EAP1 Features

Feature	Description	Notes
Machine Learning Malware Detection	Intercept X includes a deep learning model to detect malware. Malware is detected by the model pre-execution and blocked. The detection results in a notification to the end user and an event in the administration console. Detections from the machine learning model are shown as ML/PE-A (Machine Learning/Portable executable, the A is for the current machinelearning model and may change in the future) From the detection event the administrator can 'Allow' the application if this is a False Positive detection. See False Positive Suppression below an RCA should be generated to assist the administrator in understanding if this is a possible false positive.	CIX - Pinned Scan only. CEA/CIX - Pinned Scan, and JIT scan (files open for read, closed on change) NOTE: A scan initiate with a right click on the file does not include the machine learning model. This will be available when the product releases.
Machine Learning Potentially unwanted applications	Intercept X includes a deep learning model to detect potentially unwanted applications. The detection behavior is identical machine learning to detect malware. Potentially unwanted applications tend to be 'commercial software' that is used for advertising, tool bars, spy ware, and device monitoring. These applications are rarely wanted by administrators or end users, but they are not quite considered malicious in themselves. Potentially unwanted applications are identified as "Generic ML PUA". From the detection event the administrator can 'Allow' the application if this is a False Positive detection.	CIX - Pinned Scan only. CEA/CIX - Pinned Scan, and JIT scan (files open for read, closed on change)

Feature	Description	Notes
False Positive Suppression	Intercept X includes a new global policy "Allowed Applications" . When Intercept detects and blocks malware and potentially unwanted applications an event is generated. From the event notification in Central the administrator can choose to allow the application. This will add it to the global allowed application policy and restore the application on affected endpoints. Sophos FP Suppression: In the early access program we are not including global FP suppression mechanisms that will be available when the product ships. Sophos global suppression allows the endpoint to check with sophos labs when an ML based detection happens, and if Sophos has determined that the model has made a mistake the detection is suppressed and the software continues to run. The net result is that during the EAP we expect a higher rate of FP notifications than will happen once the product is released.	By Hash and Certificate/Signer. NOTE: If you are not sure the detection is a mistake, it is best to leave it classified as malicious or PUA. If you are interested in digging deeper, you can review the RCA chain to determine how the application reached the device and use the SHA256 hash value of the identified application to search Virus Total or other internet sources for more information. If the SHA256 is not found in Virus Total it is likely Intercept X has detected new zero day malware.

Known Issues

Headlines

Issue	Details	Status
Bulk malware test – some malware started running, but was eventually detected and removed	If you deploy and launch >25 malware samples simultaneously some may start and eventually get detected and removed as the on-execution scanner catches up	This will be resolved prior to GA.

ID - WINEP-10708	The recommendation if you are going to test with real malware is to perform the tests for each sample with a delay between file executions. Also only test on an isolated machine that can be re-imaged easily incase the malware is not detected.	
Application Control not working	When deployed with Sophos Endpoint Advanced the application control feature available in Endpoint Advanced is disabled	This feature will be available when Intercept X is released
Potentially Unwanted Application authorization ID - CESG-1328	When deployed with Sophos Endpoint Advanced the ability for an administrator to allow PUA applications at a policy level is disabled. If you have PUA applications allowed they are likely going to be detected by the new machine learning model and will have to be added to the Allowed Application list	This feature will be available when Intercept X is released
Right Click Scan not finding malware ID WINEP-8554	Right Click scanning does not include the ML based malware/pua detection models	This will be resolved by GA
Second instance of same malicious/pua file is not removed during clean	Currently if the same malware sample is on the device in two locations only the one that was attempted to be started will be cleaned up. The other instance of the malware/pua will be on the device, but will be blocked if it is launched	This will be resolved by GA
After ML malware/PUA detections the scan takes a long time and consumes a lot of CPU ID WINEP-8544	If an exploit or malicious traffic detection occurs the endpoint will perform a full system scan. This can take time and consume significant CPU and disk resources. In addition when malware is detected an RCA is generated and the process of collecting the root cause information will consume significant CPU resources. As these events only happen when malicious software has been detected the real-world user experience when no malware is present is acceptable with less than 1% cpu consumption for general use.	When released the scanning will be more targeted and significantly faster
Suppression of FP by Certificate or Filename/Path not		The Early Access Program does include the ability to suppress

available		malware/PUA detections by Certificate, and filename. Suppression by path is not available yet, and will be for GA.
HMPA App Verifier mitigation prevents Application Verifier normal operation ID WINEP-9907	HMPA appears to prevent AppVerifier from being used legitimately, meaning that if you attach it to any application, the application will crash on startup. Note that Application Verifier itself always seems to add at least two whitespace-separated DLL names to the list at IFEO\<application_name>\VerifierDlls (vrfcore.dll as well as one or more test-specific DLLs).	A KBA will be produced for this prior to GA