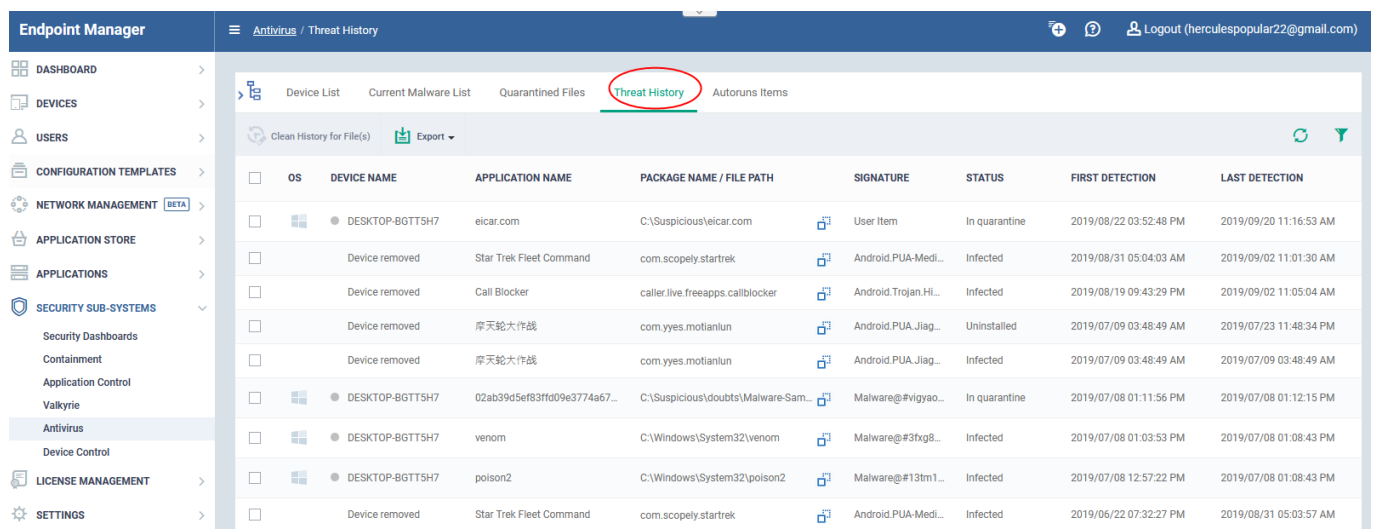


- The 'Threat History' area shows all malicious events found on managed devices over time.
- The list shows items that have been removed from devices and those which are still present.
- The list is useful for auditing, troubleshooting and analyzing customer networks.
- You can filter the list by various criteria, export the list to .csv, and clear history items you no longer require.

View and manage threat history

- Login to ITARIAN
- Click 'Applications' > 'Endpoint Manager'
- Click 'Security Sub-systems' > 'Antivirus'
- Click the 'Threat History' tab:



OS	DEVICE NAME	APPLICATION NAME	PACKAGE NAME / FILE PATH	SIGNATURE	STATUS	FIRST DETECTION	LAST DETECTION
	DESKTOP-BGTT5H7	eicar.com	C:\Suspicious\eicar.com	User Item	In quarantine	2019/08/22 03:52:48 PM	2019/09/20 11:16:53 AM
	Device removed	Star Trek Fleet Command	com.scopely.startrek	Android.PUA-Medi...	Infected	2019/08/31 05:04:03 AM	2019/09/02 11:01:30 AM
	Device removed	Call Blocker	caller.live.freeapps.callblocker	Android.Trojan.Hi...	Infected	2019/08/19 09:43:29 PM	2019/09/02 11:05:04 AM
	Device removed	摩天轮大作战	com.yyes.motianlun	Android.PUA.Jlag...	Uninstalled	2019/07/09 03:48:49 AM	2019/07/23 11:48:34 PM
	Device removed	摩天轮大作战	com.yyes.motianlun	Android.PUA.Jlag...	Infected	2019/07/09 03:48:49 AM	2019/07/09 03:48:49 AM
	DESKTOP-BGTT5H7	02ab39d5ef83fd09e3774a67...	C:\Suspicious\doubts\Malware-Sam...	Malware@#vigyo...	In quarantine	2019/07/08 01:11:56 PM	2019/07/08 01:12:15 PM
	DESKTOP-BGTT5H7	venom	C:\Windows\System32\venom	Malware@#3fxg8...	Infected	2019/07/08 01:03:53 PM	2019/07/08 01:08:43 PM
	DESKTOP-BGTT5H7	poison2	C:\Windows\System32\poison2	Malware@#13tm1...	Infected	2019/07/08 12:57:22 PM	2019/07/08 01:08:43 PM
	Device removed	Star Trek Fleet Command	com.scopely.startrek	Android.PUA-Medi...	Infected	2019/06/22 07:32:27 PM	2019/08/31 05:03:57 AM

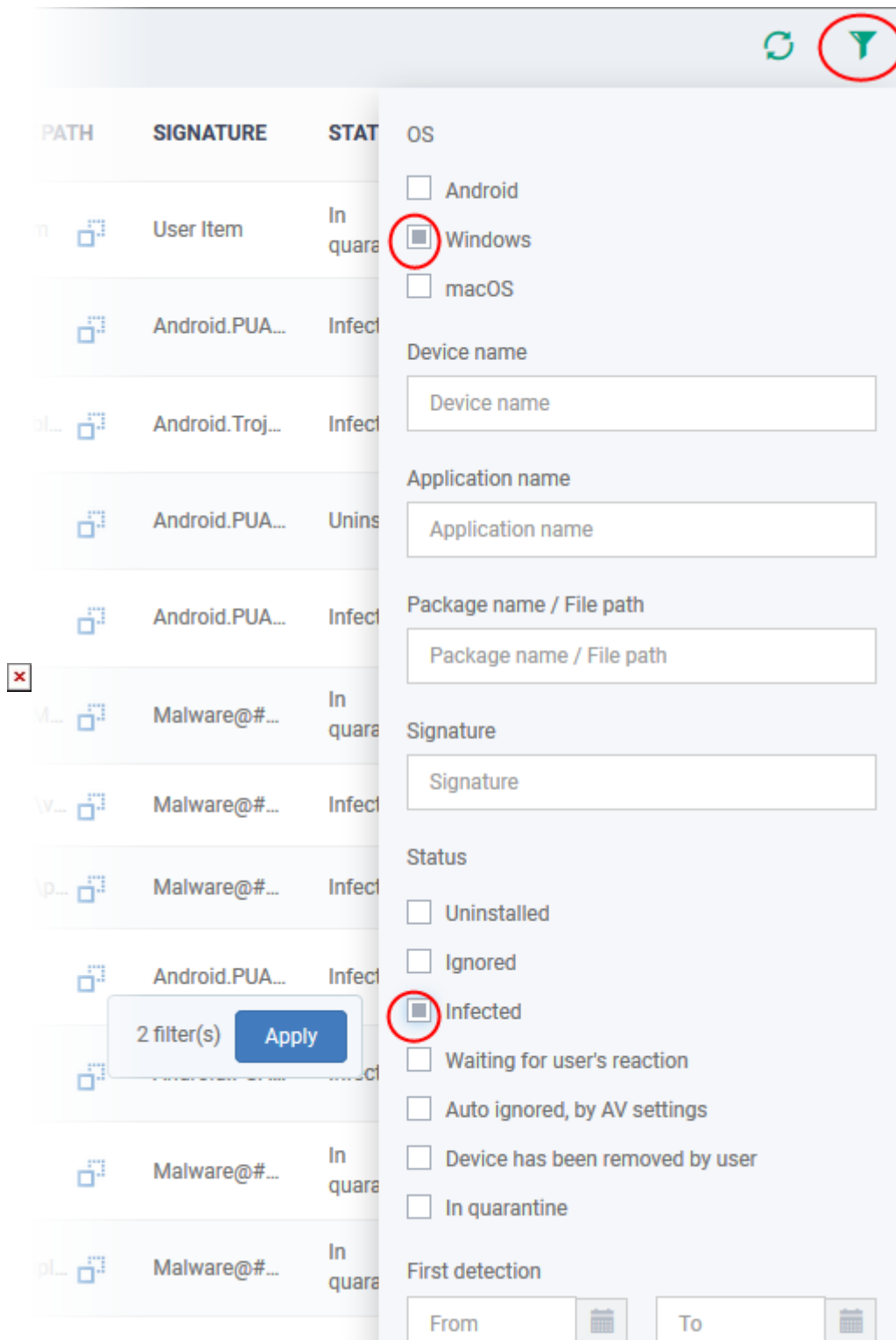
- Click a company name in the middle strip to view malware found on specific company devices

Or

- Select 'Show All' to view malware found on all enrolled devices

Sort, Search and Filter Options

- Click any column header to sort items in ascending/descending order of the entries in that column.
- Click the funnel icon on the right to filter items by various criteria. You can filter by OS, device name, application name, package name/file path, signature, status and first/last detection date:



- To view all items again, clear any filters and search criteria and click 'Apply'.

Remove unwanted entries

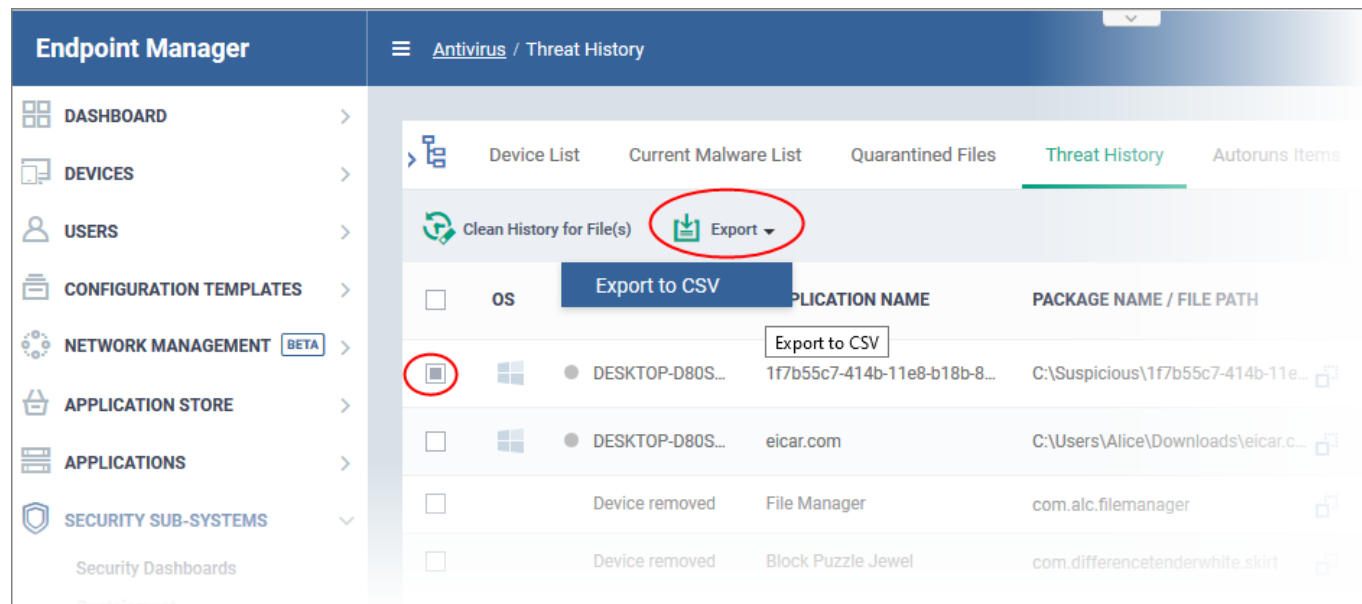
- Deleting file history will only remove the log entry. The file will not be removed from the device or from any other interfaces in which it is listed (for example, the quarantine list).
- Select the events you want to remove then click 'Clean History for File(s)' at the top:



- Click 'Confirm' to remove the entries from the list

Export threat history as a CSV file

- Click 'Security Sub-Systems' > 'Antivirus' > 'Threat History' tab
- Click the funnel icon to filter which records are included in the report.
- Click the 'Export' button and choose 'Export to CSV':



The screenshot shows the Endpoint Manager interface. On the left is a navigation sidebar with categories like DASHBOARD, DEVICES, USERS, CONFIGURATION TEMPLATES, NETWORK MANAGEMENT, APPLICATION STORE, APPLICATIONS, and SECURITY SUB-SYSTEMS. The main content area is titled 'Antivirus / Threat History'. At the top of this area are tabs for 'Device List', 'Current Malware List', 'Quarantined Files', 'Threat History' (which is active), and 'Autoruns Items'. Below the tabs, there's a section with a 'Clean History for File(s)' button and an 'Export' button with a dropdown arrow, which is circled in red. A blue box highlights the 'Export to CSV' option in the dropdown. Below this is a table with columns: 'OS', 'APPLICATION NAME', and 'PACKAGE NAME / FILE PATH'. The first row of the table has a red square icon in the 'OS' column and a tooltip that says 'Export to CSV'. The table lists several threat records, including one for 'eicar.com' and others for 'File Manager' and 'Block Puzzle Jewel'.

OS	APPLICATION NAME	PACKAGE NAME / FILE PATH
DESKTOP-D80S...	1f7b55c7-414b-11e8-b18b-8...	C:\Suspicious\1f7b55c7-414b-11e...
DESKTOP-D80S...	eicar.com	C:\Users\Alice\Downloads\eicar.c...
Device removed	File Manager	com.alc.filemanager
Device removed	Block Puzzle Jewel	com.differencetenderwhite.skirt

- Click 'Dashboard' > 'Reports' to view the report.