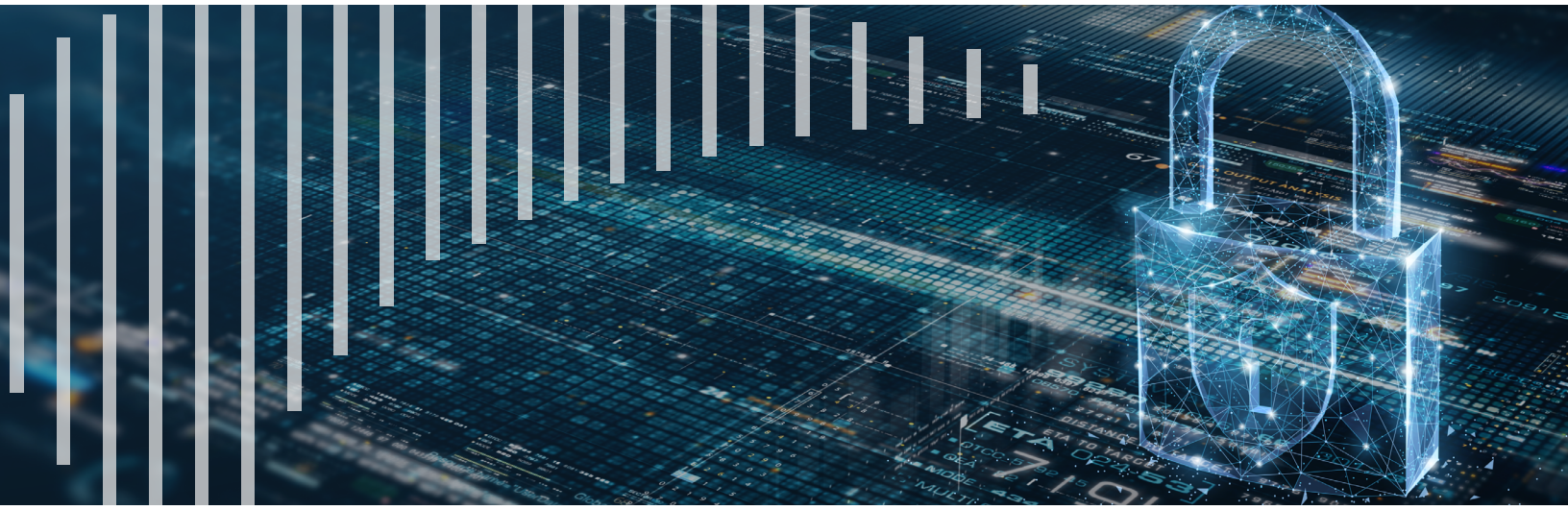


RESUMEN EJECUTIVO

Nuevas estrategias para nuevas amenazas

Introducción

El panorama de la ciberseguridad evoluciona rápidamente, y las empresas deben adaptarse a ello.

La realidad de la TI distribuida, que se expande masivamente, crea una explosión de puntos de exposición sin precedentes, que los sofisticados ciberdelincuentes y atacantes aprovechan.

Ante unos entornos híbridos y totalmente remotos cada vez más habituales, los vectores de los ciberataques también crecen, a través de esa oleada de nuevos puntos de exposición. Las amenazas habituales y los ataques multiescenario son cada vez más difíciles de detectar. Muchas organizaciones están buscando la forma de potenciar su ciberseguridad y adelantarse a los atacantes. Existen muchas estrategias y tecnologías que las empresas pueden aprovechar para conseguir un enfoque de seguridad más sólido con el que proteger su organización.

Implementación de la autenticación multifactor

La autenticación multifactor o MFA es imprescindible tanto para empresas como para particulares. La MFA funciona como una barrera más que protege las redes contra los ciberdelincuentes. Habilitar la MFA puede dificultar los ataques o incluso hacer que sean poco rentables para los delincuentes. La MFA puede detener modalidades comunes de ataque, como phishing, registradores de pulsaciones, fuerza bruta y ataques de intermediario (MITM). Existen distintas clases de MFA:

- MFA basada en un dispositivo personal: puede ser algo similar a un mensaje de texto o una app de autenticación.
- MFA basada en hardware: utiliza un componente de hardware real, como un USB, una Smart Card o un token RSA.
- Biológica: por ejemplo, una huella dactilar o un escáner de retina.

Como con cualquier tecnología o software, las empresas deben llevar a cabo los protocolos correspondientes de investigación y pruebas para implementar la política MFA que mejor encaje con sus necesidades de seguridad.

Aprenda a evaluar mejor los riesgos

Para lograr una estrategia de seguridad efectiva, las empresas deben evaluar con precisión los riesgos, diferentes en cada organización. En un organismo público, puede consistir en proteger sus activos globales y asuntos de seguridad nacional. En una pequeña empresa, puede ser el desarrollo de su reputación de marca y proteger sus activos financieros. Independientemente del tamaño de la organización, muchos profesionales de la seguridad tienen como referente al Instituto Nacional de Estándares y Tecnología (NIST) para asegurarse del cumplimiento de los estándares y las mejores prácticas. Aunque los frameworks pueden constituir una base sólida, las organizaciones deben evaluar los riesgos particulares de sus respectivos entornos. Las empresas deben tener una amplia perspectiva, pero sin perder de vista los matices particulares de sus propios riesgos. Los líderes de los departamentos interfuncionales pueden proporcionar sus propias perspectivas. De esa forma, los profesionales de la ciberseguridad pueden descubrir que los demás departamentos tienen unas perspectivas diferentes, pero válidas, sobre los riesgos. Cuando la organización tenga un conocimiento exhaustivo de los riesgos en todo su ecosistema, los profesionales de la seguridad podrán trazar una ruta para implementar una estrategia de seguridad más sólida.

Aborde las lagunas de *know-how*

Las empresas necesitan profesionales cualificados que defiendan la infraestructura de la organización frente a los ciberataques. La necesidad de un personal de asistencia eficaz crece a la par que la complejidad de la red. La mayoría

de las organizaciones descubren que necesitan personas muy cualificadas para proteger con eficacia el hardware, el software y las redes corporativas frente a los ciberdelincuentes. Atraer a los mejores talentos es imprescindible para el negocio, pero a muchas organizaciones les resulta difícil encontrarlos. Contratar y conservar a los profesionales de la ciberseguridad ha demostrado ser una tarea titánica. SonicWall tiene una extensa red de partners que se puede utilizar para ayudar a las empresas de cualquier tamaño a conseguir sus objetivos y metas de seguridad.

Elija la tecnología adecuada

Con el avance de los sistemas de seguridad, los responsables informáticos disponen hoy de más opciones a la hora de proteger los activos y mantener a salvo las redes. Una estrategia sólida incluye una protección multicapa y una cobertura sin fisuras en todas las superficies.

Los atacantes intentan dirigir los ataques aprovechando una infraestructura cada vez más compleja y el creciente número de aplicaciones, dispositivos y redes. Atacan con todo, desde phishing y variantes totalmente nuevas de malware, hasta ransomware, ataques de canal lateral, de IoT, etc.; todos, especialmente difíciles de detectar.

SonicWall le ayuda a eliminar los ángulos muertos y a proteger una plantilla «sin límites» en todos los entornos. Puede ver todo en todos lados y gestionar mejor los eventos importantes.

Nuestro Capture Security Center elimina la visibilidad basada en silos. Mediante una sola consola y un punto unificado de control, puede ver todas las superficies de ataque en varias generaciones de infraestructura TI (local, en la nube, endpoints y en Secure Network as a Service).

La inteligencia de amenazas permanente y en tiempo real revela las vulnerabilidades en el panorama en cuanto suceden y siempre sabe dónde están los atacantes y dónde intentan infiltrarse. Las métricas de riesgo personalizado minimizan la exposición y priorizan las acciones según el perfil de riesgos, mientras que las analíticas y los informes relevantes aceleran los tiempos de respuesta y ayudan a moldear la estrategia.

La tecnología patentada Real-Time Deep Memory Inspection™ (RTDMI) de SonicWall bloquea amenazas de día cero y desconocidas en la pasarela, incluso aquellas ocultas mediante cifrado o que no presentan un comportamiento malicioso. La tecnología está diseñada para que el usuario comprenda cómo operan los atacantes. Las amenazas de día cero no tienen una definición de ataque hasta que se usan por primera vez, por lo que las empresas son vulnerables. RTDMI detecta esas amenazas y permite un nivel de visibilidad que permite ver los cambios en la conducta de los atacantes.

Sea más exigente

Las organizaciones necesitan saber que sus proveedores toman las medidas de seguridad oportunas al desarrollar sus productos. Lo ideal es que los proveedores implementen sistemas como análisis de composición de software y pruebas estáticas de seguridad de aplicaciones. Es crucial contar con visibilidad del *pipeline* de desarrollo para comprender su riesgo de exposición ante varias vulnerabilidades. Los delincuentes saben que el perímetro es el lugar de más difícil acceso de la organización; por tanto, buscan vulnerabilidades en todos sus componentes, incluidos el software y el hardware de terceros. Las empresas pueden crear cuestionarios para proveedores en los que se evalúen los estándares que



estos deben cumplir para ser aceptados. El escrutinio de los proveedores a través de los cuestionarios proporciona abundantes datos para decidir quiénes encajan mejor en su modelo de negocio. Exigir más a los proveedores puede ayudar a las organizaciones a reforzar su estrategia de ciberseguridad.

Conclusión

Los ciberdelincuentes cambian constantemente de estrategia para infiltrarse en las empresas y causar todo el daño posible. En un mundo en el que los ciberdelincuentes siempre están buscando la forma de pillar desprevenidas a las organizaciones, estas pueden implementar estrategias que les permitan ir un paso por delante.

- Implementar la autenticación multifactor para que a los ciberdelincuentes les cueste más infiltrarse en las redes.
- Desarrollar mejores estrategias de análisis de riesgos para garantizar que la empresa esté protegida en todos los potenciales puntos de entrada.
- Contratar y capacitar a un personal muy cualificado para optimizar y mantener todos los sistemas de seguridad.
- Seleccionar la mejor tecnología para redes, endpoints y puntos de acceso para proteger datos y usuarios.
- Imponer a los proveedores unos requisitos rigurosos, que garanticen que la empresa no «importa» vulnerabilidades de terceros en hardware o software.

En última instancia, cada organización tiene la responsabilidad de determinar qué estrategias de ciberseguridad funcionan mejor para su negocio. Para obtener más información sobre cómo desarrollar, escalar y gestionar la seguridad en entornos en la nube, híbridos y tradicionales, contacte hoy mismo con un experto en seguridad de SonicWall.



Acerca de SonicWall

SonicWall proporciona una Ciberseguridad sin límites, sin perímetro, para la era hiperdistribuida y una realidad laboral caracterizada por la movilidad, el teletrabajo y la inseguridad. Al detectar amenazas desconocidas, proporcionar visibilidad en tiempo real y ofrecer una alta rentabilidad, SonicWall cierra la brecha de la ciberseguridad para empresas, gobiernos y pymes en todo el mundo. Si desea obtener más información, visite www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Si desea obtener más información, consulte nuestra página Web.
www.sonicwall.com

© 2023 SonicWall Inc. TODOS LOS DERECHOS RESERVADOS.
SonicWall es una marca comercial o marca comercial registrada de SonicWall Inc. y/o sus filiales en EEUU y/u otros países. Las demás marcas comerciales y marcas comerciales registradas son propiedad de sus respectivos propietarios. La información incluida en este documento se proporciona en relación con los productos de SonicWall Inc. y/o sus filiales. No se otorga mediante este documento, ni en relación con la venta de productos SonicWall, ninguna licencia, expresa ni implícita, por doctrina de los propios actos ni de ningún otro modo, sobre ningún derecho de propiedad intelectual. A excepción de lo establecido en los términos y condiciones tal y como se especifican en el contrato de licencia de este producto, SonicWall y/o sus filiales no asumen ninguna responsabilidad y rechazan cualquier garantía expresa, implícita o legal en relación con sus productos, incluidas, entre otras, las garantías implícitas de comercialización, adecuación para un determinado propósito o no violación de derechos de terceros. SonicWall y/o sus filiales no se harán responsables en ningún caso de daños directos, indirectos, consecuentes, punitivos, especiales ni incidentales (incluidos, sin limitación, los daños relacionados con la pérdida de beneficios, la interrupción del negocio o la pérdida de información) derivados del uso o de la incapacidad de utilizar el presente documento, incluso si se ha advertido a SonicWall y/o sus filiales de la posibilidad de que se produzcan tales daños. SonicWall y/o sus filiales no ofrecen declaración ni garantía alguna con respecto a la precisión ni a la integridad de la información contenida en el presente documento y se reservan el derecho de modificar las especificaciones y las descripciones de productos en cualquier momento y sin previo aviso. SonicWall Inc. y/o sus filiales no se comprometen a actualizar la información contenida en el presente documento.

ExecBrief-EvolvedThreats_EvolvedStrategies-A4-JK-7925