365 across Financial Services Institutions (FSI).
- **Suspicious and Risky Activity**: A high level of suspicious download activity and O365 Risky Exchange Operation seen could give attackers access to sensitive information.
- **Closing the Gap**: Artificial intelligence (AI) provides the vision and visibility required to truly know what's going on in your cloud environment.

Recent Vectra analysis based upon observations from Cognito Network and Cloud Detection Platform deployments in FSI, reveal the top threat detections in Microsoft Azure AD and Office 365. The information in this report is part of Vectra's 2021 Q2 Spotlight Report, Vision and Visibility: Top 10 Threat Detections Across Microsoft Azure AD and Office 365.

Top Threat Detections Across FSI

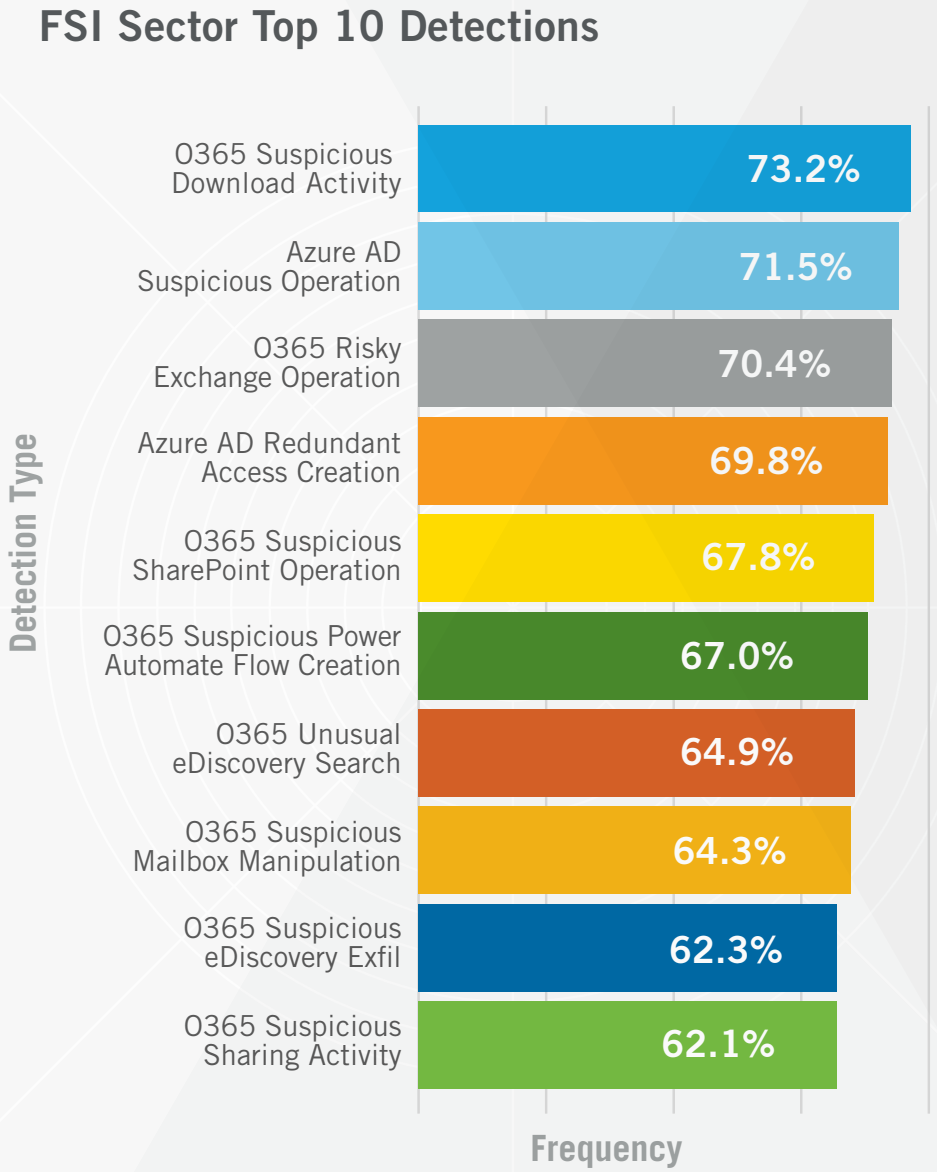
While these insights focus on the top detections spanning across our financial services customer base, it's important to keep in mind that threat detection and response is easiest when adversaries take actions that are obviously malicious. This makes it critical that modern network defenders understand 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.

Risky Business

Result: Financial institutions experience a high prevalence of O365 Risky Exchange Operation and Azure AD Redundant Access Creation detections.

Analysis: The O365 Risky Exchange Operation detection can indicate that access is being provided to sensitive information that would be available in email. This can also indicate that an attacker is manipulating Exchange to gain access to data to move further into their attack progression. If this is the case, the risk here is that this type of access would enable attackers to create backdoors and provide a means to establish persistence. On the other hand, Azure AD Redundant Access Creation detection may indicate that attackers are escalating privileges and performing admin-level operations after an account takeover.

Additional threat detections found in FSI's top 10 were: O365 Suspicious Download Activity, O365 Suspicious Power Automate Flow Creation and



O365 Suspicious eDiscovery Exfil. These activities may indicate that data is being moved out of the environment. But regardless of if an attacker is using SharePoint or OneDrive to download and exfiltrate data or if they're configuring a persistence mechanism like the Power Automate Flow Creation would indicate—the security team needs to know.

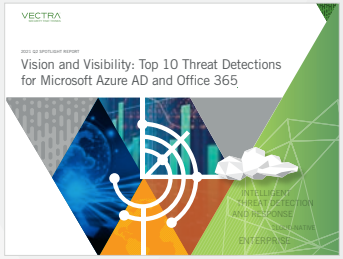
As financial services continue to embrace cloud technologies as a way to bring speed and efficiency to their organizations, this could also bring on more sharing and collaboration with outside entities. Still, the threat detections seen here highlight the available attack surface actors can use to find and extract information, or further their actions within an organization. All customers should ensure their security program has processes in place to routinely review security controls, as well as investigate anomalous activity that could result in data acquisition and loss.

Knowing "Your" Account Behavior

Financial services certainly isn't the only industry that has made recent 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. Due to the strict regulations and prioritizing penetration testing, these institutions generally do a good job of protecting against attacks, but that doesn't mean cybercriminals should be underestimated. They're crafty and will find ways to hide in areas that aren't blocked, making it more important than ever to be able to detect unusual activity. 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 a defined 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 Azure AD and Office 365 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 in your sector? It probably wouldn't hurt to know.

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.

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

Email info@vectra.ai vectra.ai