VECTRA
SECURITY THAT THINKS.®

DATA SHEET

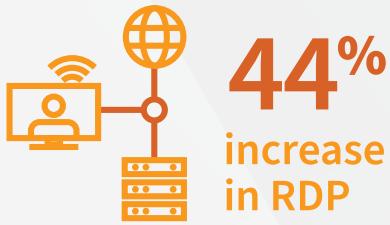
Remote work, not remote control: Detection guidance

In order to contain the spread of COVID-19, employees are being asked to work remotely when possible. This sudden and immediate shift of employees who would normally work in an office to a remote location in those organizations that normally are not already fully remote will naturally create a shift in internal movement of network traffic, which directly impacts the behavioral detections identified from the Cognito platform.

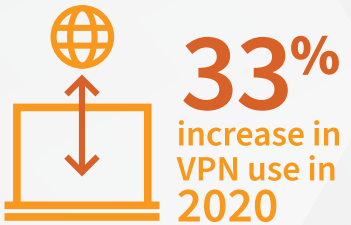
Vectra is making the following recommendations for users of the Cognito platform to identify and manage the expected increase in behavioral detections related to certain remote worker conditions.

Summary

- Identify the organization's VPN pool using the Groups page to identify remote workers faster.
- If the video conference detections become too noisy, create triage filters based on Templates available within the platform for the software in use.
- After some basic investigation to confirm authorization, write rules for remote access tools if they become too noisy.
- Use Custom Templates as a guide but create rules specific to the organization
- Heavy VPN usage may cause a sudden uptick of lateral movement detections related to administration. Learnings will eventually pick up this new paradigm with proper host attribution.



Are your RDP / VDI services unknowingly exposed?



Are your VPN credentials being abused?

Can you identify unprotected devices remotely accessing your systems?

When building a triage filter in Cognito, the configuration of source condition rule suggestions is to use non- datacenter source IP space. If the analyst is unable to differentiate between data center and non-datacenter source IP space in the Cognito platform, then Vectra recommends to us All Hosts.

Web conferencing

As remote workers need to continue to be connected to their peers, clients and partners without in-person communication, the uses of web conferencing and instant messaging software is expected to grow. This usage will encompass not only peer-to-peer video communication, but will also be used for sharing information through multiple methods including file sharing, screen sharing, and other related activities. These communications and file sharing behaviors will likely increase the number of behavioral detections in the Cognito platform. It is recommended that users identify the expected communication services within their organization and create custom filters to mark those as expected behaviors.

These communications and file sharing behaviors will likely increase the number of behavioral detections in the Cognito platform.

For example, Microsoft Teams can be easily identified either by the IP range in use: 52.112.0.0/14 or by the primarily used protocol and ports: UDP 3478 to 3481. By leveraging this information, triage rules can be written with minimum impact to normal operations.

By default, several video conferencing providers' IP ranges are already part of Cognito Groups pages, as show in Figure 1, that help identify known legitimate behavior.

Cognito - Teamviewer	IP	178.77.120.0/24, 185.188.32.0/24, 185.188.33.0/..
Cognito - Terminal Servers	Host	—
Cognito - VPN Pool	IP	—
Cognito - Webex	IP	114.29.192.0/19, 173.243.0.0/20, 173.39.224.0/1..
Cognito - Zoom	IP	103.122.166.0/23, 109.94.160.0/24, 115.114.131.0..

Figure 1. Cognito Groups

The expected network behaviors related to the use of web conferences tools would be the following:

Command & Control

Web conferencing software is a commonly used remote application within most organizations and has the capability of controlling another user's system. For this reason, there are known attacks that lever existing web conferencing software for malicious purposes. Common behavioral detections related to the use of web conferencing software including the following:

- **Hidden HTTPS Tunnel** – Writing a rule based upon the destination IPs is suggested.
- **Suspicious Relay** – Writing a rule based upon the destination IPs is suggested

Exfiltration

As exfiltration detections are based upon traffic patterns and the amount of data usually sent to a specific destination, an increase in related exfil detections may be seen, as users share files or send video.

- **Data Smuggler** – Writing a rule based upon the destination IPs and ports is suggested.
- **Hidden HTTPS Tunnel** – Writing a rule based upon the destination IPs is suggested

- **Smash & Grab** - Writing a rule based upon the destination IPs is suggested

Figure 2. Smash and Grab behavior for Teams

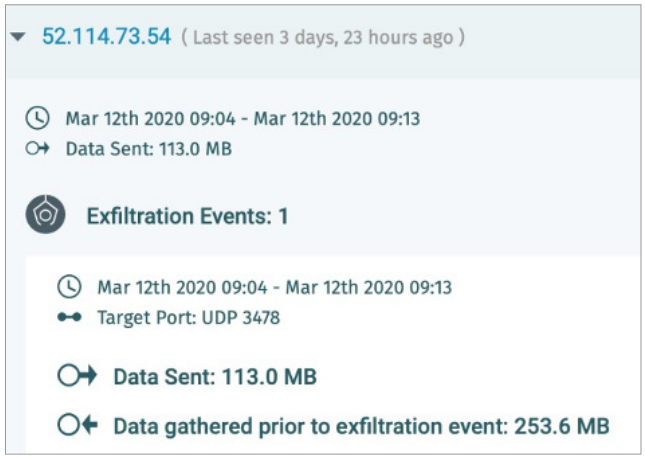


Figure 3. Data Smuggler behavior for Teams

In addition to configuration custom rules, Cognito has predefined triage templates for known web conferencing software designed to reduce the noise generated by web conferencing software.

Remote access software

Another expected area of growth will be in the use of remote access tools such as TeamViewer to access internal resources. This will especially be true if the corporate VPN is not able to handle the traffic for the entire company as alternative means of managing internal resources.

In the same way an administrator would use remote access software to manage a server, an attacker regularly wants to access and manage these internal systems as part of their attack lifecycle. Because there is a sudden and sharp increase in legitimate remote access, this detection model may trigger an immediate increase in previously seen remote access behaviors. Vectra recommends identifying these expected services and creating custom filters to mark as approved.

By design, remote access tools provide the ability to control both other users' machines and servers, which is also an attacker's goal. The more popular tools leverage the vendors external servers as relays (LogMeIn, TeamViewer) between the user requesting access and the system to managed. This makes these tools more easily identifiable as they occur from a known address space. For example, TeamViewer servers are explicitly named in the remote access behavior detection description field, which can then be leveraged for a triage filter after an analyst strict validation that this is authorized remote network traffic.

In addition to third party remote access tools, Windows natively provides native remote access functionality that allows a user to directly access internal devices that would usually be restricted but now require remote access for an administrator to function remotely. For example a jump server could allow the Microsoft Remote Desktop Protocol to access specific systems to a privileged user. Due to the versatility of these tools, we recommend rule creation be as narrow as possible.

The expected network behaviors related to the use of remote access tools would be the following:

Command & Control

- **Hidden HTTPS Tunnel** – Depending of the amount of noise generated by such detections, writing a rule as narrow as possible, based upon the destination IPs and source IP(s) is suggested.

- **External Remote Access** – Depending of the amount of noise generated by such detections, writing a rule as narrow as possible, based upon the destination IPs and source IP(s) is suggested

- **Suspicious Relay** – This detection can be triggered when a user uses a jump server or a relay for remote desktop access on a specific host. Vectra recommends an analyst tag the source host as authorized for this action and use one-time mark as custom, assuming a low volume of noise. If these types of behaviors are prevalent from a system, consider writing a custom filter based upon the destinations IPs and ports.

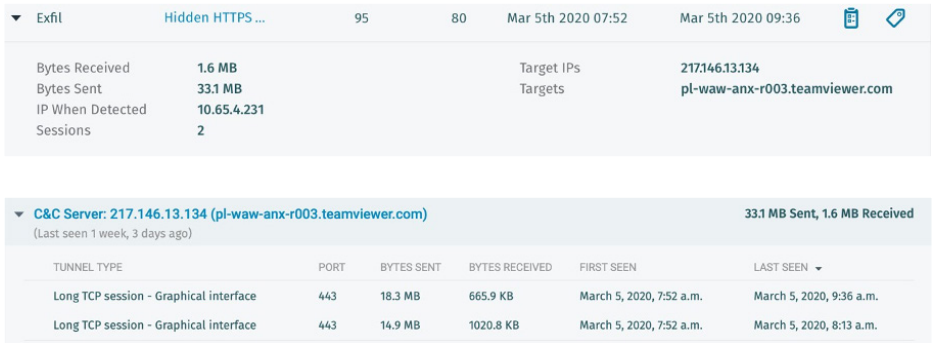


Figure 4. Hidden HTTPS Tunnel detection

Figure 5. External Remote Access

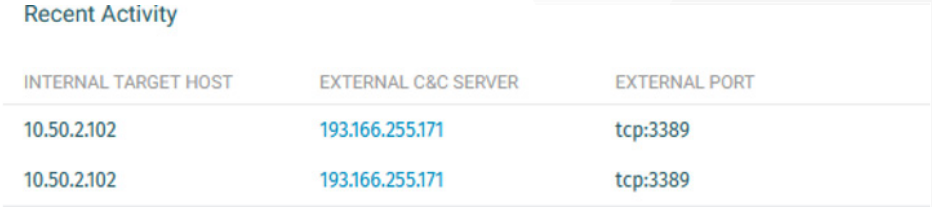


Figure 6. Suspicious Relay

File sharing

While online file sharing services like OneDrive and Dropbox are already popular in the enterprise and for consumers, we expect to see increased usage and leveraging of file sharing services as the primary means of document sharing and editing. Understanding how these file sharing services will be used within the organization is critical. Analysts can investigate if file sharing services currently in use and seen in the Cognito platform are approved by validating if the external host complies to the company's security policy.

Exfiltration

Exfiltration behavior detections are related to the volume of data sent and destination. We expect to see a deviation in both attributes which will trigger the following behaviors during the extended work at home time period:

- **Smash and Grab** – If these detections became too noisy, and the external host is identified as authorized, it is suggested to create a filter for the external destination.
- **Data Smuggler** – If these detections became too noisy, and the external host is identified as authorized, it is suggested to create a filter for the external destination.

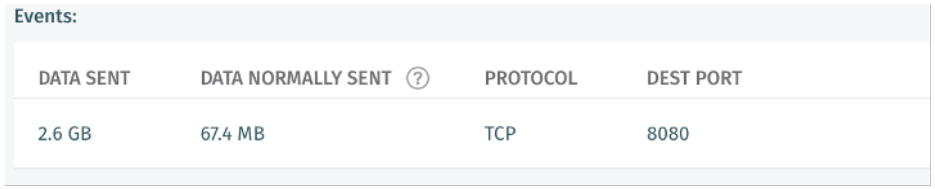


Figure 7. Smash and Grab detection

Usage of non-corporate managed system through VPN access

As users work from home, they may be inclined to leverage a personal system in their home environment. In the eventuality that this does occur a new system is leveraged over VPN access to internal resources, the Cognito platform will identify these devices as new hosts, which may lead to a variety of privilege anomalies and other new behavior detections based upon never before seen system to user to service access patterns. The Cognito Host Details page provides details to identify an unknown host by name, accounts, and last seen time and date. This information, along with the identification of the organizational VPN IP Pool in the Groups Page will help an analyst identify unknown user devices efficiently.

Lateral movement

- As the host will be considered "new", it represents an unknown device within an organization which could be an attacker's computer. As attackers would like to extend their attack accessing various internal resources, some authorized behaviors can be detected as lateral movement attempts.
- **Privilege Access Anomaly: Unusual Host** – After identification of the VPN IP space and investigation into the event, Vectra recommends using one-time Mark as Custom triage filters.
- **Suspicious Remote Desktop** - After identification of the VPN IP space and investigation into the event, Vectra recommends writing a rule based upon source host and target domain. If the RDP traffic is not encrypted internally there will be more options for filtering, such as Client Name.

Note: Vectra strongly encourages analysts to not to write custom filters without initial investigation due to the nature of the behaviors expressed in the above detection models. For hosts that are identified and authorized by an analyst, filters should be written for those specific hosts only.

Bandwidth surveillance

We expect to see a large increase in VPN use as the bulk of organization users work remotely but still need access to the same internal resources they had when working in the office. This means that VPN availability will be critical for the organization to function and will be required to handle a much larger volume of traffic than usually seen.

Some user behaviors that would normally be innocent and benign when performed inside a network, such as listening to music apps on a PC while working, could be a problem on a full tunnel VPN. A full tunnel VPN sends all internet traffic through the organization internal network, thus consuming large volumes of network bandwidth which causes VPN resource exhaustion.

Users of Cognito Recall and Stream can track this type of normally benign traffic in order to identify users with large volumes of bandwidth consumption.

Use of VPN

If the corporate VPN uses network address translation (NAT) to assign the same IP to multiple concurrent users, Vectra recommends the following procedures:

- Add the VPN pool IPs to the list of proxies under Manage -> proxies.
- Add the IPs to an IP group called VPN pool.
- Look at a detection view for the detections on the VPN group (instead of a host-based view). Manual correlation will be required to know which user logged in using that IP address at that time

If NAT functionality is not available and only one user can be assigned an IP from the VPN pool, Vectra recommends the following procedures:

- Add the IPs to an IP group called VPN Pool.
- Look at a detection view for the detections on the VPN group. Manual correlation will have to be performed to know which user logged in using that IP address at that time.

Split VPN

Please note that if the organization userbase is using a split VPN, analysts can expect a reduced number of behavior detections. With a split VPN, some of the user's traffic will go straight out to the internet without first traversing the organization internal infrastructure.

For more information please contact a service representative at info@vectra.ai.

Email info@vectra.ai vectra.ai