White Paper

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

Sumner Blount, Soluciones de Seguridad de CA
Agosto de 2006

Contenido

Introducción

Hoy en día, su organización enfrenta desafíos significativos para la seguridad, donde proteger los datos de negocio vitales puede ser costoso y desalentar la propuesta. Por ejemplo, usted debe atender proactivamente las preocupaciones de seguridad que impactan en las aplicaciones, bases de datos y otros activos de negocio esenciales para las operaciones diarias; convertir los datos de seguridad sin procesar en información empresarial procesable y cumplir con regulaciones gubernamentales e industriales, tales como Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act, Basel II y Gramm-Leach-Bliley Act (GLBA). Aún más, debe asegurar operaciones de negocio continuas al mitigar el riesgo, virtualmente, en cada nivel de su organización, mientras mantiene los presupuestos y alcanza la eficiencia operativa.

Atender estos desafíos requiere una nueva perspectiva; un nuevo modelo para administración de la seguridad que integre los elementos dispares que protegen sus activos de negocio dentro de una solución completa y fácilmente administrable. Este nuevo modelo 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, la administración de las amenazas y la administración de la información de 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 proactivo y respuestas según demanda a los eventos dentro del dinámico entorno de seguridad.

Cuando está implementada apropiadamente, la administración integrada de la seguridad le permite comprender su entorno de seguridad en toda su complejidad, convertir los datos de seguridad en información procesable, obtener respuestas oportunas a las preguntas críticas sobre su entorno de TI y, según esas respuestas, tomar medidas proactivas y agresivas para proteger los activos y la información en toda su empresa. Una amplia solución para administración de la seguridad ofrece múltiples beneficios, incluyendo costos reducidos, menor tiempo de inactividad, menor riesgo de TI, mayor productividad y cumplimiento de las regulaciones. Además, preventiva o real, la administración de la seguridad mejora su postura global de seguridad e incrementa su eficiencia y efectividad.

Administración Integrada de TI

Para que las organizaciones de TI puedan resolver los desafíos relacionados con la TI, es necesario adoptar un enfoque integral que involucre a las personas, procesos y tecnología. La Administración Integrada de TI es la visión de CA para unificar y simplificar la administración y la seguridad de TI, brindando soporte al negocio.

Esta visión requiere que todas las funciones de administración de TI trabajen juntas para atender las necesidades del negocio. El foco de la Administración Integrada de TI es administrar y proteger todos los aspectos del entorno de TI, desde los activos y usuarios hasta los entornos de aplicación que los reúnen y, finalmente, los servicios de TI utilizados por la empresa. Al administrar la TI de forma integrada, las organizaciones pueden unificar y simplificar la TI para que sea continuamente optimizada y brinde soporte a las necesidades del negocio (ver Figura 1).

Figura 1. Administración Integrada de TI de CA

Las funciones de administración claves para la Administración Integrada de TI pueden ser agrupadas en cuatro categorías:

Security Management. Incluye la administración de la identidad y el acceso, la información de seguridad, las vulnerabilidades y las amenazas. La administración de seguridad garantiza el acceso seguro y auditable a los sistemas e informaciones apropiadas y mitiga los riesgos de amenazas de seguridad.

Storage Management. Incluye la administración de los recursos de almacenamiento, backup y recuperación, cumplimiento y optimización.

Enterprise Systems Management. Incluye la administración de redes, sistemas, bases de datos, aplicaciones, dispositivos de desktop y cliente, e infraestructura web.

Business Service Optimization. Incluye la administración de servicios, activos, portfolio y proyectos.

La visión de Administración Integrada de TI brinda un enorme valor para cualquier empresa porque permite:

- **Administrar riesgos**. Controla quién tiene acceso a los activos, sistemas e información corporativa, y brinda un enfoque completo para el backup, la recuperación y el restablecimiento de la información.
- **Mejorar el servicio**. Administra y protege los servicios críticos de TI para atender las necesidades dinámicas de las funciones de negocio a las que brindan soporte.
- **Administrar costos**. La automación reduce los costos de la mano de obra necesaria para mantener las operaciones de TI, liberando esos recursos para proyectos estratégicos y nuevos desarrollos que apuntan al crecimiento de la empresa.
- **Alinear las inversiones de TI al negocio**. Usa información sobre cómo la TI está siendo utilizada y cuánto cuesta brindar soporte al negocio, para administrar y optimizar el uso de TI, garantizando que todos los recursos de TI, incluyendo personal, tecnología y proyectos, sean utilizados de forma efectiva.

Para más información sobre la Administración Integrada de TI de CA, visite www.ca.com/eitm

Los componentes claves de la administración de seguridad

La seguridad es un componente significativo de las infraestructuras de TI actuales. En un entorno informático dinámico, con una variedad de activos que necesitan protección, así como con una población de usuarios grande y diversa, es fundamental garantizar:

- La protección de los activos críticos contra códigos maliciosos, tales como virus, worms y rootkits, y malware, como spyware y spam
- La mitigación proactiva del riesgo al reducir las vulnerabilidades del sistema
- La implementación centralizada de políticas de acceso para protección de hosts, aplicaciones y datos
- El aprovisionamiento y mantenimiento automatizado de las identidades digitales
- Soluciones integradas, con control centralizado de la infraestructura extendida de seguridad
- Las auditorías y la generación de reportes centralizadas, para un cumplimiento regulatorio efectivo

La integración de los tres componentes claves de la administración de seguridad -administración de la identidad y el acceso, de las amenazas y de la información de seguridad- en una solución completa lo ayuda a alcanzar la eficiencia operativa y el cumplimiento regulatorio, así como contener los costos, mitigar el riesgo y asegurar operaciones de negocio continuas.

El siguiente gráfico ilustra las tres áreas claves de administración de seguridad y enumera las principales funciones para cada área:

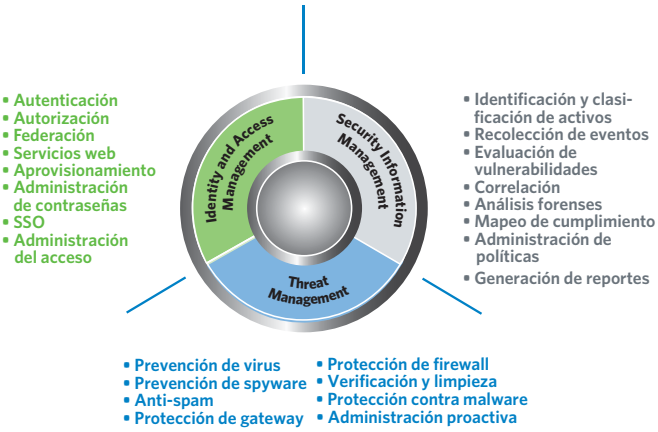

Figura 2. Areas claves de Administración de Seguridad

Administración de la Identidad y el Acceso

En la mayoría de las compañías, las identidades y los privilegios de acceso de los usuarios son críticos para conducir el negocio. Detrás de esas identidades están los empleados, contratistas, socios, clientes, etc., que guían cada aspecto del negocio. La Administración de la Identidad y el Acceso (IAM) automatiza y administra quién tiene acceso a todas las aplicaciones, bases de datos y plataformas críticas, así como las condiciones bajo las cuales fue autorizado ese acceso.

Las preguntas claves que deben ser respondidas por el componente de identidad y acceso de la administración de 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 de negocio, proteger activos vitales, agilizar las operaciones de negocio y alcanzar el cumplimiento regulatorio.

En muchos casos, 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. Un enfoque de administración de seguridad amplio reúne estas dos funciones, permitiendo la integración de los componentes y el acceso apropiado según la identidad. Además, barre con los usuarios no autorizados desde los sistemas, mientras otorga a los usuarios autorizados el acceso a la información y las aplicaciones necesarias para realizar sus tareas y mantener a la compañía operando.

Las capacidades claves de una solución completa e integrada para la administración de la identidad y el acceso, son:

- **Administración y aprovisionamiento de la identidad**, que permite la creación y administración sencilla de las identidades del usuario, el acceso a los recursos protegidos y el establecimiento automático de cuentas. Este componente automatiza la configuración requerida para establecer un usuario nuevo, permitiéndole tener nuevos usuarios online y productivos mucho más rápido que con los procedimientos manuales. También, le permite delegar la administración de usuarios a las unidades organizativas o los socios externos que poseen esos usuarios. Aún más importante, un aprovisionamiento bien implementado permite a sus administradores manejar todo el ciclo de vida de una identidad, incluyendo cambios y eliminación de roles una vez que el usuario ya no está autorizado.
- **Aplicación del acceso**, que ayuda a asegurar que su organización mantenga la integridad de la información al prevenir el acceso sin autorización. Esto le permite tener un control detallado sobre quién accede a qué recursos, y dónde están ubicados. También, debería incluir la aplicación de políticas de acceso para sistemas host, aplicaciones, bases de datos y otros recursos protegidos.
- **Auditoría**, que facilita el seguimiento y la generación de reportes sobre el acceso y es requerida para cumplir con las regulaciones y realizar un análisis forense luego de los eventos. Esto lo ayudará a determinar dónde se originan las amenazas y prevenir otros ataques.

Un importante beneficio de una solución IAM completa es que permite la creación y expansión de robustos ecosistemas cliente/partner de todo tipo. Muchas organizaciones desean integrar proveedores, distribuidores, subcontratistas y otros socios de marketing dentro de una infraestructura de TI unificada que permita a los miembros de una organización acceder de forma segura a las aplicaciones y la información de otra organización.

La *Federación de Identidades* es una tecnología de administración de seguridad que, junto con los estándares industriales relacionados, permite el establecimiento de sofisticados ecosistemas de partners. Brinda los servicios fundamentales que permiten la administración de identidades externas, para que la información y las aplicaciones puedan ser compartidas por diversas organizaciones. La federación puede así ayudar a conducir nuevas y significativas oportunidades de negocio.

Una práctica o sistema sólido de administración de la identidad y el acceso proporciona una base para la administración de seguridad al garantizar que todos los usuarios tengan los derechos de acceso apropiados para todos los recursos protegidos, y que esos derechos sean ejecutados de forma adecuada. También, ayuda a reducir los costos administrativos al automatizar muchas funciones administrativas del sistema, así como al aprovisionar y desaprovisionar las cuentas y derechos de acceso. A su vez, mejora enormemente el cumplimiento regulatorio al brindar filtrado y análisis automatizado de eventos. Finalmente, permite el crecimiento del negocio y ayuda a fortalecer las relaciones con clientes existentes.

Administración de las Amenazas

Dentro del entorno tradicional de seguridad, las empresas dependen de una multitud de soluciones puntuales diferentes para prevenir la infiltración de malwares, tales como virus, worms, spyware, adware, spam y otro contenido malicioso en sus redes, así como también para asegurar que los datos de negocio 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 de negocio diarias se interrumpen, disparando grandes pérdidas, o la publicidad alrededor de una brecha de seguridad causa un daño significativo en la reputación empresarial y el valor de marca. Incluso en situaciones mucho menos dramáticas, estas pestes pueden causar pérdidas significativas de tiempo y productividad, tanto para usuarios como para administradores de TI.

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

- Detecta intrusiones, filtra el contenido y detiene worms, virus, keyloggers y otros malware
- Combate amenazas y vulnerabilidades potenciales, incluyendo nuevas y complejas amenazas combinadas, antes de que afecten su sistema
- Identifica las vulnerabilidades conocidas dentro sus sistemas antes de que ocurran los ataques
- Bloquea el spam para mejorar la productividad del usuario y reduce potencialmente el robo de identidad

La implementación de la administración proactiva de las amenazas también atiende otras preocupaciones

corporativas, tales como el acceso a contenido y uso inapropiado. Ayuda a asegurar que la información que sale y entra en su red sea la adecuada y no sea confidencial, y bloquea el acceso a sitios web donde el contenido no es el apropiado o no está relacionado con la empresa. La administración proactiva 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.

La reciente aparición de complejas amenazas combinadas reforzó la necesidad de un enfoque integrado para la administración de amenazas. Los componentes antivirus y anti-spyware separados, por ejemplo, normalmente no ofrecen el mismo nivel de protección contra amenazas combinadas que una solución única e integrada para administración de amenazas.

Administración de la Información de Seguridad

La administración de la información de seguridad es un área crítica de la administración de 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 uno de estos componentes 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 de seguridad e impacta negativamente en las operaciones de negocio. Aún más, sin la posibilidad de analizar automáticamente este aluvión de información sobre eventos, la probabilidad de no reconocer un evento serio es significativa. Sin una 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.

Las herramientas para administración de la información de seguridad utilizan reglas de correlación, visualización y análisis forenses avanzados para transformar los datos de seguridad sin procesar en información de negocio 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 de negocio son afectados por los exploits de red, el robo de datos internos o las violaciones de las políticas de seguridad o RH; además, proporcionan los seguimientos de auditorías necesarios para el cumplimiento de las regulaciones.

Las soluciones para administración de la información de seguridad también reducen, agregan, correlacionan y priorizan los diversos datos de seguridad de múltiples dispositivos de seguridad y tecnologías de software, integrando sus entornos de seguridad física y de TI. Las herramientas para administración de la información de seguridad se integran perfectamente con la mayoría de sus aplicaciones críticas, incluyendo contaduría, planilla de sueldos, RH 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 de 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 del negocio, 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 de negocio, 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:

- **Agregado y filtrado de eventos**. Reduce el volumen de datos de seguridad a información de negocio procesable, suministrando sólo lo que es necesario para el sistema de administración de la red y los sistemas.
- **Correlación y visualización de eventos**. Automatiza el proceso de identificación de tendencias sospechosas, a partir del análisis de eventos aparentemente no relacionados, y brinda a los administradores las herramientas para monitorear visualmente el estado actual del entorno de seguridad de TI.
- **Análisis post-evento**. Emplea análisis forenses sofisticados para determinar lo que ha ocurrido y localizar tendencias dañinas potenciales.

Cuando se implementa de forma apropiada, la administración de la información de seguridad entrega una solución de negocio segura 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 Security Management de CA

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

Durante más de 28 años, CA ha entregado una amplia gama de soluciones líderes para administración de TI que fortalecen todos los aspectos de la administración de los procesos de negocio, 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 administración de CA ofrece capacidades reales de administración de TI, como se evidencia en el hecho de que es utilizado actualmente por más del 95% de las compañías Fortune 1000.

Las soluciones Security Management de CA están diseñadas tanto para proteger como para hacer posible su negocio. Estas soluciones administran proactivamente las complejidades de un entorno de seguridad al manejar todos los accesos a los recursos, atendiendo los eventos desde su identificación hasta su resolución, asegurando operaciones de negocio continuas y entregando la eficiencia operativa que solo puede ser provista a través de una solución completa e integrada.

Las soluciones de CA atienden los requerimientos del nuevo modelo de administración de seguridad al brindar un paquete completo y altamente integrado para este tipo de administración. Le dice quién tiene acceso a qué, determina qué ocurre en su entorno y ayuda a asegurar que usted tome las decisiones adecuadas en el momento justo. Además, las soluciones Security Management de CA ponen en orden el caos del exceso de información de seguridad, permitiéndole enfocarse en su empresa.

Visión general de los productos Security Management de CA

Administración de la Identidad y el Acceso

CA lidera la industria al brindar capacidades de aprovisionamiento, ejecución y auditoría integradas que permiten administrar efectivamente sus usuarios y accesos. Los principales componentes de la solución CA Identity and Access Management son:

- **CA Identity Manager**. Brinda una plataforma integrada para administración de identidades que automatiza la creación, modificación y suspensión de las identidades y accesos de los usuarios a los recursos corporativos, incrementando los niveles de seguridad y cumplimiento, reduciendo los costos administrativos y mejorando la experiencia del usuario. Además, CA Identity Manager brinda servicios de auditoría que pueden ser usados por auditores internos y externos para ayudar a determinar si las prácticas de concesión de derechos en la organización son controladas y mantienen la privacidad de los datos personales.
- ***e*Trust® SiteMinder®**. Solución líder de mercado para administración del acceso y el inicio de sesión único basado en la Web. Para garantizar el acceso seguro de empleados, clientes y partners a las aplicaciones e informaciones esenciales, *e*Trust SiteMinder ofrece capacidades de administración y políticas de seguridad centralizadas que permiten reducir los costos y la complejidad operativa de la TI.
- ***e*Trust® SiteMinder® Federation Security Services (FSS)**. Amplía la comprobada funcionalidad de *e*Trust SiteMinder, facilitando la federación de identidades en los dominios de seguridad tanto dentro como fuera de la empresa. La federación de identidades permite que las organizaciones aprovechen los beneficios de conectar las aplicaciones de negocio distribuidas en todos los dominios, sin sacrificar la seguridad.
- ***e*Trust® TransactionMinder®**. Ofrece capacidades seguras y centralizadas de administración de la autenticación y autorización basada en políticas para servicios web. *e*Trust TransactionMinder se integra con estructuras de servicios web estándar y brinda control detallado de acceso a documentos XML en múltiples transacciones comerciales.
- ***e*Trust® 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 el acceso. También, brinda control detallado de los derechos de acceso del "súper usuario" para una mayor seguridad y responsabilidad.
- ***e*Trust® CA-ACF2® Security y *e*Trust® CA-Top Secret® Security**. Brinda seguridad líder para entornos de transacciones de negocio 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 usuarios y sus derechos de acceso.

- ***e*Trust® Cleanup for CA-ACF2® Security, *e*Trust® Cleanup for CA-Top Secret® Security y *e*Trust® Cleanup for RACF.** *e*Trust Cleanup brinda limpieza automatizada, continua y autónoma de bases de datos de seguridad. Remueve derechos de acceso obsoletos, no utilizados, redundantes y excesivos, mejorando así el control de seguridad, el cumplimiento y el desempeño, además de simplificar la auditoría. Más específicamente, identifica y genera comandos que remueven ACIDs, permisos y conexiones de perfiles que los usuarios tienen pero no utilizan. *e*Trust Cleanup brinda una respuesta inmediata y sustancial que ayuda a enfrentar las crecientes presiones de esfuerzo y personal debidas a los requisitos regulatorios, reglamentarios y de auditoría.
- ***e*Trust® CA-Examine™ Auditing**. Realiza una revisión y auditoría automatizada de la integridad y la verificación del sistema operativo z/OS. Además, 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.
- ***e*Trust® Single Sign-On**. Solución líder de mercado para administración del inicio de sesión único (SSO). Para clientes que requieren acceso seguro a aplicaciones cliente-servidor o legadas, *e*Trust Single Sign-On brinda capacidades de administración de contraseñas e inicio de sesión único, garantizando una ejecución robusta de la seguridad.

Administración de las Amenazas

Las soluciones Threat Management de CA incorporan tecnologías que previenen que malwares, tales como virus, spyware, adware, spam y otro contenido malicioso, se infiltren e infecten sus sistemas y aplicaciones de negocio, e impacten la continuidad del servicio. 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 en su organización. Las soluciones Threat Management de CA también confrontan los desafíos para la seguridad del contenido, manteniendo la confidencialidad del contenido corporativo y controlando el contenido malicioso al permitir la creación, implementación y monitoreo de políticas de uso efectivas. Combinadas con la identificación y la remediación automatizada de las debilidades de seguridad, las soluciones Threat Management de CA mitigan el riesgo a medida que reducen el costo total de las operaciones de seguridad.

Cuatro soluciones merecen especial atención:

- ***e*Trust® Antivirus**. Brinda protección de clase corporativa contra, virtualmente, todas las formas de ataques costosos de virus, desde el perímetro hasta el PDA. Una consola única simplifica la administración de entornos corporativos heterogéneos; proporciona métodos simples de implementación, administración y actualización de firmas, y protege su empresa de virus y códigos maliciosos antes de que ingresen a su red.
- ***e*Trust® PestPatrol® Anti-Spyware Corporate Edition r8**. Detecta y remueve spywares, malwares no virales y pestes molestas como adware, para proteger las empresas contra la disminución en el desempeño de las PCs, el acceso no autorizado y el robo de información. *e*Trust PestPatrol Anti-Spyware Corporate Edition complementa las tradicionales defensas de seguridad, incluyendo tecnologías antivirus, de firewall y de detección de intrusiones, brindando un componente clave de cualquier estrategia de seguridad de múltiples niveles.
- **CA Integrated Threat Management**. Combina *e*Trust® PestPatrol® Anti-Spyware Corporate y *e*Trust® Antivirus en una única consola de administración que aumenta la eficiencia gracias a un agente común, recursos de conexión y herramientas de actualización. La solución advierte, detecta, analiza y soluciona ataques, minimizando los riesgos, la inactividad del sistema y la pérdida de productividad.
- ***e*Trust® 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. *e*Trust Secure Content Manager también ofrece capacidades de autoadministración del usuario y permite la administración común de las políticas de seguridad en todos los puntos potenciales de exposición.

Administración de la Información de Seguridad

Las soluciones Security Information Management de CA ayudan a asegurar 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 mejoran 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 de negocio procesable. Aún más, estas herramientas aseguran operaciones de negocio continuas y proporcionan las visiones de seguridad requeridas para alcanzar el cumplimiento regulatorio. Las soluciones Security Information Management de CA incluyen:

- ***e*Trust® Security Command Center**. Ofrece una solución completa para monitorear y administrar todos los aspectos de su seguridad corporativa desde una consola de administración centralizada. *e*Trust Security Command Center le permite reunir, correlacionar, analizar y priorizar fácilmente los

datos y tomar medidas correctivas inmediatas. También, brinda reportes avanzados de auditoría que le ayudan a atender los requerimientos de cumplimiento de las regulaciones.

- **eTrust® Vulnerability Manager**. Protege proactivamente sus activos de TI contra ataques externos y amenazas internas a la seguridad al correlacionar los datos exclusivos sobre vulnerabilidades con sus activos. *e*Trust Vulnerability Manager ofrece evaluación de las vulnerabilidades, remediación mediante parches y configuración, y análisis del cumplimiento a través de una interfaz de usuario basada en la Web y un dispositivo fácilmente desplegable.
- **eTrust® Network Forensics**. Captura los datos de red sin procesar y utiliza análisis forenses avanzados para identificar cómo son afectados sus activos por los exploits de red, el robo de datos internos y las violaciones a la política de seguridad o RH. Su tecnología patentada permite que su personal de seguridad y de TI visualice la actividad de red, descubra el tráfico anormal e investigue las brechas con una solución única y conveniente.
- **eTrust® Policy Compliance**. Automatiza el proceso de evaluación de la configuración del servidor y el host, permitiendo la administración de seguridad con las herramientas que controlan la complejidad del monitoreo y ejecución del cumplimiento de la seguridad. Al reducir la dependencia del factor humano, los alertas y reportes agilizan el tiempo de respuesta y terminan con los costos auxiliares imprevistos.

Conclusión

La continuidad del negocio, el cumplimiento regulatorio, la mitigación real del riesgo, la optimización de los activos de seguridad existentes y la eficiencia operativa son fáciles de alcanzar si implementa una solución de administración de seguridad completa e integrada. Para determinar su perfil actual 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 administrar centralmente las políticas de acceso para todos los recursos protegidos, incluyendo sistemas, aplicaciones (web y no web), archivos y bases de datos?
- ¿Puede aprovisionar inmediatamente a los empleados cuando cambian sus roles?
- ¿Sus empleados son desaprovisionados totalmente cuando sus derechos de acceso y cuentas deben ser removidos?

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?
- ¿Está protegido adecuadamente frente a la extensión del spyware?
- ¿La productividad de sus usuarios se ve afectada por grandes cantidades de spam?
- ¿Sus empleados utilizan el ancho de banda de Internet para propósitos no relacionados con la empresa?

Administración de la Información de Seguridad

- ¿Puede transformar los datos de seguridad sin procesar en información de negocio procesable?
- ¿Puede garantizar que toda la información sobre eventos de seguridad sea recolectada y analizada efectivamente, para detectar y resolver rápidamente los eventos serios?
- ¿Puede proporcionar los seguimientos de auditorías necesarios para el cumplimiento de las regulaciones?
- ¿Posee un proceso automatizado para identificar, rastrear y remediar las vulnerabilidades actuales detectadas en todos sus sistemas?

Al obtener control de su entorno a través de las soluciones altamente integradas para administración de la seguridad, usted puede fortalecer su seguridad global, mejorar la productividad del usuario, reducir los costos administrativos de TI y permitir el cumplimiento regulatorio.

Para más información sobre las soluciones Security Management de CA, visite ca.com/etrust

Quality System
Quality Endorsed Company
ISO 9001
Lic. 2443

MP305510806