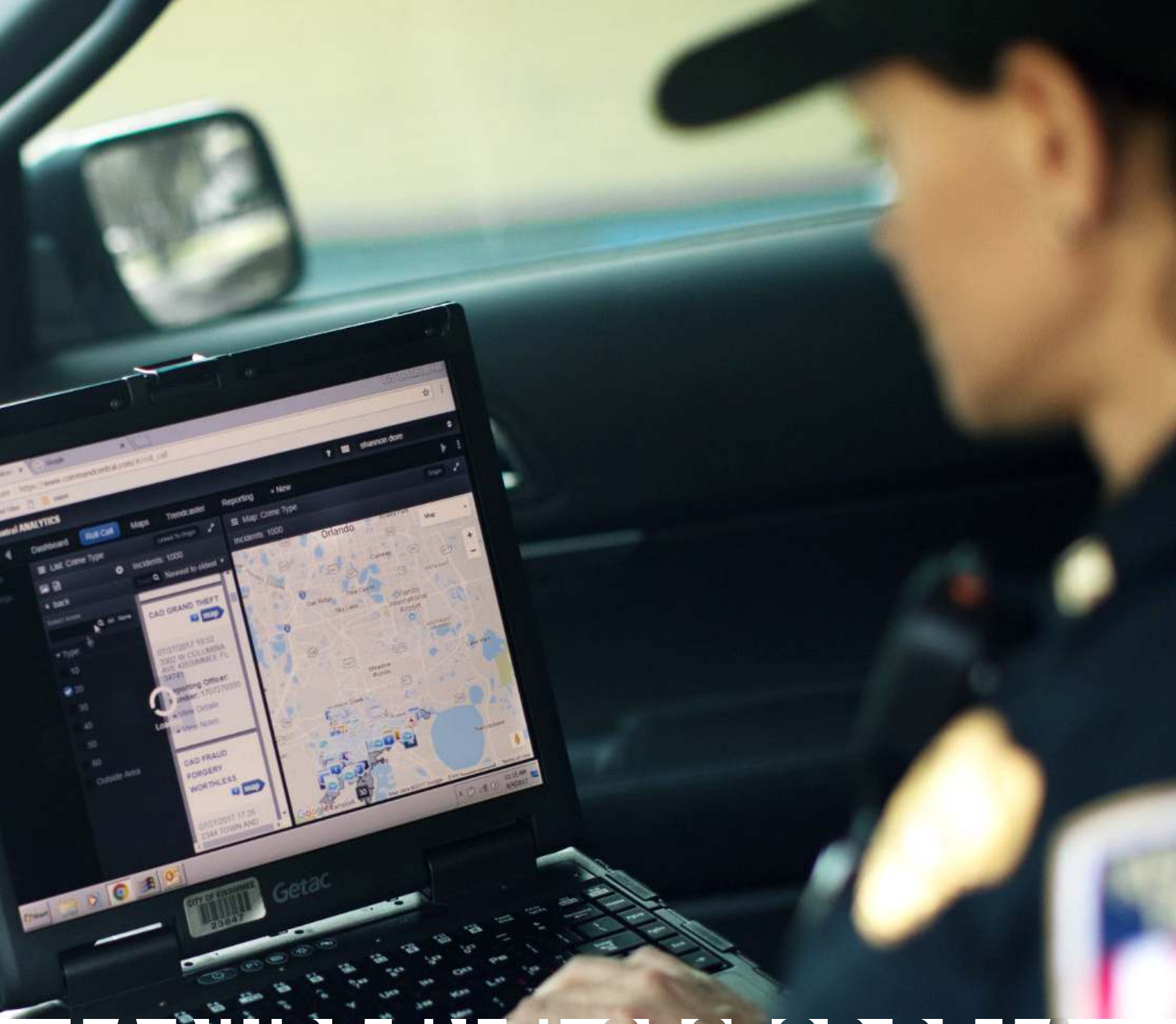

LA NUBE EN EL SECTOR DE LA SEGURIDAD PÚBLICA

LO QUE DEBE SABER AHORA

MOTOROLA SOLUTIONS

1

¿POR QUÉ USAR LA NUBE Y POR QUÉ AHORA?

La informática basada en la nube se utiliza hace años en el ámbito empresarial y, actualmente, suscita mucho más interés entre los organismos gubernamentales por distintos motivos, entre ellos, ahorro de costos, agilidad y simplificación de redes. Sin embargo, presenta ciertos desafíos especiales en torno a los requerimientos y los datos. Entonces, ¿cuál es el modo más eficaz de utilizar soluciones basadas en la nube para el cumplimiento de la ley y por qué motivo debería pasarse a la nube ahora?

Si bien el costo es un factor importante, la mayor ventaja que observará en sus operaciones es la capacidad que tiene la nube de mejorar drásticamente la utilización y administración general de los datos. Y esto, en última instancia, se refleja en una mayor protección de los ciudadanos.

EXPLOSIÓN DE DATOS

Los datos, en todas sus formas, están creciendo exponencialmente. Según Cisco, el tráfico anual de IP a nivel mundial alcanzará los 3,3 zettabytes (ZB) por año para el 2021, o 278 exabytes (EB) por mes. Como referencia, solo en 2016, la tasa de proyección anual del tráfico de IP a nivel mundial fue de 1,2 ZB por año, o 96 EB por mes (1 zettabyte equivale a 1 billón de gigabytes). En una era digital, la policía se siente desbordada ante la disponibilidad de datos estructurados y, cada vez más, datos no estructurados, como videos, medios sociales, datos de sensores y correo electrónico. Este tsunami de datos dificulta la eficacia del trabajo. Por ejemplo, una orden de allanamiento típica suma aproximadamente 3 terabytes de pruebas digitales y, sin las herramientas adecuadas, los investigadores pueden tardar cuatro semanas en revisar apenas 1 terabyte.[1] Además, deben procesar los tradicionales datos estructurados, como órdenes de detención, antecedentes de arrestos y expedientes penales.

El auge de la Internet de las Cosas (IoT) también da origen a una serie de capacidades mejoradas de seguridad pública y genera incluso más datos. Lo mismo sucede con los videos tomados con cámaras sujetas al cuerpo, cámaras instaladas en los automóviles, cámaras fijas de vigilancia y, ahora, incluso con drones.
Para poder asimilar toda esta información, se utilizan herramientas analíticas avanzadas que le ayudan a aprovechar al máximo los datos obtenidos. Le permiten combinar y correlacionar datos históricos e información en tiempo real que actualmente se encuentran dispersos en todas las operaciones de seguridad pública. Esto es fundamental para mejorar la seguridad pública. De este modo, la presión es cada mayor para transformar su estrategia de administración de datos y mejorar los sistemas y procesos ya existentes. Las soluciones basadas en la nube pueden y deben desempeñar un papel esencial en esta evolución.

ALGUNAS CIFRAS

1 Zettabyte

=

1 Billón de Gigabytes

1 Zettabyte = 1000 Exabytes

1 Exabyte = 1000 Petabytes

1 Petabyte = 1000 Terabytes

1 Terabyte = 1000 Gigabytes

LA EVOLUCIÓN DE LOS SISTEMAS DE ADMINISTRACIÓN DE DATOS

En la actualidad, la mayoría de los organismos encargados del cumplimiento de la ley siguen dependiendo de sistemas obsoletos y dispares que almacenan información en silos, lo cual les impide obtener e intercambiar información con eficacia donde y cuando más lo necesitan.

Claramente la policía quiere tener acceso en tiempo real a información detallada para poder destinar recursos y combatir los delitos de manera más inteligente y certera. Ahora que las ciudades han comenzado a adoptar nuevos sistemas y tecnologías, se están empezando a ver importantes logros. Por ejemplo, el Departamento de Policía de Chicago (CPD) actualmente está implementando herramientas predictivas y analíticas de manera generalizada tras haber observado resultados iniciales positivos. El alcalde de Chicago Rahm Emanuel y los oficiales de policía creen que la utilización de lo último en TI, incluida la vigilancia por video y la vigilancia policial basada en datos, se ve reflejada en una reducción de los delitos violentos en la ciudad.

Los cambios demográficos en las fuerzas policiales también afectarán el uso generalizado de tecnologías basadas en datos. Para el año 2020, los millennials representarán el 50 % de la fuerza de trabajo.2 Esta generación que ha nacido en la era digital sabe mucho de tecnología y tiene la capacidad de realizar varias tareas a la vez. Los organismos ya notan su influencia, pues utilizan aplicaciones en sus smartphones para asistirlos en sus tareas. Mantenerse actualizado con la tecnología puede servir para mitigar los posibles desafíos en la contratación de personal en el futuro y mejorar la retención de empleados calificados.

El volumen y la velocidad de los datos seguirán en aumento. La nube no solo será realmente útil para manejar esta explosión de datos y brindar potentes herramientas analíticas, sino que, dado que los servicios basados en la nube se consideran una tecnología modular que no requiere una sustitución completa, los departamentos pueden seguir aprovechando las inversiones existentes y, a la vez, continuar aumentando sus capacidades.

Desde la administración de enormes volúmenes de datos hasta la contratación de millennials que esperan contar con las últimas herramientas tecnológicas, la nube es clave para satisfacer las necesidades de la comunidad de seguridad pública en constante evolución.

> **Los cambios demográficos en las fuerzas policiales afectarán el uso generalizado de tecnologías basadas en datos. Para el año 2020, los millennials representarán el 50 % de la fuerza de trabajo.2**

2 ¿QUÉ ES LA NUBE?

La nube adopta un enfoque diferente en cuanto a la compra, administración e implementación de infraestructuras de TI y soluciones de software. En el caso de las soluciones privadas in situ, son los clientes quienes implementan las aplicaciones en sus propios equipos, con lo cual la administración también queda a cargo del cliente. Los clientes son responsables de todo lo concerniente a la disponibilidad del servicio, la durabilidad y seguridad de los datos, la redundancia geográfica y la ampliación, entre otros aspectos.

Por el contrario, las soluciones hospedadas basadas en la nube se ofrecen como un servicio y se implementan en una nube privada, comunitaria o pública en un centro de datos del proveedor del servicio basado en la nube. En este caso, es el proveedor quien administra la infraestructura, que puede funcionar únicamente para una organización o un pequeño grupo de organizaciones (nube privada o comunitaria), o bien puede estar disponible para el público en general o para un grupo de mayor tamaño típicamente dirigido a un sector en particular (nube pública).

Por último, las soluciones híbridas pueden ser una combinación de soluciones in situ privadas y soluciones hospedadas basadas en la nube.

MODELOS DE IMPLEMENTACIÓN DE TECNOLOGÍA

NUBE

Hospedada y completamente administrada por el proveedor de servicios basados en la nube

IN SITU

Centro de datos completamente administrado por el cliente

HÍBRIDA

Combinación de nube e in situ

MODELOS DE IMPLEMENTACIÓN DE LA NUBE

PRIVADA	La infraestructura de la nube funciona únicamente para una organización y su administración está a cargo de un proveedor de servicios basados en la nube. Por lo general, se trata de una infraestructura aislada dentro del centro de datos del proveedor.
COMUNITARIA	La infraestructura de la nube se comparte entre varias organizaciones y admite una comunidad específica con intereses comunes (por ej. misión, requisitos de seguridad, política y consideraciones de cumplimiento).
PÚBLICA	La infraestructura de la nube está disponible para el público en general o para un grupo de mayor tamaño perteneciente a un sector específico.

PROPUESTAS EN LA NUBE

En lo que respecta a las soluciones hospedadas basadas en la nube (ya sea en un entorno de nube privada, comunitaria o pública), existen distintos modelos para la interacción y el consumo de recursos. En términos generales, se clasifican de la siguiente manera: Infraestructura como Servicio (IaaS), Plataforma como Servicio (PaaS) y Software como Servicio (SaaS).

El modelo IaaS proporciona la menor cantidad de recursos de un proveedor de servicios basados en la nube. Los clientes adquieren y consumen infraestructura, que incluye informática, redes y recursos de almacenamiento. Este es el modelo más flexible pero el que exige más trabajo por parte del consumidor, ya que los clientes adquieren capacidades básicas e implementan su propia solución en los recursos de IaaS. Los clientes son totalmente responsables del desempeño de dichas implementaciones.

Más arriba en la pila, el modelo PaaS permite que los consumidores de la nube también adquieran servicios de un proveedor de servicios basados en la nube, en lugar de tan solo adquirir recursos básicos como sucede en el modelo IaaS. Los servicios varían según el proveedor, pero pueden incluir bases de datos, herramientas de administración de contenedores, mensajería, puertas de enlace de API y equilibrio de carga. Con PaaS, dispone de los componentes básicos de su solución. Ahora bien, dado que los servicios y las interfaces varían según el proveedor de servicios basados en la nube, la portabilidad de las aplicaciones desarrolladas utilizando recursos PaaS es mucho menor entre los distintos proveedores de servicios basados en la nube. Aun en el caso de la implementación simplificada de aplicaciones que ofrece PaaS, el consumidor de la nube igualmente necesita realizar una cantidad de trabajo significativa para poder crear soluciones completas.

SaaS ofrece a los consumidores soluciones de software completas en la nube. Los clientes de soluciones SaaS adquieren o alquilan recursos de aplicaciones para resolver directamente un problema. Un ejemplo conocido para todos es Netflix, un proveedor de soluciones SaaS que ofrece a sus clientes una solución completa de streaming de video desarrollada a partir de una serie de aplicaciones de streaming, facturación, administración de cuentas, etc. Para entenderlo mejor, Netflix es un consumidor que contrata PaaS e IaaS en Amazon Web Services (AWS), y utiliza estos recursos y servicios para desarrollar aplicaciones e implementar una solución SaaS que sus clientes le alquilan pagando una tarifa mensual para acceder.

Para la mayoría de los organismos de seguridad pública estatales y locales, las soluciones SaaS serán la alternativa más integral para responder a sus necesidades de vigilancia policial.

MODELOS DE CONSUMO DE LA NUBE

= Administración propia = Administración a cargo de terceros

IN SITU	INFRAESTRUCTURA COMO SERVICIO	PLATFORMA COMO SERVICIO	SOFTWARE COMO SERVICIO
Aplicaciones	Aplicaciones	Aplicaciones	Aplicaciones
Datos	Datos	Datos	Datos
Tiempo de ejecución	Tiempo de ejecución	Tiempo de ejecución	Tiempo de ejecución
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualización	Virtualización	Virtualización	Virtualización
Servidores	Servidores	Servidores	Servidores
Almacenamiento	Almacenamiento	Almacenamiento	Almacenamiento
Redes	Redes	Redes	Redes

3

PROTECCIÓN DE DATOS EN LA NUBE

Al analizar la seguridad de las diferentes tecnologías, es muy importante comprender que las mayores amenazas a las que están expuestos los sistemas de una organización no tienen tanto que ver con el lugar en donde están ubicados los sistemas, sino con su modo de acceso, el método de protección de los datos mientras están en reposo o en tránsito, y el tipo de seguridad de las aplicaciones.

La mayoría de los ataques no están dirigidos a la infraestructura, sino más bien a la capa de aplicaciones a través de ataques por inyección, pérdida de autenticación, control de acceso insuficiente y configuración incorrecta de la seguridad. Todo esto se combina con un nivel inadecuado de registro y supervisión. Y es aquí donde se destacan los proveedores de servicios basados en la nube en conjunto con los proveedores de soluciones SaaS que ofrecen aplicaciones. Si bien las soluciones in situ, en teoría, podrían funcionar igual, el presupuesto destinado a la seguridad de TI de los proveedores de servicios basados en la nube supera ampliamente el presupuesto de cualquier departamento informático, por más grande que sea. Aun así, la seguridad es una cuestión de mitigación de riesgos y análisis de costo-beneficio, y en este sentido, cada modelo de implementación tiene aspectos positivos y negativos.

Las mayores amenazas a las que están expuestos los sistemas de una organización no tienen tanto que ver con el lugar en donde están ubicados los sistemas, sino con su modo de acceso, el método de protección de los datos mientras están en reposo o en tránsito, y el tipo de seguridad de las aplicaciones.

IN SITU

Hay tres áreas principales en donde se destaca la seguridad in situ:

1. Cuando es necesario aislar físicamente un equipo o, por alguna razón, este no deba conectarse a la Internet pública
2. Cuando es necesario, ya sea porque así lo establece una reglamentación de privacidad de datos u otro requisito de cumplimiento normativo, que los datos residan en un área no compatible con la nube
3. Cuando se desea tener un control absoluto de la seguridad.

Sin embargo, control no equivale necesariamente a seguridad. La protección adecuada de las aplicaciones, los datos, los servicios y la infraestructura implica un costo significativo, tanto en términos de gastos de capital como de contratación de recursos de seguridad de TI para configurar y mantener las herramientas de seguridad y la estrategia de protección. Este tiempo y dinero podrían tener un mejor destino: la misión principal de su organización.

NUBE

En el caso de las implementaciones SaaS en la nube, gran parte de la seguridad es responsabilidad del proveedor de servicios basados en la nube (por ej., AWS) y el proveedor de la solución SaaS (por ej., Netflix). Esto permite liberar a los valiosos recursos de seguridad de TI para que se dediquen a controlar quién debería tener acceso a los datos. El conjunto de herramientas que estos proveedores ofrecen simplifica la administración de la seguridad, pues es posible controlar el acceso a los datos y servicios con solo hacer clic. Además, cuenta con interfaces simples para auditar y notificar a los administradores cuando se modifican las configuraciones de seguridad. Estas herramientas administrativas hacen que las configuraciones incorrectas de la seguridad sean prácticamente una cosa del pasado.

La nube también es especialmente valiosa por su resiliencia cibernética y su capacidad de eludir los ataques por denegación de servicio distribuido (DDoS) dirigidos y constantes, como los ataques de Botnets. Si bien los detractores de la nube podrían insinuar que la concentración de información de la nube resulta muy atractiva para los actores maliciosos, solo la nube, por su gran tamaño y magnitud, tiene los recursos necesarios para manejar adecuadamente los ataques a gran escala. Los proveedores de la nube hacen todo lo posible por protegerse de los ataques. Sería casi imposible igualar ese nivel de defensa in situ.

La inteligencia sobre amenazas es otra área en donde se destaca la nube. Los proveedores de servicios basados en la nube tienen herramientas de supervisión extremadamente sofisticadas y es muy probable que sean los primeros en advertir un intento de ataque o vulneración.

Ante la detección, alertan de inmediato al proveedor de la solución o incluso al propio usuario. En un mundo donde los actores maliciosos actúan en conjunto y bien coordinados, es sumamente beneficioso contar con un proveedor de servicios basados en la nube que se encargue de esta tarea. Además, dado que estos proveedores lidian con tantos ataques perpetrados contra otros de sus usuarios, son los primeros en implementar prácticas de seguridad recomendadas según el tipo de patrones de ataque que observan. De este modo, una organización se beneficia de todo lo aprendido de otras organizaciones, que son muchas.

Los proveedores de servicios basados en la nube y los proveedores de soluciones SaaS también permiten eliminar gran parte del trabajo costoso y minucioso que supone la obtención de certificaciones de cumplimiento de seguridad, como las certificaciones DoD, FIPS e ISO, así como el cumplimiento de otros requisitos específicos de cada país. Gracias a estas certificaciones, su departamento de TI no solo tiene la confianza de que la solución es segura, sino que además puede ahorrar tiempo y recursos para destinar fondos del presupuesto a otras actividades.

HÍBRIDA

Para quienes desean aprovechar muchas de las ventajas de seguridad de la nube, pero que prefieren seguir manteniendo cierto control de sus datos, un enfoque híbrido podría ser lo ideal. Las implementaciones de nubes híbridas brindan al cliente distintos grados de control. Por ejemplo, el cliente puede desde controlar las claves de cifrado de datos que aún hay en la nube hasta mantener las claves de cifrado in situ y cifrar datos in situ antes de enviarlos a la nube. En el último ejemplo, todos los datos de la nube se cifran mientras están en tránsito y en reposo mediante la utilización de claves de cifrado que nunca salen de las instalaciones del cliente.

La seguridad híbrida también puede adoptar otras formas. Por ejemplo, los clientes pueden seguir aprovisionando y otorgando credenciales a sus empleados in situ, y luego utilizar esas mismas identidades y credenciales para acceder a una solución SaaS. Esto permite reutilizar las soluciones de administración de acceso e identidad existentes, y también ofrece un único lugar para
agregar o quitar usuarios independientemente de que accedan a una solución in situ o en la nube. Este es apenas un ejemplo de combinaciones de nubes híbridas. Hay otras opciones posibles, en donde el cliente mantiene un control absoluto de lo que tiene in situ y un alto grado de control sobre las partes que existen en la nube.

REFERENCES

1. "Digital age a turning point for policing, says commissioner Leppard," ComputerWeekly, May 14, 2015, http://www.computerweekly.com/news/4500246279/Digital-age-a-turning-point-for-policing-says-commissioner-Leppard
2. "PwC: Millennials at Work" https://www.pwc.com/gx/en/managing-tomorrows-people/future-of-work/assets/reshaping-the-workplace.pdf

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 EE.UU. **motorolasolutions.com**