TENABLE NESSUS EXPERT

The Gold Standard for Vulnerability Assessment

Scarce resources, limited time, a constantly changing attack surface – it's a challenge for security practitioners on the front lines to keep pace with threat actors. What is needed is a fast, easy way to proactively find, prioritize and remediate vulnerabilities. What is needed is Tenable Nessus® Expert.

Nessus Expert automates point-in-time assessments to help you quickly identify and remediate vulnerabilities, including software flaws, missing patches, malware, and misconfigurations, across a variety of operating systems, devices and applications.

The Evolving Modern Attack Surface

When Nessus was introduced in 1998 as the industry's first vulnerability assessment (VA) tool, the attack surface was made up of traditional IT devices - desktops, workstations, network equipment, etc. However, as new technologies have emerged over the years, the modern attack surface has expanded and threat actors are taking advantage.

New attack vectors are emerging that go way beyond traditional IT assets and have to be defended.

Vulnerabilities in areas like cloud infrastructure, your external attack surface and web applications have all been exploited by attackers to infiltrate countless networks. Security practitioners, consultants, developers and pentesters need a single vulnerability assessment solution that addresses both traditional threats and those connected to the modern attack surface.

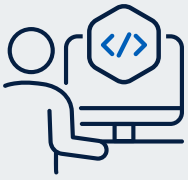
Breadth and Depth of Coverage

Tenable Research works closely with the security community to discover new vulnerabilities and provide insights to help organizations mature their vulnerability assessment practices. Tenable's zero day team has discovered more than 465 zero-day vulnerabilities since 2019.

Adding More to Your Assessment Tool Belt

Nessus is the industry's most recognized vulnerability scanner because it provides unmatched visibility into the vulnerabilities, misconfigurations and non-compliant conditions associated with your traditional IT assets. Nessus Expert adds to that legacy by providing the same visibility into the modern attack surface that includes your internet-facing assets, cloud infrastructure, and web applications - all under one roof.

Discover and Assess Your IT Assets



Fortify Your Web Applications

Secure Cloud Infrastructure Before Deployment

Gain Visibility Into Your Internet-Facing Attack Surface

NESSUS EXPERT AND THE MODERN ATTACK SURFACE

Shift Left & Securing Cloud Infrastructure

With the emergence of cloud services and infrastructure, deploying new apps and workloads can be simple to do. But, with speed and agility comes a tradeoff of additional, unknown cyber risks within those environments. There are existing solutions designed to protect the cloud, but they are applied too late. Nessus Expert allows you to scan your infrastructure as code (IaC) code repositories for security weaknesses before pushing to production to prevent unknown risk.

KEY BENEFITS:

- Provides a proactive approach to vulnerability assessment for cloud workloads
- Scan for disruptive and costly vulnerabilities before code is deployed
- Leverage 500 prebuilt policies for IaC scanning
- Prevent misconfigurations and vulnerabilities from reaching cloud production instances

Gain Visibility Into Your Internet-Facing Attack Surface

The modern attack surface is comprised of internet-facing assets that are commonly unknown due to missing inventory controls and the ability for developers to spin up cloud instances in minutes. From an attacker's perspective, internet facing assets provide a simple yet stealthy way to probe for vulnerabilities and infiltrate a network, especially if you don't know they even exist. Nessus Expert allows you to discover and assess these unknown assets for vulnerabilities, misconfigurations and non-compliant conditions.

KEY BENEFITS:

- Discover internet-connected assets that were previously unknown to the organization
- Kick off assessment scans for newly identified assets
- Scan up to five domains every 90 days to understand all associated subdomains
- Build a continuous inventory of your internet-connected assets
- Understand risk and close the gap for assets outside of your perimeter

Multi-Tiered Analysis to Fortify Your Web Applications

The average web application has between 3-5 vulnerabilities, including many that are high severity. With nearly 2 billion web applications across the world, it's no surprise that web applications remain one of the most common attack vectors causing data breaches. Web application scanning in Nessus Expert provides a dynamic application security testing (DAST) feature that provides comprehensive visibility and insight into web application security issues. It safely scans modern web applications, accurately identifying vulnerabilities in custom application code as well as vulnerable versions of third-party components that make up the bulk of the application.

KEY BENEFITS:

- Supports five fully qualified domain names (FQDN) with option to add more.
- Easily set-up new web app and API scans and generate comprehensive results.
- Identify vulnerabilities in both your custom application code and the web components supporting it.
- Quickly identify web application cyber hygiene Issues relating to SSL/TLS certificates and HTTP header misconfigurations.
- Confidently and safely scan environments without disruptions or delays.
- Built and backed by Tenable Research, #1 in vulnerability coverage and accuracy.

Nessus is #1 in Vulnerability Assessment

#1 in Accuracy
Nessus has the industry's lowest false positive rate with six-sigma accuracy (measured at .32 defects per 1 million scans).

#1 in Coverage
Nessus has the deepest and broadest coverage with more than 77,000 CVEs and over 100 new plugins released weekly within 24 hours of vulnerability disclosure.

#1 in Adoption
Nessus is trusted by more than 30,000 organizations globally, including 2 million downloads. 50% of the Fortune 500 and more than 30% of the Global 2000 rely on Nessus technology.

Leverage the Power of Predictive Prioritization

Take advantage of Tenable's Vulnerability Priority Rating (VPR) to help you zero in on the vulnerabilities that pose the greatest risk to your environment and remediate them first. The VPR is generated by combining Tenable and third-party vulnerability data with external threat data and analyzing it using an advanced data science algorithm developed by Tenable Research.

WHY NESSUS LEADS THE WAY

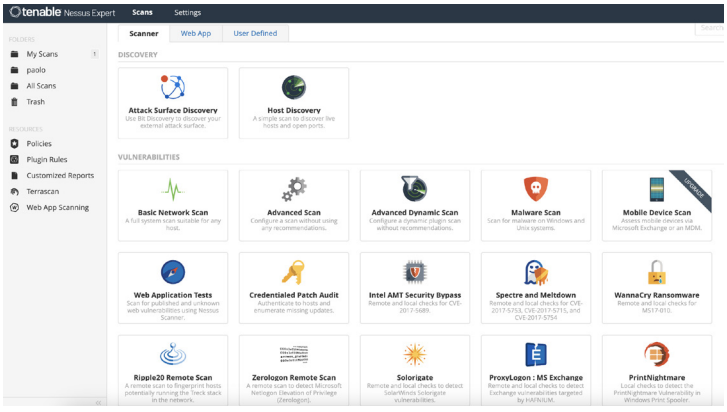
Ease of Use

Built for security practitioners, by security practitioners, Nessus was created with the single focus of providing an intuitive experience for security pros on the front lines to find and remediate vulnerabilities, faster and more confidently.

UX updates have made navigation and user experience easier and more intuitive. Nessus' new resource center provides users with relevant information at their fingertips. User specific guides provide actionable tips and guidance based on the operations and functions being performed.

Quickly See Vulnerabilities with Pre-Built Policies and Templates

Out-of-the-box, pre-configured scan templates help you quickly understand where you have vulnerabilities, misconfigurations and con-compliant conditions. Scan templates are provided for IT and mobile assets, cloud infrastructure, external attack surface and web applications.



More than 450 compliance and configuration templates allow you to audit configuration compliance against CIS benchmarks and other best practices .

Value Beyond Vulnerabilities

While Nessus is the gold standard for vulnerability assessments, the value it provides doesn't stop there. Nessus Expert can be used to deliver additional services to organizations to improve their risk awareness. These include:

Asset Discovery - Maintain a current inventory list all software, hardware, and cloud assets in an environment

OS/DB/Applications and Network Infrastructure Audits - Ensure that IT assets are compliant with over 428 different policies and standards

Security Frameworks/Compliance Standards Audits - Ensure that configuration and administrative settings are secure and in compliance with internal or regulatory requirements, security framework standards and best practices

Active Directory (AD) Checks - utilize 10 foundational AD checks to detect commonly exploited weaknesses to help protect credentials, prevent privilege escalation and prevent lateral movement

Unsupported OS and Third-Party Software - Quickly identify operating systems and applications that are unsupported or end-of-life (EOL) that put organizations at risk

Version and Change Control - Establish and flag version changes or drift from the approved "gold image" for servers and endpoints

Audit Cloud Assets - Audit assets in AWS, GCP, Azure, SFDC, Rackspace, and Zoom environments for account-level misconfigurations, and/or all cloud-based assets on a particular domain

Integration - Enhance your operational security and awareness by integrating Nessus scan results into many third-party IT and security solutions

About Tenable

Tenable® is the Exposure Management company. Approximately 43,000 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 tenable.com.

Configure Reports Easily

Create reports based on customized views (e.g., specific vulnerability types, vulnerabilities by host/plugin, by team/ client) – in a variety of formats (HTML, CSV and Nessus XML). Independent security consultants can customize the report title, logo, and layout, enabling you to prepare reports for different stakeholders

Laser focus with Grouped View

Similar issues or categories of vulnerabilities are grouped together and presented in one thread. Snoozing allows users to select issues to disappear from view for a specified period of time. This helps with prioritization, allowing you to focus only on the issues you are working on at a given time.

Drilldown and Troubleshooting

As networks become more sophisticated and complex, zeroing in on potential issues have become increasingly time consuming. The Nessus packet capture feature enables a powerful debugging capability to troubleshoot scanning issues.

Intelligent Vulnerability Assessment with Live Results

Live Results performs intelligent vulnerability assessment in offline mode with every plugin update – without having to run a scan. Just log in and see the results of potential vulnerabilities based on your scan history. With a click of a button, you can run a scan to validate the presence of the vulnerability, creating a faster, more efficient process for assessing, prioritizing and remediating issues.

Portable and Flexible

For portability and ease of use, Nessus is available on Raspberry Pi. This enables remote Nessus analysis when there is no network infrastructure to support Nessus running on a laptop. This is specifically useful for pen testers, consultants and others whose job function requires mobility between locations.

Advanced Support Available

Nessus Expert customers can access email, portal, chat and phone support 24 hours a day, 365 days a year with a subscription to the Advanced level of technical support. This will also help ensure faster response times and resolution. Full details about support plans can be found here.