Endpoint manager has the feature of viewing the new infection detected in a device via Email alert. The email alert consists of newly infected device name and the "Follow the link to see details." option to view the malware that caused the infection.

**Infected Device Name** - The email has infected device name. By clicking the device name, the users can get the Device summary information.

"Follow the link to see details" - To see the details about the New Infection, click the "link". This link will redirect the user to the malware that caused infection in the device. The details of OS, Device name, application name, package name, file path, file hash, signature, detection date about the malware are available in the Current Malware list.

This feature is explained with a below example:

A New Infection Detected in a device is sent to a user email.

When the user clicks the infected device name "DESKTOP-ETJM9P5" in the email, it will redirect the user to the infected device's summary information.



The infected device's ("DESKTOP-ETJM9P5") Summary Information is given below

Endpoint Manager			DESKTOP-ETJM	19P5 / Summ	ary		Li	cense O	ptions 🔁	Ø 2	Logout	UTC+C
DASHBOARD	>			_								
DEVICES	~	DESKTOP Owner:	-ETJM9P5									
Device List Bulk Installation Package		Ē,			21	≣□	Þ		S		Ê <b>™</b>	
	>	Manage Profiles	Remote Control	File Transfer	Remote Tools	Run Procedure	Install or N Packa		Refresh Device Information	Power Options	Export Security Configuration	More
CONFIGURATION TEMPLATES	>			_								
S NETWORK MANAGEMENT	>	Device Name	Summary	Network	s Associa	ated Profiles	Software	Inventor	ry File List	Exported Co	onfigurations	MSI Installation Stat 🕨
	>	Device Summary OS Summary										
APPLICATIONS	>	Custom d	evice name	DESKTO	P-ETJM9P5			os		Wind	ows	
SECURITY SUB-SYSTEMS	>	Name			DESKTOP-ETJM9P5			OS name		Micro	Microsoft Windows 10 Enterprise (x86)	
		Logged in user			c194-1032			OS version			10.0.10240	
	>	AD\LDAP			N/A			Service pack		N/A		
🔅 SETTINGS	>	gp		PC	WORKGROUP			Build version Reboot time		10240 2020/12/14 05:12:46 PM		
		Model	)r	VirtualB	OX				ot time		712/14 03.12.40 r	-101
		Communication Client     6.39.39672.20120     C:\Windows\system       version     (DESKTOP-ETJM99)       Processor     Intel(R) Core(TM) i3 CPU 540 @ 3.076Hz       1032 for the follow     1032 for the follow		indows\system32 KTOP-ETJM9P5)								
				tel(R) Core(TM) i3 CPU 540 @ 3.07GHz					behalf of user DESKTOP-ETJM9P5\c194- 1032 for the following reason; No title for			
				0	0					this r	this reason could be found Reason Code:	
				VirtualB	VirtualBox							rype: restart
		System m	anufacturer	innotek	GmbH							

To view the infection details , click the "link" in the email

🔐 Write 👌 🎧 Forward 👌 🗑 View 👌 😓 🖌 🔪						
	w Infection Detected! noreply@c1notifications.com> 14	Encoding: worldwide (utf-8)	~			
	You are receiving this e-mail because you are using Endpoint Manager product. 2020-12-15 03:04:31. New Infection Detected on device <u>DESKTOP-ETJM9P5</u> . Follow the <u>link</u> to see details. Best Regards, EM Team					
	Sincerely, Endpoint Manager team.					

This "link" will redirect user to the Current Malware List tab. This tab has the infected device name, application name, package name, file hash, signature and detection date.

Endpoint Manager		urc+es:
DASHBOARD >		
DEVICES >	Ø Search group name	Current Malware List Quarantined Files Android Threat History Autoruns Items
<u>A</u> USERS >	🖼 Show all	📴 Delete Malware 🛛 Ignore Malware 🖉 Quarantine Malware 🧟 Rate as Trusted 🚥 More 🧭 🍸
CONFIGURATION TEMPLATES >	<ul> <li>→ ➡ Carey</li> <li>→ ➡ cloudconnect</li> </ul>	OS DEVICE NAME APPLICATION NAME PACKAGE NAME / FILE PATH FILE HASH SIGNATURE
NETWORK MANAGEMENT	E Default Customer	DESKTOeicar_com (1).zip C:\Users\c194-1032\Do 📅 D27265 🔂 ApplicUnwrt
APPLICATION STORE	+ 🖶 KGF	
APPLICATIONS >	🔹 🖶 Steve_Smith	Results per page: 20 V Displaying 1 of 1 results
SECURITY SUB-SYSTEMS		
Security Dashboards		
Containment		
Application Control		
Valkyrie		·
Antivirus		
Device Control		
Data Loss Prevention BETA		
LICENSE MANAGEMENT >		
☆ SETTINGS >		