



Computer Associates®

White Paper

Administración de la Seguridad: un nuevo modelo para alinear la seguridad con las necesidades de la empresa

Susan Read-Miller

Mayo de 2004

Introducción

Su organización enfrenta desafíos significativos para la seguridad en el mundo actual, donde proteger los datos empresariales vitales puede ser costoso y desalentar la propuesta. Por ejemplo, usted debe atender preventivamente las preocupaciones sobre seguridad que impactan en las aplicaciones, bases de datos y otros activos empresariales esenciales para las operaciones diarias. Debe convertir los datos de seguridad sin procesar en información empresarial procesable. Usted debe cumplir con regulaciones, tales como aquellas dictadas por el gobierno, Health Insurance Portability and Accountability Act (HIPAA), Sarbanes–Oxley Act, Basel II y SafeHarbor. Aún más, debe asegurar operaciones empresariales continuas mediante la mitigación del riesgo, virtualmente, en cada nivel de su organización, mientras mantiene los presupuestos y alcanza una eficiencia operativa.

Atender estos desafíos requiere un nuevo modo de ver; un nuevo modelo para administración de la seguridad que integre los elementos dispares que protegen sus activos empresariales dentro de una solución única, completa y fácilmente administrable. El nuevo modelo para administración de la seguridad alinea la seguridad con las necesidades de la empresa al integrar tres componentes críticos en el entorno de seguridad: la administración de la identidad y el acceso del usuario, la administración de las amenazas y la administración de la información sobre seguridad. Cada componente debe ser abierto, flexible y fácilmente integrable con los demás, así como con las soluciones de terceros. Finalmente, la administración de la seguridad requiere un enfoque preventivo y respuestas según demanda a los eventos dentro del cambiante entorno de seguridad.

Cuando está implementada apropiadamente, la administración integrada de la seguridad le permite comprender su entorno de seguridad en toda su complejidad, convirtiendo los datos de seguridad en información procesable, obteniendo respuestas oportunas a las preguntas críticas y, según esas respuestas, tomando medidas preventivas y agresivas para proteger los activos y la información en toda su empresa –cualquiera sea su modelo empresarial o estructura organizativa-. Una amplia solución para administración de la seguridad ofrece múltiples beneficios, incluyendo costos reducidos, menor tiempo de inactividad, mayor productividad y cumplimiento de las regulaciones. Le permite tomar las decisiones acertadas en el momento justo. Además, preventiva o real, la administración de la seguridad mejora su postura global de seguridad e incrementa su eficiencia y efectividad.

Los componentes claves de la seguridad administrada

La seguridad es un componente significativo de las infraestructuras empresariales actuales. En un entorno informático dinámico, donde la reconfiguración e implementación del sistema son hechos permanentes, es fundamental asegurar:

- La protección de los activos críticos contra códigos maliciosos, tales como virus y worms
- La mitigación preventiva del riesgo al reducir las vulnerabilidades
- La implementación de políticas de seguridad
- El aprovisionamiento y mantenimiento automatizado de las identidades digitales
- El acceso conveniente y seguro a las aplicaciones por todos los usuarios
- Soluciones integradas, con control centralizado de la infraestructura extendida de seguridad
- El cumplimiento de las regulaciones

El nuevo modelo de soluciones para administración de la seguridad según demanda entrega la flexibilidad necesaria para alinear cada aspecto de las cuestiones de seguridad de su organización con sus necesidades empresariales al automatizar, simplificar y agilizar los procesos. Además, proporciona visibilidad en tiempo real para una multitud de eventos de seguridad que ocurren diariamente en su entorno empresarial, permitiendo la respuesta adecuada en el momento justo.

La integración de los tres componentes claves de la administración de la seguridad –administración de la identidad y el acceso del usuario, de las amenazas, y de la información sobre seguridad- en una solución preventiva lo ayuda a alcanzar la eficiencia operativa y el cumplimiento de las regulaciones, así como también contener los costos, mitigar el riesgo y asegurar operaciones empresariales continuas.

Administración de la Identidad y el Acceso

En la mayoría de las compañías, las identidades y los privilegios de acceso de los usuarios son las funciones centrales en la conducción de la empresa. Detrás de esas identidades están los empleados, contratistas, partners, inversores, etc., que conducen cada aspecto de las operaciones. La administración de la identidad determina quién tiene acceso a determinadas intranets, aplicaciones, bases de datos y plataformas, y permite funciones básicas como el e-mail. Las preguntas claves que deben ser respondidas por el componente de identidad y acceso de la administración de la seguridad son:

- ¿Quiénes tienen acceso a qué?
- ¿Qué pueden hacer?
- ¿Cuándo pueden hacerlo?

Al responder estas preguntas, usted puede alinear efectivamente la seguridad con las metas empresariales, proteger activos empresariales vitales, agilizar las operaciones de negocios y alcanzar el cumplimiento de las regulaciones.

Hasta ahora, la identidad y el acceso del usuario han sido tratados como entidades separadas cuando, de hecho, están estrechamente relacionadas y deberían ser consideradas como un todo. El nuevo modelo para administración de la seguridad integra estas dos funciones, permitiendo la comunicación y el acceso apropiado según la identidad, sin crear vulnerabilidades. Además, barre con los usuarios no autorizados desde la red mientras otorga a los usuarios autorizados acceso a la información necesaria para realizar sus tareas y mantener la compañía operando.

Las capacidades claves, que deben ser combinadas para una administración exitosa de la identidad y el acceso, son:

- **Aprovisionamiento**, que automatiza la configuración requerida para establecer un usuario nuevo, permitiéndole tener nuevos usuarios online y productivos en un día. Aún más importante, un aprovisionamiento bien implementado permite que sus administradores manejen todo el ciclo de vida de una identidad, incluyendo cambios y eliminación de roles una vez que el usuario ya no está autorizado.
- **Ejecución**, que ayuda a asegurar que su organización mantenga la integridad de su información al prevenir el acceso sin autorización. Esto le permite tener control granular sobre quién accede a qué recursos, y dónde están ubicados.
- **Auditoría**, que facilita el seguimiento y la generación de reportes sobre el acceso requeridos para cumplir con las regulaciones y, si fuera necesario, realizar un análisis forense luego de los eventos. Esto lo ayudará a determinar dónde se originan las amenazas y prevenir ataques adicionales

La administración firme de la identidad y el acceso proporciona una base para la administración de la seguridad al atender las exposiciones del sistema relacionadas con la identidad, ejecutar políticas consistentes de seguridad en toda la empresa y delegar la facultad administrativa de acceso. Ayuda a reducir los costos administrativos a través de controles de acceso basados en roles, auditoría integrada y administración automatizada. Cuando se implementa de forma apropiada, también entrega el mejor valor empresarial para un rápido retorno de la inversión (ROI), seguridad mejorada, productividad incrementada y costos reducidos.

Administración de las Amenazas

Dentro del entorno tradicional de seguridad, las empresas dependen de una multitud de soluciones puntuales diferentes para prevenir la infiltración en sus redes por parte de virus, worms, spam y contenido malicioso, así como también para asegurar que los datos empresariales y la información privada no se vean comprometidos. El problema crece cuando una amenaza conocida evade estos detectores y se convierte en un evento de seguridad, algunas veces, de proporciones catastróficas. En el peor de los casos, las operaciones empresariales diarias se interrumpen, disparando grandes pérdidas. La información empresarial sensible o vital puede ser comprometida o destruida. Este caos total continúa hasta que se encuentra y aplica el parche adecuado.

Un entorno con administración preventiva de las amenazas detiene estos sucesos catastróficos de las siguientes maneras:

- Detecta intrusiones, filtra el contenido y detiene los worms y virus
- Eleva la administración de las amenazas hacia un nivel mayor al atender las amenazas y vulnerabilidades potenciales antes de que impacten negativamente en su sistema
- Identifica las vulnerabilidades conocidas dentro sus sistemas antes de que ocurran los ataques
- Entrega remediación automatizada con parches para proporcionar una protección rápida, removiendo las amenazas sin afectar el tiempo de su administrador de red
- Bloquea el spam mientras permite los e-mails auténticos

La implementación de la administración preventiva de las amenazas también atiende otras preocupaciones corporativas, tales como el contenido y uso inapropiado. Ayuda a asegurar que la información que sale y entra en su red sea la adecuada, y bloquea el acceso a sitios web donde el contenido no es el apropiado o no está relacionado con la empresa. La administración preventiva de las amenazas ofrece una mayor seguridad, incrementa la productividad y es mucho más rentable que la respuesta reactiva que se dispara una vez que los recursos han sido comprometidos.

Administración de la Información sobre Seguridad

La administración de la información sobre seguridad es un área emergente de la administración de la seguridad que se ha hecho necesaria debido al embate de datos de seguridad generados por sistemas de seguridad física y de TI, plataformas y aplicaciones dispares. Cada una de estas entidades genera información de forma diferente, la presenta en formatos distintos, la almacena en lugares diferentes y la reporta en

ubicaciones que no son las mismas. Este flujo incesante de datos – literalmente, millones de mensajes por día- desde tecnologías de seguridad incompatibles abruma la infraestructura de seguridad, lo que resulta en una sobrecarga de información sobre seguridad e impacta negativamente en las operaciones empresariales. Sin forma de administrar e integrar la información, este enfoque fragmentado, a menudo, conduce a una duplicación del esfuerzo, costos administrativos elevados, modelos de seguridad débiles y auditorías fallidas.

Tradicionalmente, las herramientas para administración de la información sobre seguridad utilizan reglas de correlación, visualización y análisis forenses avanzados para transformar los datos de seguridad sin procesar en información empresarial procesable, facilitando la administración de eventos en tiempo real o la investigación posterior a los eventos. Permiten que su personal de seguridad y de TI visualice la actividad de la red y determine de qué manera los activos empresariales son afectados por los exploits de red, el robo de datos internos o las violaciones de las políticas de seguridad o HR; además, proporcionan los seguimientos de auditorías necesarios para el cumplimiento de las regulaciones.

Las soluciones para administración de la información sobre seguridad también reducen, agregan, correlacionan y priorizan los diversos datos de seguridad desde múltiples dispositivos de seguridad y tecnologías de software, integrando sus entornos de seguridad física y de TI. Las herramientas para administración de la información sobre seguridad se integran, de forma ideal, con la mayoría de sus aplicaciones basadas en la empresa, incluyendo contaduría, planilla de sueldos, HR y fabricación, proporcionando administración de la seguridad y los eventos para estos sistemas vitales. Finalmente, estas herramientas permiten que su organización administre todos estos datos –cualquiera sea su fuente- desde una ubicación única y centralizada, poniendo el caos en orden.

La administración de la información sobre seguridad también debe integrarse con la administración de la red y los sistemas. Tradicionalmente, estas dos administraciones basaron sus operaciones en dos supuestos distintos y aparentemente contradictorios. El equipo de administración de la red y los sistemas se enfoca en los procesos y la continuidad de la empresa, asumiendo que el perímetro mantendrá a los “chicos malos” fuera. Por el contrario, el equipo de seguridad da por hecho que los “chicos malos” están alrededor del perímetro, demandando –y, algunas veces, obteniendo- acceso. Esta situación se agrava por el hecho de que los requerimientos empresariales, tales como el cumplimiento de las regulaciones, raramente dividen las responsabilidades o los requisitos entre las

áreas apropiadas; ya que la mayoría de los reguladores no se interesa por las diferentes partes, usted necesita asegurar que la totalidad del proceso sea administrado. Poner el caos en orden requiere tres funciones críticas:

- **Tiempo real:** ayuda a asegurar la continuidad empresarial al responder según demanda a las amenazas y vulnerabilidades
- **Perspectiva:** emplea análisis forenses para determinar lo que ha ocurrido y localizar tendencias dañinas potenciales
- **Comunicaciones:** reduce la masa voluminosa de datos de seguridad a información empresarial procesable, suministrando solo lo que es necesario para el sistema de administración de la red y los sistemas

Cuando se implementa de forma apropiada, la administración de la información sobre seguridad entrega una solución para la seguridad de la empresa que ayuda a reducir el costo y la complejidad de la administración de los eventos, incrementa la eficiencia administrativa, asegura el cumplimiento de las regulaciones y mejora la postura global de seguridad de su compañía.

Soluciones de CA para la administración de la seguridad

La administración de la seguridad es una parte fundamental de cualquier estrategia global de administración. No obstante, la seguridad no existe aisladamente. Para asegurar la continuidad empresarial y conectarse con los procesos globales de negocios de su empresa, la seguridad debe integrarse de manera uniforme con su infraestructura de administración.

Durante más de 28 años, Computer Associates International, Inc. (CA) ha entregado una amplia gama de soluciones de talla mundial para administración que fortalecen todos los aspectos de la administración de los procesos empresariales, la información y la infraestructura de su organización. A través de una integración uniforme y un enfoque abierto y basado en estándares, el software de CA para administración ofrece capacidades reales de administración y beneficios considerables que devienen en un enfoque amplio.

Las soluciones eTrust™ Security Management de CA, diseñadas tanto para proteger como para hacer posible su negocio, aplican esta experiencia al problema de la administración de la seguridad. Estas soluciones según demanda administran preventivamente las complejidades de un entorno de seguridad al atender los eventos desde su identificación hasta su resolución, asegurando operaciones empresariales continuas y entregando la eficiencia operativa que solo puede ser proporcionada a través de una solución completa e integrada.

Las soluciones eTrust atienden los requerimientos del nuevo modelo de administración de la seguridad al proporcionar un paquete completo e integrado de manera uniforme para este tipo de administración. Le dice quién tiene acceso a qué, determina qué ocurre en su entorno y asegura que usted tome las decisiones adecuadas en el momento justo. Además, las soluciones eTrust de CA ponen en orden el caos de la sobrecarga de información sobre seguridad, permitiéndole enfocarse en su empresa.

Visión general del producto eTrust

eTrust™ Identity and Access Management

CA lleva la delantera en la industria al integrar estas funciones estrechamente relacionadas, ofreciendo capacidad de aprovisionamiento, ejecución y auditoría para administrar efectivamente sus usuarios y su acceso. Algunas de las soluciones de eTrust Identity and Access Management son:

- **eTrust™ Access Control:** ofrece una política de acceso consistentemente fuerte para sistemas operativos y plataformas distribuidas. Esta solución proporciona control basado en políticas sobre: quiénes tiene acceso a sistemas, aplicaciones y archivos específicos; qué pueden hacer dentro de ellos, y cuándo les fue permitido acceder.
- **eTrust™ Admin:** brinda soporte para el aprovisionamiento automatizado de los recursos de la TI y de los que no pertenecen a esta, el restablecimiento de la password de autoservicio del usuario y la sincronización de la password para el entorno según demanda. Esta solución de clase corporativa implementa las políticas de seguridad y proporciona conexión y generación end-to-end de reportes para una responsabilidad máxima. Incluye un motor de flujo de trabajo y administración incorporada de roles así como la integración con cualquier directorio de Lightweight Directory Access Protocol (LDAP), además de una interfaz abierta para sistemas HR y de autenticación.
- **eTrust™ CA-ACF2® Security y eTrust™ CA-Top Secret® Security:** permite aprovechar la confiabilidad, escalabilidad y rentabilidad del mainframe al proporcionar seguridad de borde frontal para entornos empresariales de transacción z/OS, z/VM y VSE, incluyendo z/OS UNIX y Linux for zSeries. Las amplias herramientas administrativas y para generación de reportes incorporadas, junto con el registro detallado de eventos, simplifican la administración de los derechos de acceso del usuario. Estos productos le dan las herramientas para monitorear la eficiencia de sus políticas de seguridad. Además, brinda seguridad end-to-end cuando se implementa con otras soluciones eTrust.



Las soluciones eTrust Security Management se basan en un enfoque basado en activos que asegura su empresa al conceder el acceso apropiado para los activos, proteger los mismos contra amenazas y reunir información de esos activos así como también de otras soluciones de seguridad, otorgándole un control completo sobre la seguridad.

eTrust™ Threat Management

Las soluciones eTrust Threat Management de CA incorporan tecnologías que previenen que virus, spam y contenido malicioso se infiltren e infecten su e-mail y sus aplicaciones empresariales. Permiten que su personal de seguridad identifique una amenaza o debilidad en su infraestructura y tome medidas inmediatas, previniendo los incidentes antes de que impacten su organización. Las soluciones eTrust Threat Management también confrontan los desafíos para seguridad del contenido, manteniendo la confidencialidad del contenido corporativo y poniendo el contenido malicioso en un aprieto al permitir la creación, implementación y monitoreo de las políticas de uso a través de los canales de comunicaciones de Internet. Combinadas con la identificación y la remediación automatizada de las debilidades en la seguridad, las soluciones eTrust Threat Management mitigan el riesgo a medida que reducen el costo total de propiedad y de las operaciones de seguridad.

Cinco soluciones en este área requieren una atención particular:

- **eTrust™ Antivirus:** proporciona protección de clase corporativa contra, virtualmente, todas las formas de ataques costosos de virus, desde el perímetro hasta el PDA. Una consola única de administración simplifica la administración de entornos corporativos heterogéneos; proporciona métodos simple de implementación, administración y actualización de firmas, y protege su empresa de virus y códigos maliciosos antes de que ingresen a su red.

- **eTrust™ CA-Examine® Auditing:** realiza una revisión y auditoría automatizada de la integridad y la verificación del sistema operativo z/OS. Además, eTrust CA-Examine Auditing proporciona información importante sobre los mecanismos de seguridad, integridad y control del sistema, que son extremadamente difíciles de obtener desde otras fuentes.
- **eTrust™ EZ Armor™:** entrega un firewall personal, amplia protección antivirus y defensa contra programas adjuntos en e-mails potencialmente destructivos, otorgándole una seguridad lista para usar contra una amplia gama de amenazas de Internet. Esta solución fácil de usar, y otras ofrecidas por **my-eTrust.com** simplifican la complicada tarea de proteger la privacidad individual, y salvaguardar sus computadoras personales y de oficina de las amenazas actuales a la seguridad.
- **eTrust™ Secure Content Manager:** ofrece una solución para administración de la seguridad del contenido completa y escalable que incluye seguridad del contenido web y de e-mail, filtrado antispam y de URL, amplia protección antivirus, monitoreo de la confidencialidad de los datos y defensa contra código malicioso. eTrust Secure Content Manager también ofrece capacidades de autoadministración del usuario y permite la administración común de las políticas de seguridad a lo largo de todos los puntos potenciales de exposición.
- **eTrust™ Vulnerability Manager:** protege preventivamente sus activos de TI contra ataques externos y amenazas internas a la seguridad al correlacionar los datos exclusivos sobre vulnerabilidades con sus activos. eTrust Vulnerability Manager ofrece evaluación de las vulnerabilidades, remediación por parche y configuración y análisis del cumplimiento a través de una interfaz de usuario basada en la Web y un dispositivo fácilmente desplegable.

eTrust™ Security Information Management

Las soluciones eTrust Security Information Management de CA aseguran que su organización controle su infraestructura de seguridad en lugar de ser controlada por ella. El control centralizado ayuda a mejorar la eficiencia del administrador y reducir los costos, mientras que la integración y la automatización mejora la efectividad y la seguridad. Además, la visualización y los análisis forenses avanzados de los datos físicos y de TI transforman los datos de seguridad sin procesar en información empresarial procesable. Aún más, estas herramientas aseguran operaciones empresariales continuas y proporcionan las visiones de seguridad requeridas para alcanzar el

cumplimiento de las regulaciones. Las soluciones eTrust Security Information Management incluyen:

- **eTrust™ Security Command Center:** ofrece una solución completa para monitorear y administrar todos los aspectos de su seguridad corporativa desde una consola de administración centralizada. eTrust Security Command Center le permite reunir, correlacionar, analizar y priorizar fácilmente los datos y tomar medidas correctivas inmediatas. Usted puede potenciar capacidades de visión basadas en roles, flexibles y personalizadas de forma única para visualizar los recursos que son relevantes para una función empresarial o de seguridad específica. Además, eTrust Security Command Center proporciona reportes avanzados de auditoría que le ayudan a atender los requerimientos de cumplimiento de las regulaciones.
- **eTrust™ 20/20™:** cierra la brecha entre el monitoreo de la seguridad física y de TI. Esta solución única recolecta y correlaciona los datos relacionados con la seguridad en toda su empresa, analizándolos y mostrándolos en una interfaz intuitiva. Esta capacidad permite que su organización detecte rápida y automáticamente los comportamientos sospechosos y establezca las responsabilidades en caso de un incidente de seguridad.
- **eTrust™ Network Forensics:** captura los datos de red sin procesar y utiliza análisis forenses avanzados para identificar cómo son afectados sus activos empresariales por los exploits de red, el robo de datos internos y las violaciones a la política de seguridad o HR. Su tecnología patentada permite que su personal de seguridad y de TI visualice la actividad de la red, descubra el tráfico anormal e investigue las brechas con una solución única y conveniente.

Conclusión

La continuidad empresarial, el cumplimiento de las regulaciones, la mitigación real del riesgo, la optimización de los activos de seguridad existentes y la eficiencia operativa son fáciles de alcanzar si usted emplea el nuevo modelo para administración de la seguridad. Para determinar su capacidad de administración de la seguridad, realice las siguientes preguntas:

Administración de la Identidad y el Acceso

- ¿Puede determinar quiénes acceden a qué, qué es lo que hacen y cuándo lo hacen?
- ¿Puede aprovisionar inmediatamente a los empleados cuando cambian sus roles?
- ¿Sus empleados son desaprovechados totalmente cuando finalizan sus empleos?

Administración de las Amenazas

- ¿El último ataque de worm o virus ha afectado sus activos críticos?
- ¿Puede iniciar las acciones apropiadas según la información que ingresa de su firewall, las soluciones antivirus y otros dispositivos de seguridad?
- ¿Sus parches han sido implementados apropiadamente?
- ¿Sus empleados utilizan el ancho de banda de Internet para propósitos no relacionados con la empresa?

Administración de la Información sobre Seguridad

- ¿Puede transformar los datos de seguridad sin procesar en información empresarial procesable?
- ¿Puede proporcionar los seguimientos de auditorías necesarios para el cumplimiento de las regulaciones?
- ¿Posee un control centralizado y una comprensión de sus dispositivos y datos de seguridad?

Al obtener control de su entorno a través de las soluciones uniformemente integradas para administración de la seguridad, usted puede alinear de manera efectiva la seguridad con sus necesidades empresariales.

Para mayor información sobre las soluciones eTrust Security Management, visite ca.com/etrust



Computer Associates®