Informe Técnico Previo de Evaluación de Software Nº 004-2025-AIT-DTI-DGA/CR SUSCRIPCIÓN DE SOFTWARE DE ANÁLISIS DE VULNERABILIDADES

1. Nombre del Área:

Área de Infraestructura Tecnológica.

2. Responsable de la evaluación:

John Blademir Anaya Veramendi.

3. Cargo:

Jefe del Área de Infraestructura Tecnológica.

4. Fecha:

16 de abril de 2025.

5. Requerimiento del Área Usuaria:

El Congreso de la República requiere contratar la suscripción por 730 días calendario, de un software para escaneo, análisis y gestión de vulnerabilidades, el software debe tener las siguientes características

- El alcance del servicio comprende la suscripción de software para escaneo y análisis de vulnerabilidades de 350 activos de red y 05 aplicaciones web.
- Todo el software debe estar integrado en una plataforma de gestión de vulnerabilidades de un único fabricante.
- Se requieren las últimas versiones de software vigentes al momento del otorgamiento de la buena pro.
- Debe contar con una consola de administración web que permita la gestión de usuarios, configuración de perfiles y grupos de activos o aplicaciones, visualización de un tablero de control ejecutivo y consolidación de los escaneos internos y externos.
- El acceso a la consola de administración debe realizarse mediante interfaz web segura (HTTPS) y ser compatible con las últimas versiones de los principales navegadores web.
- La suscripción tendrá validez por un periodo de dos (02) años, equivalente a 730 días calendario.
- El software debe ser compatible con los sistemas operativos utilizados por los usuarios del Congreso de la República (Windows, Linux).
- El proveedor deberá ofrecer asistencia técnica y soporte durante el período de validez de las licencias.

Software para escaneo y análisis de vulnerabilidades de activos de red:

- El software debe estar licenciado para permitir el escaneo/análisis de 350 activos de red.
- El modelo de licenciamiento debe estar basado en activos, en el cual se consume una única licencia por activo, incluso si el activo tiene múltiples direcciones IP.
- Capacidad para programar y ejecutar las actividades de escaneo/análisis de manera centralizada desde la interfaz web de la plataforma de gestión de vulnerabilidades del fabricante, del mismo modo la visualización de los resultados y los reportes deben centralizarse en la misma plataforma.

- Debe permitir el despliegue y el uso combinado de escáneres y/o agentes y/o sensores y/o conectores para tener la visibilidad de toda la red de datos de la institución y así maximizar la cobertura del análisis.
- Los agentes, escáneres, sensores y conectores que se desplieguen no deben tener un costo adicional.
- Rastreo de los cambios de los activos.
- Escaneo de redes hibridas IPv4/IPv6.
- Permitir identificar y priorizar las vulnerabilidades de acuerdo a su impacto y riesgo.
- Debe escanear y analizar vulnerabilidades y errores de configuración.
- Debe contar con tableros de control de visualización intuitiva para realizar un análisis rápido.
- Debe clasificar las vulnerabilidades por CVE/CVSS e identificar los últimos parches y recomendaciones para su remediación.
- Descubrimiento de vulnerabilidades con o sin credenciales.
- Descubrir vulnerabilidades en bases de datos.
- Gestionar las exploraciones desde una interfaz web para escaneos diarios, semanales, mensuales y otros tipos de auditoría.
- Detectar virus, puertas traseras, host que se comunican con sistemas boot-infected, procesos conocidos/desconocidos, servicios web que enlazan a contenido malicioso.
- Generación de informes / reportes personalizados.

Software para escaneo y análisis de vulnerabilidades de aplicaciones web:

- El software debe estar licenciado para permitir el escaneo/análisis de 05 aplicaciones web.
- Solución dinámica de prueba de seguridad de aplicaciones (DAST).
- Programar y ejecutar las actividades de escaneo/análisis de manera centralizada desde la interfaz web de la plataforma de gestión de vulnerabilidades del fabricante, del mismo modo la visualización de los resultados y los reportes deben centralizarse en la misma plataforma.
- Permitir un escaneo externo seguro que garantice que las aplicaciones web de producción, no se vean interrumpidas o demoradas a causa del escaneo.
- Permitir excluir partes de la aplicación web que se analizara mediante las URL o extensiones de archivos a excluir del análisis. Ello con el fin de prevenir latencia o interrupción de las aplicaciones críticas.
- Definir parámetros de frecuencia y horario para programar y automatizar el escaneo de aplicaciones web.
- Debe escanear desde los 10 principales riesgos de OWASP hasta los componentes vulnerables de las aplicaciones web en una única plataforma.
- Capacidad para detectar existencia de certificados SSL/TLS por caducar o emitidos incorrectamente.
- Detectar configuraciones incorrectas en el servidor web.
- Permitir escaneos configurables para auditorias personalizadas.
- Capacidad de escaneo con y sin autenticación.
- Debe permitir crear tableros de control y visualizaciones personalizadas.
- Clasificar por nivel de riesgo de las vulnerabilidades, en base a la explotabilidad y de acuerdo a CVSS (Common Vulnerabily Scoring System).
- Debe tener plantillas de escaneo y permitir generar nuevas plantillas en base a las que viene por defecto.

- Capacidad para guarda la información histórica de escaneos previos, para poder compararlos.
- Permitir programar los escáneres para un momento, plantilla y grupo específico, con opción de programarse para ser recurrente.
- Brindar recomendaciones de solución para superar las vulnerabilidades encontradas.

6. Justificación:

Como parte de los controles recomendados por la NTP ISO / IEC 27001:2022 Anexo A (A.8.8 Gestión de vulnerabilidades técnicas), en el Congreso de la Republica se desarrollarán actividades de identificación, evaluación y corrección de las vulnerabilidades técnicas existentes sobre los activos TI.

Actualmente existe la necesidad de identificación, evaluación y corrección de las vulnerabilidades técnicas de los activos de red sobre los cuales se debe realiza el análisis de vulnerabilidades, por esta razón se requiere contratar la suscripción por 730 días calendario, de un software para escaneo, análisis y gestión de vulnerabilidades.

Para ello se necesita contar con una herramienta que permita automatizar este proceso con el fin de tener resultados preventivos y se realice de forma permanente, evitando así que se materialicen riesgos que afecten la seguridad de la información en la institución.

El presente informe se elabora en cumplimiento de la Ley N° 28612 Ley que norma el Uso, Adquisición y Adecuación del software en la Administración Pública, dejándose constancia que la adquisición en cuestión responde a los principios de vigencia y neutralidad tecnológica, trasparencia y eficiencia, y a los criterios de austeridad y ahorro de los recursos públicos mencionados en dicha Ley.

La solución debe permitir el análisis y gestión de vulnerabilidades técnicas y el cumplimiento de buenas prácticas de seguridad para al menos 350 equipos y 05 aplicaciones web, considerando tanto infraestructura de red, de virtualización, servidores, almacenamiento, física y de seguridad, como las bases de datos, aplicaciones y sistemas de información implementados en esta infraestructura. La solución debe cumplir con las siguientes especificaciones técnicas mínimas:

- El alcance del servicio comprende la suscripción de software para escaneo y análisis de vulnerabilidades de 350 activos de red y 05 aplicaciones web.
- Todo el software debe estar integrado en una plataforma de gestión de vulnerabilidades de un único fabricante.
- Se requieren las últimas versiones de software vigentes al momento del otorgamiento de la buena pro.
- Debe contar con una consola de administración web que permita la gestión de usuarios, configuración de perfiles y grupos de activos o aplicaciones, visualización de un tablero de control ejecutivo y consolidación de los escaneos internos y externos.
- El acceso a la consola de administración debe realizarse mediante interfaz web segura (HTTPS) y ser compatible con las últimas versiones de los principales navegadores web.
- La suscripción tendrá validez por un periodo de dos (02) años, equivalente a 730 días calendario.
- El software debe ser compatible con los sistemas operativos utilizados por los usuarios del Congreso de la República (Windows, Linux).

- El proveedor deberá ofrecer asistencia técnica y soporte durante el período de validez de las licencias.

7. Alternativas

Las alternativas del mercado actual para el software para escaneo, análisis y gestión de vulnerabilidades son las siguientes:

- Tenable Vulnerability Management
- Rapid 7 Insight Vulnerability Managent

8. Análisis Comparativo Técnico

El análisis comparativo técnico se hará sobre productos finales, es decir, sobre productos ensamblados que vienen en formato de ejecutables o como una suscripción. Para lo cual se debe:

- Comparar productos con similares características.
- Validar que las alternativas seleccionadas sean las más convenientes para la institución.
- Seleccionar una alternativa entre productos competitivos.

El análisis técnico se ha realizado en conformidad con la metodología establecida en la "Guía Técnica de Evaluación de Software" aprobada por Resolución Ministerial N° 139-2004-PCM, en el cual se han tomado en cuenta las siguientes consideraciones:

- **Propósito de la evaluación:**
  Determinar los atributos o características mínimas para asegurar que las alternativas evaluadas se ajustan a las necesidades y requerimientos de la institución.

- **Identificación del producto**
  Software para escaneo, análisis y gestión de vulnerabilidades.

- **Especificaciones del modelo de calidad**
  Se aplicará el modelo de Calidad de Software Descrito en la parte I de la Guía de Evaluación de software aprobado por Resolución Ministerial Nº 139-2004-PCM.

- **Selección de métricas:**
  Las métricas fueron seleccionadas en base al análisis de los requerimientos técnicos y a la información técnica de los productos de software señalados en el punto 7 Alternativas.

Del análisis realizado, se han determinado las siguientes características técnicas mínimas y sus respectivas métricas.

Informe Técnico Previo de Evaluación de Software Nº 004-2025-AIT-DTI-DGA/CR SUSCRIPCIÓN DE SOFTWARE DE ANÁLISIS DE VULNERABILIDADES

ATRIBUTOS INTERNOS Y EXTERNOS			
ITEM	**CARACTERÍSTICA**	**SUB CARACTERÍSTICA**	**PUNTAJE**
1	**ADECUACION**	Facilita la generación de informes de vulnerabilidad estándar y de cumplimiento y provee una vista unificada	7
2	**INTEGRACION**	Se integra y complementa con la plataforma de infraestructura existente	7
3	**FUNCIONALIDAD**	Capacidad para el descubrimiento de activos	5
4		Capacidad y cobertura para la detección de vulnerabilidades	5
5		Detección de malware	5
6		Motor de búsqueda avanzado	4
7		Plantillas y políticas preconfiguradas y personalizables listas para realizar escaneos	5
8		Automatización de tareas, permite definir parámetros de frecuencia y horario	4
9		Escaneo activo que se integra y/o complementa con servicios de escaneo pasivo	5
10		Configuración y despliegue de agentes para escaneo y monitoreo	5
11		Escaneo por direcciones IP y nombres DNS	4
12		Integración con soluciones de administración de parches y administración de credenciales	4
13		Manejo de pruebas avanzadas	5
14		Conexiones concurrentes	4
15	**PORTABILIDAD**	Facilidad para la instalación, despliegue y configuración	5
16		Actualizaciones automáticas	3
17	**FIABILIDAD**	Proporciona disponibilidad y escalabilidad	3
18		Soporta estándares	3
19	**USABILIDAD**	Facilidad de uso a través de una interfaz simple e intuitiva	5
20		Generación de reportes, análisis y métricas	3
21		Licenciamiento basado en activo y no en direcciones IP	3
22	**SEGURIDAD**	Acceso basado en roles	3
23		Cumplimiento de estándares de seguridad	3
		TOTAL	**100**

Luego de determinar las características técnicas mínimas y las métricas aplicables, se procedió al análisis comparativo técnico, para lo cual se aplicó el modelo de calidad de software descrito en la Parte I Guía Evaluación de Software por Resolución Ministerial N° 139-2004 PCM.

Informe Técnico Previo de Evaluación de Software Nº 004-2025-AIT-DTI-DGA/CR SUSCRIPCIÓN DE SOFTWARE DE ANÁLISIS DE VULNERABILIDADES

Se tomarán en consideración para la evaluación costo – beneficio, aquellas alternativas que obtengan un puntaje igual o superior a 85 en el análisis comparativo técnico:

ITEM	CARACTERÍSTICA	SUB CARACTERÍSTICA	PUNTAJE	Tenable Vulnerability Management	Rapid 7 Insight Vulnerability Managent
1	ADECUACION	Facilita la generación de informes de vulnerabilidad estándar y de cumplimiento y provee una vista unificada	7	6	6
2	INTEGRACION	Se integra y complementa con la plataforma de infraestructura existente	7	7	6
3	FUNCIONALIDAD	Capacidad para el descubrimiento de activos	5	5	5
4		Capacidad y cobertura para la detección de vulnerabilidades	5	5	4
5		Detección de malware	5	4	4
6		Motor de búsqueda avanzado	4	4	3
7		Plantillas y políticas preconfiguradas y personalizables listas para realizar escaneos	5	5	4
8		Automatización de tareas, permite definir parámetros de frecuencia y horario	4	4	4
9		Escaneo activo que se integra y/o complementa con servicios de escaneo pasivo	5	5	5
10		Configuración y despliegue de agentes para escaneo y monitoreo	5	4	4
11		Escaneo por direcciones IP y nombres DNS	4	4	3
12		Integración con soluciones de administración de parches y administración de credenciales	4	3	3
13		Manejo de pruebas avanzadas	5	3	4
14		Conexiones concurrentes	4	3	4
15	PORTABILIDAD	Facilidad para la instalación, despliegue y configuración	5	4	3
16		Actualizaciones automáticas	3	3	3
17	FIABILIDAD	Proporciona disponibilidad y escalabilidad	3	3	2
18		Soporta estándares	3	3	3
19	USABILIDAD	Facilidad de uso a través de una interfaz simple e intuitiva	5	5	4
20		Generación de reportes, análisis y métricas	3	3	3
21		Licenciamiento basado en activo y no en direcciones IP	3	3	2
22	SEGURIDAD	Acceso basado en roles	3	3	3
23		Cumplimiento de estándares de seguridad	3	3	3
		TOTAL OBTENIDO	**100**	**92**	**85**

Informe Técnico Previo de Evaluación de Software Nº 004-2025-AIT-DTI-DGA/CR
SUSCRIPCIÓN DE SOFTWARE DE ANÁLISIS DE VULNERABILIDADES

9. Análisis Comparativo Costo – Beneficio

- **Licenciamiento:**
  La evaluación de estas alternativas incluye solo los costos de licencias por suscripción anual del software, de los cuales el costo referencial de uno de los productos evaluados ha sido tomado desde la página web del fabricante de software.

Alternativa	Costo	Costo Total Soles
Tenable Vulnerability Management *LIcencia de 300 activos por 01 año* No incluye IGV	S/ 52,136.00	S/ 52,136.00
Rapid 7 Insight Vulnerability Managent *Licencia de 300 activos por 01 año / Costo por activo: $23.18* Fuente: https://www.rapid7.com/products/insightvm/pricing/ No incluye IGV Tipo de cambio SBS del 15/04/2025 = 3.724	$ 6,954.00	S/. 25,896.67

Los detalles de las cotizaciones se adjuntan al final del documento.

- **Hardware necesario para su funcionamiento:**
  El software utilizará a la plataforma informática existente en el Congreso de la República, por lo tanto, no será necesario adquirir hardware adicional para implementar la herramienta de análisis de vulnerabilidades.

- **Soporte y mantenimiento externo:**
  Con la suscripción de la licencia del software para el análisis de vulnerabilidades, se tiene derechos de soporte, actualizaciones de los parches de y actualización de versiones ultimas liberadas por el fabricante durante el periodo de la garantía del producto en mención.

- **Personal y mantenimiento interno:**
  En los términos de referencia del requerimiento se solicita que la empresa que proveerá el software debe contar con los servicios de un técnico certificado en el producto propuesto.

- **Capacitación:**
  En las especificaciones técnicas del requerimiento se solicita que la empresa provea la capacitación respectiva en el producto propuesto.

10. Conclusiones

Considerando los resultados del Análisis Comparativo Técnico y Análisis Comparativo Costo Beneficio, se concluye, que los productos evaluados y que son señalados en el punto 7 Alternativas

son adecuados para la gestión de vulnerabilidades digitales. Asimismo, dado que las prestaciones son similares, sería recomendable adquirir la solución cuyas condiciones de contratación sean las más favorables para la entidad.

PERÚ CONGRESO de la REPÚBLICA Firmado digitalmente por: ANAYA VERAMENDI John Blademir FAU 20161749126 hard Motivo: Soy el autor del documento Fecha: 16/04/2025 12:46:07-0500	PERÚ CONGRESO de la REPÚBLICA Firmado digitalmente por: PRIETO HERNANDEZ Eduardo Celso FAU 20161749126 hard Motivo: En señal de conformidad Fecha: 16/04/2025 15:16:43-0500
EVALUADO POR: John Blademir Anaya Veramendi **Jefe del Área de Infraestructura Tecnológica**	**APROBADO POR:** Eduardo Celso Prieto Hernández **Jefe del Departamento de Tecnologías de la Información**

PROPUESTA COMERCIAL

IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.
RUC: 20552075341
Dirección: Av. Jose Pardo 434, Oficina 401, Miraflores. Lima
Contacto: 0800 74024 | ventas@imperia.com.pe
www.imperia.com.pe

N° Cotización: 0006600
Cliente: CONGRESO
Fecha: 4 de Abril de 2025
Referencia: TENABLE

Razon Social:	CONGRESO DE LA REPUBLICA		
Dirección:	Jr. Huallaga Nro. 358 Lima Lima, Perú		
R.U.C.	20161749126		
Atención:	Wilfredo Rivera	**Consultor:**	Merly La Rosa
Cargo / Área:		**Cargo:**	Account Manager
E-Mail:		**E-Mail:**	merly.larosa@imperia.com.pe
Telefono:		**Celular:**	923 267 482

Item	Descripción	Cantidad	P. Unitario S/	P. Total S/	Tiempo Entrega e Implementación
	NOMBRE DEL REQUERIMIENTO: TENABLE				
1	**TIOVM** : Tenable Vulnerability Management Dates: 4/2/2025 to 4/1/2026 Term: 12 Months Assets: 300 Order Type: New	1	S/ 52,136.00	S/ 52,136.00	15 días calendarios
	SERVICIOS PROFESIONALES IMPERIA				
2	**SSP01:** Servicios de Instalación	1	S/ 6,333.33	S/ 6,333.33	
3	**SSP02:** Servicios de Soporte 24x7 durante 12 meses	1	S/ 8,233.33	S/ 8,233.33	

Subtotal	S/ 66,702.67
IGV (18%)	S/ 12,006.48
TOTAL (SOLES)	S/ 78,709.15

Observaciones:

Tiempo de entrega: 15 días calendarios
Garantía de fabrica: Doce (12) meses de fábrica
Impuestos: Los precios incluyen IGV (18%)
Entrega de Productos y Envíos: De Lunes a Viernes. Previa coordinación.

Condiciones Comerciales:

Forma Pago: Al Contado
Lugar Entrega: Oficinas del Cliente
Validez Oferta: 30 días calendarios
T. Cambio: 3.8

Los productos o servicios que no estén expresamente estipulados, no son parte integrante de esta cotización.
La solución propuesta es el resultado de la evaluación de los requerimientos e información provista por el cliente.
El envío de una Orden de Compra significa la aceptación de las condiciones anteriores.
Números de cuenta:
Cta Cte BBVA CONTINENTAL (SOLES): 0011-0186-0100037567-43
Cta CCI BBVA CONTINENTAL (SOLES): 011-186-000100037567-43
Cta Detracción BANCO DE LA NACIÓN (SOLES): 00-023-027178

InsightVM Pricing

Starting cost for Rapid7's vulnerability management solution

LET'S TALK START FREE TRIAL

$2.19/month*

For **250** Assets, Per Asset

$26.25/year*

$1.93/month*

For **500** Assets, Per Asset

$23.18/year*

$1.79/month*

For **750** Assets, Per Asset

$21.43/year*

$1.71/month*

For **1000** Assets, Per Asset

$20.54/year*

$1.62/month*

For **1250** Assets, Per Asset

$19.43/year*

Cover your entire network with volume-based discounts.

*Price based on 512 **assets** minimum. Billed annually. All amounts are shown in U.S. dollars. International prices vary.

REQUEST QUOTE

Frequently asked questions

How do you define an asset?

Does the pricing differ depending on the type of asset?

Can I try before I buy?

How am I billed? What payment methods do you support? +

How can I get a custom quote? +

What information do I need to provide to get a custom quote? +

Where can I find pricing outside of the U.S.? +

How can I upgrade from Nexposeto InsightVM? +

Is this pricing also for one-off vulnerability scans? +

Do you have an MSSP pricing model? +

Is this pricing based on assets at one location? Can they spread between different locations? +

Does this pricing include support? How much support will I receive? +

What if I need more support? +

Does this pricing include Managed Vulnerability Management?

Available on AWS Marketplace

VIEW →

Rapid7's Insight cloud platform is trusted by more than 10,000 customers in over 140+ countries.

LET´S TALK

START FREE TRIAL

tenable.sc™

DATA SHEET

Vulnerability Management Managed on-Prem

The Tenable.sc™ platform provides the most comprehensive and integrated view of enterprise security posture so you can accurately identify, investigate and prioritize vulnerabilities.

Tenable.sc is a vulnerability management solution that provides visibility into your attack surface so you can manage and measure your cyber risk. Through advanced analytics, customizable dashboards, reports and workflows, you can understand your risk and know which vulnerabilities to fix first.

Built on leading Nessus technology, Tenable.sc gathers and evaluates vulnerability data across multiple Nessus® scanners distributed across your enterprise and illustrates vulnerability trends over time to assess risk and prioritize vulnerabilities. Finally, Tenable.sc includes a configurable workflow engine that helps your security team speed up response and remediation, to reduce overall risk and streamline compliance.

Tenable.sc includes Predictive Prioritization, which combines data and threat intelligence across multiple sources, and analyzes them all with a data science algorithm that uses machine learning to anticipate the probability of a vulnerability being leveraged by threat actors. You get real-time insight to help you prioritizing patching and understand which vulnerabilities to remediate first.

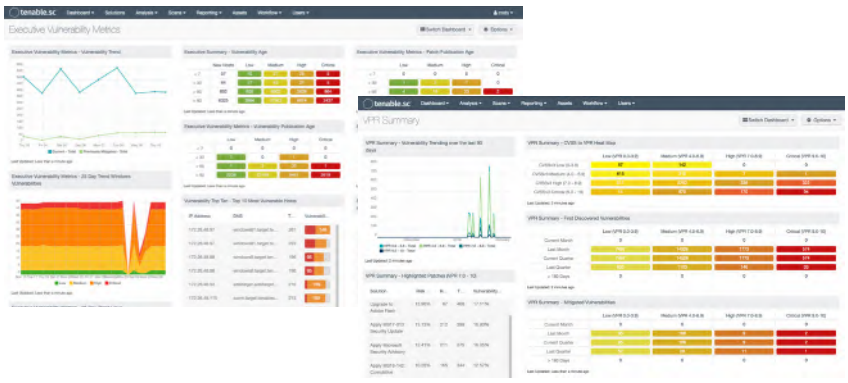

Figure 1: Highly customizable dashboards, reports, workflows and security policies to suit your specific business needs.

Key Benefits

- Identify weaknesses by scanning network connected assets for known vulnerabilities, misconfigurations and malware
- Prioritize vulnerabilities with the greatest impact and understand the likelihood a given vulnerability will be exploited in the next 28 days
- Focus on what matters most by quickly identifying what patches to prioritize for the biggest risk reduction.
- Rapidly respond to changes with configurable alerts, notifications and automated actions
- Streamline compliance for the widest range of regulatory/IT standards and best practices

Predictive Prioritization

Tenable.sc CV includes Predictive Prioritization, which combines data and threat intelligence across multiple sources, and analyzes them all with a data science algorithm that uses machine learning to anticipate the probability of a vulnerability being leveraged by threat actors. You get real-time insight to help you prioritize patching and understand which vulnerabilities to remediate first for the greatest risk reduction.

Tenable Research

Tenable.sc is back by Tenable Research, delivering world-class Cyber Exposure intelligence, data science insights, alerts and security advisories. Frequent updates from Tenable Research ensure the latest vulnerability checks, zero-day research, and configuration benchmarks are immediately available to help you secure your organization.

Key Features

Vulnerability Priority Rating: combines threat intelligence and machine learning to determine the likelihood a vulnerability will be exploited in your unique environment.

Lumin: Calculate and manage cyber risk across your organization, and see how you stack up against the competition with the Tenable.sc and Lumin integration.

Highly customizable dashboards/reports: HTML-5 based user interface satisfies the specific needs of CISOs, security management, analysts and practitioners/operators.

Broad asset coverage: assess servers, endpoints, network devices, operating systems, databases and applications in physical, virtual and cloud infrastructures.

Continuous asset discovery: discover all mobile devices, physical, virtual and cloud instances on the network, including unauthorized assets.

Dynamic asset classification: group assets based on policies that meet specific criteria: e.g., Windows 7 assets with vulnerabilities > 30 days old.

Tenable.sc Director Integration: Single-pane-of glass to manage and view your network across multiple consoles.

Vulnerability management: multiple scanning options, including passive network monitoring, non-credentialed and credentialed scanning for deep analysis and configuration auditing.

Agent-based scanning: available for organizations to more easily scan mobile and hard to reach assets.

Malware detection: leverage built-in threat intelligence feeds (malware indicators, blacklists) to identify advanced malware.

Assess network health: continuously monitor network traffic looking for suspicious traffic to/from vulnerable systems/ services, unknown devices, botnets, command/control servers.

Anomaly detection: use statistical and anomalous behavior analysis techniques on external log sources, to automatically discover activity that deviates from he baseline.

Advanced analytics/trending: provide contextual insight and actionable information to prioritize security issues associated with security posture of all enterprise assets.

Notification: configurable alerts for administrators to take manual actions via emails, notifications, trouble tickets or to take automated actions via APIs.

Streamlined compliance: pre-defined checks for industry standards and regulatory mandates, such as CERT, DISA STIG, DHS CDM, FISMA, PCI DSS, HIPAA/HITECH and more.

Integrations: use out-of-box integrations with patch management, mobile device management, threat intelligence and other third-party products, or use Tenable.sc APIs to develop custom integrations.

Tenable.sc Editions

tenable.sc™

Tenable.sc is a next-generation vulnerability analytics solution. Built on leading Nessus technology, you get a comprehensive view of your network so you can discover unknown assets and vulnerabilities, prioritize vulnerabilities and monitor network changes before they turn into a break.

tenable.sc™ Continuous View

Tenable.sc Continuous View is a market-leading vulnerability management platform. It integrates Tenable.sc with multiple Nessus Network Monitor sensors and network traffic and event monitoring to provide continuous monitoring and real-time asset discovery and vulnerability detection.

Capabilities	tenable.sc	tenable.sc Continuous View
Centralized vulnerability management with multiple scanners	●	●
Dynamic asset classification (mail server, web server, etc.)	●	●
Policy-based configuration auditing	●	●
Malware detection with built-in threat Intelligence	●	●
Pre-defined dashboards/reports with automatic feeds from Tenable	●	●
Incident response with configurable alerts, notifications, ticketing	●	●
Assurance Report Cards (ARCs)	●	●
Vulnerability Priority Rating (VPR)	●	●
Integration with Tenable.sc Director	●	●
Integration with Tenable Lumin	●	●
Continuous asset discovery (virtual, mobile, cloud)		●
Passive vulnerability detection of new and “unsafe-to-scan” assets		●
Real-time detection of botnet and command & control traffic		●
Anomaly detection using statistical/behavioral techniques		●
Streamlined compliance with proactive alerts on violations		●

For More Information: Please visit tenable.com
Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact