**Lab – 31: Protecting your organization from ransomware.**

**Objective:** The objective of this lab is –

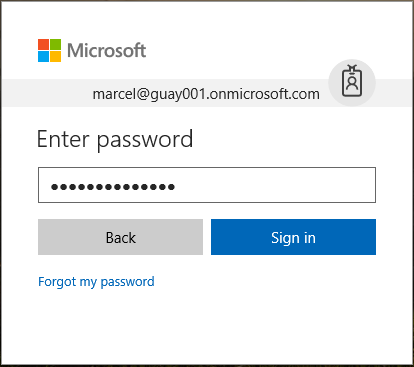
* To protect your organization from ransomware.

In latest massive ransomware attack, WannaCry hit the cyber world hard, infecting an estimated 200,000 computers across 150 countries. With the increase of ransomware attacks over the last few years, an average of 25,000 attacks per month in 2015 and 56,000 in 2016, it's becoming a cybersecurity necessity to be proactive about making sure your network and your cloud aren't at risk. In this lab, we will learn how we can use Cloud App Security to monitor our cloud so that we can detect and mitigate threats and apply best practices for protecting our environment against ransomware.

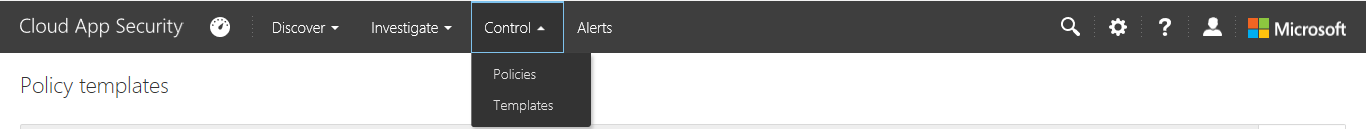
**Prerequisite:** EMS Enterprise Mobility + Security E5. To set up Cloud App Security, you must be a Global Administrator, a Compliance Administrator or a Security Reader in Azure Active Directory or Office 365. Connect at least one cloud app (Office 365, G Suite, Box and Dropbox) to Cloud App Security.

**Steps:**

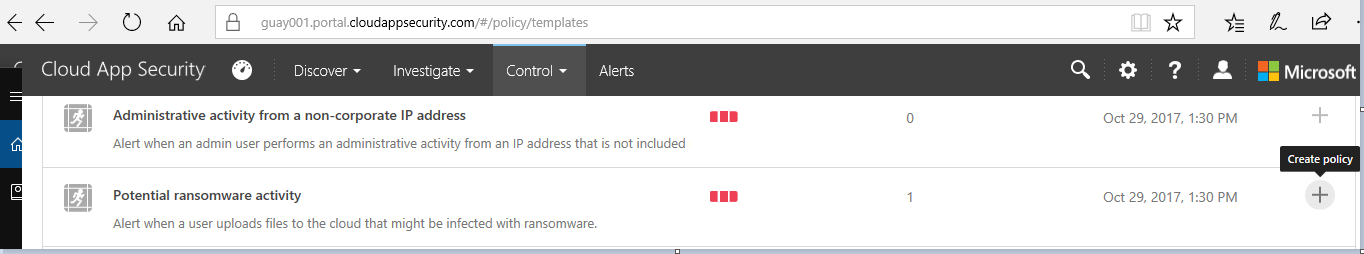
1. To access the Cloud App Security portal, go to <https://portal.cloudappsecurity.com>.



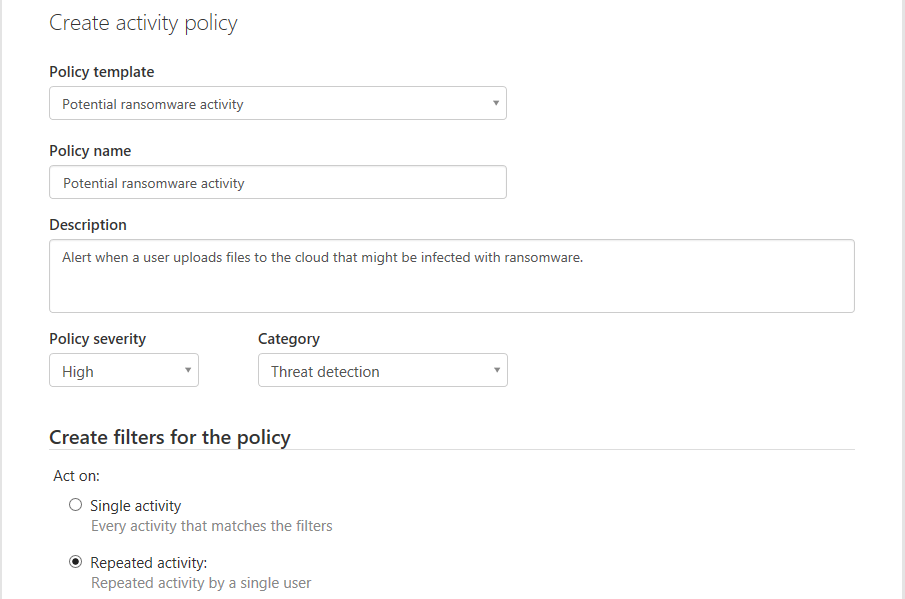
1. When you sign-in to Cloud App Security a general dashboard will be shown.
2. It is important to start monitoring your cloud apps by setting up a policy that will watch your cloud apps for massive downloads and alert you if something out of the ordinary happens. For this:
3. On the **Control** tab, click **Templates**.



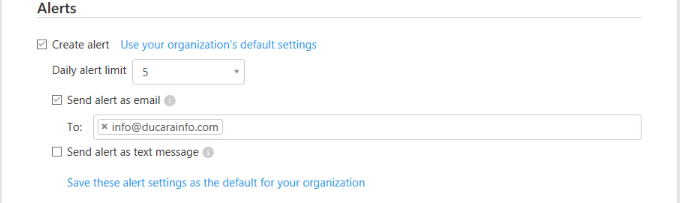
1. From the **Policy template** list, choose **Potential ransomware activity**. Click + icon to create a policy. Use this policy to get an alert when a user uploads files to the cloud that might be infected with ransomware.



1. Enter the fields or keep it by default. Policy severity should be High and Category should be Threat detection. You can also create filters for the policy.



1. This template is designed out-of-the-box to search for activity typical of ransomware attacks, and files and folders associated with known ransomware. Optionally, you can set the type of alert you receive (email and text message) when the policy is matched.



1. Click **Create**.
2. You will get notification at the top right corner, **Created activity policy successfully**.
3. Now you can see Potential ransomware activity policy is added. Click  to **Disable** or **Delete** this policy.
4. You can investigate the match by clicking on a specific policy to open the activity log.
5. So, in this way you can use Cloud App Security to monitor your cloud so that you can detect and mitigate threats.