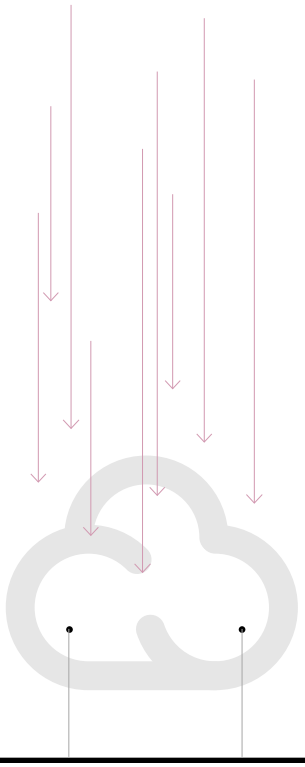
¿LE DEBERÍAMOS TEMER A LA NUBE?

Podría ser la clave de la seguridad

EBOOK

5

TABLA DE CONTENIDO

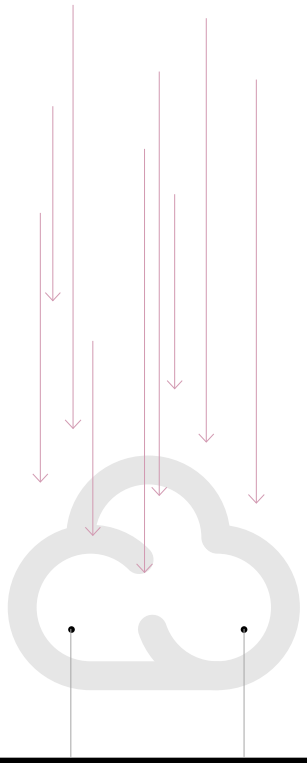


¿ES LA NUBE NUESTRO MAYOR RIESGO EN SEGURIDAD O NUESTRA MAYOR OPORTUNIDAD?

¿CUÁL ES EL COSTO REAL DE UNA VIOLACIÓN DE DATOS?

¿ES LA NUBE INSEGURA O SOMOS NOSOTROS LOS INSEGUROS?

Es un temor que muchas organizaciones tienen: una violación importante de la seguridad en la que los datos sensibles de consumidores se ven comprometidos y la organización enfrenta no sólo una grave responsabilidad sino también la pérdida del valor de marca. Podría adoptar la forma tanto de un ataque en un centro de cómputo tradicional como de un ataque en la nube. Sin embargo, el primero es un escenario más realista. Mientras que las violaciones de datos son posibles en la nube, los ataques a los centros de cómputo tradicionales son más comunes.



¿ES LA NUBE NUESTRO MAYOR RIESGO AD O YOR AD?

¿CUÁL ES EL COSTO REAL DE UNA VIOLACIÓN DE DATOS?

¿ES LA NUBE INSEGURA O SOMOS NOSOTROS LOS INSEGUROS?

CERRAR X

$3.5
MILLONES

El costo financiero de una violación de datos va en aumento. El costo promedio de una violación de datos aumentó un 15% durante el último año, a US$ 3,5 millones.[1]

Las violaciones de datos suelen causar una pérdida de clientes, y esta deserción anormal es particularmente grave en los sectores farmacéuticos, de servicios financieros y salud.[2]

1, 2 Ponemon Institute (patrocinado por IBM), *2014 Cost of Data Breach Study: Global Analysis, mayo de 2014.*

ones
la
bles de
os y la
rave
dida
a
tro de
aque en
un
e las
n la

nunes.

¿ES LA NUBE NUESTRO MAYOR RIESGO EN SEGURIDAD O NUESTRA MAYOR OPORTUNIDAD?

¿CUÁL ES EL COSTO REAL DE UNA VIOLACIÓN DE DATOS?

¿ES LA NUBE INSEGURA O SOMOS NOSOTROS LOS INSEGUROS?

CERRAR X

250 ALTOS EJECUTIVOS DE TI Y NEGOCIOS

2% EXPERIMENTARON UNA VIOLACIÓN DE SEGURIDAD RELACIONADA CON CLOUD

De 250 tomadores de decisiones de TI y negocios entrevistados en el Reino Unido, sólo 2% dijo haber experimentado una violación de seguridad relacionada con Cloud.[3]

3 The Cloud Industry Forum, *"Cloud FUD fails to match up with experiences, says CIF,"* comunicado de prensa, septiembre de 2014.

ones
la
bles de
os y la
rave
dida
a
tro de
aque en
un
e las
n la

hunes.

Cuando uno planifica pasarse a la nube y administrar un entorno híbrido, la seguridad es una preocupación importante. Pero el entorno Cloud no es necesariamente menos seguro que un entorno tradicional. De hecho, sería posible ofrecer una seguridad aún mayor en un entorno de nube híbrida porque ofrece oportunidades nuevas y avanzadas.

En este e-book descubrirá cómo los hackers están usando las tácticas tradicionales de una nueva manera para atacar la nube. También verá cómo la nube puede ayudarlo a aumentar la seguridad con enfoques innovadores, diseñados para detectar amenazas mucho antes de que pongan en peligro a su empresa.

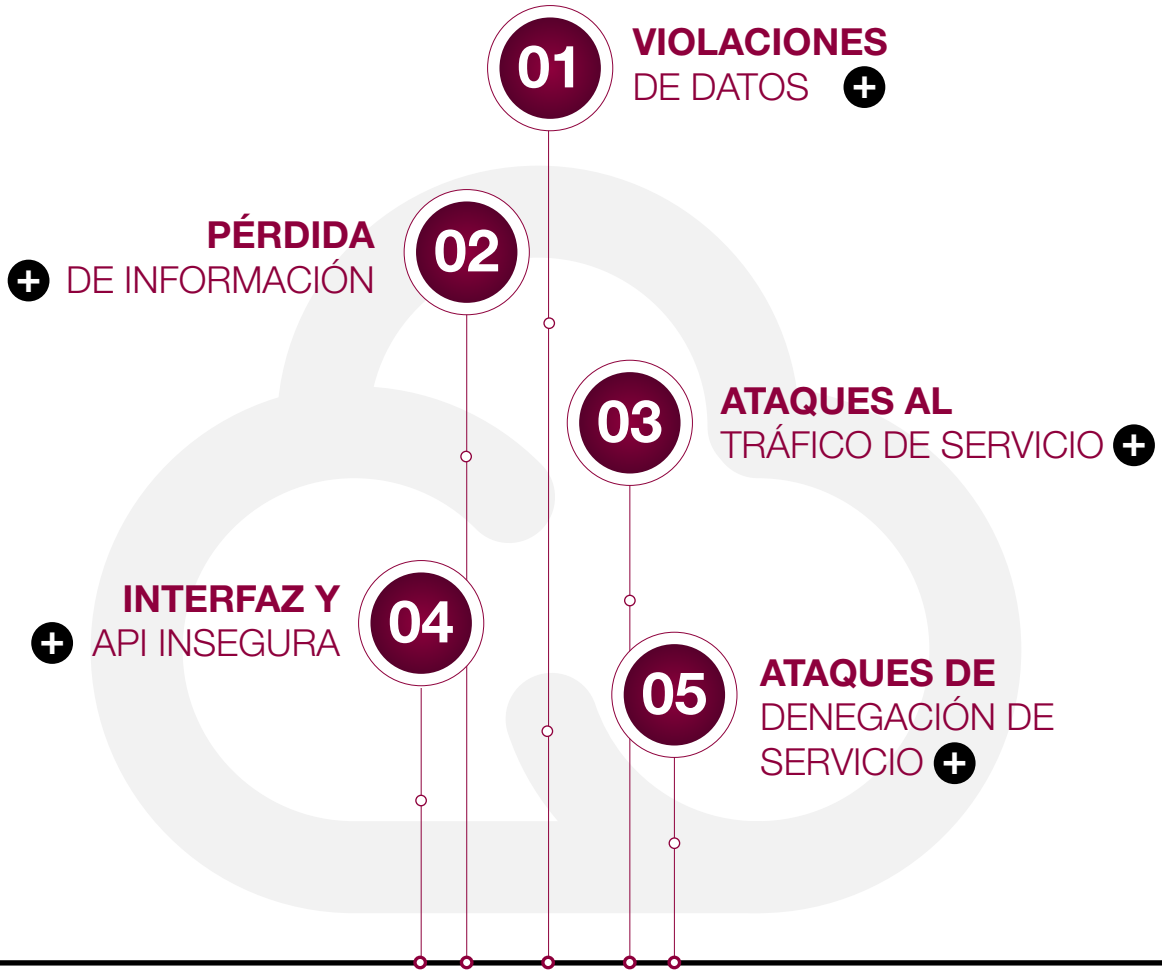
5

LAS 5 PRINCIPALES AMENAZAS DE SEGURIDAD DE HOY:
amenazas viejas, entorno nuevo.

Nuestros temores por la seguridad en la Cloud pueden tener más asidero en el escenario cambiante de las amenazas –los “botnets”, las amenazas persistentes avanzadas y el malware dinámico de nuestro mundo– que en la propia tecnología Cloud.

De hecho, no hay nada fundamental en la nube que la haga más vulnerable que un entorno tradicional. Con cada nueva innovación en computación, los hackers han explotado nuevas vulnerabilidades para lanzar ataques, y la nube es simplemente su objetivo más nuevo. Conforme más cargas de trabajo pasan a la nube, aumentan los datos, y los hackers apuntan precisamente adonde están los datos. En este momento, están usando tácticas tradicionales de nuevas maneras para infiltrarse en un nuevo entorno.

Armamos una lista de las cinco principales amenazas y recomendamos cómo protegerse contra cada una.



Violaciones de datos

1

CERRAR X

01 VIOLACIONES DE DATOS

Su proveedor Cloud puede no alertarlo si hay un ingreso no autorizado a sus servidores

Los hackers están usando tácticas sofisticadas para sustraer datos en la nube, tal como lo hacen en otros entornos, pero están encontrándose con enfoques de seguridad Cloud sofisticados. Si los datos están cifrados solo durante una parte de su recorrido Cloud, quedan expuestos a violaciones. Pero la violación puede prevenirse si los datos se cifran durante todo el recorrido Cloud, hasta que son procesados por la aplicación autorizada.

Recomendación: Responda rápidamente

Debe responder rápidamente ante una violación de datos: la velocidad y habilidad son factores críticos, y cada minuto que pasa cuenta. No obstante, como las leyes de protección contra violaciones varían según el estado y el país, puede ser que el proveedor Cloud no esté obligado a alertarlo cuando se produce una amenaza a la seguridad. Para limitar la interrupción de sus operaciones, la pérdida de datos, complicaciones de cumplimiento y el daño a su reputación corporativa, necesita tener un plan de respuesta a las violaciones de datos que evalúe rápidamente la fuente del problema y permita empezar a mitigar de inmediato cualquier daño adicional. Una solución posible es un plan que implementa un sistema unificado de respuesta a las violaciones, en conjunto con consultores, para minimizar el efecto de un incidente de seguridad y prevenir violaciones de datos en el futuro. Este sistema debería supervisar su entorno de TI 24x7.

Pérdida de información

2

CERRAR X

02 PÉRDIDA DE INFORMACIÓN
El riesgo de una eliminación accidental de datos

Muchos sectores tienen una preocupación comprensible por este riesgo, ya que ante una pérdida sustancial de información una empresa podría llegar a tener que cerrar sus puertas. En la nube, las causas potenciales de la pérdida de datos pueden ser más expansivas que en un entorno tradicional, donde las fallas de hardware o sistemas suelen ser las culpables. La pérdida de información en la nube puede ser causada por error del proveedor de servicio Cloud, eliminación accidental de máquinas virtuales, corrupción de archivos y corrupción de discos virtuales internos, entre otras causas.

Recomendación: Foco en seguridad de puntos terminales

Para evitar esto, necesita una solución de prevención de pérdida de información que se concentre en mejorar la seguridad de los puntos terminales. La solución que elija debe proteger los datos sensibles en cada punto en que se acceda, se almacene o transmita la información en los dispositivos de punto terminal. Una solución que prevenga el acceso a datos en caso de robo o pérdida de un dispositivo, cifre el e-mail y los mensajes instantáneos y bloquee el comportamiento no autorizado y abusivo le dará una gran protección.

Ataques al tráfico de servicio

CERRAR X

03 ATAQUES AL TRÁFICO DE SERVICIO
Sus servicios pueden estar comprometidos

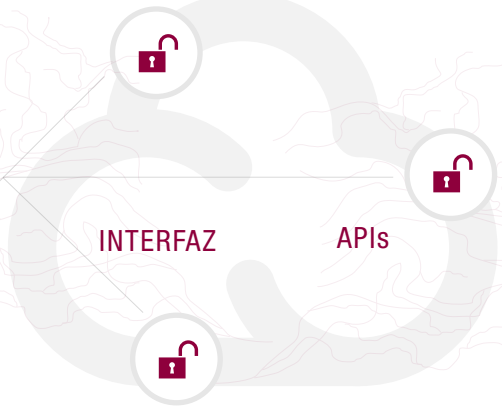
Hace unos años, un bug de cross-site scripting (XSS) dio a los hackers pase libre a las credenciales de un sitio web, y se aprovecharon de la confianza que la compañía se había ganado, para perjudicar a los clientes. En la nube, los hackers pueden crear caos, manipular datos y redirigir a los clientes a sitios ilícitos.

Los ataques XSS como este existen, entre otros motivos, porque los desarrolladores confían en los usuarios. Los desarrolladores pueden pensar que los usuarios nunca realizarán acciones maliciosas, y crean aplicaciones sin filtros para bloquear la información ingresada por los usuarios. Otro motivo para la frecuencia de este tipo de ataques es que tienen muchas variantes. A veces, una aplicación que trata como es debido de filtrar scripts maliciosos se confunde y permite el acceso de un script, abriendo la puerta a los ataques.

Recomendación: La solución: codificación de salida contextual o escape

La defensa primaria contra XSS es la codificación de salida contextual o escape. Es posible usar varias técnicas de escape, dependiendo de dónde debe colocarse el string no confiable dentro de un documento HTML, incluso codificación de entidad HTML, escape JavaScript, escape Cascading Style Sheets (CSS) y codificación URL (o porcentaje). La mayoría de las aplicaciones web que no necesitan aceptar rich data pueden usar el escape para eliminar en gran medida el riesgo de XSS de manera bastante directa. Como la codificación puede ser complicada, se recomienda una librería de codificación de seguridad.

Interfaz y API insegura



4

CERRAR X

04 | INTERFAZ Y API INSEGURA
Acceso malicioso en la nube

Si las interfaces y APIs (interfaces de programación de aplicaciones) no son seguras, los servicios Cloud tampoco lo serán. Estas son algunas de las fallas de seguridad que pueden ocurrir: acceso malicioso o no identificado, autorizaciones incorrectas y contraseñas reutilizables.

Recomendación: Necesita un proveedor seguro

El acceso a los servicios Cloud debe ser seguro en el frente estático y dinámico, y eso al fin de cuentas equivale a elegir a un proveedor de servicios Cloud que le ofrezca seguridad. El proveedor debe captar en forma continua –y proporcionar toda la cadena de procedencia– el acceso a cualquier servicio cloud, comenzando por la raíz de confianza del hardware para el entorno runtime. El acceso seguro mismo puede establecerse a través de seguridad multinivel (MLS), que incluye control de acceso obligatorio (mandatory access control, MAC).

Ataques de denegación de servicio

5

CERRAR X

05 ATAQUES DE DENEGACIÓN DE SERVICIO
El mercado negro de la nube

No es inusual que los proveedores de servicios cloud se vean comprometidos por ataques distribuidos de denegación de servicio (DDoS) que consumen el tiempo, los recursos y la potencia de procesamiento de los clientes. En la nube, las máquinas virtuales son atacadas como zombies y usadas para lanzar los ataques. Los hackers también tienen un "mercado negro en la nube", en el que ofrecen DDoS como un servicio. Una clave para prevenir estos ataques es la supervisión integral de las cargas de trabajo.

Recomendación: Su mejor defensa: Interceptar y eludir

Tan pronto como ocurra un ataque, el DDoS entrante y el DDoS saliente deben ser interceptados y eludidos. Esto significa proporcionar una supervisión continua del entorno Cloud y emitir alertas tempranas para aquellos sistemas físicos y máquinas virtuales que fueron atacadas como zombies. Un proveedor de servicios Cloud también debe bloquear el ataque DDoS saliente que podría ser lanzado por estas máquinas saboteadas (y suspenderlo una vez detectado).

LA PRÓXIMA GENERACIÓN EN SEGURIDAD CLOUD

Aunque los hackers están usando métodos tradicionales para atacar la nube, los métodos de seguridad tradicionales probablemente no puedan detener los ataques. Anteriormente, algunos proveedores Cloud aplicaban controles estáticos, delimitados por el perímetro, como firewalls y sistemas de protección contra intrusiones (IPS), con capas adicionales de defensa, suponiendo que múltiples capas integradas proporcionan una defensa superior.

Pero este es el modelo tradicional de la seguridad, que puede ser que ya no brinde la mayor seguridad posible, porque presenta tres vulnerabilidades clave:

- Numerosos controles de la seguridad pueden llevar a una postura fragmentada de la seguridad, “overhead” en la gestión de seguridad y un flujo interminable de alertas.
- Los ataques a la seguridad son sofisticados y pueden saltar más fácilmente a la generación actual de controles estáticos de la seguridad.
- Los atacantes pueden explotar rápidamente las transformaciones de plataformas, como entornos definidos por software, para sacar provecho.

UN NUEVO PARADIGMA DE LA SEGURIDAD

Para combatir verdaderamente las amenazas actuales, se necesitan medidas de seguridad que eliminen estas deficiencias. Al pasar cargas de trabajo de alto valor y específicas de industria al entorno Cloud, debe incorporar la seguridad correcta desde el comienzo. Supervisar quién accede a los datos sometidos a regulaciones no sólo será crítico para el cumplimiento regulatorio sino también para proporcionar las garantías de seguridad que usted y sus clientes esperan.

Nuevas exposiciones

Las nubes públicas también tienen ciertas exposiciones que los nuevos enfoques de seguridad deben tener en cuenta. Esto puede intensificar las preocupaciones de seguridad:

- Compartir “cajas negras” en nubes puede reducir la visibilidad y el control y aumentar el riesgo de accesos y divulgaciones no autorizadas.
- Una compatibilidad limitada con la infraestructura de seguridad empresarial existente puede restringir la adopción para aplicaciones críticas para la misión.
- La experiencia limitada y el bajo grado de aseguramiento pueden generar dudas sobre la confiabilidad Cloud (disponibilidad operativa, perspectiva de largo plazo).
- Las regulaciones en materia de privacidad y rendición de cuentas pueden prevenir la adopción de Cloud para ciertos datos y en ciertas geografías.

ENFOQUES INNOVADORES DE LA SEGURIDAD

Tres nuevos y avanzados enfoques de la seguridad pueden ayudarlo a fortalecer sus entornos Cloud contra las amenazas de seguridad tradicionales y nuevas. Juntos, la seguridad contextual de granularidad fina, la procedencia y el método conocido como “honey pot” pueden proporcionar mayor visibilidad, supervisar datos, ubicaciones y accesos, y satisfacer el cumplimiento regulatorio.

SEGURIDAD CONTEXTUAL FINA

PROCEDENCIA

HONEY POT

SEGURIDAD CONTEXTUAL FINA

Obtenga una visión 360° de su escenario de amenazas Cloud

Como muchas violaciones de la seguridad de Cloud pueden ser el resultado de cargas de trabajo mal supervisadas, la seguridad contextual de granularidad fina, diseñada para dar una visión 360° del panorama de cargas de trabajo y amenazas en la nube, es crítica para proteger sus datos en ese entorno. Considerémosla una defensa perimetral para el entorno virtual.

CÓMO FUNCIONA ⊕ | CUÁL ES EL BENEFICIO ⊕

Seguridad contextual de granularidad fina

SEGURIDAD CONTEXTUAL FINA

Obtenga una visión 360° de su escenario de amenazas Cloud

Como muchas violaciones de la seguridad en Cloud pueden ser el resultado de cargas de trabajo mal supervisadas, la seguridad contextual de granularidad fina, diseñada para dar una visión 360° del panorama de cargas de trabajo y amenazas en la nube, es crítica para proteger sus datos en ese entorno. Considerémosla una defensa perimetral para el entorno virtual.

CÓMO FUNCIONA ⊕ | CUÁL ES EL BENEFICIO ⊕

FASE **1** ***Supervisar y destilar.*** Aquí, casi todos los aspectos de las cargas de trabajo están instrumentados, incluso los datos, las aplicaciones y los procesos de negocio, para supervisar y recopilar datos relacionados con la seguridad. Estas observaciones construyen una visión 360° de la carga de trabajo en la nube.

FASE **2** ***Correlacionar y predecir.*** La postura de seguridad se predice sobre la base de esta visión 360°, los acuerdos de nivel de servicio (SLA) que rigen la carga de trabajo en la nube y la evaluación de alternativas de respuesta. Aquí, se usan las técnicas de minería de datos, aprendizaje de máquina y computación cognitiva para asistir a los administradores de la seguridad con métodos automatizados para construir modelos, supervisar el comportamiento normal y señalar anomalías.

FASE **3** ***Adaptar y prevenir.*** En esta fase, se insertan controles de seguridad aprovechando la agilidad de cómputo, almacenamiento y redes definidas por software, para aumentar la carga de trabajo del atacante. Este enfoque puede elevar las apuestas del defensor en la carrera por la seguridad.

Cómo funciona

SEGURIDAD CONTEXTUAL FINA

Obtenga una visión 360° de su escenario de amenazas Cloud

Como muchas violaciones de la seguridad en Cloud pueden ser el resultado de cargas de trabajo mal supervisadas, la seguridad contextual de granularidad fina, diseñada para dar una visión 360° del panorama de cargas de trabajo y amenazas en la nube, es crítica para proteger sus datos en ese entorno. Considerémosla una defensa perimetral para el entorno virtual.

CÓMO FUNCIONA ⊕ | CUÁL ES EL BENEFICIO ⊕

- Le da la seguridad de la comunicación entre dominios, sabiendo que son totalmente confiables y están totalmente registrados y auditados
- Facilita la rápida migración de cargas de trabajo con la mínima interrupción
- Le permite reaccionar a violaciones SLA, identificar actividades de largo plazo causadas por amenazas bajas y progresivas, y aislar actividad de dispositivos infrecuente e imprevista

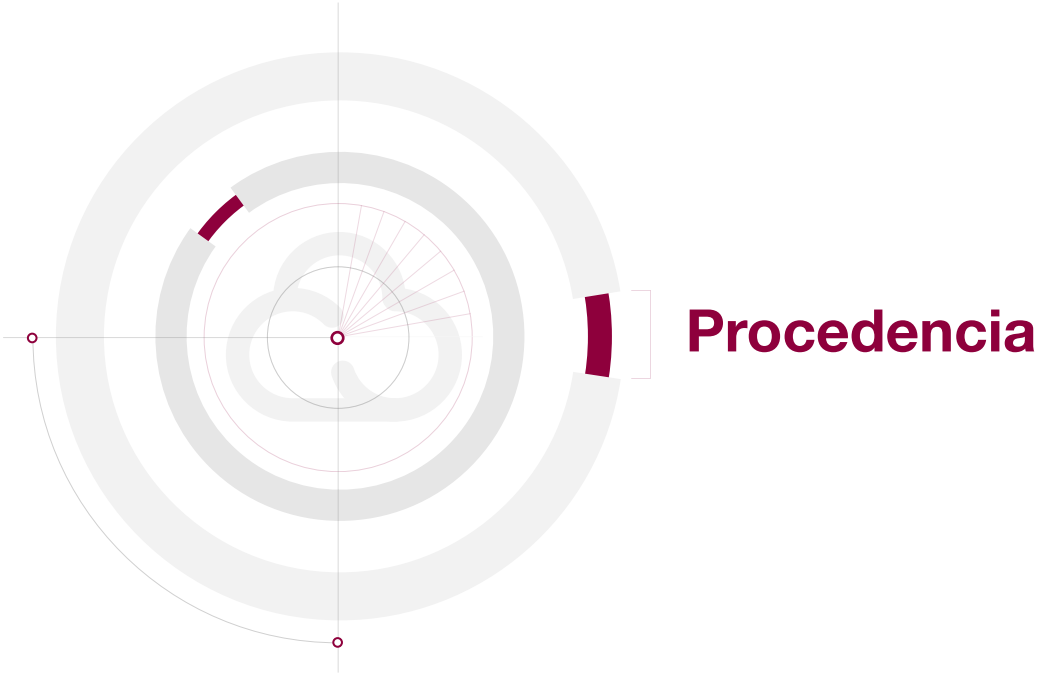
EXPLORAR LA PROCEDENCIA

Cierre el círculo de las amenazas al cumplimiento

La procedencia, un término que se toma prestado de bellas artes, describe cómo un objeto llegó a adquirir su estado actual. Por ejemplo, la procedencia de la Mona Lista establece quién la pintó y en qué época, cuándo fue rasgada y restaurada, y en qué museos se exhibió. En la tecnología, la procedencia son metadatos que representan el linaje de una aplicación y muestran dónde se desarrolló, dónde se emparchó o actualizó, y quién la usó y para qué fin. También puede ser los metadatos para un dato en términos de cuándo se creó y cuándo, cómo, dónde y por quién fue alterado.

CÓMO FUNCIONA ⊕

CUÁL ES EL BENEFICIO ⊕



Procedencia

SEGURIDAD CONTEXTUAL FINA ⊕

PROCEDENCIA

HONEY POT ⊕

EXPLORAR LA PROCEDENCIA

Cierre el círculo de las amenazas al cumplimiento

La procedencia, un término que se toma prestado de bellas artes, describe cómo un objeto llegó a adquirir su estado actual. Por ejemplo, la procedencia de la Mona Lista establece quién la pintó y en qué época, cuándo fue rasgada y restaurada, y en qué museos se exhibió. En la tecnología, la procedencia son metadatos que representan el linaje de una aplicación y muestran dónde se desarrolló, dónde se emparchó o actualizó, y quién la usó y para qué fin. También puede ser los metadatos para un dato en términos de cuándo se creó y cuándo, cómo, dónde y por quién fue alterado.

CÓMO FUNCIONA ⊕ | CUÁL ES EL BENEFICIO ⊕

La procedencia vincula los datos de registro y auditoría de todo el mapa para proporcionar la historia completa de un evento. Rastrea los datos y procesos que viajan por la nube para que usted pueda conocer el cómo, qué, dónde, cuándo, quién y porqué de casi cualquier amenaza.

Cómo funciona

EXPLORAR LA PROCEDENCIA

Cierre el círculo de las amenazas al cumplimiento

La procedencia, un término que se toma prestado de bellas artes, describe cómo un objeto llegó a adquirir su estado actual. Por ejemplo, la procedencia de la Mona Lista establece quién la pintó y en qué época, cuándo fue rasgada y restaurada, y en qué museos se exhibió. En la tecnología, la procedencia son metadatos que representan el linaje de una aplicación y muestran dónde se desarrolló, dónde se emparchó o actualizó, y quién la usó y para qué fin. También puede ser los metadatos para un dato en términos de cuándo se creó y cuándo, cómo, dónde y por quién fue alterado.

CÓMO FUNCIONA ⊕ | CUÁL ES EL BENEFICIO ⊕

- Le permite aislar la información contextual correcta y eliminar potenciales interferencias de cargas de trabajo adyacentes que no tienen nada que ver con la carga en cuestión
- Lo ayuda a administrar y facilitar el cumplimiento porque le da una pista de auditoría clara, completa y totalmente autenticada
- En un entorno en el que las regulaciones y las normas de seguridad cambian entre estados y países, puede ayudarlo a determinar dónde falla la seguridad y dónde causa demoras en el recorrido de los datos

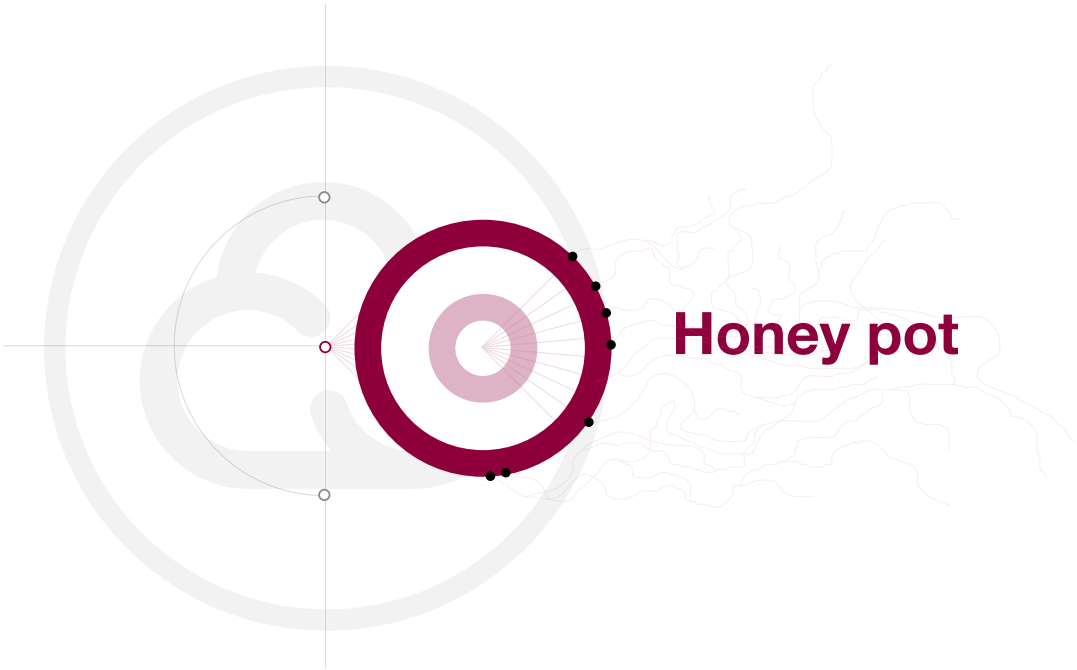
Cuál es el beneficio

PRESENTAMOS A HONEY POT

Un ardid para confundir a los hackers

“Honey pot” es como se denomina a un entorno de computación falso, una trampa, expresamente construido para atrapar a hackers y sus métodos de ataque nuevos o no convencionales. Da a los hackers un campo de juego (creen que es real) en donde pueden desatar sus amenazas, y revelan sus métodos e identidades, antes de que lleguen al entorno de computación real. El resultado es la cuarentena eficaz del malware, junto con la satisfacción (y diversión) más intangible, asociada a ser más listos que los hackers más astutos.

CÓMO FUNCIONA ⊕ CUÁL ES EL BENEFICIO ⊕



PRESENTAMOS A HONEY POT

Un ardid para confundir a los hackers

"Honey pot" es como se denomina a un entorno de computación falso, una trampa, expresamente construido para atrapar a hackers y sus métodos de ataque nuevos o no convencionales. Da a los hackers un campo de juego (creen que es real) en donde pueden desatar sus amenazas, y revelan sus métodos e identidades, antes de que lleguen al entorno de computación real. El resultado es la cuarentena eficaz del malware, junto con la satisfacción (y diversión) más intangible, asociada a ser más listos que los hackers más astutos.

CÓMO FUNCIONA + | CUÁL ES EL BENEFICIO +

El método conocido como "honey pot" redirige el tráfico a un sitio falso dentro de un entorno bien controlado y en cuarentena. Luego genera un informe detallado, diseñado para revelar la identidad del objetivo, archivos, hackers y amenazas. Los ataques enviados por email o en formas inesperadas o poco convencionales (como por sistema de aire acondicionado, HVAC) nunca deben llegar a la red con una defensa del tipo honey pot.

PRESENTAMOS A HONEY POT

Un ardid para confundir a los hackers

"Honey pot" es como se denomina a un entorno de computación falso, una trampa, expresamente construido para atrapar a hackers y sus métodos de ataque nuevos o no convencionales. Da a los hackers un campo de juego (creen que es real) en donde pueden desatar sus amenazas, y revelan sus métodos e identidades, antes de que lleguen al entorno de computación real. El resultado es la cuarentena eficaz del malware, junto con la satisfacción (y diversión) más intangible, asociada a ser más listos que los hackers más astutos.

CÓMO FUNCIONA ⊕ | CUÁL ES EL BENEFICIO ⊕

- Le da la tranquilidad de saber que el malware será puesto en cuarentena antes de llegar a su infraestructura
- Lo hace menos vulnerable a métodos de ataque no convencionales porque este enfoque detecta los ataques que otros enfoques podrían no detectar
- Lo ayuda a acelerar el análisis de amenazas con información precisa en un formato fácil

CÓMO PONER ESTOS ENFOQUES A TRABAJAR PARA SU EMPRESA

A la hora de determinar qué enfoque de seguridad es el correcto para su organización, probablemente lo mejor sea optar por un enfoque de valor en riesgo, considerando el valor de la información y el valor de la infraestructura. La evaluación también debe ser realizada en términos de nivel de amenaza.

Para aprovechar estos nuevos enfoques, también podrá ser necesario agregar nuevas herramientas y habilidades, que incluyen:

- Metodología y habilidades de evaluación de riesgo y valor
- Generación de procedencia y captación, integración y fusión
- Sondeo y monitoreo proactivo; profunda introspección y modelado de comportamiento de sistema, usuario y carga de trabajo
- Aprovechar su entorno definido por software para configurar dinámicamente, poner en cuarentena y definir un perímetro de granularidad fina
- Auditoría continua de ciclo cerrado; aseguramiento continuo y remediación continua

Más información

Para ver más información sobre otros temas relacionados con Cloud e iniciar el recorrido, vea los **“Pasos para la experticia en Cloud”.**

ibm.com/cloud/expertise

Para que un especialista le cuente más sobre la nube híbrida, **haga click aquí.**

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Producido en los Estados Unidos de América
Noviembre de 2014