tenable

SOLUTION OVERVIEW

Tenable for ManageEngine

STREAMLINING COLLABORATION BETWEEN SECOPS & ITOPS WITH UNIFIED VULNERABILITY DETECTION AND REMEDIATION

Business Challenge

Each year, tens of thousands of vulnerabilities are disclosed by members of the security community and internal research teams at organizations around the world. These vulnerabilities are cataloged by the National Vulnerability Database as Common Vulnerabilities and Exposures (CVEs). Over a five year period from 2018 through 2022, the number of reported CVEs increased at an average annual growth rate of 26.3%. It's even more important to leverage an integrated solution to insulate your network and keep vulnerabilities at bay while 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). Oftentimes this lack of SecOps and ITOps collaboration can lead to a backlog of vulnerabilities, and an overwhelmed ITOps team that needs to decide how to prioritize remediations. In fact, many organizations struggle with how to decide which vulnerabilities to remediate first. On average, cybersecurity teams must address 870 vulnerabilities across 960 assets every day. When every threat is a high priority, none of them are. It's not enough to know threats exist – you need to know what to fix first.

Solution

Leverage the ManageEngine - Tenable integration to identify, investigate, and prioritize critical vulnerabilities. With Tenable, which has the industry's most extensive CVE and configuration coverage you can quickly see scan results and determine exposures then seamlessly determine next steps with ManageEngine.

Once detected via periodical scans, 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.

ManageEngine

Technology Components

- Tenable Vulnerability Management
- Tenable Security Center
- ManageEngine Patch Manager Plus
- ManageEngine Endpoint Central

Supported Plugin Families:

- Windows
- Windows: Microsoft Bulletins
- Databases
- 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

About Tenable

Tenable® is the Exposure Management company. More than 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies.

Learn more at www.tenable.com.

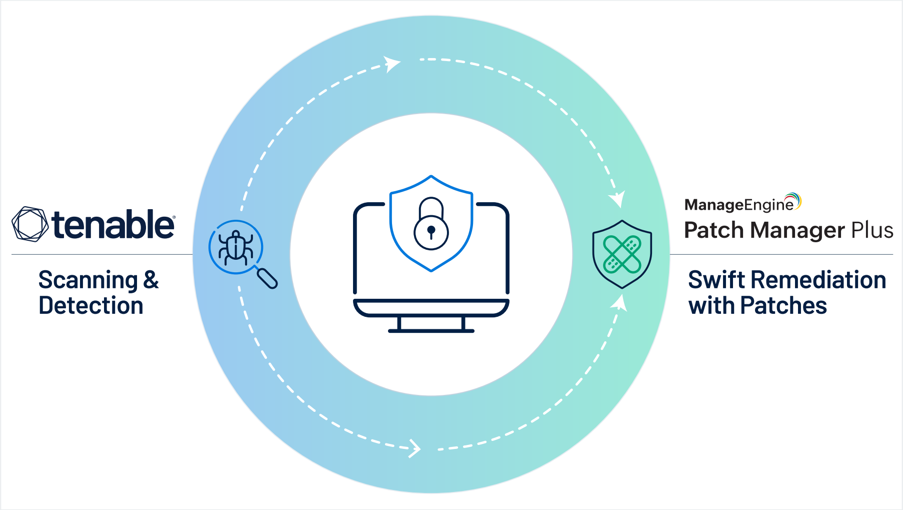
About ManageEngine

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.

Value

With this integration, you can achieve:

- **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 pane of glass



More Information

You can get the latest ManageEngine apps here: Endpoint Central; Patch Manager Plus

Installation and configuration documentation: Endpoint Central; Patch Manager Plus

Full list of Supported Applications: www.manageengine.com/patch-management/supported-applications.html

These integrations are built and supported by ManageEngine.
For support please contact: Endpoint Central; Patch Manager Plus