tenable | Data Sheet

Vulnerability Exposure

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. Enter: 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 your external attack surface and web applications have 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 Research provides 24/7 updates into new and emergent vulnerabilities so you'll always have full situational awareness.

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 and web applications — all under one roof.

Discover and assess your IT assets

Fortify your web applications

Gain visibility into your internet-facing attack surface

Nessus Expert and the Modern Attack Surface

Gain visibility into your internet-facing attack surface

The modern attack surface consists 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:

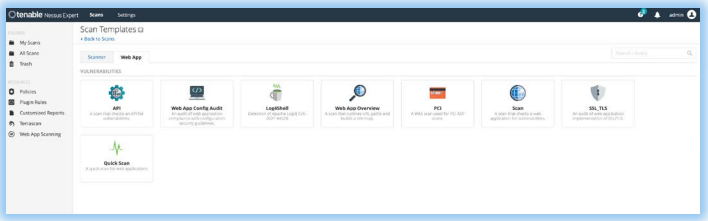
- Discover internet-connected assets that were previously unknown to the organization
- Kick off assessment scans for newly identified assets
- Scan up to five domains every 90 days to understand all associated sub-domains
- Build a continuous inventory of your internet-connected assets
- Understand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

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.

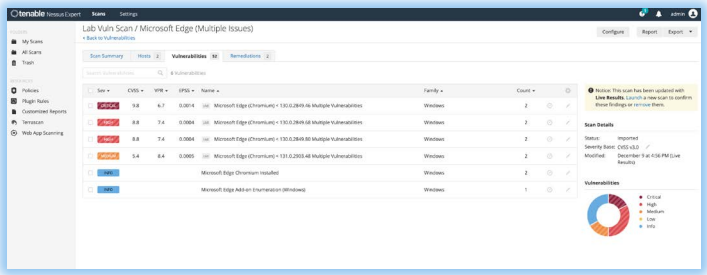
Key Benefits:

- Supports 5 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.



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. 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: An intuitive interface and resource center with user-specific guides help security pros find and remediate vulnerabilities faster.

Pre-built policies & templates: Get quick visibility into vulnerabilities, misconfigurations, and non-compliant conditions with pre-configured scan templates for IT, web apps, and external internet-facing assets.

Customizable reports: Easily create and export reports in various formats (HTML, CSV, PDF, Nessus XML), with customizable titles, logos, and layouts for different stakeholders.

Grouped view: Focus on what matters most by grouping similar vulnerabilities and snoozing issues for a specified period to streamline prioritization.

Drilldown & troubleshooting: Use the Nessus packet capture feature for powerful debugging to quickly zero in on potential scanning issues.

Intelligent assessment: "Live Results" shows potential vulnerabilities based on your scan history with every plugin update — without running a full scan.

Portable & flexible: Nessus is available on Raspberry Pi for remote analysis and ultimate mobility, ideal for pen testers and consultants.

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 helps ensure faster response times and resolution. Full details about support plans can be found here.

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 of all software and hardware in an environment.
- **OS/DB/applications and network infrastructure audits -** Ensure that IT assets are compliant with over 450 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.
- **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, exposing and closing the cybersecurity gaps that erode business value, reputation and trust. The company's AI-powered exposure management platform radically unifies security visibility, insight and action across the attack surface, equipping modern organizations to protect against attacks from IT infrastructure to cloud environments to critical infrastructure and everywhere in between. By protecting enterprises from security exposure, Tenable reduces business risk for approximately 44,000 customers around the globe. Learn more at tenable.com.

Contact Us

Please email us at sales@tenable.com or visit tenable.com/contact.

080425