PROMISEC
ENDPOINT SECURITY MANAGEMENT

Achieving Endpoint Visibility with PEM

Quick guide for endpoint monitoring and management

Introduction

In many cybersecurity incidents, malicious actors gain access through company endpoints. In fact, 60% of cyber breaches involving vulnerabilities for which a security patch was available but not applied.

To stop this from happening, the role of IT management is to set a unified security standard for an organization and enforce it. To enable this, most companies invest heavily in multiple security tools to prevent cyber-attacks, and yet the company remains vulnerable due to disabled or missing security agents. Software patches and licenses remain outdated or expired, and unauthorized applications that threaten endpoints go unnoticed for lengthy periods of time.

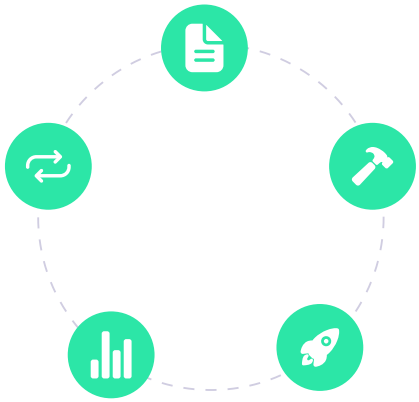
Achieving complete endpoint visibility with PEM

PEM (Promisec Endpoint Manager) is an advanced agentless solution that delivers complete endpoint detection and remediation capabilities across the enterprise. PEM leverages patented technology to quickly inspect your entire enterprise to identify, analyze, and remediate security gaps. The solution is engineered to run at scale on any network, covering use cases from compliance through cyber.

> PEM inspects your entire network, analyzes the data, identifies security issues or noncompliance to your specified standards, and helps you remediate the issues to keep your network secure.

PEM Features

- Endpoint vulnerability detection
- Flexible management dashboard
- Compliance assurance
- Full visibility of endpoint hardware and software
- Integration with third-party security solutions and SIEMs



- AV/EDR activation and updates
- Software license management
- AV/EDR activation and updates
- Program management with whitelists/backlists
- Automatic GPO and golden image implementation

PEM Dashboard

Within PEM, your data is presented in an advanced dashboard, which features clear and comprehensive charts, granular filtering and issue drilldown capabilities. You can also export your data in PDF or CSV format, as well as syncing PEM with third-party reporting solutions to leverage your data in whatever way works best for you.

1 - Statistics

Shows charts and graphs, presenting your data in clear and comprehensible fashion. There are different categories within the statistics component for the varying types of issues which PEM identifies. This component gives you an overview of what issues you have in your network and how prevalent they are.

2 - View

Allows you to see at a glance where your issues are, and the status of different groups of endpoints within your network. You can easily define these groups depending on your needs, dividing according to geography, task, environment, topology or any delineation you wish. You can create a group for an ad-hoc project, for a certain type of issue, or for a certain worker.

3 - Trends

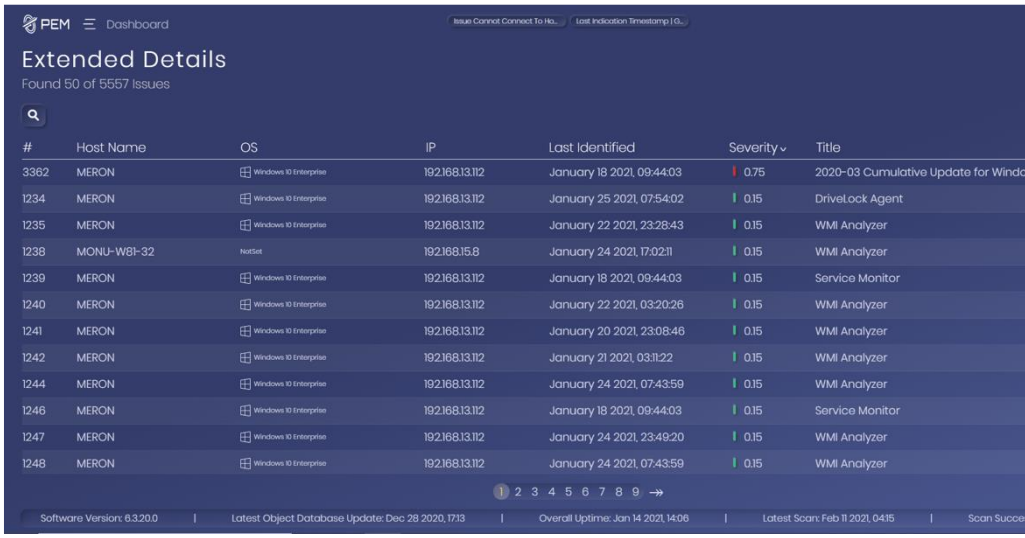
Shows the positive or negative trend of any selected group, endpoint, or of the network as a whole. This component calculates the number of issues together with their severity through time.

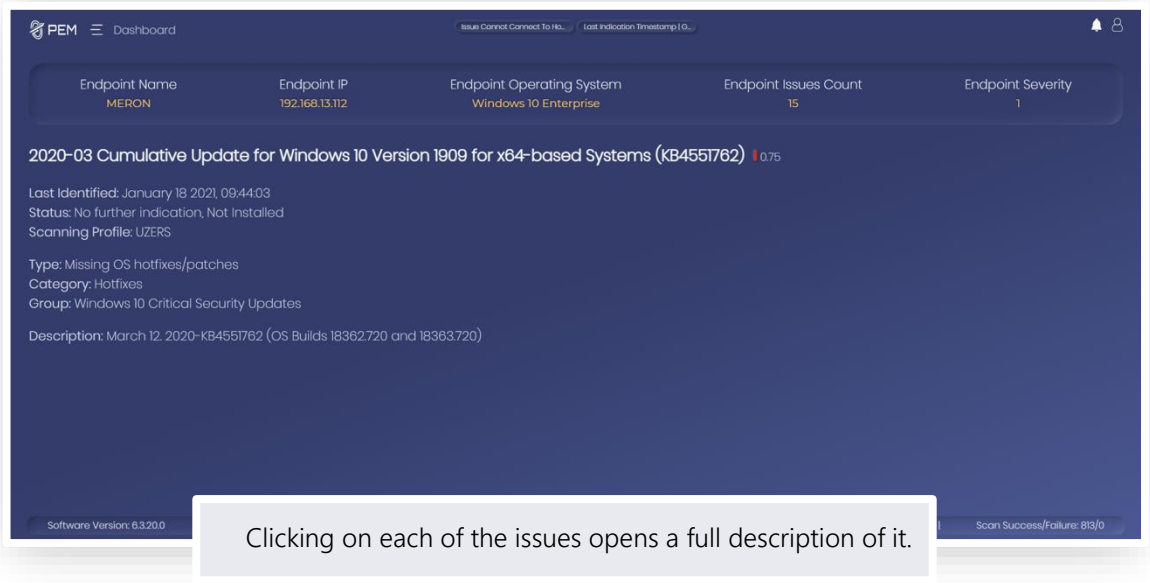
4 - Details

Presents a list of issues identified by PEM, ordered by severity, showing the name of the issue and where it was identified. This component can be expanded to the Extended Details screen.

Extended Details Screen

The Details component on the right of the main dashboard indicates the most critical issues identified by PEM, including the severity of the issue, which IP the issue was identified on, and the name of the issue. Users can click the extend icon to see move to the Extended Details screen. In this section, all identified issues are depicted in chart form, along with information about each issue.

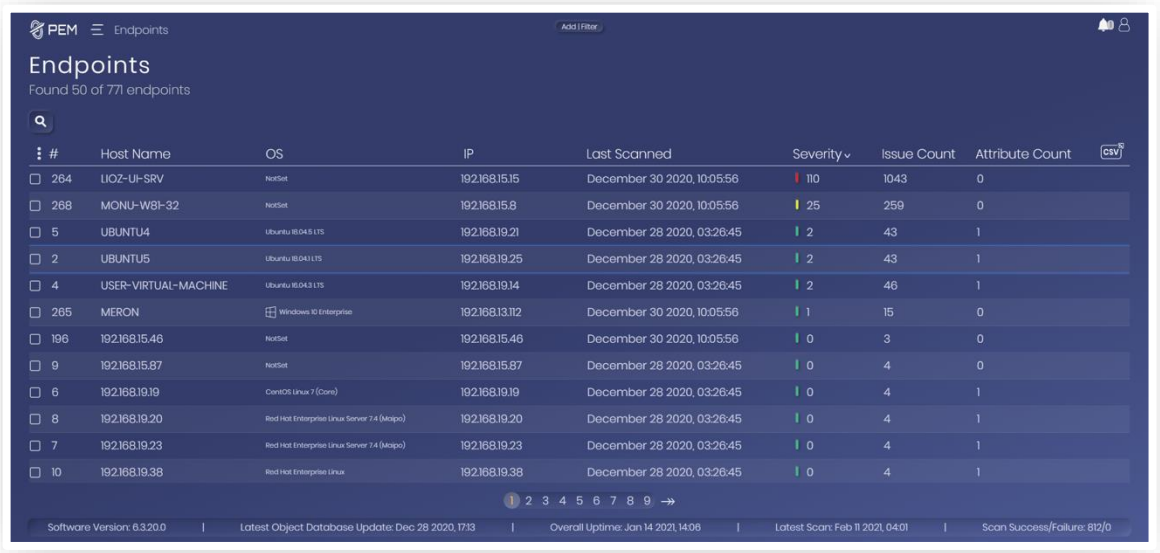




Clicking on each of the issues opens a full description of it.

Endpoints Screen

By selecting the “Endpoints” section from the menu, users can access the Endpoints screen. This screen shows a list of all endpoints within the scope of the current filter.



Within the list, users can see the details of each of the endpoints, including:

- Host Name
- IP Address
- Last Scanned timestamp
- Endpoint severity score
  Calculated by adding together the scores of all issues currently identified on that endpoint
- How many issues are currently identified on the endpoint
- How many attributes the endpoint has

From the Endpoints screen, users can select specific endpoints and create groups with attributes, with which they can they parse the data identified by PEM. For example, users can create a group for Linux machines, for a certain branch within a company, for computers belonging to C-level executives, for an ad-hoc project, for endpoints with a certain issue or above a certain severity level, or for any other necessary delineation within the network.

Filters

The content which populates the dashboard is controlled by a filter, which appears at the top of the screen and persists throughout the interface. With this filter, users can add rules to filter the information appearing in the dashboard. By default, the filter has two rules, one of which limits the data presented in the dashboard to findings from the past month, and the other filtering out issues pertaining to scan issues (host connection problems do not constitute security gaps).

Additional rules can be added, allowing users to filter by attribute, time, or any other type of data which PEM parses. For example, users can add a group of endpoint to the filter, the effect of which will be to populate the dashboard solely with data pertaining to those endpoints. Users can also use to filter to show issues from a certain day, or to show only issues of a certain type, or above a defined severity level. In this way, users can leverage the filter to show anything from all identified issues through the network to a specific defined query about a certain type of issue on a single endpoint.

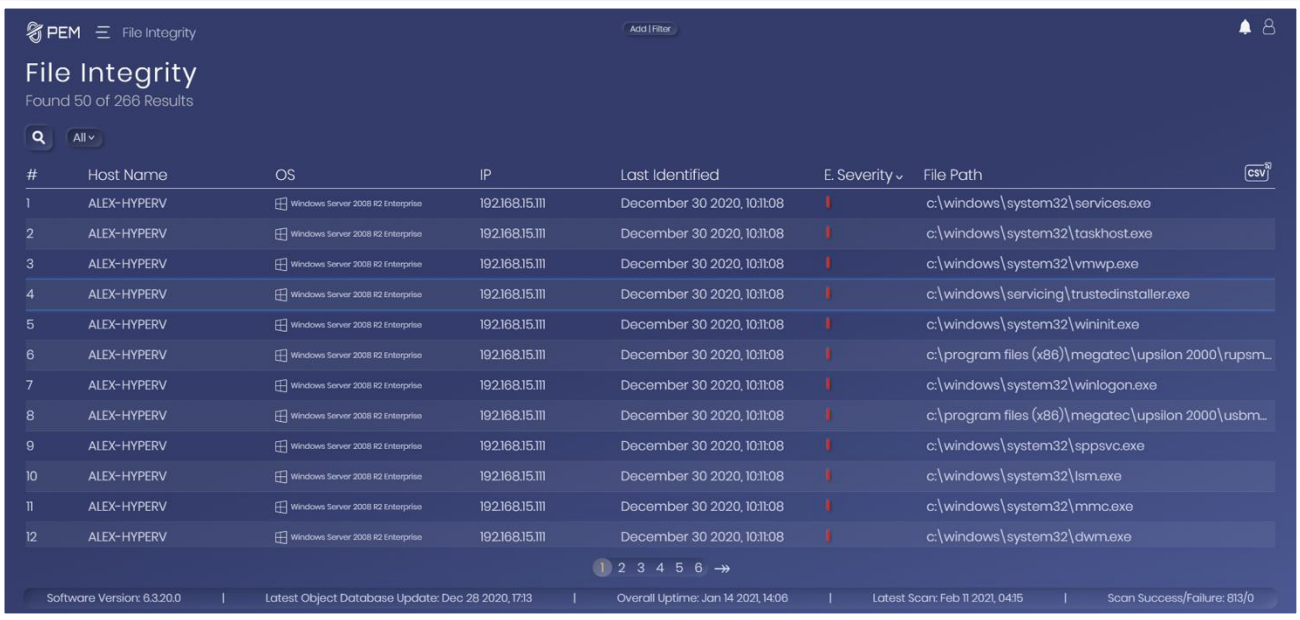
Since the filter persists through the interface, it can be used to filter the list of endpoints on the Endpoint screen and limit it to certain parameters, from which a group can then be created. Similarly, the filter controls the data shown in the Extended Details screen and in any other screen in the interface.

Rules can be removed from the filter at any time, and the any/all toggle can be changed to filter out data that answers any of the rules or all of them. The filter can be returned to default configurations at any time by simply refreshing the browser tab.

The filter is minimized when not in use, and when minimized, shows what it is currently filtering in the bar at the center of the top of the screen.

File Integrity Screen

The File Integrity screen can be accessed from the menu, and shows issues identified by PEM that are relevant to file integrity. These issues are subject to the general filter and can also be parsed according to type by clicking on the dropdown menu above the chart. By default, all issues of file integrity types are shown in the chart, but the type can also be limited to file reputation, hash changes (modified), hash changes (all scanned), and hash match. Clicking on one of the issues shown in the chart opens a screen with a full description of the issue, including details about it, which IP it was identified on, the file hashes where relevant, and the issue severity.



Additional Features

There is a built-in search functionality in all screens which contain charts, including the Endpoints screen, the Extended Details screen, and the File Integrity screen. This search function does not fetch data from the database, and as such does not re-filter the results. This means that the search is very quick, but is limited in capability, and thorough filtering should be done through the filter.

Edit options or additional options are accessed by clicking the icon at the top of each component in the

Data in the dashboard can be exported in PDF and CSV format wherever relevant, by clicking the CSV or PDF button at the top right of the component in question.

The bar at the bottom of the screen shows system details, including software version, last object database update, system uptime, last scan timestamp, and the success/failure rate of the recent scans.