NUCLEUS RESEARCH

GUÍA

IBM QRADAR ON CLOUD

PROGRAMA: SEGURIDAD E INFRAESTRUCTURA
DOCUMENTO Q170 • AGOSTO 2016

ANALISTA
Seth Lippincott

Nucleus Research Inc. 100 State Street Boston, MA 02109 **NucleusResearch.com** Teléfono: +1 617.720.2000

EL RESULTADO FINAL

IBM QRadar on Cloud presta servicios de recolección de registros a un entorno de nube administrado que permite a los clientes subcontratar elementos de su sistema de seguridad.

Nucleus descubrió que los clientes podían aprovechar el modelo de suscripción en la nube y evitar comprar costosas infraestructuras, seleccionando IBM QRadar on Cloud. Adicionalmente, los clientes se benefician de lo fácil que es la implementación y pueden extraer valor rápidamente al comenzar a identificar activos comprometidos en unos pocos días y no en meses.

•••

LA SITUACIÓN

La seguridad de la información y la integridad de la red se están volviendo un importante foco para los departamentos de TI en compañías de todos los tamaños. Al mismo tiempo, las compañías son más conscientes del costo sobre las compras tecnológicas. Encontrar la tecnología adecuada de protección contra violaciones y de prevención de amenazas para satisfacer las necesidades de la organización es un componente fundamental para lograr mantener los gastos dentro del presupuesto. Para muchos, la respuesta está en soluciones de seguridad que subcontratan la infraestructura y tareas menores.

Nucleus descubrió que, aunque las compañías están aumentando los gastos en seguridad, aquellas que implementan soluciones en la nube gastan en promedio un 22 % menos que quienes gastan en activos instalados localmente (Nucleus Research, *q23 – Buying intentions survey – security*, febrero de 2016). Muchas firmas están llegando al final de la vida de sus soluciones legacy y se han dado cuenta de que han incurrido en grandes costos y han logrado resultados combinados a lo largo de su implementación. Aún así, en la medida en que las compañías continúan gastando dinero en soluciones locales de seguridad con utilidad y desempeño inconsistentes, muchas están buscando alternativas más eficientes que siguen el ritmo de los cambios en el panorama de las amenazas.

Incluso aunque muchos segmentos del sector de la tecnología han empezado a utilizar soluciones de software como un servicio (Software as a service: SaaS), el modelo de implementación SaaS no ha sido un elemento para las soluciones de seguridad. Anteriormente, los clientes no tenían alternativa viable a los sistemas de seguridad de red instalados localmente que proporcionaban la mejor tecnología pero podían requerir altos costos de capital. Además de la infraestructura, los

compradores pagaban licencias de software y cuotas anuales de soporte y mantenimiento continuo. La seguridad fue lograda por las organizaciones compilando sus propios datos y realizando análisis internos dedicando personal de TI altamente especializado. Este modelo era efectivo en la protección de activos de gran valor pero el panorama de amenazas ha cambiado: los ataques son dirigidos más ampliamente, obligando a las organizaciones medianas a requerir un modelo diferente.

Para que las soluciones de seguridad SaaS sean adoptadas en el sector de las soluciones de seguridad, deben superar dos obstáculos: la reticencia de los clientes a cambiarse a nuevos sistemas de seguridad y la brecha de confianza en la seguridad de un entorno de nube administrado. Los clientes presentados con un cambio en cómo los servicios son brindados por los proveedores pueden elegir no hacer nada o adoptar una nueva capacidad de seguridad. A los clientes reacios se les puede persuadir más fácilmente pues sus recursos limitados se emplean mejor monitoreando el entorno que manteniendo el software. Para los proveedores de seguridad, las soluciones que cubren las necesidades de la organización e incorporan nuevo valor o capacidades superarán la resistencia de los clientes al cambio. Por ejemplo, las soluciones SaaS no requieren de acción por parte del cliente cuando se aplican parches o actualizaciones, simplificando así un proceso complejo y arduo para las implementaciones instaladas localmente.

Para los clientes que están considerando una actualización de su solución actual de recolección de registros, tanto el valor como las capacidades no son a veces suficientes para superar una brecha de confianza en la seguridad de una infraestructura gestionada en la nube. A pesar del beneficio financiero de eliminar o evitar los costos de capital en infraestructura subcontratando sus capacidades de recolección de registros, algunos clientes aún percibirán que sus datos y procesos de negocios sensibles están más expuestos en un entorno en la nube. Sin embargo, las opciones de industria están madurando rápidamente y los proveedores comienzan a ofrecer alternativas basadas en la nube con características a la par de las implementaciones instaladas localmente. Más aún, Nucleus descubrió que los sistemas de seguridad en la nube con frecuencia son mejores que los entornos internos, contrario a lo que los clientes podrían creer (Nucleus Research, *Cloud data center security benefits*, noviembre de 2015).

Los clientes tienen una cantidad de opciones frente a ellos con respecto a su tecnología de seguridad de recolección de registros: seguir teniendo una infraestructura instalada localmente, desactualizada y costosa que no puede cubrir las necesidades de seguridad de la compañía, actualizar su sistema e infraestructura instalada localmente para atender mejor sus necesidades, reducir gastos generales

cambiando la infraestructura de recolección de registros por un entorno gestionado, o subcontratar tanto la infraestructura como el personal a un proveedor de servicios de seguridad gestionada.

LA SOLUCIÓN

IBM QRADAR ON CLOUD

IBM QRadar on Cloud es un sistema de fuente de registros y recolección del flujo de la red implementado en un entorno de nube gestionado. Atiende a las organizaciones que buscan subcontratar la implementación y el mantenimiento de su solución de recolección de datos de seguridad de la red. Al implementar QRadar on Cloud, los clientes pueden mantener o expandir sus capacidades de monitoreo desarrolladas internamente a la vez que evitan tareas rudimentarias y permiten a los analistas emplear más tiempo comprendiendo los datos de inteligencia de la última amenaza o aplicando seguridad a los activos existentes. Nucleus espera que los siguientes lanzamientos y actualizaciones del software expandan sus capacidades y presten servicios adicionales a los clientes para satisfacer la variedad de necesidades de seguridad.

Capacidades claves:

- Recolección de datos de fuente de registro hasta 80.000 eventos por segundo (EPS)
- Recolección de flujo de la red hasta 300.000 flujos por minuto
- Actualizaciones automáticas de software
- Servicios de configuración del cliente
- Posibilidad de escalamiento a demanda para atender las necesidades del cliente
- Fuente de alertas X-Force Threat Intelligence para situaciones en desarrollo
- Accesibilidad del buscador web
- Configuración del servicio altamente disponible
- Opcional la adición de servicios gestionados

¿POR QUÉ IBM QRADAR?

Nucleus analizó la experiencia de los clientes de IBM QRadar on Cloud para entender por qué eligieron IBM en lugar de otras soluciones. Como una de las pocas soluciones en proporcionar características de seguridad SaaS, IBM se beneficia de tener la iniciativa y está respaldado por la experiencia desarrollada a través del monitoreo de 15.000 millones de eventos de seguridad a diario para más de 4.000 clientes en sus implementaciones instaladas localmente. Aunque los clientes tenían

varias motivaciones para implementar QRadar on Cloud, las credenciales del servicio de seguridad de IBM fueron un factor que contribuyó.

MODELO DE SUSCRIPCIÓN EN LA NUBE

IBM QRadar on Cloud expande el mercado de posibles clientes prestando sus servicios como un gasto operativo mensual predecible. Los clientes sin solución previa de gestión de fuente de registro, que dudaron debido a la alta inversión inicial de capital y los costos continuos de las soluciones instaladas localmente, son candidatos ideales para aprovechar el sistema de seguridad basado en la nube. Con costos de infraestructura que promedian USD 12.000 por servidor y USD 25.000 por servidor por año para implementaciones de alta disponibilidad, las organizaciones que optan por QRadar on Cloud evitan los gastos iniciales sustanciales y continuos.

Con la gestión de infraestructura delegada al equipo de soporte de IBM, las pequeñas y medianas empresas pueden implementar la solución porque solo incurren en un gasto operacional mensual en base al modelo de suscripción. Además, las compañías más grandes se enfrentan a la posibilidad de instalar costosas soluciones de seguridad localizada de hardware en múltiples ubicaciones y mercados. La integración y la consolidación de estos datos de fuente de registros se suman a la complejidad, algo que las grandes compañías pueden evitar implementando una solución basada en la nube.

El modelo de suscripción también permite a las compañías la flexibilidad de ajustarse en base a sus necesidades de seguridad. Con la velocidad a la que las soluciones de seguridad están cambiando para ir al ritmo de las amenazas, QRadar on Cloud no encierra a los clientes en una determinada tecnología, y así permite la fácil integración de actualizaciones y nuevos servicios. Los clientes dijeron:

- *"El valor de la nube fue varias veces mayor que las opciones instaladas localmente".*
- *"Nos beneficiamos de la nube con intangibles como la gestión de actualizaciones para que nuestra infraestructura esté actualizada y para la facilidad del mantenimiento continuo".*
- *"Ninguna licencia perpetua era una motivación para nosotros.* [Con una solución en la nube] *en el peor de los casos, nos quedamos afuera un año".*
- *"Poder acceder desde cualquier parte es otro gran beneficio para nosotros".*
- *"El espacio evoluciona demasiado rápido como para estar atrapado."*

FLEXIBILIDAD, POSIBILIDAD DE ESCALAMIENTO Y VELOCIDAD DE IMPLEMENTACIÓN

Con IBM QRadar on Cloud, los clientes pueden reunir datos de fuente de registros hasta 80.000 eventos por segundo y 300.000 flujos de red por minuto. Los clientes informaron que la flexibilidad de la nube les permitía proveer solo lo que necesitaban y escalar su implementación si cambiaban sus necesidades. Los clientes pueden escalar su recolección de registros sin instalar infraestructura adicional ni dedicar recursos adicionales para administrar la solución. Los clientes también quedaron impresionados con lo rápido que la solución se pudo configurar y comenzó a reunir registros.

Sumado a esto, los clientes informaron que la solución les dio la flexibilidad de manejar más de 1.000 fuentes y más de 5.000 registros por segundo sin establecer un equipo de gestión interno. Además, la solución solo requería cambios menores de infraestructura, tales como instalar un puerto abierto en el firewall. La velocidad de implementación permitió a los clientes hacer una transición rápida a tareas que agregan valor. La diligencia interna de cuáles fuentes de registros es importante reunir frente a cuáles son ruido ayuda a acelerar el proceso de recolectar información útil una vez que IBM QRadar on Cloud está implementado. Los clientes dijeron:

- *"La decisión interna de ida y vuelta llevó alrededor de un mes. Una vez que nos decidimos por IBM, nos tomó cerca de un día ponerlo en pie y reunir los primeros registros".*
- *"La facilidad de implementación definitivamente fue uno de los mayores beneficios para nosotros".*
- *"Teníamos a una o dos personas trabajando en la implementación —ni siquiera a tiempo completo— para que hicieran la configuración técnica del gateway y la conexión a la nube".*
- *"Teníamos dos muchachos trabajando durante dos meses para perfeccionar las fuentes de registros y ajustar los registros que no hacían ruido".*

EQUIPO IBM SECURITY

IBM QRadar on Cloud está respaldado por expertos de seguridad de IBM y permite que los clientes dediquen su energía a otras tareas en lugar de a gestionar la solución de fuente de registros. Algunos clientes informaron que su solución anterior les había estado dando cero valor porque el proveedor no había dado suficiente ayuda a su implementación aunque continuaban pagando el soporte. Antes de cambiarse a IBM QRadar on Cloud, los clientes tuvieron discusiones internas sobre la necesidad de realizar una prueba de concepto para la herramienta de gestión de eventos de seguridad pero se dieron cuenta de que IBM brindaba el servicio que ellos

necesitaban y tenía la experiencia para abordar cualquier inconveniente que pudiera surgir.

El equipo de seguridad de IBM puede educar al equipo interno de un cliente sobre qué buscar y qué es sospechoso, poniendo a disposición años de experiencia con la plataforma de IBM QRadar. Los expertos en seguridad de IBM pueden ayudar a los clientes a entender su población de fuentes de registros y a clasificar lo que inicialmente puede ser una cantidad arrolladora de información. Un cliente dijo: *"No teníamos una idea clara de qué eran todas las fuentes de registros disponibles para nosotros en el entorno. Empleábamos el tiempo para conectar el registro y consumirlo solo para descubrir que hacía ruido".*

BENEFICIOS CLAVES

Al implementar y usar IBM QRadar on Cloud, los clientes se benefician de diversos modos. Algunos beneficios son característicos de cualquier implementación en la nube relativa a la contraparte instalada localmente (Nucleus Research, *q65 – Cloud delivers 2.1 times more*, abril de 2016). En donde IBM QRadar on Cloud se diferencia es en su habilidad para aprovechar la experiencia existente que IBM tiene en seguridad para ayudar a los clientes a comenzar a extraer rápidamente valor del producto.

MENORES COSTOS CONTINUOS E IMPLEMENTACIÓN

Como una solución en la nube, IBM QRadar on Cloud elimina o reduce drásticamente los costos en que los clientes incurren inicialmente y de manera continua. Las implementaciones tradicionales instaladas localmente requieren de costos intensivos de hardware. Con frecuencia, los costos adicionales asociados al hardware se pasan por alto, lo que incluye tiempo de análisis, aprovisionamiento y pruebas por parte de asesores o personal interno. Una vez que una compañía introduzca el hardware y compre la licencia perpetua del software, el personal interno de TI, generalmente con habilidades especializadas y costosas, debe gestionar la solución, y todo esto suma costos importantes.

En claro contraste con los costos de implementación locales, IBM QRadar on Cloud evita los costos de infraestructura y asigna a los expertos en seguridad de IBM la gestión de la solución. Además, como la implementación del sistema se puede lograr en cuestión de días en lugar de meses, los clientes evitan los altos honorarios de consultores externos y el tiempo del empleado dedicado a tarea sin valor agregado. La implementación en la nube administrada también elimina la gestión continua aplicando parches y actualizaciones por parte del personal interno. Los clientes evitan el riesgo permaneciendo atrás en la cadencia de actualización del

proveedor y quedándose con una solución que ya no recibe soporte del proveedor. El gasto continuo de una cuota de suscripción mensual predecible disminuye la carga sobre los clientes cambiando la implementación de un gasto de capital, que se debe amortizar, a un gasto operacional. Un cliente observó: *"Una ventaja es que como es una solución en la nube no requerimos de un equipo de gestión. Además, no tenemos que aplicarle parches ni actualizaciones".*

MAYOR PRODUCTIVIDAD DE TI

Con la gestión de soluciones subcontratada a IBM, los clientes pueden dedicar más tiempo al análisis de posibles inconvenientes de seguridad que a la administración de soluciones de seguridad. Nucleus descubrió que el personal de TI del cliente podía usar QRadar on Cloud de modo más eficaz que su solución previa. Los clientes citaron que las características que IBM ha implementado ayudan a agilizar el proceso de administración de registros y a dar a los usuarios rápidamente la información que necesitan. Como resultado, el personal de TI puede identificar y abordar los problemas más velozmente, lo que les permite a ellos dedicar su tiempo a tareas que aportan valor agregado a la compañía, tales como ejecutar simulacros de rutas de ataque, adaptar normas y alertas, y/o registrar y remediar las vulnerabilidades descubiertas. Los clientes dijeron:

- *"Nuestra solución anterior no daba la información correcta, así que nadie la estaba consultando. Con IBM, los usuarios realmente se fijan en la solución y obtienen valor de ella".*
- *"Con la tenencia compartida, podemos ver todos los eventos de todas nuestras ubicaciones y podemos agregar y correlacionar un conjunto de datos mucho mayor, mejorando nuestra analítica".*

SERVICIOS EXTENDIDOS

Los clientes de IBM QRadar on Cloud tienen la opción de expandir los servicios de gestión de seguridad que compran a IBM. Los clientes pueden atender las brechas de habilidades internas externalizando soporte y servicios especializados, tales como monitoreo de fin de semana y respuesta ante emergencias. Nucleus anticipa que IBM continuará expandiendo servicios con subsiguientes lanzamientos del producto hasta incluir opciones de almacenamiento de datos, estudios forenses de redes usando tecnología de captura del paquete completo y respuesta ante incidentes. Como resultado, IBM se está posicionando para satisfacer todas las necesidades de seguridad del cliente. Un cliente dijo: *"La funcionalidad SIEM* [gestión de eventos e información de seguridad] *para usar dentro de las instalaciones es básicamente lo mismo que en la nube. Dado que nuestra infraestructura en las instalaciones tiene varios años, nos gustaría ver paridad en las capacidades de seguridad de la nube".*

MEJORES PRÁCTICAS

IBM QRadar on Cloud puede ser el paso inicial para muchas compañías en el traspaso de sus soluciones de seguridad a la nube. A medida que más firmas se vayan dando cuenta de que su sistema de seguridad es solo tan bueno como su proveedor y el personal que lo gestiona, la necesidad de mantener las soluciones en las instalaciones disminuirá. En una encuesta de profesionales de seguridad de TI, Nucleus descubrió que las compañías con estrategia de nube gastaban en promedio el 22 % menos en tecnologías de seguridad en relación con aquellas que no se han pasado a la nube (Nucleus Research, *q23 – Buying intentions survey – security*, febrero de 2016). La tendencia indica que las compañías desearán expandir sus implementaciones de nube y abandonar los costosos sistemas legacy. Como resultado, IBM QRadar on Cloud está posicionado para brindar servicios de seguridad adicionales a los clientes a medida que el producto madura.

IBM QRadar on Cloud ya ofrece configuraciones para los clientes que optan por implementar sus capacidades de flujo de red y recolección de registros en un entorno híbrido. De la mano del agnosticismo de la configuración, IBM QRadar es agnóstico con respecto al tamaño del cliente. Con la nube, IBM puede brindar servicios de recolección de datos de seguridad a un rango más amplio de compañías, particularmente a las organizaciones pequeñas y medianas que han estado reacias a implementar una solución instalada localmente. El límite superior de tráfico que QRadar on Cloud puede capturar es 80.000 eventos por segundo, pero considerar que algunos clientes tienen más de 600 ubicaciones en todo Estados Unidos y tienen todas sus necesidades cubiertas significa que la tecnología puede satisfacer las necesidades de la mayoría de los clientes, grandes y pequeños.

CONCLUSIÓN

Nucleus descubrió que IBM QRadar on Cloud aporta valor a los clientes eliminando la necesidad de la supervisión de personal de TI y hardware costoso, implementando velozmente -cuyo resultado es la valorización más rápida- y ofreciendo un rango creciente de servicios de seguridad adicionales en la nube. Los clientes existentes informaron que hacer la transición de sus capacidades de recolección de fuentes de registro de un gasto de capital a un gasto operativo mensual los ha ayudado a alcanzar una valorización más rápida que las soluciones tradicionales instaladas localmente. Cuando más compañías comprenden los beneficios de dejar su infraestructura vieja y posiblemente ya caduca y moverse a un entorno de nube administrado, IBM QRadar on Cloud ofrece un camino creíble hacia adelante por parte de un líder en tecnología de seguridad bien establecido.