

# SecurityCenter

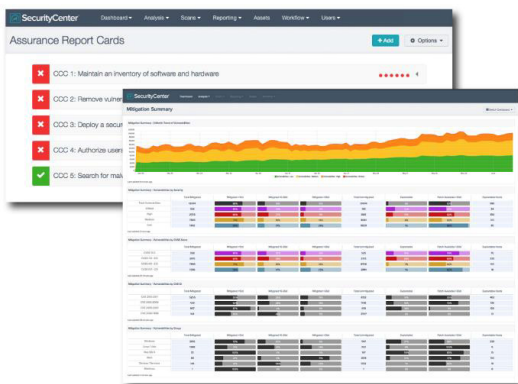
La plataforma de SecurityCenter brinda la perspectiva más integral y exhaustiva sobre la posición de seguridad empresarial para reducir los riesgos comerciales y garantizar la conformidad.

## Solución analítica de vulnerabilidades de última generación

SecurityCenter® es una solución analítica de vulnerabilidades integral que brinda visibilidad completa sobre la posición de seguridad y conformidad de su infraestructura de TI distribuida y compleja. SecurityCenter logra esto a través de análisis avanzados, paneles/informes personalizables y flujos de trabajo para identificar puntos débiles en sus activos de TI al detectar todas las vulnerabilidades, configuraciones incorrectas y malware.

El motor analítico de vulnerabilidades de SecurityCenter evalúa los datos de vulnerabilidad recopilados en diversos escáneres Nessus® distribuidos en su empresa, ilustra las tendencias de vulnerabilidad con el paso del tiempo y analiza los riesgos para priorizar las acciones que necesita tomar. Por último, SecurityCenter incluye un motor de flujos de trabajo configurable que ayuda a que su equipo de seguridad acelere las respuestas y correcciones para reducir los riesgos generales y simplificar la conformidad.

SecurityCenter incluye Assurance Report Cards® (ARC), que le permite medir, analizar y visualizar de forma continua la efectividad de su programa de seguridad, basado en los objetivos comerciales de alto nivel y en las políticas personalizables subyacentes que preocupan a los CISO y ejecutivos.



*SecurityCenter brinda análisis de vulnerabilidades, tendencias, informes y flujos de trabajo personalizables que satisfacen las necesidades de su programa de seguridad.*

## Beneficios clave

- Detecte los puntos débiles a través del escaneo de todos los activos en busca de vulnerabilidades, configuraciones incorrectas y malware
- Evalúe qué tan bien está funcionando la gestión de parches según las tendencias de vulnerabilidades con el paso del tiempo
- Responda a los cambios rápidamente con alertas configurables, notificaciones y acciones automatizadas
- Mida la posición de seguridad según las políticas de seguridad alineadas con objetivos comerciales de alto nivel
- Simplifique la conformidad para la más amplia gama de prácticas recomendadas y normativas/normas de TI
- Manténgase actualizado con el contenido proporcionado por Tenable™

## Investigación de Tenable

El equipo de investigación de Tenable proporciona actualizaciones frecuentes de información sobre amenazas y vulnerabilidades, análisis avanzados, políticas de seguridad/cumplimiento, paneles, informes y Assurance Report Cards a todos los clientes de SecurityCenter. Este contenido listo para usar está basado en las prácticas recomendadas de la industria y los clientes recopiladas por Tenable, lo que pone el poder de nuestro equipo de investigación de seguridad a su disposición. Este contenido es parte de la suscripción de SecurityCenter.

## Características clave

- **Assurance Report Cards:** mida de manera continua la efectividad de las políticas de seguridad definidas por los clientes según los objetivos comerciales de alto nivel para identificar y cerrar posibles brechas.
- **Paneles/informes altamente personalizables:** nueva interfaz de usuario basada en HTML5 para satisfacer las necesidades específicas de CISO, gestión de seguridad, analistas y profesionales médicos/operadores.
- **Amplia cobertura de activos:** evalúe servidores, terminales, dispositivos de red, sistemas operativos, bases de datos y aplicaciones en infraestructuras físicas, virtuales y en la nube.

- **Clasificación de activos dinámicos:** agrupe activos según las políticas que cumplen con determinados criterios: por ej., activos de Windows 7 con vulnerabilidades > 30 días de antigüedad.
- **Gestión de vulnerabilidades:** diversas opciones de escaneo, incluidos el escaneo con credenciales y sin credenciales, el escaneo para análisis profundo y la auditoría de configuración.
- **Escaneo basado en agentes:** disponible para que las organizaciones escaneen con mayor facilidad activos móviles y de difícil acceso.
- **Posición de seguridad administrada:** escanee hosts, dispositivos de seguridad, virtuales y móviles en busca de vulnerabilidades, configuraciones incorrectas y malware a través del uso de programaciones personalizables y ventanas de suspensión.
- **Resultados de escaneos cumulativos:** consolide datos de diversos escáneres Nessus en las instalaciones y proporcione información sobre tendencias de corrección.
- **Análisis/tendencias avanzadas:** proporcione información contextual y práctica para priorizar los problemas de seguridad asociados con la posición de seguridad de todos los activos empresariales.
- **Flujos de trabajo/respuesta a incidentes:** alertas y flujos de trabajo personalizables para que los administradores realicen acciones manuales a través de correos electrónicos, notificaciones, avisos de problemas, o para que realicen acciones automatizadas.
- **Modelo de gestión gradual:** respaldo para organizaciones que distribuyen responsabilidades en diversos lugares y equipos a través del control de acceso basado en funciones.
- **Equilibrio de carga automatizado:** optimice (paralelice) los ciclos de escaneo en entornos distribuidos.
- **Integraciones:** use integraciones listas para usar con gestión de parches, gestión de dispositivos móviles, información sobre amenazas y otros productos de terceros, o use las API de SecurityCenter para desarrollar integraciones personalizadas.
- **Conformidad simplificada:** verificaciones predefinidas para los estándares industriales y los mandatos normativos, como CERT, DISA STIG, DHS CDM, FISMA, SCADA, PCI DSS, HIPAA/HITECH y mucho más.

## Ediciones de SecurityCenter

### SecurityCenter

SecurityCenter es la solución analítica de vulnerabilidades de última generación que incluye diversos escáneres Nessus, el escáner de vulnerabilidades más ampliamente utilizado del mundo. Proporciona la visibilidad más integral sobre la posición de seguridad de su infraestructura de TI distribuida y compleja.

### SecurityCenter Continuous View®

SecurityCenter Continuous View es la plataforma de monitoreo de red continuo líder en el mercado. Integra SecurityCenter con diversos sensores de red Passive Vulnerability Scanner® (PVS™) y Log Correlation Engine® (LCE®) para proporcionar un monitoreo de red continuo e integral.

Capacidades	SecurityCenter	SecurityCenter CV™
Gestión de vulnerabilidades centralizada con diversos escáneres	✓	✓
Clasificación de activos dinámicos (servidor de correo, servidor web, etc.)	✓	✓
Auditoría de configuración basada en políticas	✓	✓
Detección de malware con información incorporada sobre amenazas	✓	✓
Paneles/informes predefinidos con fuentes automáticas de Tenable	✓	✓
Respuesta ante incidentes con alertas, notificaciones y avisos configurables	✓	✓
ARC (Assurance Report Cards)	✓	✓
Detección continua de activos (virtuales, móviles, en la nube)		✓
Detección pasiva de vulnerabilidades de activos nuevos y “no seguros de escanear”		✓
Detección en tiempo real de botnet y tráfico de control y comandos		✓
Detección de anomalías a través de técnicas estadísticas/conductuales		✓
Conformidad simplificada con alertas proactivas para infracciones		✓



Para obtener más información: Visite [tenable.com](https://tenable.com)  
 Contáctenos: Envíenos un correo electrónico a [sales@tenable.com](mailto:sales@tenable.com) o visite [tenable.com/contact](https://tenable.com/contact)

Copyright © 2017. Tenable Network Security, Inc. Todos los derechos reservados. Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View, Passive Vulnerability Scanner, Log Correlation Engine, LCE y Assurance Report Cards son marcas comerciales registradas de Tenable Network Security, Inc. Tenable, SecurityCenter CV y PVS son marcas comerciales de Tenable Network Security, Inc. Todos los demás productos o servicios son marcas comerciales de sus respectivos propietarios. EN-APR142017-V3