Known Issues

Early Access Program (July) Intercept X
Sophos Intercept X Endpoint
C:\Program Files (x86)\HitmanPro.Alert\hmpalert.exe (build 713)

As of Aug 14st 2017

Call to action

If you experience an issue with the EAP and the issue is not included below or in one of the existing forum threads please add a question describing the problem so that we can investigate further.

Supported Platforms

- Windows 7 up to Windows 10 current shipping version
  - Excluding the current Beta for Window 10 'Windows 10 Insider' and 'RedStone 3'

Supported new features

Issue	Details	Status
Any operation on any office 2016 app [Licenced through Office 365 pro plus] fails	Only solution is to completely remove Intercept X [including older version], restart, disable the HitmanPro.alert service, uninstall Sophos Endpoint. Then remove computer from the EAP for Intercept X, and reinstall current version.	We are aware of the issues and investigating.
Incompatibility issue with CIX EAP and Forcepoint Triton AP-Endpoint(only used for DLP). c	We have also seen issues with CIX 3.6.5 on forcepoint May see code cave detection in windows services Run32.dll and others	We are working with the forcepoint engineering team on a fix
Install not completing	When EP is added to EAP program the 3.7 software is not completely install until Reboot is completed	Correct to complete the install a reboot is required.
Sophos Tester HydraCrypt	Some accounts are indicating the SoposTester for HydraCrypt is not being detected	Under investigation not reproduced
Meterpreter hashdump, and Mimikatz LSAdump are blocked but user not notified	We have reports where credential theft blocks hashdumps but the end user does not get a notification and no event is sent to Central	This will be resolved in the GA version.
Privilege escalation NO RCA when metasploit ms14_058+track_popup_menu_module used	The attack technique is blocked and the user notified but no RCA is generated	Under investigation
Privilege escalation Metasploit ms16_032_secondary_logon_handle_privesc module	This exploit appears to be blocked but no notification or RCA happens	Under investigation
Issues from Launch to Aug 1st		

Lost network connectivity when EAP deployed on Windows 10 Insider (Redstone 3)	The early access agent is not yet supported on the upcoming Windows 10 release (Microsoft is indicating this will launch in the fall.)	We continue to work with Microsoft to ensure compatibility of intercept X with the upcoming Windows 10 Insider (RedStone 3) release. Support will be available on or about the same time as Microsoft releases
Red Security Health State not set when Credential Theft prevented, or other active adversary detections	Integration with Synchronized Security to place the endpoint into a red security health state until the admin indicates the issues have been resolved is not included in the early access program.	This will be available in the finished product
Code Caved Process not terminated	When the code cave application is launched from session zero Intercept X will notify of the threat but not terminate the process. (A metrepter shell after some exploits can be running at this level)	We are evaluating if we can be more strict in the termination of an application at this level for code cave detections and other exploits/active adversary techniques
Firefox “LoadLib” plug-in False Positive	When connecting with a Firefox browser to some web sites the browser is terminated and the following event is shown. “LoadLib” exploit prevented in Firefox	We are aware of a FP with LoadLib in firefox related to some plug-ins. We expect to be able to address this by Mid Aug, No update to the endpoint will be required.
Missing Security Heartbeat with XG Firewall	In some instances the EAP agent will lose the security heartbeat connection to the XG Firewall.	This appears to be related to an expired certificate for accounts that deployed the XG firewall some time ago. We expect a Knowledge Base article to be available to assist customers in resolving this by mid to late august.
CredentialGuard event flood	Some tests have shown that multiple CredentialGuard events are generated for a single test, In some instances this is generating 1 event per minute, until the endpoint is restarted. We are investigating the issue	
Application Verifier protection not working	Application verifier registry hack is not detected	This feature is not yet available in the EAP
Install with Symantec	With Symantec endpoint protection the install of the service for Malicious Traffic Detection can be blocked as a low reputation file	Rebooting and re-install of Intercept X EAP appears to resolve the conflict.
Paused Update conflict	Sophos central’s support for ‘paused updates’ can conflict with the EAP agent.	If using paused updates, then endpoints selected for the EAP program will need to have tamper protection turned off if they are removed from the EAP program so that updates can resume correctly. After the successful update you can re enable tamper protection. This will be resolved when we ship

Aug 1 2017		