



#### Rápido repaso de sus principales características

- **Identificación de activos e inventariado de la tecnología**
- **Evaluación de vulnerabilidades**
- **Security Advisory Team global y 24 x 7**
- **Administración y registro de tareas**
- **Actualizaciones automatizadas del contenido y el código**
- **Integración con eTrust™ Security Command Center**

#### Qué hay de nuevo

- **Remediación mediante parches de seguridad**
- **Remediación mediante la configuración de seguridad**
- **Directivas de seguridad y procedimientos de fortalecimiento**
- **Evaluación del cumplimiento**
- **Generación de reportes definida por el usuario**
- **Roles y agrupamiento de los usuarios**
- **Clasificación y agrupación de activos**
- **Eficiencia en la administración de tareas**
- **Integración con Unicenter® Software Delivery**



## eTrust™ Vulnerability Manager r8

eTrust™ Vulnerability Manager r8 es una solución integrada, escalable y comprobada que ayuda a que las empresas administren las vulnerabilidades al combinar la evaluación de vulnerabilidades con la remediación mediante la configuración y los parches de seguridad en un dispositivo fácilmente montable. Utilizando un enfoque basado en activos e información de seguridad validada, eTrust Vulnerability Manager ayuda a proteger preventivamente su empresa antes que se vean comprometidos los sistemas.

### Desafíos para la administración de las vulnerabilidades

Las compañías públicas y privadas de todo el mundo están luchando por hacer frente al número cada vez mayor de incidentes de seguridad en sus entornos de TI. Los reportes muestran que esos eventos se están incrementando como resultado de una gran cantidad de vulnerabilidades nuevas. Los analistas y otros especialistas descubren que más del 90% del aumento de los incidentes es resultado directo de que las organizaciones no configuran o reparan apropiadamente sus sistemas.

Tradicionalmente, la implementación de una solución para resolver este desafío era cara y consumía demasiado tiempo, además de requerir inversiones en múltiples expertos y soluciones puntuales. Esencialmente, los administradores se ven agobiados, las configuraciones del sistema y las vulnerabilidades quedan al descubierto y los ejecutivos no tienen conciencia de los riesgos y los ataques ocurridos que causan interrupciones en los sistemas críticos del negocio. Las organizaciones de TI se ven forzadas a enfocarse en la administración de múltiples soluciones puntuales antes que en la de las vulnerabilidades.

La única forma efectiva de prevenir los incidentes de seguridad es identificar y remediar preventivamente las vulnerabilidades y las malas configuraciones, reparándolas antes de

que sean explotadas, los sistemas sean comprometidos y la empresa se vea afectada de forma negativa. Esto comienza con la implementación de una **solución** única y completa para la administración de las vulnerabilidades que lo ayuda a agilizar sus procesos.

### Subiendo el nivel con una solución para administración de las vulnerabilidades de clase corporativa

Computer Associates International, Inc. (CA) lo ayuda a superar estos desafíos al ofrecer eTrust Vulnerability Manager, una solución basada en un dispositivo que le permite mitigar el riesgo al realizar un inventario en tiempo real de los activos y correlacionarlo con conocimiento de seguridad validado. Los riesgos son identificados y mostrados en una lista de tareas prioritarias, a través de una interfaz basada en la Web, permitiéndole apuntar al riesgo de seguridad más importante, remediar el riesgo, verificar la remediación realizada y medir el progreso hacia la mitigación del riesgo.

eTrust Vulnerability Manager asegura la continuidad del negocio al administrar los sistemas vulnerables y mal configurados en tiempo real. Agiliza la administración del riesgo a través de la remediación mediante parches de seguridad y la configuración del sistema basada en el riesgo. Además, ayuda a reducir el costo y la complejidad de la identificación, administración y evaluación de los sistemas vulnerables a lo largo de su empresa.



A diferencia de otras soluciones para administración de las vulnerabilidades, eTrust Vulnerability Manager lo ayuda a comprender preventivamente qué activos posee en su entorno, junto con las exposiciones de esos activos. Explica cómo reparar las exposiciones y le permite hacerlo, y luego valida si han sido reparadas o no. Además, eTrust Vulnerability Manager le permite implementar un proceso uniforme para la administración de las vulnerabilidades desde la identificación hasta la validación.

### Características y funcionalidades distintivas

**Evaluación de las vulnerabilidades.** Las organizaciones luchan por identificar los sistemas vulnerables dentro de su infraestructura de red a través de métodos no intrusivos. El enfoque innovador y basado en activos de CA entrega una amplia visión de las vulnerabilidades en su entorno de TI.

- **Identificación de activos.** eTrust Vulnerability Manager brinda un método para identificar los activos dentro de su entorno a través de un escaneo no intrusivo de un rango de IP específico. El proceso de identificación reúne información importante acerca de los

activos encontrados dentro del rango de IP escaneado, como direcciones de IP, nombre del host y sistema operativo. Este proceso para identificación de activos nuevos dentro de su entorno puede ser ejecutado de forma circunstancial o planificadamente.

- **Inventario de activos.** eTrust Vulnerability Manager le permite realizar un inventario en tiempo real, identificando aquellas tecnologías que se ejecutan en sus activos a nivel del parche o la configuración del sistema. Más capacidades son provistas para agrupar los activos identificados, clasificar su riesgo y asignar los privilegios administrativos.
- **Correlación y priorización de vulnerabilidades.** eTrust Vulnerability Manager correlaciona automáticamente los datos del inventario de activos con una base de datos validada sobre vulnerabilidades, que cubre más de 15.000 versiones de tecnologías a lo largo de los sistemas operativos, las bases de datos, las aplicaciones y los dispositivos. Además, prioriza las vulnerabilidades identificadas basadas en el riesgo mediante una lista de tareas para cada activo. El detalle de tareas incluye las instrucciones posteriores, detalladas y manuales para la remediación, para los casos en que la entrega automatizada de parches y configuraciones del sistema no es factible (ver Figura 1).

Select All	State	Rank	Remediation	Type	Risk	CAID	Assets	Asset Groups
<input type="checkbox"/>	Open	48	WindowsServer2003-K893294-x86-ENU	Vendor Provided	Medaw	26496, 26702, 26796, 27328, ...	1	IT Services
<input type="checkbox"/>	Open	36	WindowsServer2003-K8928741-x86-ENU - Windows Server 2003 Standard Edition	Vendor Provided	Medaw	26342, 27899, 27901, 27902, ...	1	IT Services
<input type="checkbox"/>	Open	16	815495 - SQL Server 2000 SP3	Vendor Provided	High	25595	1	IT Services
<input type="checkbox"/>	Open	15	WindowsServer2003-K8429028-x86-ENU - Windows Server 2003 Standard Edition	Vendor Provided	High	27322	1	IT Services
<input type="checkbox"/>	Open	13	WindowsServer2003-K84303E2-x86-ENU - Windows Server 2003 Standard Edition	Vendor Provided	Medaw	37324	1	IT Services
<input type="checkbox"/>	Open	12	NDP1.3v1-K886746D-x86 - Net Framework 1.1	Vendor Provided	Medaw	31594	1	IT Services
<input type="checkbox"/>	Open	12	Windows XP SP1 - NetMeeting 3.01	Vendor Provided	Medaw	23238	1	IT Services
<input type="checkbox"/>	Open	11	WindowsFt (x86)K5019639-x86-DNL	Vendor Provided	Medaw	22085	1	IT Services
<input type="checkbox"/>	Open	11	818639	Vendor Provided	Medaw	32085	1	IT Services
<input type="checkbox"/>	Open	10	QQ41976	Vendor Provided	Medaw	23184	1	IT Services
<input type="checkbox"/>	Open	10	QQ44954	Vendor Provided	Medaw	26012	1	IT Services
<input type="checkbox"/>	Open	9	WindowsServer2003-K813643-x86-ENU	Vendor Provided	Medaw	28824	1	IT Services

Figura 1. Lista de tareas de la remediación



- **Verificación y registro de las tareas.**

Una vez que una vulnerabilidad haya sido mitigada por un activo, eTrust Vulnerability Manager brinda métodos para revisar la disposición del status de la tarea de la vulnerabilidad. Esto incluye notas administrativas apropiadas que permiten seguir el progreso y verificar la finalización del trabajo.

**Información sobre seguridad validada.**

El CA Security Advisory Team investiga y valida las vulnerabilidades y configuraciones del sistema a través de un proceso de investigación pendiente de patente, que brinda soporte para la administración preventiva del riesgo. Además, el proceso de investigación y validación de CA remueve de raíz los falsos positivos, permitiendo que sus administradores se enfoquen únicamente en los riesgos reales para su entorno.

- **Equipo de investigación global.**

eTrust Vulnerability Manager le brinda acceso a un equipo de investigación global 24x7, que integra y valida las amenazas a la seguridad y sus soluciones. El CA Security Advisory Team está comprometido en entregar rápidamente información sobre seguridad validada y firmas para tecnologías prioritarias dentro de las 72 horas de su identificación pública.

- **Actualizaciones automatizadas del contenido y los códigos.**

eTrust Vulnerability Manager proporciona actualizaciones automáticas del contenido sobre seguridad producido por el CA Security Advisory Team. Las actualizaciones del contenido pueden ser planificadas para una entrega por hora o diaria. Además, brinda descarga automática de códigos poniendo en práctica las últimas mejoras del código que son aplicadas a eTrust Vulnerability Manager durante la ventana de mantenimiento definido por el usuario, creando mantenimiento del software sin intervención.

**Integración con las soluciones**

**eTrust™.** eTrust Vulnerability Manager le permite administrar las amenazas a través de la correlación de datos con las

herramientas para administración de la información sobre seguridad.

- **eTrust™ Security Command Center.**

Permite visualizar los reportes y datos de eTrust Vulnerability Manager en combinación con otros productos, eventos y procesos de seguridad, a través de la consola de eTrust Security Command Center, brindando una visión única e integrada de los datos de seguridad dispares. Además, eTrust Security Command Center entrega notificaciones sobre eventos desde eTrust Vulnerability Manager y correlaciona esta información con los incidentes de seguridad identificados por otros dispositivos en tiempo real. Al correlacionar los riesgos de seguridad con los activos, usted puede tomar acciones correctivas e investigar los incidentes de seguridad a través de un centro de comando y control centralizado.

**Qué hay de nuevo en r8**

**Remediación mediante parches de seguridad.**

La mayoría de los incidentes de seguridad ocurren como resultado de activos que no han sido empatchados apropiadamente. eTrust Vulnerability Manager brinda métodos para automatiza este proceso, reduciendo sus costos administrativos y la exposición al riesgo.

- **Reparación automatizada mediante parches.**

eTrust Vulnerability Manager le permite implementar la reparación mediante parches de seguridad a través de una consola común en un activo o grupo de activos.

- **Procedimientos de prueba y distribución.**

eTrust Vulnerability Manager le permite implementar las remediaciones mediante parches en un entorno de prueba, ayudando a minimizar el potencial de interrupción del sistema de producción y brindar soporte para las políticas de administración del cambio.

**Planificación preventiva de la configuración del sistema.**

Algunas organizaciones se esfuerzan por definir las mejores prácticas para asegurar o fortalecer los activos. eTrust Vulnerability Manager brinda el contenido y la funcionalidad para complementar las políticas organizativas para reducir las exposiciones relacionadas con la configuración, un componente que a menudo es dejado de lado cuando se atienden las vulnerabilidades.

- **Directivas y procedimientos de fortalecimiento.**

eTrust Vulnerability Manager brinda las directivas de configuración de las



Mejores Prácticas para las tecnologías críticas para la empresa de proveedores tales como Microsoft, HP y Cisco. Usted puede configurar y fortalecer apropiadamente sus activos utilizando tanto los conjuntos de estándares de las Mejores Prácticas como sus propios conjuntos personalizados de estándares para la configuración. Además, usted puede asociar los conjuntos de estándares con los grupos de activos, ayudando a asegurar una configuración consistente de los activos en toda la empresa.

- **Revisión del cumplimiento.** eTrust Vulnerability Manager brinda el mecanismo para que su organización mida un activo contra el conjunto asignado de Estándares de Configuración para una indicación del progreso hacia el cumplimiento.
- **Remediación automatizada de la configuración.** eTrust Vulnerability Manager le permite implementar las remediaciones de la configuración del sistema relacionada con la seguridad sobre un activo o una base de grupo de activos de forma circunstancial o planificada.

- **Procedimiento de prueba y distribución.** Así como con la remediación mediante parches, eTrust Vulnerability Manager lo ayuda a implementar las remediaciones de la configuración en un entorno de prueba antes de que puedan ser implementadas en una población productiva mayor.

**Capacidades de administración.** eTrust Vulnerability Manager r8 ofrece mejoras administrativas adicionales para ayudarlo a administrar fácilmente los activos y administrar sus riesgos.

- **Clasificación y agrupamiento de activos.** eTrust Vulnerability Manager le permite agrupar activos, que pueden ser definidos automáticamente según los diversos parámetros de activos. Además, cada grupo de activos puede tener asignado una categoría de protección para ayudar a establecer el estado empresarial de urgencia de los activos.
- **Roles y permisos del usuario.** eTrust Vulnerability Manager ahora ofrece diversos roles predefinidos para ayudarlo a administrar la gama de funcionalidades a la cual tienen acceso los usuarios. Cada usuario también puede ser asignado a un grupo de activos específico, otorgándole acceso a los activos que administra.

eTrust™ Vulnerability Manager																	
VULNERABILITIES TOTAL OPEN AND CLOSED REPORT																	
To print this report, select File > Print.																	
Report Date: 8/19/04 11:30:00 AM																	
Asset	Asset Risk			Vulnerability Status Totals				Vulnerability Risk Statistics									
	Vulns	Risk	Average	Total	Open	%	Closed	%	High			Medium			Low		
Asset	Accept	Open	Average	Total	Open	%	Closed	%	Total	Open	Closed	Total	Open	Closed	Total	Open	Closed
LHW2K301	0.0	5.7	5.7	261	141	54.0	120	46.0	40	6	34	216	130	86	5	5	0
LHWXPD03	6.2	5.7	5.7	382	158	41.4	224	58.6	57	8	49	318	143	175	7	7	0
LHNSO14	0.0	5.8	5.8	258	147	57.0	111	43.0	38	7	31	215	135	80	5	5	0
LHRAS04	0.0	5.7	5.7	284	188	66.2	96	33.8	39	7	32	238	174	64	7	7	0

Copyright © 2004 Computer Associates International, Inc. All rights reserved.  
 Browser requirements are Internet Explorer 6.0 and higher or Mozilla 1.4 and higher.

Figura 2. Reporte total abierto/cerrado sobre vulnerabilidades



- **Actualizaciones globales.** eTrust Vulnerability Manager le permite realizar un único cambio administrativo en múltiples perfiles de activos, como el cambio de la designación del agrupamiento de activos o la eliminación de un grupo de activos. El dispositivo también le permite definir un status global para una vulnerabilidad específica en toda su organización. Además, sus administradores de sistema pueden cerrar tareas en múltiples grupos de activos, mejorando la performance de la rutina diaria.
- **Inventario automático según demanda.** Cuando utilizan la funcionalidad de inventario automático, sus administradores ahora tienen la opción de administrar los activos según demanda. Haciendo un click, se reingresa a inventarios por activos agrupados, brindando una actualización inmediata del riesgo de los activos.

**Generación de reportes.** eTrust Vulnerability Manager lo ayuda a comprender su postura de seguridad al verificar y medir los riesgos. Además, incluye los esfuerzos de mitigación y el cumplimiento en todo su entorno.

- **Generación de reportes en toda la empresa.** eTrust Vulnerability Manager brinda reportes en tiempo real sobre las exposiciones al riesgo en toda la empresa y avanza hacia la mitigación del riesgo (ver Figura 2).
- **Los 10 reportes principales.** eTrust Vulnerability Manager reporta sobre los 10 activos de riesgo más importantes según la categoría de protección.

- **Cumplimiento con los estándares y regulaciones de la industria.** eTrust Vulnerability Manager mide el cumplimiento de los valores de la configuración del sistema de sus activos respecto de los requerimientos regulatorios Gramm-Leach-Bliley Act (GLBA) y Health Insurance Portability and Accountability Act (HIPAA), junto con la ISO 17799 o los 20 estándares SANS más importantes de la industria según activo o base de grupo de activos.
- **Búsqueda ad-hoc.** eTrust Vulnerability Manager le permite crear búsquedas definidas por el usuario a través de un wizard de búsqueda fácil de usar, que puede exportar los resultados de los datos.

**Integración con Unicenter®.** La integración con las soluciones para administración de la infraestructura permiten que eTrust Vulnerability Manager se vincule con los procesos de administración del cambio en su organización.

- **Unicenter® Software Delivery.** Esta solución única brinda integración uniforme, permitiéndole aprovechar la infraestructura de Unicenter Software Delivery existente para implementar las remediaciones desde la interfaz basada en la Web de eTrust Vulnerability Manager.

**Para mayor información, visite [www.ca.com](http://www.ca.com)**



Computer Associates®