

Streamlining collaboration between SecOps & ITOps with unified vulnerability detection and remediation

The challenges at hand

Vulnerabilities are on an exponential increase and so are the organizations that fall prey to cyberattacks. With over 97,000 vulnerabilities reported in the last 5 years, the solution to insulate your network and keep vulnerabilities at bay lies in devising a workflow to detect and remediate threats instantaneously.

Most organizations today are reliant on a dedicated SecOps team to detect and monitor the network for threats, while it falls upon the ITOps team to mitigate potential threats by leveraging proactive measures such as patch management.

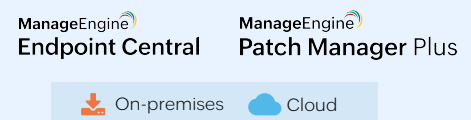
While this team dynamic is popular, the latency in collaboration between the two teams can often lead to unprecedented delays—thereby further slowing a process, that is supposed to be instantaneous (theoretically). In addition, the fragmented workflow paves the way for an increased operational overhead and a lack of visibility on the latest status of the process.

ManageEngine & Tenable: Fostering collaboration to bolster your network security

Detection, monitoring, and deployment—all from a single console. Leverage the ManageEngine - Tenable integration to identify, investigate, and prioritize critical vulnerabilities using Tenable's comprehensive vulnerability coverage.

Once detected via periodical scans, the vulnerabilities are auto-correlated and mapped with the available patches, right in the console. Admins can then deploy the required patches based on the organization's patching schedules. The unification of the two different processes in real time ensures a coherent collaboration between the SecOps and ITOps teams, enhancing the organization's threat response system.

Integrations available in



This integration displays patches for vulnerabilities listed under the following categories:

- Windows
- Windows: Microsoft Bulletins
- Databases
- Misc
- CentOS Local Security Checks
- Debian Local Security Checks
- Oracle Linux Local Security Checks
- Red Hat Local Security Checks
- Rocky Linux Local Security Checks
- SUSE Local Security Checks
- Ubuntu Local Security Checks

Benefits at a glance

- Risk-based patch management
- Rapid detection and mitigation from a unified console
- Secured patch deployment to endpoints
- Real-time visibility of assets in the network
- Reduced threat mitigation response times
- Enhanced collaboration of SecOps and ITOps teams



Scanning &
Detection



Swift remediation with
patches

Key takeaways of the integration

Here's a list of the key points of the integration and how the ManageEngine - Tenable collaboration benefits you:

- **Rapid detection & identification** of critical, zero-day, and other vulnerabilities by leveraging Tenable's comprehensive database
- **Decreased manual dependencies** via automated correlation of the vulnerabilities with their available patches
- **Risk-based prioritization of vulnerabilities** with Tenable's vulnerability priority rating (VPR)
- **Secured deployment to endpoints** by leveraging ManageEngine's automated patch testing and approval
- **Enhanced end-user productivity** and patch compliance via flexible deployment policies and self service portal for patches
- **Real-time visibility** of the vulnerability resolution status across all assets in the network
- **Reduced response times** by increased coordination and communications between SecOps and ITOps via a single glass pane

Get started with the solution

Leverage the collaboration by simply downloading [Endpoint Central](#) or [Patch Manager Plus](#) and integrating with [Tenable Security Center](#) or [Tenable Vulnerability Management](#).

About ManageEngine

ManageEngine is the enterprise IT and service software division of Zoho Corporation that crafts the industry's broadest suite of IT management software, with more than 60 enterprise products and over 60 free tools. Our on-premises and cloud solutions have powered the IT of over 280,000 companies around the world, including 9 of every 10 Fortune 100 companies.

Endpoint Central - our flagship Unified Endpoint Management and Security product supports patch management along with additional IT operation capabilities like mobile device management, OS deployment, asset management, and other security capabilities such as ransomware protection, peripheral device security and so on. It is available both on-premises and in the cloud.

Patch Manager Plus - our standalone patch management solution automates the patching of Windows, Mac, and Linux systems, along with over **850 third-party applications**. Patch Manager Plus is also available on-premises and in the cloud.

ENDPOINT CENTRAL

PATCH MANAGER PLUS

For more details, write to us at:

Endpoint Central support: endpointcentral-support@manageengine.com

Patch Manager Plus support: patchmanagerplus-support@manageengine.com