**Carbon Black and ServiceNow Integration**

**Current Behavior:**

Tickets on ServiceNow are not synchronized with Carbon Black meaning that both services need to be updated in order to have them synchronous.

**Desired Behavior:**

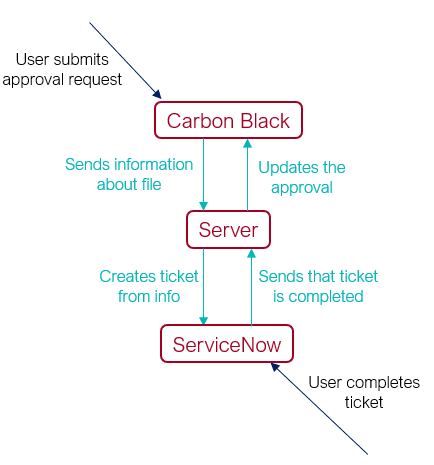
When one service is updated, the other one is as well. The information that Carbon Black sends to create a ticket is more specific to the instance.

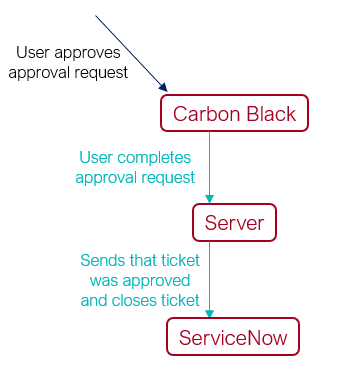
**Potential Solution:** Intermediate Server

Currently, the two services are separate, but both of them have APIs that can be used to do remote actions. One option is to try and configure it so they have a “direct” link to each other, but it might be better to have each one link to an intermediate server. That server would serve as a man in the middle that would be able to formulate API calls between the two properly.

Using an intermediate server would allow more complicated logic, and it would expand what we are able to do with the information we send it. For example, data about the requested file is sent to the server, and the server forms the API call to ServiceNow. However, that data could also be used for a different purpose, and it is easy to implement that with the server.

Due to the nature of synchronization, there needs to be two-way communication between the services. The server eases the pain of doing this because every time something is updated on one, it will ping the server which will update it on the other. This is nicer than having to create two one-way connections. There just needs to be setup so that each service can both send and receive to/from the server.

**Data Flow:**



As seen above in the first diagram, a user will submit a request for approval to Carbon Black, and Carbon Black will then send the information of that request to the server which is how there can be more detailed/specific tickets. The server then sends that information to ServiceNow to create the ticket which a user then completes. Once completed, ServiceNow then sends that to the server which then synchronizes with Carbon Black.

The second diagram shows what happens when there is already a pending approval request, and someone completest it on Carbon Black. Once completed on Carbon Black, it will tell the server that it is completed, and the server will then ping ServiceNow to close the ticket.

**Technical Details:**

Carbon Black API:

* Can complete approval requests
  + If the intended behavior is that the approval requests can be completed in ServiceNow, this will be used

ServiceNow API:

* It is possible to update and create a ticket using the ServiceNow API

**Notes:**

It is likely possible to approve the requests through ServiceNow rather than just Carbon Black if that is desired. It would require that ServiceNow has some interface that allows for a yes/no for the ticket, and if it presses “yes” then it will send the signal to the server which can use the Carbon Black API to approve or deny the request.

The details of the server are in its own document and the document for the Virus Total automation.

**Conclusion/Summary:**

The desired behavior is that when someone makes an approval request for Carbon Black, it creates a specified ticket on ServiceNow, and when either side is updated, it synchronizes to the other as well. When the request is approved on Carbon Black, it will also close the ticket on ServiceNow. (The reverse may be desired as well).

The implementation of this could be an intermediate server that each service connects to rather than forming a direct link. This server can formulate the specific API calls necessary for both services, and when one side updates, it will ping the server which will update the other.

Both services seem to have the API’s necessary to do this, but the challenges are likely in getting it to trigger things on specific actions, but these issues would persist in any implementation of a solution.