SONICWALL

RESUMEN DE SOLUCIONES: UN ENFOQUE UNIFICADO PARA ADMINISTRAR LA GESTIÓN, LOS RIESGOS Y EL CUMPLIMIENTO

Integración de la administración global de seguridad en red

Resumen

Un enfoque conectado para la organización, el control, el análisis y la generación de informes de la seguridad no es solo fundamental en prácticas de seguridad preventiva, sino que también constituye la base para una estrategia unificada de administración de la gestión, el cumplimiento y los riesgos en materia de seguridad.

Una imagen grande coherente y más simple

La simplicidad en la práctica de la administración de seguridad promueve mejores decisiones y coordinaciones de seguridad. Para eso, hay que librarse del caos y la rutina manual de las operaciones diarias.

Una de las mejores formas de eliminar estas complejidades es emplear software de administración inteligente como base. Este software debe ser sistemático en sus métodos y flujo de trabajo para reducir la cantidad de intervenciones personales cuando se administra el entorno de seguridad. En vez de esforzarse por reaccionar cuando los sistemas desarrollan problemas o se hacen cambios no autorizados a las reglas de firewall, el software inteligente reconoce de forma automática estos tipos de riesgos de seguridad, los informa y ayuda a resolverlos con rapidez.

Además, el hecho de no tener una vista de imagen grande y coherente de todo el ecosistema de seguridad pone a las empresas en riesgo de infracciones del cumplimiento o ataques cibernéticos que se pueden evitar. La adopción de esta plataforma común les brinda a las empresas de cualquier tamaño, incluidas las empresas distribuidas y los proveedores de servicios, datos detallados para tomar más decisiones informadas sobre la seguridad. También permite que los equipos de seguridad operen más rápido e incorporen colaboración, comunicación

y conocimientos a todo el marco de seguridad compartido.

Administración integrada, segura y extensible

Para simplificar y unificar, **una solución óptima ofrecería** una arquitectura basada en la nube integrada, segura y extensible para administrar todo la gama de seguridad. Esta plataforma unificada en la nube permitiría a los equipos de seguridad consolidar fácilmente la administración de dispositivos de seguridad y federar todos los aspectos operativos de la infraestructura de seguridad. Esto incluye el cumplimiento y la administración de políticas centralizadas, el monitoreo de eventos en tiempo real, las actividades de usuario, el control de las aplicaciones, el uso de los datos, el análisis del flujo y los datos de desglose, además de la generación de informes de auditoría, cumplimiento y análisis, y más. También cumpliría con los requisitos de la administración del cambio de firewalls de las empresas gracias a una función de automatización de flujos de trabajo.

Administración de riesgos, cumplimiento y gestión

Un enfoque integral formaría la base para una estrategia unificada de administración de riesgos, cumplimiento y gestión de la seguridad. A usted le gustaría establecer un enfoque conectado y holístico para la organización de la seguridad, a fin de federar todos los aspectos operativos de su ecosistema de seguridad en red. Se deben simplificar y automatizar varias tareas para promover una mejor coordinación de la seguridad a fin de reducir la complejidad, el tiempo y el gasto de la realización de operaciones de seguridad y la administración. Entre las tareas se incluyen las siguientes:

- Aprovisionamiento de red y seguridad
- Cumplimiento de políticas
- Aplicación de parches
- Detección de dispositivos
- Inventario
- Configuración y diagnóstico
- Monitoreo
- Generación de informes
- Análisis
- Auditoría
- Recolección de estadísticas de seguridad

Automatización del flujo de trabajo

El proceso de flujo de trabajo garantiza la precisión y el cumplimiento de cambios en las políticas a través de procedimientos rigurosos de validación y cumplimiento antes de la implementación. Los grupos de aprobación deben ser flexibles y de conformidad con las pautas de seguridad del personal de la empresa. Esto ayudará a mitigar los riesgos, reducir los errores, mejorar la eficiencia y asegurar una eficacia de alta seguridad. Con una automatización de flujo de trabajo y una auditoría de cambios de políticas apropiadas, los equipos de seguridad tendrán agilidad y confianza para implementar las políticas de firewall adecuadas, en el momento correcto y de acuerdo con las regulaciones de cumplimiento.

Implementación *zero touch*

Al aprovechar la nube, una solución ideal simplificaría y aceleraría la implementación y el aprovisionamiento de los firewalls de manera remota. Esto reduciría el tiempo, el costo y la complejidad asociados con la configuración del dispositivo. Al mismo tiempo, la seguridad y la conectividad pueden ocurrir de forma instantánea y automática. Los administradores pueden hacer operativa una gran cantidad de firewalls a escala con una mínima intervención del usuario. Desde una única consola de administración basada en la Web, por ejemplo, uno puede impulsar políticas, realizar actualizaciones de firmware y sincronizar licencias.

Análisis

Una solución eficaz permitiría al área de TI realizar análisis forenses y de investigación profundos de datos de seguridad enriquecidos. Les brindaría a las partes interesadas visibilidad de un solo panel y conocimiento de la situación del entorno de seguridad en red. De esta manera, les permitiría tomar decisiones sobre políticas de seguridad informadas basadas en información de amenazas consolidada y crítica con respecto al tiempo. El área de TI puede calibrar las políticas y controles de seguridad a medida que se descubren las amenazas y los riesgos potenciales. En consecuencia, reduciría el tiempo de respuesta ante incidentes con inteligencia de amenazas factible en tiempo real.

> Los equipos de seguridad deben tener agilidad y confianza para implementar las políticas de firewall adecuadas, en el momento correcto y de acuerdo con las regulaciones de cumplimiento.

Conclusión

Con la plataforma correcta de administración de seguridad basada en la nube, las empresas y los proveedores de servicios pueden establecer una estrategia completamente coordinada de administración de riesgos, cumplimiento y gestión de la seguridad. La plataforma correcta también puede reducir los gastos operativos y las complejidades del soporte de una infraestructura de propiedad exclusiva a la vez que proporciona lo último en visibilidad, agilidad y capacidad para gestionar todo el ecosistema de seguridad en red SonicWall con mayor claridad, precisión y velocidad. Y todo desde un único lugar.

Obtenga información sobre cómo el servicio de seguridad de SonicWall Capture puede mejorar su línea de base en sonicwall.com/capture-security-center.

© 2018 SonicWall Inc. TODOS LOS DERECHOS RESERVADOS.

SonicWall es una marca comercial o marca comercial registrada de SonicWall Inc. o sus afiliados en EE. UU. u otros países. Todas las demás marcas comerciales y marcas comerciales registradas son propiedad de sus respectivos dueños.

La información presentada en este documento se proporciona en relación con los productos de los afiliados de SonicWall Inc. No se otorga ninguna licencia, expresa o implícita, por impedimento legal o de otro modo, a ningún derecho de propiedad intelectual o en relación con la venta de los productos SonicWall. EXCEPTO LO ESTABLECIDO EN LOS TÉRMINOS Y CONDICIONES ESPECIFICADOS EN EL ACUERDO DE LICENCIA PARA ESTE PRODUCTO, SONICWALL, O SUS AFILIADOS, NO GARANTIZA RESPONSABILIDAD ALGUNA Y RENUNCIA A CUALQUIER GARANTÍA EXPRESA, IMPLÍCITA O REGLAMENTARIA RELACIONADA CON SUS PRODUCTOS, INCLUIDAS, ENTRE OTRAS, LA GARANTÍA IMPLÍCITA DE COMERCIABILIDAD, ADECUACIÓN PARA ALGÚN FIN EN PARTICULAR O NO INFRACCIÓN. EN NINGÚN CASO SONICWALL, O SUS AFILIADOS, SE HARÁ RESPONSABLE POR DAÑOS DIRECTOS, INDIRECTOS, DE CARÁCTER CONSECUENTE, PUNITIVOS, ESPECIALES NI INCIDENTALES (INCLUIDOS, ENTRE OTROS, DAÑOS POR PÉRDIDA DE GANANCIAS, INTERRUPCIÓN DEL NEGOCIO O PÉRDIDA DE LA INFORMACIÓN) QUE SURGIERAN POR EL USO O LA INCAPACIDAD DE USAR ESTE DOCUMENTO, INCLUSO SI SONICWALL, O SUS AFILIADOS, LE HUBIERA ADVERTIDO SOBRE LA POSIBILIDAD DE TALES DAÑOS. SonicWall, o sus afiliados, no efectúa declaraciones ni otorga garantías con respecto a la precisión o la integridad de los contenidos de este documento y se reserva el derecho de realizar modificaciones en las especificaciones y descripciones del producto en cualquier momento sin previo aviso. SonicWall Inc. o sus afiliados no se comprometen a actualizar la información que figura en este documento.

Acerca de nosotros

SonicWall ha luchado contra la delincuencia cibernética durante más de 25 años, defendiendo a las pequeñas y medianas empresas en todo el mundo. Nuestra combinación de productos y socios ha permitido ofrecer una solución de defensa cibernética en tiempo real adaptada a las necesidades específicas de más de 500.000 empresas en más de 150 países, para que pueda hacer más negocios con menos temor.

Si tiene alguna pregunta sobre el posible uso de este material, comuníquese con:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Visite nuestro sitio web para obtener más información.
www.sonicwall.com

© 2018 SonicWall Inc. TODOS LOS DERECHOS RESERVADOS. SonicWall es una marca comercial o marca comercial registrada de SonicWall Inc. o sus afiliados en EE. UU. u otros países. Todas las demás marcas comerciales y marcas comerciales registradas son propiedad de sus respectivos dueños.

SolutionBrief-AUnifiedApproach-US-KJ-MKTG2444