Managing Endpoints Using SanerNow

4.0 User Guide

secpod

Contents

Endpoint Management

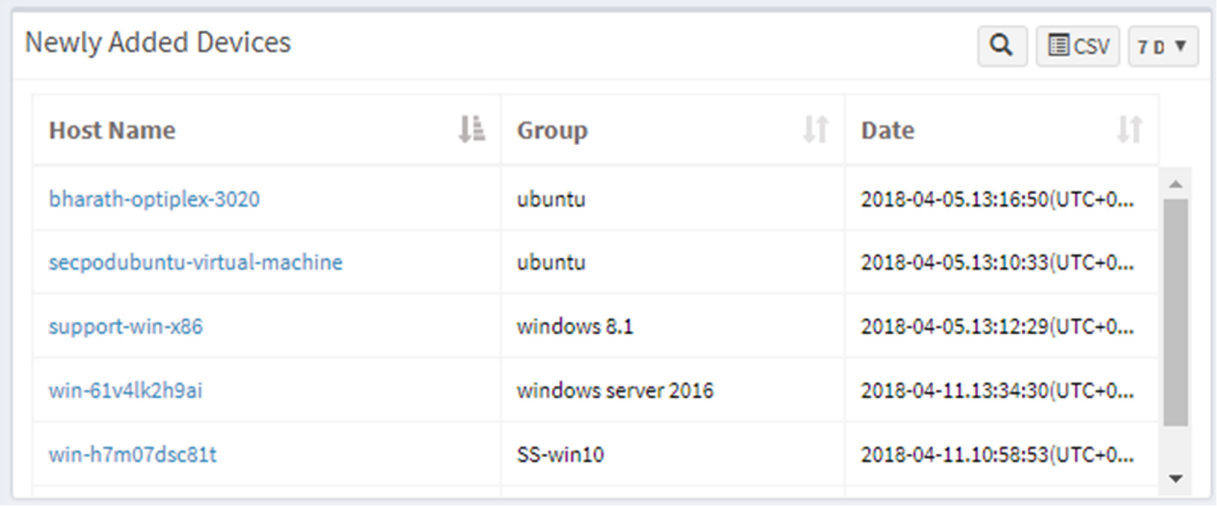
The SanerNow Endpoint Management tool provides total visibility over your managed endpoints. Built-in actions help you keep your endpoints compliant to regulations and up-to-date with software and hardware patches. You can use queries to check on the health of your endpoints. Automated actions enable you to debug and resolve issues and control the deployment or uninstallation of applications and service packs.

To access the Endpoint Management tool:

1. Logon to SanerNow using your SanerNow credentials.
2. Select an account to manage by clicking the icon at the upper left corner of the window. A dashboard with the summary view of the account is displayed.
3. Click the SanerNow icon on the header. Click the Endpoint Management icon. The Endpoint Management dashboard is displayed, which shows at a glance the total number of devices on the network with a breakdown by OS, the number of devices with the SanerNow Agent running, and the number of currently active devices.

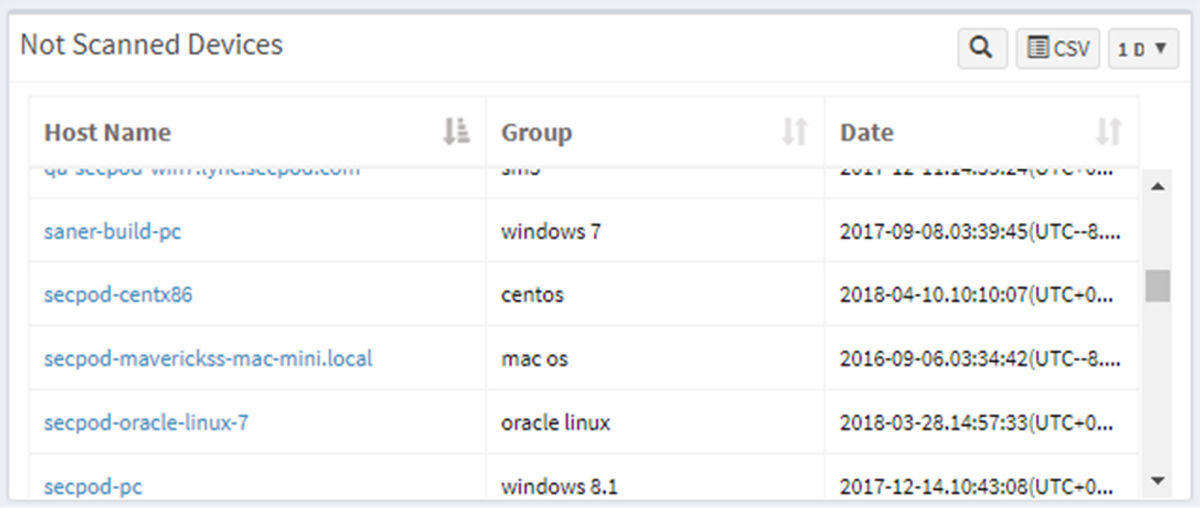
Newly Added Devices

This pane shows the list of devices that have been recently added to the network, based on the date and time.



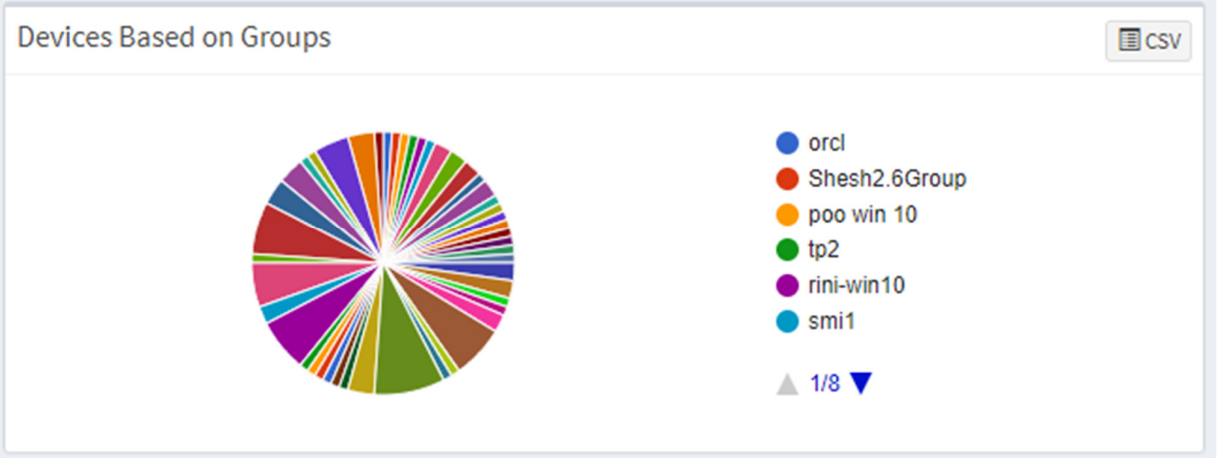
Not Scanned Devices

This pane shows the list of devices on the network that have not been scanned for 24 hours or longer based on the date and time. You can choose to view devices not scanned for over 1 day, 3 days or 5 days and then troubleshoot why the device is not being scanned.



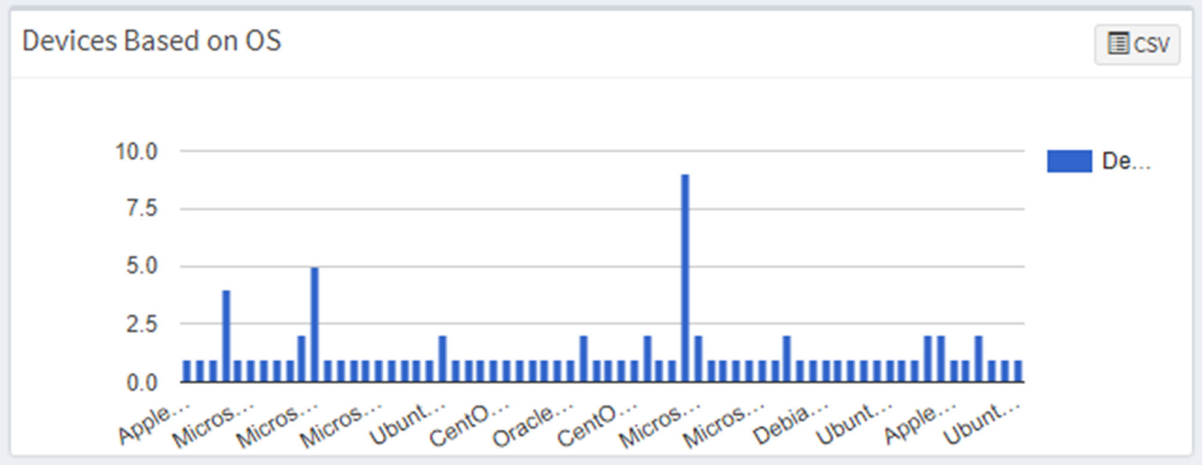
Devices Based on Groups

This pane shows devices based on default (classified by OS) and user-created groups. Click the up or down arrow to scroll through the list of device groups. Clicking a segment on the chart shows the number of devices in the group.



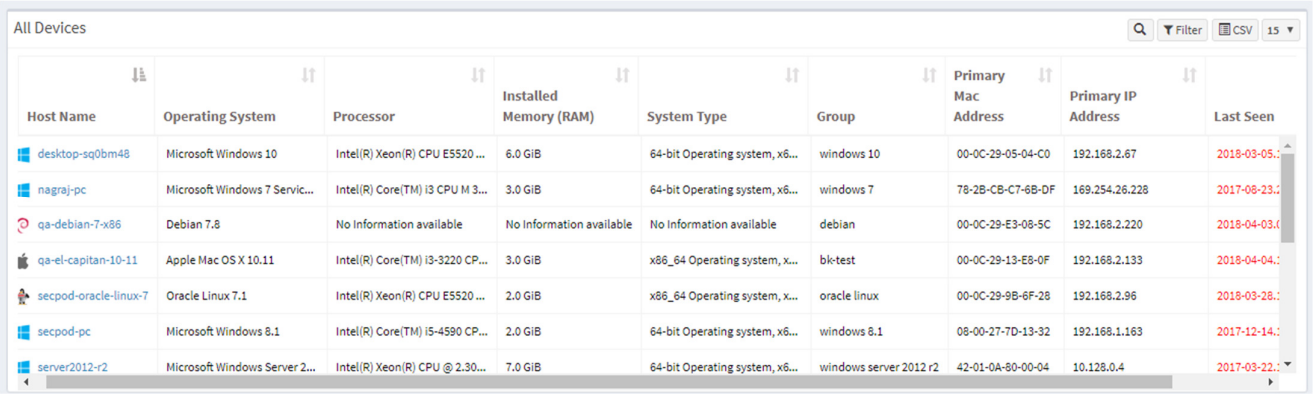
Devices Based on OS

This pane shows the number of devices in each OS group.



All Devices

This pane shows all devices on the network, and details for each device, such as operating system, memory, processor, group, IP address, etc. You can search for a particular device or filter this list by groups or OS. If you want to download all details for all endpoints on the network, click the CSV icon.



Host Name	Operating System	Processor	Installed Memory (RAM)	System Type	Group	Primary Mac Address	Primary IP Address	Last Seen
desktop-sq0bm48	Microsoft Windows 10	Intel(R) Xeon(R) CPU E5520 ...	6.0 GiB	64-bit Operating system, x6...	windows 10	00-0C-29-05-04-C0	192.168.2.67	2018-03-05...
nagraj-pc	Microsoft Windows 7 Servic...	Intel(R) Core(TM) i3 CPU M 3...	3.0 GiB	64-bit Operating system, x6...	windows 7	78-2B-CB-C7-6B-DF	169.254.26.228	2017-08-23...
qa-debian-7-x86	Debian 7.8	No Information available	No Information available	No Information available	debian	00-0C-29-E3-08-5C	192.168.2.220	2018-04-03...
qa-el-capitan-10-11	Apple Mac OS X 10.11	Intel(R) Core(TM) i3-3220 CP...	3.0 GiB	x86_64 Operating system, x...	bk-test	00-0C-29-13-E8-0F	192.168.2.133	2018-04-04...
secpod-oracle-linux-7	Oracle Linux 7.1	Intel(R) Xeon(R) CPU E5520 ...	2.0 GiB	x86_64 Operating system, x...	oracle linux	00-0C-29-9B-6F-28	192.168.2.96	2018-03-28...
secpod-pc	Microsoft Windows 8.1	Intel(R) Core(TM) i5-4590 CP...	2.0 GiB	64-bit Operating system, x6...	windows 8.1	08-00-27-7D-13-32	192.168.1.163	2017-12-14...
server2012-r2	Microsoft Windows Server 2...	Intel(R) Xeon(R) CPU @ 2.30...	7.0 GiB	64-bit Operating system, x6...	windows server 2012 r2	42-01-0A-80-00-04	10.128.0.4	2017-03-22...

Actions and Checks

Checks are predefined queries for the most routine probes that the IT Security team may want to execute regularly. They provide a way to save time and make it simpler and faster to do repetitive checks. If you click the arrow, the Checks page is displayed. You can select the OS and the type or category of checks from the drop-down to display a set of relevant queries. For example, you may wish to check if a user has installed torrent on their system. A list of available checks is given below.

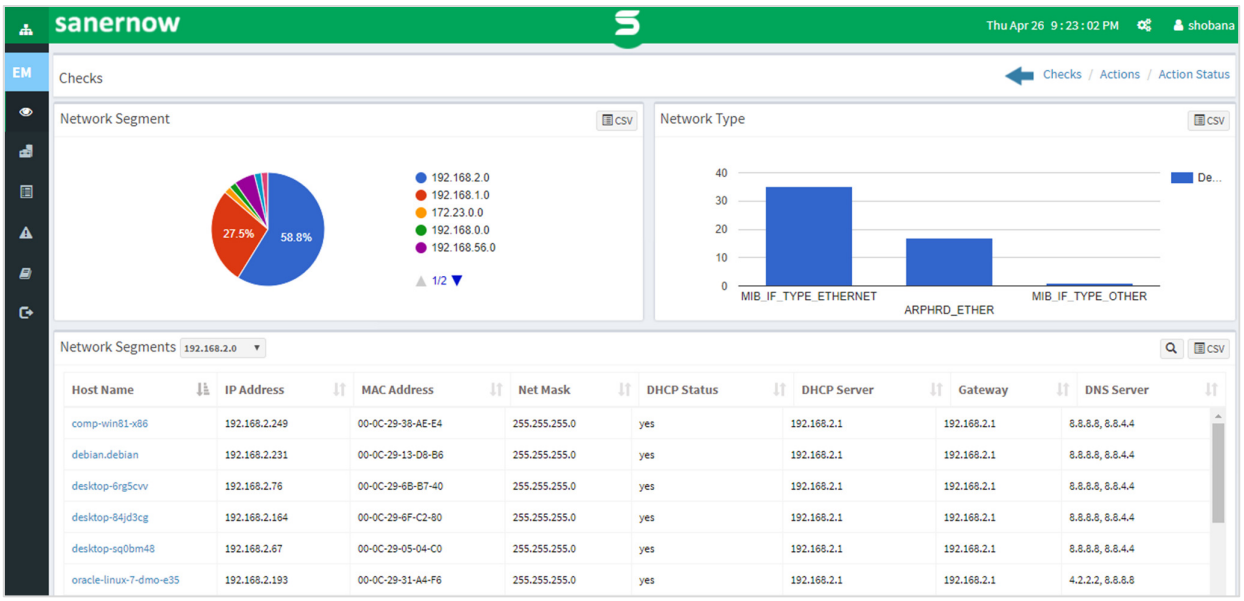
Actions are predefined responses to remediate the results of the checks. If you click the arrow, the Actions page is displayed. For example, if a predefined check has detected that a user is using uTorrent, a blacklisted application, you can run the Application and Device Control Response to block the torrent application or run the Software Deployment Response to uninstall the application. A list of predefined actions are given below. You can choose to enforce some of the actions as an organization rule, for example blocking a USB mass storage device. You can also customize the response to run at specified intervals for as many times as required.

Checks	System Time - Linux	Deviation in Co-existing Services - Windows	RAM or CPU Usage - Windows	Scheduled Programs - Windows	Important Missing Patches - Windows	Antivirus Information - Windows	›
Actions	Application and Device Control	Network	Process	Registry	Security	Services	›

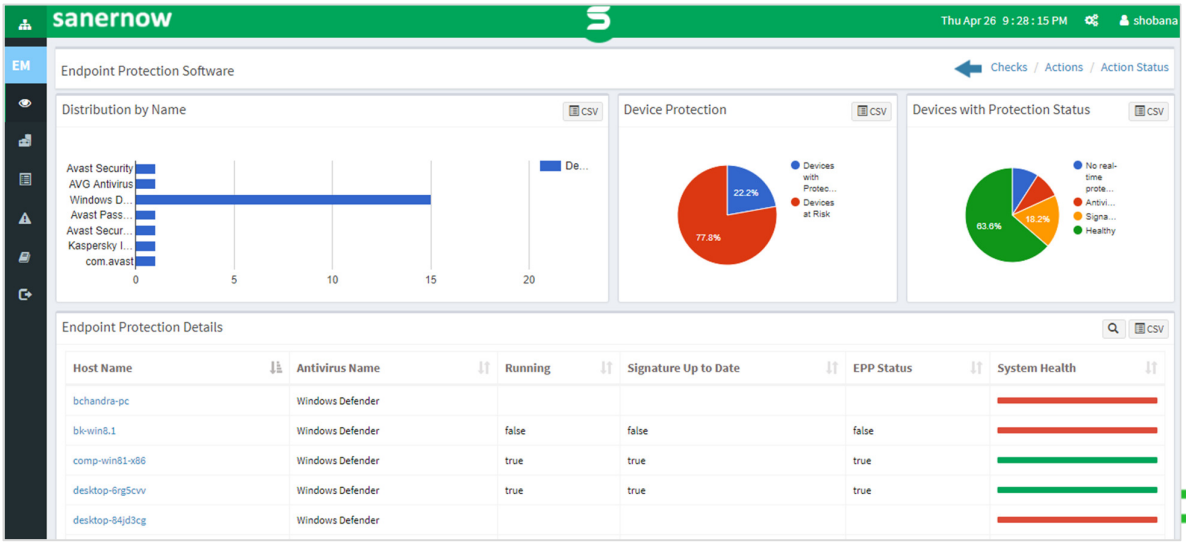
Predefined Checks

Some of the extremely important or routine checks are displayed at the top of the Checks page:

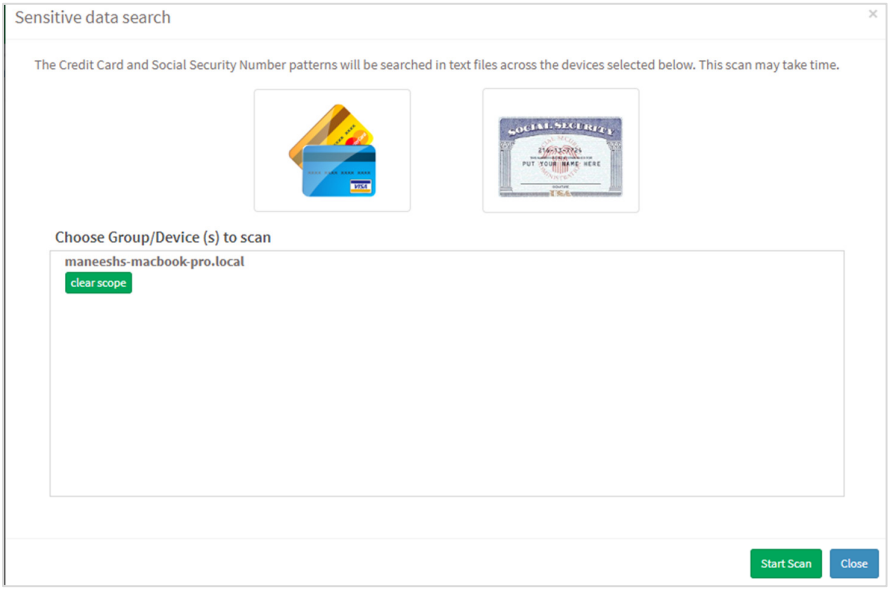
- Network Segments - Checks for the different network segments and lists the number of devices on each segment, along with the device details.



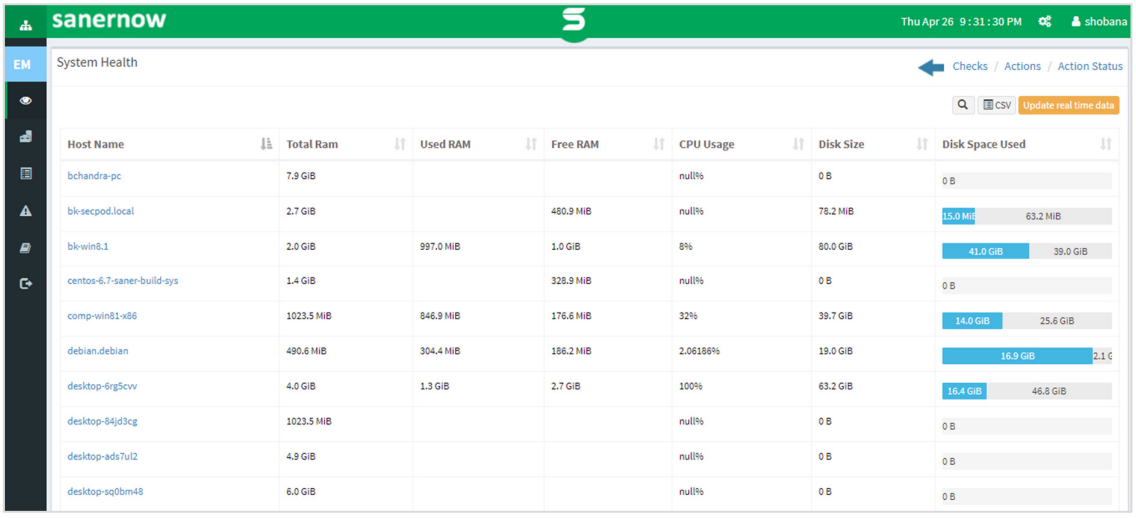
- Endpoint Protection Software - Checks if antivirus protection is running on devices and shows a distribution of the different types of protection on devices, as well as how many devices are protected, how many devices are at risk, and the system health of individual devices.



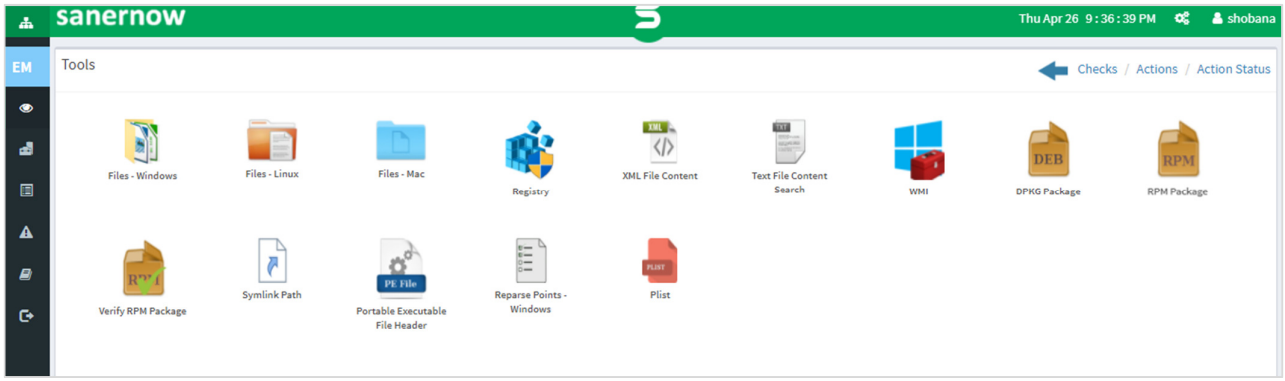
- Sensitive Data Detection - Checks if the user has stored credit card or social security numbers as a text file. Running this check may take a long time as the query has to go through the entire data on the disk. Depending on how much data a user has, this could be a time-intensive check.



- System Health - Checks for the total RAM, free RAM, used RAM, CPU usage, free disk space, etc. For instance, having very little disk space is a system health issue. Click Update real time data for the latest system health information. Specify how many times you want the query to be executed, at what intervals of time, and for which devices. This helps you monitor the system health of devices for a specific reason, such as unnatural system behavior that may indicate an attack in progress.



- Tools – A number of tools are available, such as checking for files larger than 1GB on devices. You can modify or update the queries to refine your search further. These tools may have an impact on resources, so they must be used after you achieve clarity on the scope.



Note: Some of these checks below may apply only to Windows Systems.

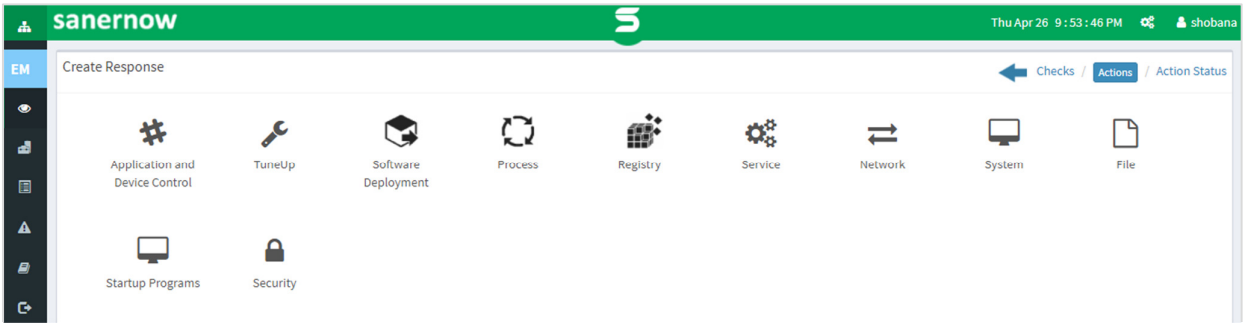
- Application Management Checks:
  - Applications with Unknown Publisher - Lists all applications that have no known publisher.
  - Potentially Unwanted Programs - Identifies potentially unwanted programs such as torrent downloader or unnecessary toolbars running on Windows systems.
  - Startup Applications – Lists the applications that are started when you boot your computer.
  - Software Licenses - Collect all software license information.
- Network Management Checks
  - Wireless Security - Checks wireless security on devices.
  - ARP Cache - Collects ARP entries that are created when a hostname is resolved to an IP address and then to a MAC address, so the computer can effectively communicate.
  - DNS - The Domain Name System (DNS) translates Internet domain and host names to IP addresses and vice versa. Collects the DNS information on devices.
  - Wireless Signal Quality - Checks wireless signal quality on devices.
  - DNS Cache - Investigates the DNS cache on systems.
  - Open Ports - Collects all open port information on devices.
  - Network Interfaces - Collects all network interface information from devices.
  - Firewall Policies - Checks all firewall policies on systems.
  - DHCP - Collects all Dynamic Host Configuration Protocol (DHCP) information on systems.
- Patch Management Checks
  - WSUS-SCCM Status - Checks the status of the Windows Update Server (WSUS/SCCM).
  - Updates Marked Hidden - Lists all software patches hidden in the Windows Updates server.
  - Installed Patches - Lists all installed patches on systems.
  - Important Missing Patches - Lists all important missing patches on systems.
- Computer Information Checks
  - Disk - Windows
  - Description Collect and investigate disk information on Windows systems.
  - Scheduled Programs - Windows
  - Description Collect all scheduled programs set in Windows systems.
  - Windows System Metric - Retrieve the specified system metric or system configuration setting on Windows

systems.

- Volumes - Collect all volume information on systems.
- Operating Systems Information - Collects operating systems information.
- RAM or CPU Usage - Investigates total RAM or CPU usage on systems.
- RAM or CPU Threshold - Investigates total RAM or CPU threshold (greater than or equal to 80%) on systems.
- System Up-time More than 7 days - Checks for systems which are up and running since 7 days.
- Run Command History - Checks the run command history on systems.
- Disk Space less than 100MB - Investigates disks running out of space (<100 MB) on systems.
- Active Directory Details - Checks all active directory details on systems.
- BIOS - Collects BIOS information such as serial number, version, manufacturer on systems.

- Process Management Checks
  - Current Processes - Identifies all current processes running on systems.
- Device Management Checks
  - Keyboard and Pointing Devices - Collects all keyboard and pointing devices connected to systems.
  - Bit-locker Status - Checks if Bit-locker protection is OFF on systems.
  - USB Mass Storage Devices - Lists all USB mass storage devices connected to systems.
  - Storage Devices Connected - Lists all storage devices connected to systems.
- System Security Checks
  - Shared Resources - Lists all shared resources on systems.
  - Antivirus Information - Checks for Anti-Virus(AV) status on systems. It is required to keep AV up-to-date and running.
  - Data Execution Prevention Status - Data Execution Prevention or DEP is a security feature that can help protect your computer by monitoring programs to make sure they use system memory safely.
  - Faulty Anti-Virus Status - Checks for faulty Anti-Virus(AV) status on systems. It is required to keep AV up-to-date and running.
  - User Access Control UAC - Checks the User Access Control (UAC) level on systems found under registry HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.
  - Account Lockout Policy - Checks the account lockout policy on systems.
  - Password Policy - Checks the password policy set on systems.
  - System Events - Collects all system events that may require your attention from the Events Log.
  - Security Events - Collects all security events that may require your attention from the Events Log.
- Service Management Checks
  - Deviation in Co-existing Services - Checks for only one primary function per server to prevent functions that require different security levels from co-existing on the same server. For example, web
  - Running Services - Collect all services that are currently running on systems.
- User Management Checks
  - Auto-logon Enabled Users - Checks if Auto-logon is enabled on systems.
  - Last-logon Users - Lists the last-logon details of users on systems.
  - Administrator Accounts - List all Administrator accounts on systems.
  - Groups - List all the Groups on systems.
  - System Users Identification - Identifies all users on systems.
  - Inactive Users - Lists all inactive users on systems.
  - Guest Accounts - Lists all Guest accounts on systems.

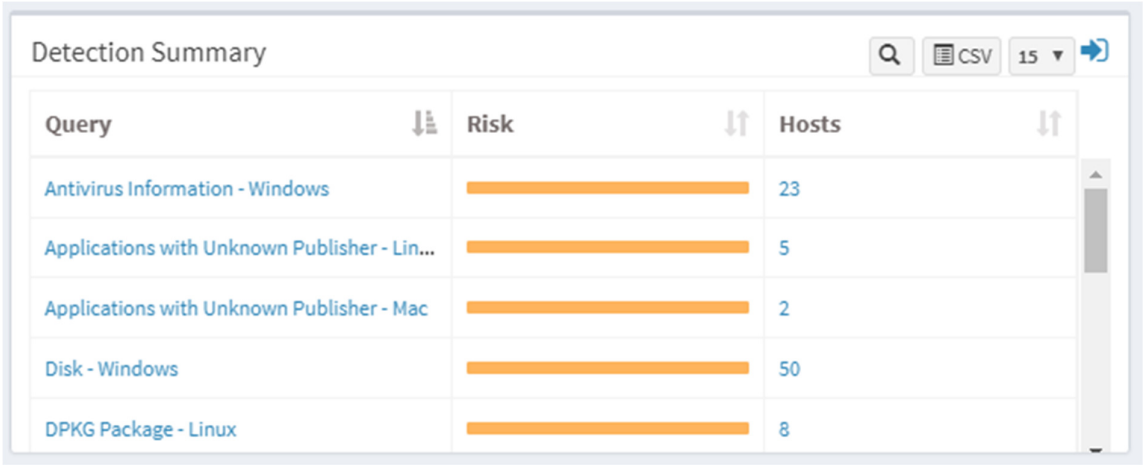
Predefined Responses



- Application and Device Control – Block or unblock applications and enable or disable devices.
- TuneUp – Clean up the system or the registry to improve the performance of devices.
- Software Deployment – Install or uninstall applications or install patches.
- Process – Unblock or start required processes or block or stop unwanted processes that are running on devices to prevent attacks.
- Registry – Add, modify or delete registry keys.
- Service – Start, restart, stop, or remove services.
- Network – Block or unblock domains, flush ARP entries, set a static IP address, etc.
- System – Reboot systems after patch or application installation, or shutdown systems that are being attacked by malware to prevent the spread of the vector or protect the device, set the hostname, mount file systems, etc.
- File – Delete infected files, or if you cannot delete them, quarantine it.
- Startup Programs – Specify programs that you want to automatically start during a system reboot or as scheduled, for example, when the application has finished executing a task; or remove programs from the startup.
- Security – Disable or enable firewalls.

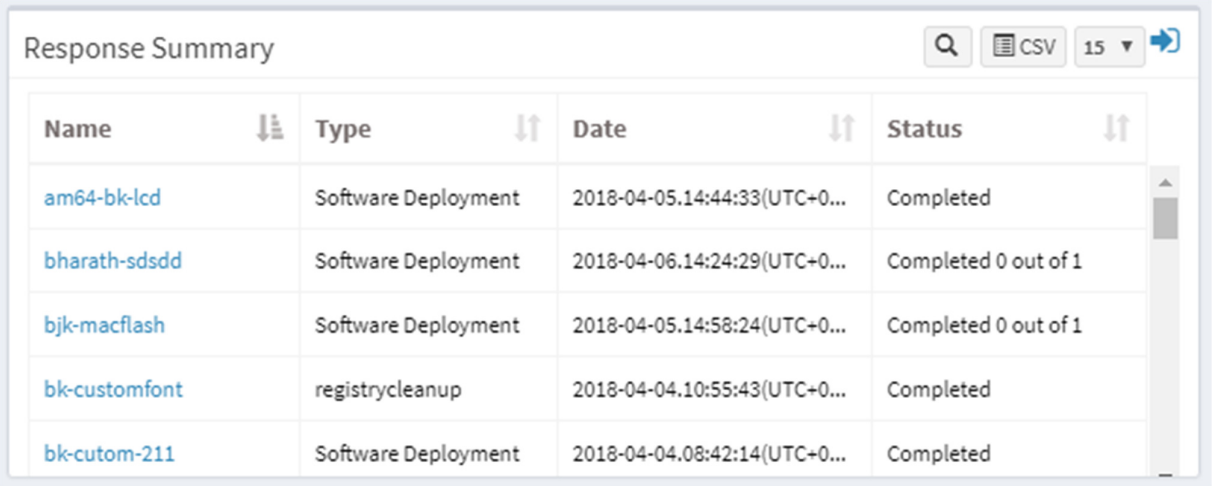
Detection Summary

This pane shows the list of all the checks that have been executed and the corresponding devices. Only checks with results are displayed.



Response Summary

This pane shows the list of all responses that were run to remediate the results from checks, and the status of the response, as well as type of response and date and time of execution. Click the Expand icon to view details of individual response actions, such as Status View which provides information on the host on which the action was taken, the type of action, and status, while the Creation View shows the script that was run.

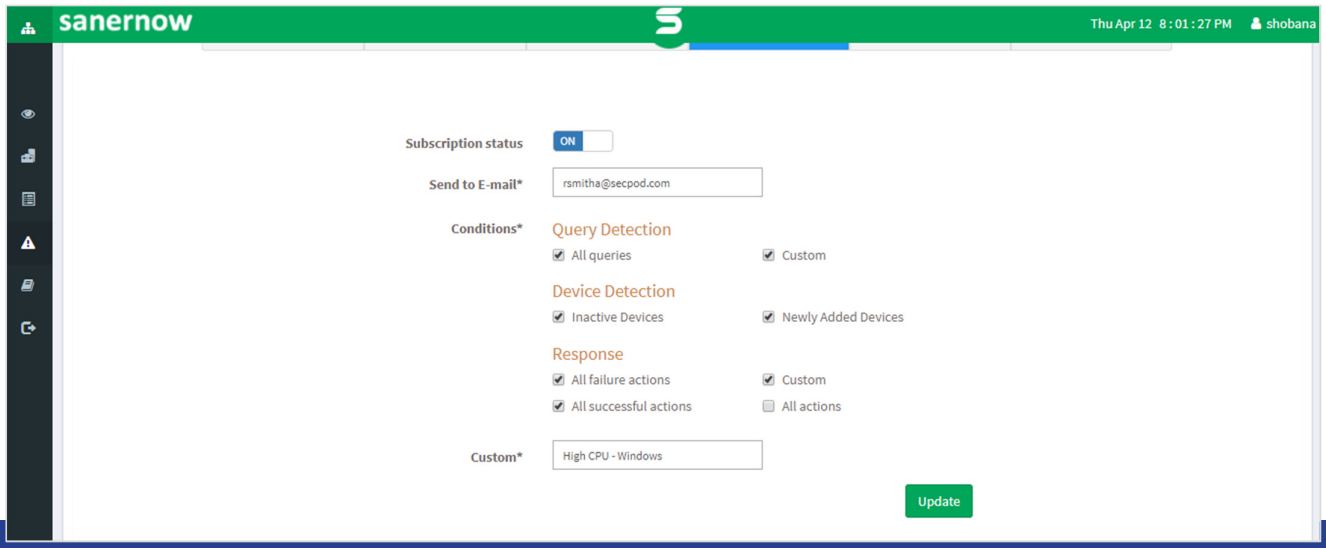


Setting Alerts for Endpoint Management

The Alerts feature is used to monitor the health of your endpoints or to view newly added endpoints.

To Set Alerts for Endpoint Management

1. Click Alerts > Endpoint Management.
2. Set the subscription status to On.
3. Specify the email address to which you want the alerts sent.
4. Specify the conditions for which you want the alerts sent:
   - Query – You can choose to receive alerts for all queries that are executed on the endpoints or for custom queries. If you select custom you must specify the condition.
   - Device - You can choose to receive alerts for Inactive devices or when devices are added to the network.
   - Response fields – You can choose to receive alerts when actions on endpoints pass, fail, or for a custom condition.
5. Click Update to complete.

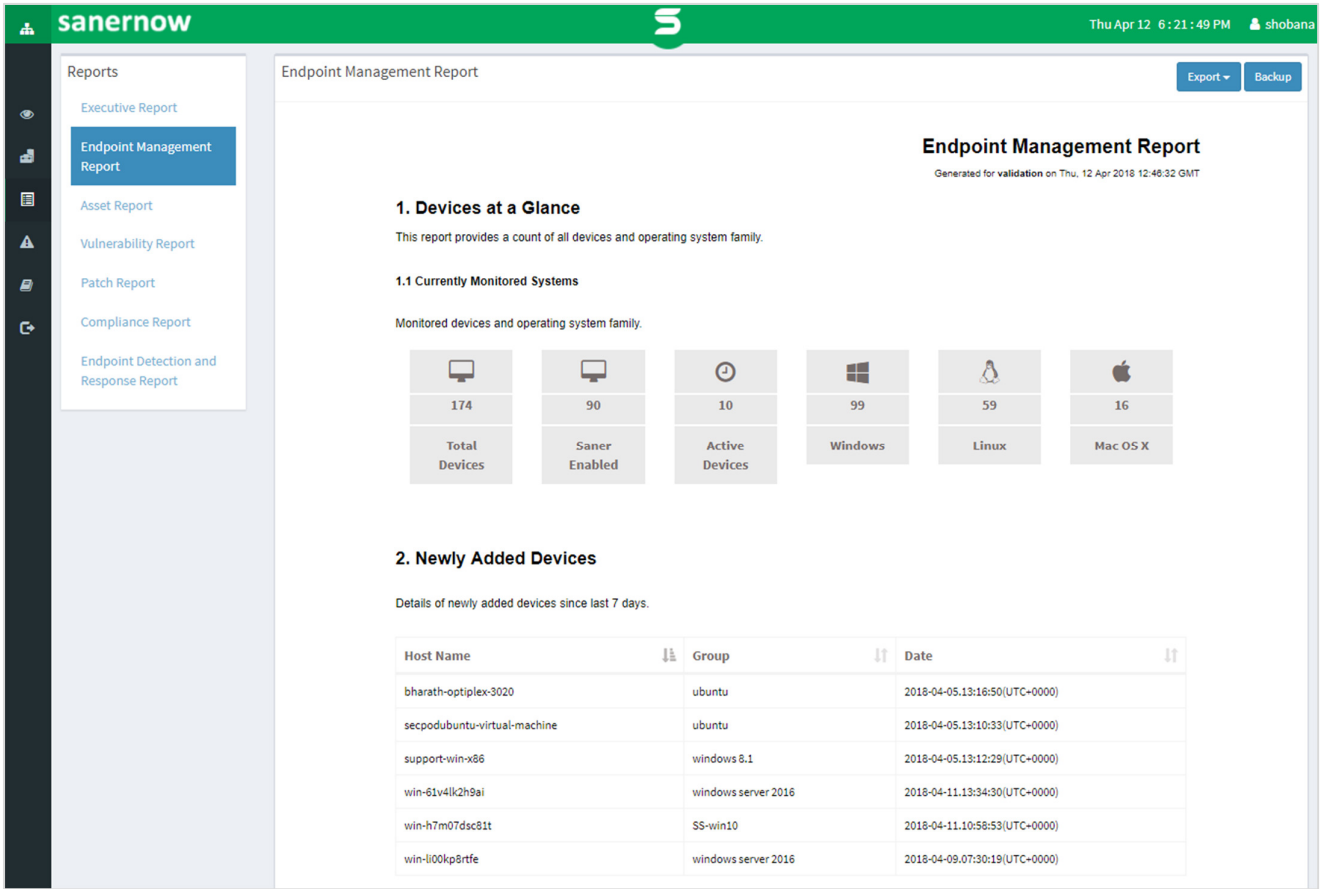


Endpoint Reports

Endpoint Reports provide a comprehensive view of the devices on the network, newly added devices, unscanned devices, groups and types of devices, details of each device, and status of the jobs for each device.

To Generate the Endpoint Management Report

- Click Reports > Endpoint Management Report.



To export the report to a PDF

- Click Export > PDF

To export the report and send it via email:

1. Click Export > Email.
2. Specify the email addresses.

To Back Up Reports

The backup settings under Reports allow IT administrators to obtain a backup report showing the history. The backup time should be scheduled. The backup report can be scheduled to run automatically daily or weekly.

To configure backup settings for reports:

1. Click **Backup**.
2. Specify the frequency of backup in the **How Often** drop-down. You can back up reports daily, or weekly. If you choose weekly, you can specify the days.
3. Specify the number of days that a backup should be maintained in the **Keep Only the Latest** box. Files older than the specified value will be deleted. You can maintain backups for a maximum of 30 days.
4. Specify the **Backup Time,** that is, the time when SanerNow will create an archive of the report. Specify **Email** ID addresses.
5. Click **Save**.

About Us

SecPod Technologies creates cutting edge products to ensure endpoint security. Founded in 2008 and headquartered in Bangalore with operations in USA, the company provides computer security software for proactively managing risks and threats to endpoint computers.

Contact Us

Web: www.secpod.com
Tel: +91-80-4121 4020 | +1-918-625-3023
Email: info@secpod.com