Windows Defender Advanced Threat Protection (ATP) Trial

Your Personal

Walkthrough Tour

Now that you've logged into the Windows Defender ATP portal, it's time to explore the various features of this service.

1 Start with the basics

Typically, investigating security incidents using the Windows Defender ATP portal involves the following stages:

1

View alerts
View an alert in the Dashboard or in the New Alerts queue or search for a file, process, IP, URL or user using the search function.

2

Review
Review alert details, machine timelines, file records and conduct deep analysis to understand the nature of the observed indication. Identify a component of a known attack or suspicious behavior that might indicate an attack on the network.

3

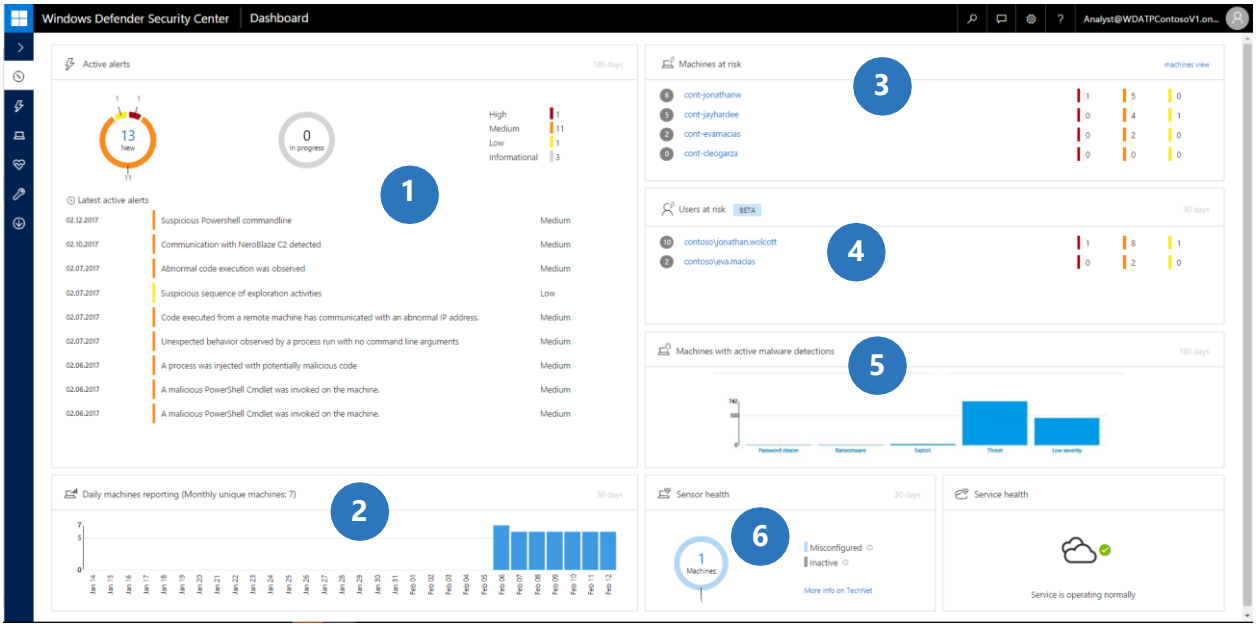
Collect information
Collect information to understand the full scope of breach, derive possible courses of action and proceed to act on them.

4

Respond
Quickly respond to detected attacks by stopping and quarantining files, isolating machines or collecting an investigation package for further analysis.

2 Dashboard

The dashboard displays a snapshot of the active alerts on your network, top machines at risk, number of machines reporting to the service and the status of the Windows Defender ATP.



Section 1 | ATP alerts

Displays active alert information across three levels of severity: high, medium, and low. Alerts are shown by their associated state in the alert queue: new, in progress, or resolved.

Section 2 | Daily machines reporting

Displays the number of machines reporting daily (24-hour) over a 30-day period

Section 3 | Machines at risk

Provides information on specific machines and is sorted by number and alert severity. The screenshot shows that Jonathan's machine has 1 high, 5 medium, 0 low alerts.

Section 4 | Users at risk **[available only for preview users]**

Displays the users that have triggered alerts in the system for further investigation.

Section 5 | Machines with active malware detections

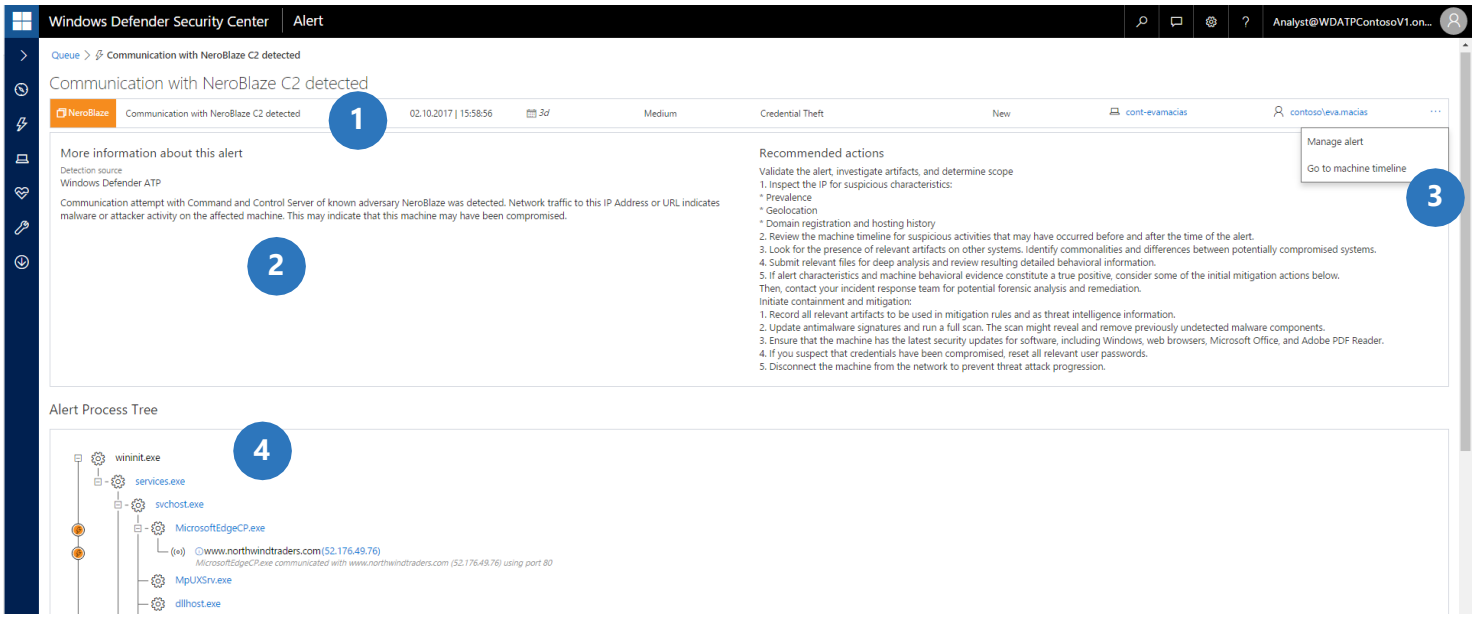
If your enterprise is using Windows Defender Antivirus, you'll be able to see malware detections in your network grouped by category. Clicking on each category will take you to the Machines view of the related machines.

Section 6 | Sensor health

Indicates the number of machines that are not reporting sensor data properly to the service: 1) Inactive - machines that have stopped reporting for more than 7 days in the past month; 2) Misconfigured - machines that are partially reporting security data and might have configuration errors that need to be addressed.

3 Viewing an alert

Clicking on a specific alert takes you to a detailed alert page that includes the following:



Section 1

Provides a brief description of the alert, when it was detected, and the affected machine.

Section 2

Provides details about the alert to give you better contextof the nature of the threat.

Section 3

You can manage an alert and bring up the alert management pane or go the Machine timeline to see where and when the alert was triggered on the machine.

Section 4

The **Alert process tree** takes alert triage and investigation to the next level by displaying the alert and its evidence with other events that occurred in the same execution context and time. This broad triage context of the alert and surrounding events is available on the alert page.

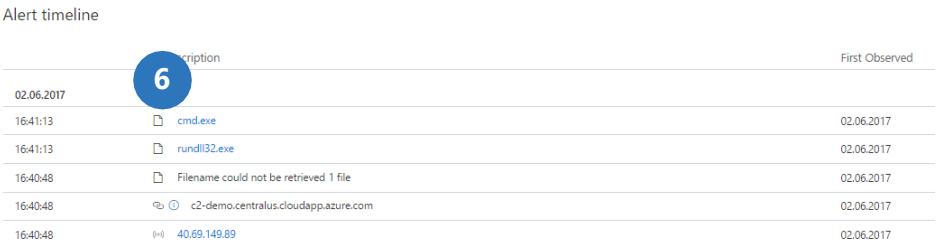
3 Viewing an alert (continued)

Section 5

The **Incident graph** provides a visual representation of where an alert was seen, the events that triggered the alert, and which other machines are affected by the event. It provides an illustrated alert footprint on the original machine and expands to show the footprint of each alert event on other machines.

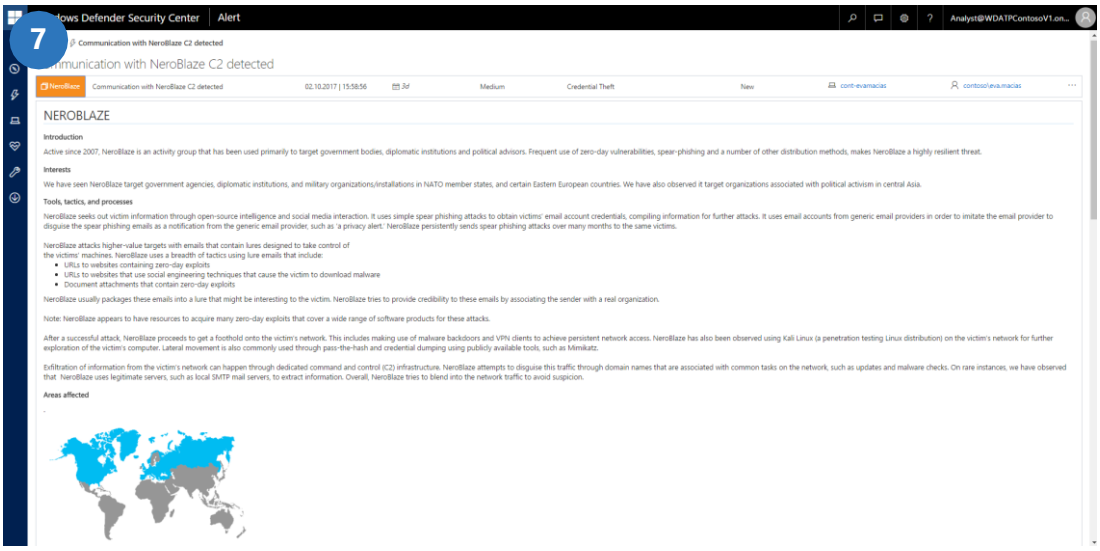
Section 6

The **Alert timeline** feature helps ease investigations by highlighting alerts related to a specific machine and events.



Section 7

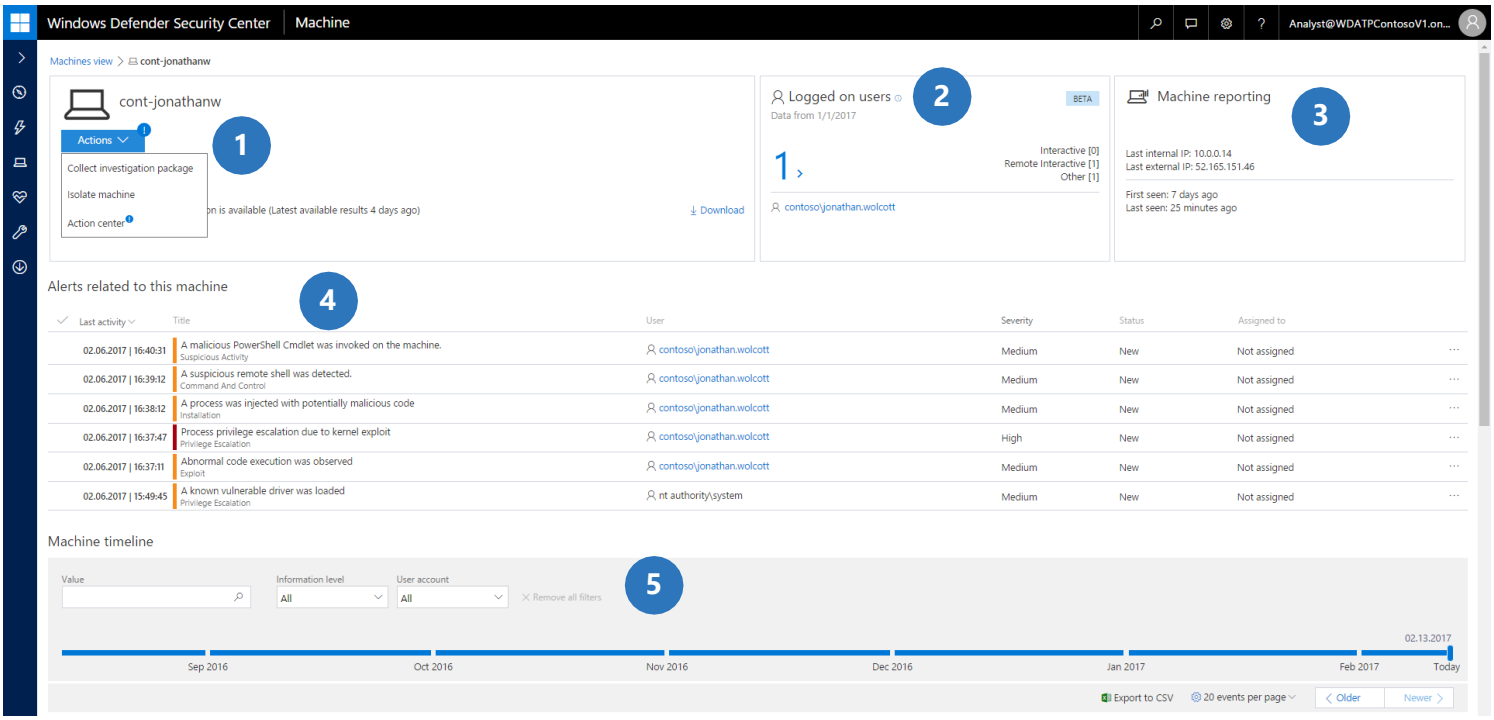
Clicking on the NeroBlaze label will display a Threat Intelligence profile of the attacker. The detailed alert profile helps you understand who the attackers are, who they target, what techniques, tools, and procedures (TTPs) they use and geolocations they are active in. In many cases, you can download a more detailed Threat Intelligence report about this attacker or campaign for offline reading.



Did you know: our Threat Intelligence (TI) reports combine Microsoft's TI with that of select 3rd party TI

4 Machine

Clicking on specific machine takes you to a detailed machine page that includes the following areas:



Did you know: You can travel back in time on protected endpoints to view and explore historical data. You can choose to store collected data for up to 6 months.

Section 1 **[part of the functionality available only for preview users]**

The first section shows details such as machine OS, domain info and "Actions" button designed to provide with the right set of activities you need to quickly respond to an attack. You can collect investigation package for further analysis, isolate machine from your network and view all your response action by selecting Action center. **Note: the "Action" button will be only visible only for preview users connecting Windows 10 machines running build #15031 or later.**

Section 2 **[available only for preview users]**

Provides information on the users that logged in to that machine. You'll see total logged on users and who frequently and less frequently logged on. Clicking on the total logged on users opens the User details pane where you'll see more information about logged on users in the past 30 days.

Section 3

Machines reporting stats, shows information such as internal and external IPs including first and last seen time indications.

Section 4

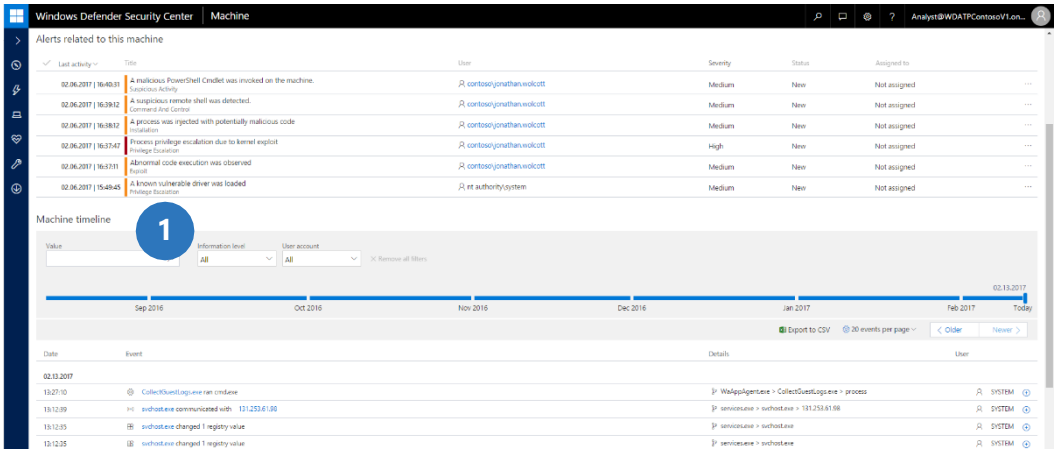
Alerts raised on the machine show the attack stage each is associated with. Viewing a sequence of alerts 'tells the story' of an attack with higher confidence than any single alert.

Section 5

The machine timeline provides a chronological view of the alerts, behaviors, and events that were observed on the machine, going back in time.

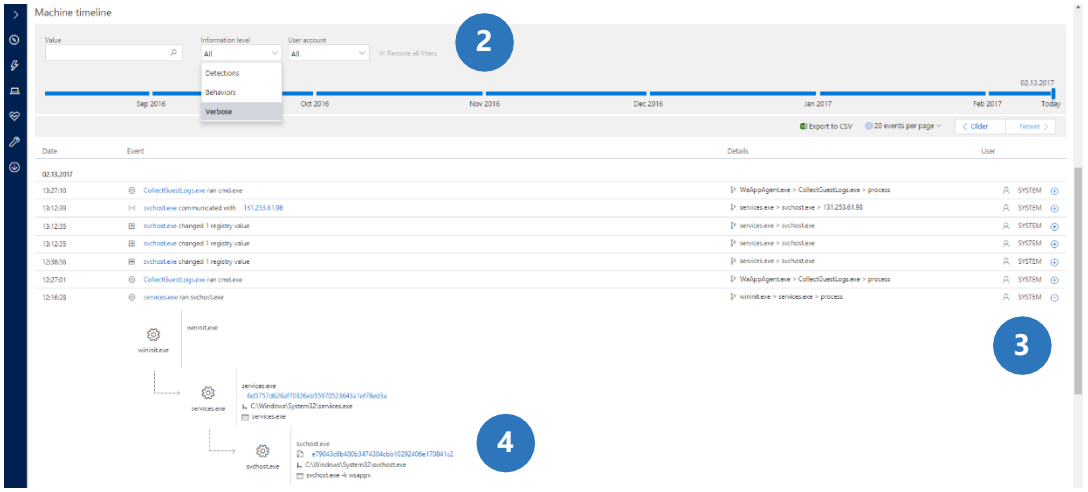
5 Machine Timeline

The Machine Timeline (1) provides a rich view of events and behaviors observed on the machine over time (up to 6 months), enabling remote investigation of any machine, as well as easy and intuitive pivoting on any indicator to view its profile and other machines it was observed on.



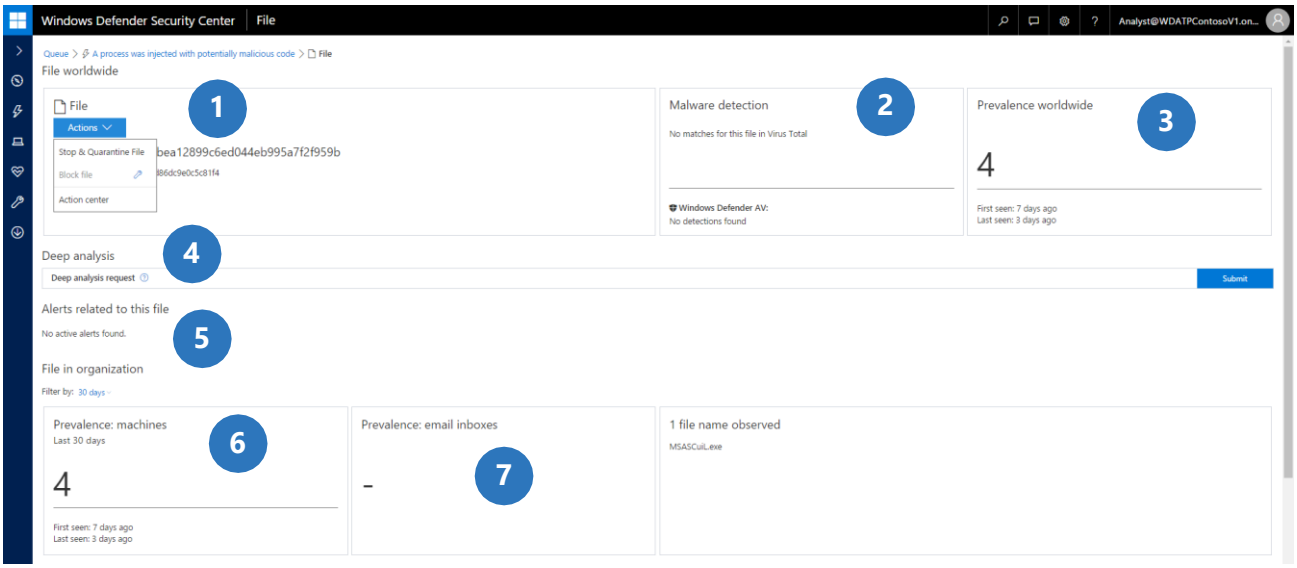
Did you know: WDATP conduct 'time travel' detection with every new detection added across six months of historical data to ensure customers uncover past unnoticed attacks.

You can apply two types of filters to help you focus on patterns that matter (2). Information level - offers three levels of granularity: Detection, Behaviors and Verbose. User account offers a variety of filtering options where events originated from, for example network, logged-on user and others. You can also export data to CSV for further investigation.



By clicking on a specific event row, you can expand and display the ancestor process tree (3). You can also pivot to a specific entity, for more information, by clicking on the desired hyperlink (4).

6 File



Clicking on a specific file will display the file's profile view that provides:

(1) Information including file hashes (in our case sha1=206407f68d83df6ac1f69c7f13e64bcadff9b911), if it is code-signed and by whom. The "Action" button allow you to preform set of immediate response actions:

   a. "Stop & Quarantine File" allows use to stop running processes, quarantining the file, and deleting persistency such as registry keys.

   b. "Block files" enable you to prevent further propagation of an attack by banning potentially malicious files. If you know a potentially malicious file, you can block it. This operation will prevent it from being read, written, or executed on machines in your organization.

   c. "Action center" provide summary view of all your response actions.

   Note: the "Action" button will be only visible only for preview users connecting Windows 10 machines running build #15031 or later.

(2) Provides information on malware detection associated with this file, including the VirusTotal detection ratio and a link to VirusTotal.

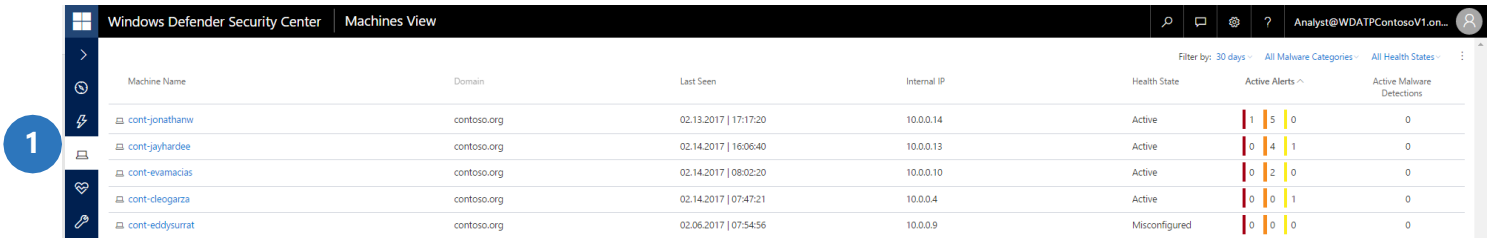
(3) Number of machines where the file was observed on worldwide and in your organization (6).

(4) You can submit the file for deep analysis, where the file is run in a secure cloud sandbox. When the analysis is complete, you'll get a detailed report that provides information about the behavior of the file.

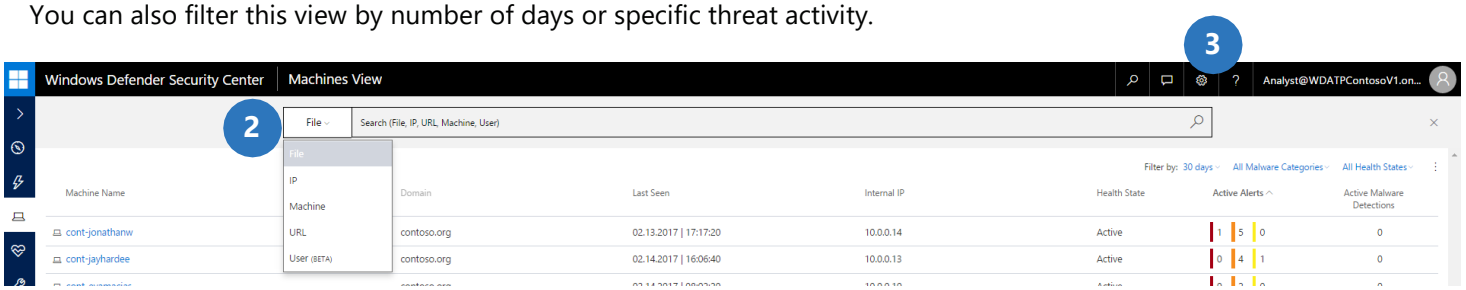
(5) See all the other related alerts raised on this file.

(7) [Office365 ATP users only] See prevalence of this file across your organization Office365 email inboxes.

7 Other Features



Machine view section (1) provides information on the various machines within your organization sorted by active alerts. You can also filter this view by number of days or specific threat activity.



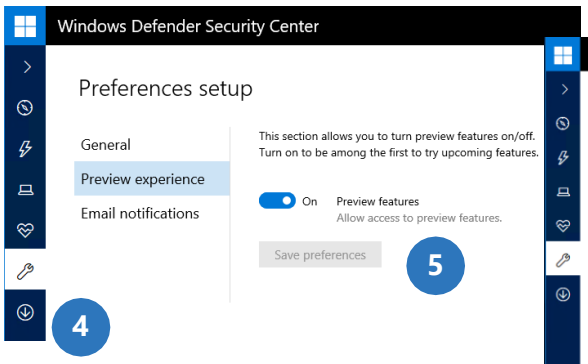
You can freely search for indicators of your choice using the Search bar (2), which lets you select the following:

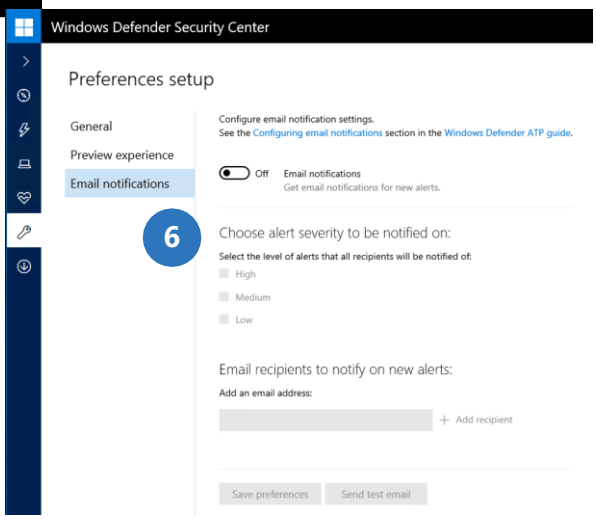
- File – View file profile information, world-wide and organization prevalence, deep analysis results, as well as organizational footprint (machines observed on), see details above.
- IP – Identify all communications between machines in your organization and external IP addresses. Use this to identify which machines communicated with an IP address – and when, to help determine the potential scope of breach in case of communication with command and control (C2) servers.
- Machine - investigate all alerts, behaviors, and observed events on a specific machine, see details above.
- URL - Identify all communications between machines in your organization and a suspected URL or domain, and view registrar information about the domain, as well as when and which machines were involved.
- User **[available only for preview users]** – investigate user account entities to see if there are alerts related to identify possible lateral movement between machines and potential compromised credentials cases.

We encourage you to submit feedback by clicking on the feedback icon (3). Your feedback is important to us and we are constantly monitoring it to improve our service.

Finally, in the preference setup section (4), you will find two great features:

- Ability to turn preview features on/off (5). **[available only for preview users]**
- Ability to get email notification with every new alert triggered in the service (6)





We hope you enjoyed this walkthrough guide.
Windows Defender Advanced Threat Protection Team