VECTRA
SECURITY THAT THINKS®

INDUSTRY INSIGHTS

Top Threat Detections Across Manufacturing Organizations

Manufacturing and Cybersecurity—a Complicated Beast

For many industries, this past year sped up the use of new technologies in order to keep people safe, connected and productive, however, the technology requirements for manufacturers came with additional challenges due to the essential nature of the sector. For example, critical manufacturing of materials for medical supplies, transportation, energy and agriculture are just a few of the instances where workers needed to maintain functions to keep operations moving not just for their own facilities, but for the supply chain too—even when the rest of the world was shut down.

So rather than closing up shop, manufacturers kept the lights on and made adjustments where needed from a technology standpoint and elsewhere throughout their operations. The technology piece might just be the one area where manufacturing did see some similarities with other industries in the sense that they continue to increase cloud usage for speed and scale, which does add a layer on top of the attack surface to the already dispersed operational technology infrastructure. So, with cybersecurity in mind, what challenges does the cloud present to manufacturing as an industry that typically prioritizes limiting downtime due to equipment failures?

Manufacturing continues to increase cloud usage for speed and scale, which adds a layer on top of the attack surface to the already dispersed operational technology infrastructure.

*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 Manufacturing organizations.
- **Suspicious and Risky Activity**: A high level of suspicious O365 Sharing Activity could indicate that attackers are using SharePoint to exfiltrate data or maintain access.
- **Closing the Gap**: Artificial intelligence (AI) provides the vision and visibility required to truly know what's going on in your cloud environment.

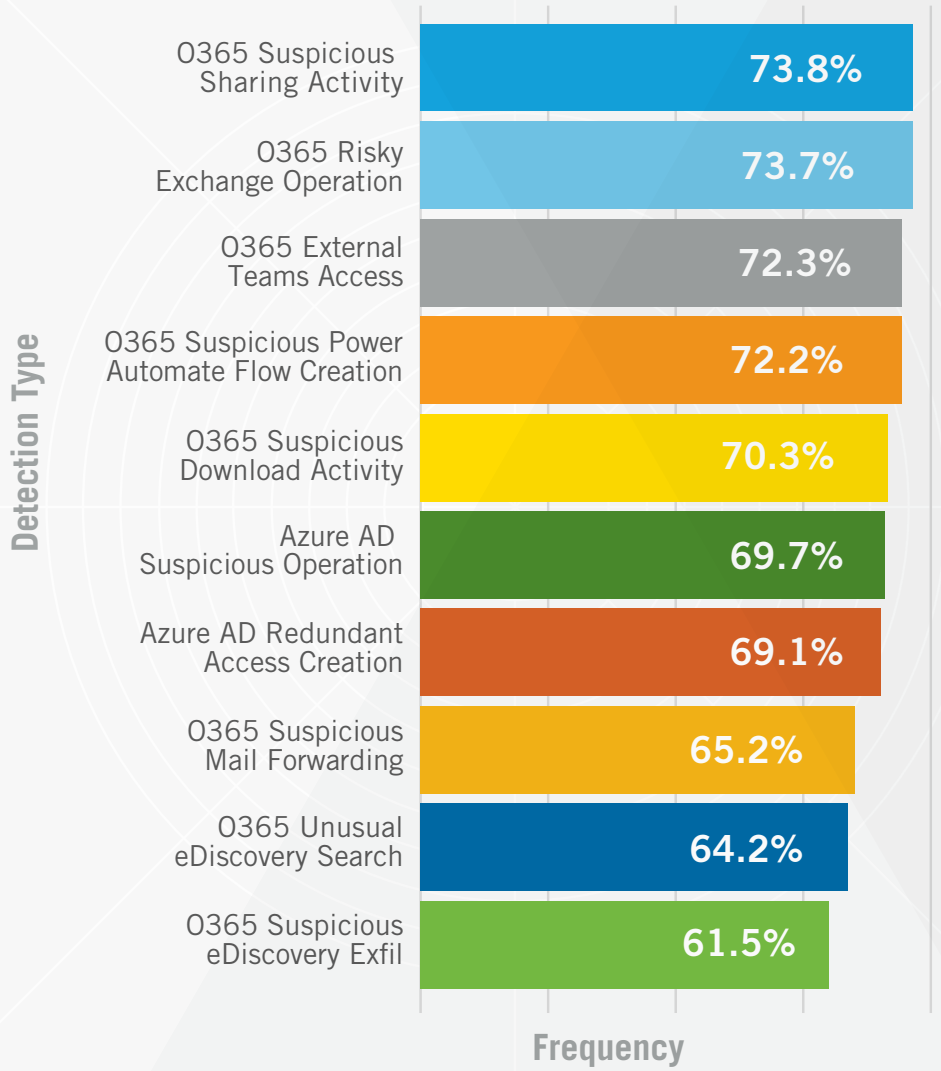
The recent Spotlight Report—Vision and Visibility: Top 10 Threat Detections Across Microsoft Azure AD and Office 365 takes a deep look at this exact scenario across all industries, however, the industry insights highlighted here focus on the manufacturing sector. These insights reveal the top threat detections across the Vectra customer base that help ratify attacks for manufacturing organizations in Microsoft Azure AD and Office 365. This detection information can be put to use along with the right vision and visibility to help keep things on track. A vision for what authorized use should look like and the visibility to monitor and measure deviations from that vision. 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.

Top Threat Detections Across Manufacturing

While these insights focus on the top detections spanning across Vectra's manufacturing customers, 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.

The manufacturing sector sees a high prevalence of O365 Suspicious Sharing Activity, O365 Risky Exchange Operation and O365 External Teams Access detections.

Manufacturing Sector Top 10 Detections



We'll Do The File Sharing Around Here, Thank You

Result: The manufacturing sector sees a high prevalence of O365 Suspicious Sharing Activity, O365 Risky Exchange Operation and O365 External Teams Access detections.

Analysis: O365 Suspicious Sharing Activity is triggered when an account is seen sharing files or folders at a higher rate than normal. The necessity of receiving this threat detection is that it could indicate that an attacker is utilizing SharePoint to exfiltrate data or even maintain access after their initial access was remediated. O365 Risky Exchange Operation was also near the top of the detection list for manufacturing and the risk here is that it could indicate that access is being provided to sensitive information that would be available in email. There is the potential with this detection that an attacker is manipulating Exchange to gain access to data and ultimately move further into their attack progression—allowing them to create backdoors and a means to establish persistence.

Also in manufacturing's top three was the O365 External Teams Access detection, which could indicate that an attacker has added an account under their control. The fact that two of the top three detections were related to sharing activities could mean that these types of activities are less common in this particular sector, which is why it's important for customers to receive them.

Two of the top three detections were related to sharing activities which could mean that these types of activities are less common in this particular sector.

Any observed abnormal mailbox changes can circumvent security controls and should be scrutinized in conjunction with email forwarding.

Another detection that should be highlighted even though it's lower down on the list is O365 Suspicious Mail Forwarding, which should raise some eyebrows because this activity could be used as a collection or exfiltration channel for attackers. Vectra actually observed a number of manufacturing customers who provide contractors or other third parties with corporate email accounts that are configured to forward messages to that individual's outside email. This process adds a level of convenience for the individual or contractor, however, it shows evidence of non-existent policies around enforcement of email forwarding. This presents a challenge for the organization because any unwanted data leakage becomes more difficult to spot, and this is also a technique that attackers use to surreptitiously obtain copies of a desirable account's email.

Looking ahead, this type of activity should always be reviewed to ensure authorized behavior. Additionally, any observed abnormal mailbox changes can circumvent security controls and should be scrutinized in conjunction with email forwarding. Based on the detections reported here and what is common knowledge about the IT systems in a manufacturing environment, these organizations should ensure that proper auditing of controls are performed and that threat detections are reviewed to confirm that any abnormal sharing or collaboration taking place is known by the security team.

Knowing "Your" Account Behavior

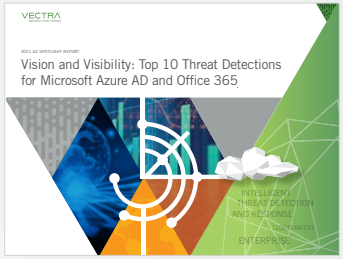
While cloud platforms like Office 365 and Azure AD may not be the first areas that manufacturing thinks of to defend, these are still part of the larger attack surface that attackers will exploit. It's important to remember that attackers will target any organization where there's an opportunity to extort money or steal assets of value. Manufacturing is especially susceptible to extortion if cybercriminals are able to impact their operational ability, where a ransomware attack for example could force the company to either pay a ransom or seize operations.

In addition to ransomware, supply chain attacks are another area where hackers are showing significant skill in evading preventative controls and causing large amounts of damage. The full Spotlight Report goes into more detail about how attackers are exploiting the supply chain and even dissects a real-life supply chain attack to show how Vectra threat detections would map back to attacker activity. The difference between attacker behavior and privileged account usage can be a blurry line without the ability to collect the right data that is properly aligned with defined vision and visibility. But it's important to get to a point where you know what authorized use looks like in order to understand the behaviors adversaries are going 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 sensitive information is shared with an outside party or when privilege is escalated within your Microsoft cloud? It probably wouldn't hurt to know.

For more information please contact us at info@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.

Email info@vectra.ai vectra.ai