

## A PUBLIC SAFETY GUIDE FOR EVALUATING CLOUD SOLUTIONS AND BENEFITS TO THEIR OPERATIONS

### WHY FOCUS ON CLOUD?

Cloud computing has been around for years and gaining interest by enterprise and government CIOs for a variety of reasons... lower cost, agility, simplification, etc. Public cloud solutions offer great promise to consumers and businesses alike, and there is a plethora of information published for every industry about cloud advantages and reasons to adopt. Yet, how does cloud best enable public safety control room operations and why consider adoption now? Cost alone is not the core reason public safety agencies should adopt cloud solutions. While cost is an important factor, organisations can benefit even more by cloud solutions to improve their data management throughout their operations resulting in more effective policing.

Data is exploding. Experts now predict that 40 zettabytes of data will be in existence by 2020<sup>1</sup> — and that's just on the Internet.<sup>2</sup> Unstructured data, such as video, social media, sensor data and email is growing at an unprecedented pace. Finding ways to extract meaning from this data is critical for enhancing public safety along with processing the traditional structured data government organisations use such as records management (arrest warrants, jail records, etc.) and criminal files. Unstructured data is placing increasing pressure on agencies to reform their data management strategy and improve legacy systems and processes.

In this digital age, police are swamped in terabytes of data which puts them at risk of becoming less efficient. For example, a typical search warrant nets approximately 3 terabytes of data for digital evidence and it can take 4 weeks for investigators to go through just 1 terabyte of that data without the proper tools.<sup>3</sup> The sheer volume of data and man hours required to extract intelligence is forcing the need to explore better, more effective policing and investigations.

Technology is also changing the nature of crime with cybercrime fueling astounding crime levels. Digital and cybercrime are now a major part of what police forces deal with on a daily basis.<sup>4</sup> In the UK, cybercrime is reported to be almost half of the crimes tracked from 2014 - 2015.<sup>5</sup> This changing crime necessitates a changing police response.

Today, the majority of public safety agencies still rely on outdated, disparate data management systems that keep information in silos, reducing the ability to effectively deliver information and intelligence to personnel where and when it is needed. A headline in the *Wall Street Journal* last October<sup>6</sup> exposed this dilemma on a national level: "Inadequate Data Hampers Law Enforcement in Fight Against Rising Crime." The article highlights how outdated federal systems for gathering national figures are impacting police deployment to deter crime with many major cities facing staggering increases in crime rates. The article elaborates how police feel having better access to real-time, in-depth data would help them focus more time and resources on the factors fueling the crime. Better data could tell them not just what is happening, but why and how to respond more effectively.

### WHAT IS A ZETTABYTE ?

It is the equivalent of 1 trillion Gigabytes. For quick reference:

- 1 Zettabyte = 1,000 Exabytes
- 1 Exabyte = 1,000 Petabytes
- 1 Petabyte = 1,000 Terabytes
- 1 Terabyte = 1,000 Gigabytes

In addition to the challenges of operating with disparate systems, the ever-expanding Internet of Things (IoT) is fueling a variety of enhanced public safety capabilities to improve mission success rates — and generating even more data. Body-worn cameras, sensors, drones and GPS trackers are just a few examples of the types of technologies already in use creating and receiving data. Extracting the greatest value from this data generated in all stages of public safety operations requires agencies to adopt leading analytics tools to aggregate and correlate both historical data with real-time information dispersed throughout an IoT ecosystem.

## BY 2020 THE IoT WILL CONNECT OVER 30 BILLION INSTALLED UNITS<sup>7</sup>

GARTNER GROUP FORECAST

Lastly, it's also important to consider the demographic changes in staffing. By 2020, millennials will make up 50% of the workforce.<sup>7</sup> This digitally-native generation is more technoliterate and skilled at multitasking. Agencies are already experiencing their influence as they rely on smartphone applications to assist with calls for service even if the apps are not sanctioned for use (e.g., video camera use). The newest and best technology is what they will come to expect; and if they don't get it, they will seek it out elsewhere.<sup>8</sup> Agencies who stay current with technology may help mitigate potential staffing challenges in the future and improve retention of qualified personnel.

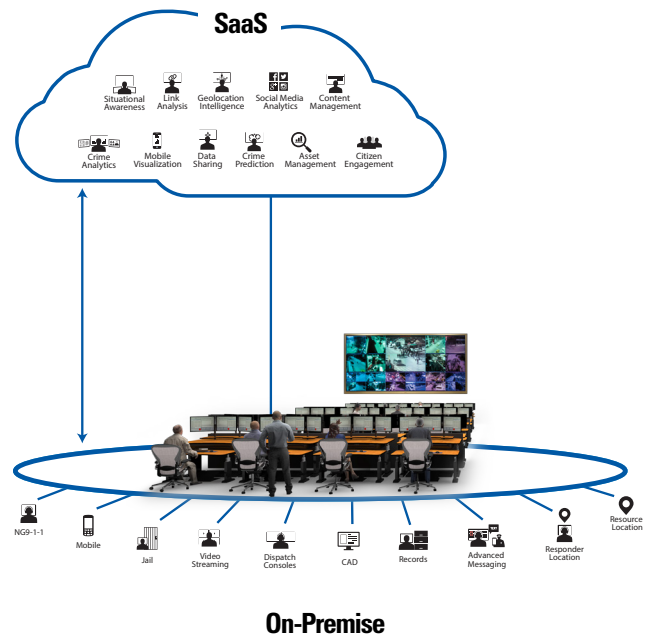
## SO WHY FOCUS ON CLOUD? TO PUT YOUR DATA TO BETTER USE BY MORE EFFECTIVELY UNIFYING AND CORRELATING THE INFORMATION AND IMPROVING DATA ACCESS THROUGHOUT YOUR OPERATIONS TO ACHIEVE SAFER OUTCOMES.

With the constantly-changing crime landscape, public safety agencies must evolve their digital capabilities to prepare for the next generation of public safety threats. Data management is key to fighting crime and responding faster to emergency calls in the digital age, and cloud technology provides the framework for success to keep pace. The ability to take action based on up-to-date, data-driven insight is becoming increasingly important to improve strategic planning, calls for service and closing more cases.

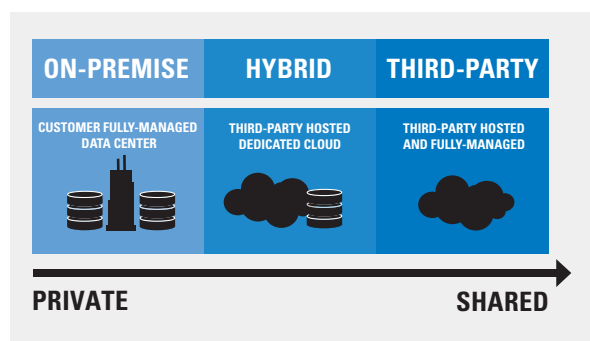
## CLOUD DEPLOYMENT CONSIDERATIONS

Deploying a cloud platform provides a flexible means to greater speed and agility in operations. For many organisations, a cloud solution can augment existing operations: in some cases it's to extend its reach and in other cases it's to provide a full migration path for maximum efficiency. These advantages, combined with the understanding that it is extremely challenging to replicate the same benefits with a traditional on-premise solution, are the reasons for considering control room operations in the cloud.

Public Safety agencies can realise significant efficiencies with a third-party cloud solution that meets the right security compliance for reliable performance. A reliable third-party partner can help deploy and integrate an effective mission-critical cloud strategy for public safety as a more reliable means of operation than an private cloud/ on-premise solution. There are some factors to consider between cloud choices:



For any cloud operation, it is important to note that one size does not fit all. Oftentimes, as a cloud strategy matures it may require a combination of various on-premise, hybrid and third-party cloud solutions that meet your unique operational needs. At this point, the true value of a third-party partner is not just in the capabilities you are provided via the cloud, but the ability they have to provide you and those capabilities seamlessly integrated with other systems and solutions, whether in the cloud or on-premise. An integrated approach allows you to realize the most value in leveraging existing technologies together for better operational outcomes.



Recognising the sensitivity of government information and the responsibility to ensure accuracy, reliability, and availability of the data in hand — securing data is crucial with any platform solution used. In 2015, the Communications-Electronics Security Group (CESG) published [Cloud Security Guidance](#) that addresses key principles for government organisations who are considering using cloud services for handling information, focusing on the importance of managing risks and implementing security principles. Standardising data security to the highest level possible will allow for a more streamlined implementation process in order to avoid any mishandling of data or placing data at risk.

### A CLOUD ARCHITECTURE MAKES IT EASIER TO CREATE SECURITY MODELS THAT LEVERAGE THE FOLLOWING CAPABILITIES<sup>10</sup>

- **More segmentation (separation).** More shared resources means a greater need for more segmentation. In a conventional data center, this separation can be very resource intensive, and many organisations believe that the risk is limited. Cloud architectures open eyes to the use of service orientation, grid and mesh communications, and other dynamic capabilities that drive the need for new protection mechanisms.
- **More encryption.** While it seems obvious that public cloud environments need encryption, many organisations have ignored the need inside their existing environments that have often become large and complex themselves. The cloud makes introducing encryption much easier.
- **Stronger authentication.** Users still frequently limit their multifactor authentication capabilities to the edge — remote VPNs accessing enterprise data centers. The move to the cloud highlights the "anytime, anywhere" use of sensitive applications and reinforces the need for strong authentication everywhere.
- **More logging and monitoring.** Once considered "too much overhead" and the bane of any IT shop, logging and monitoring are facts of life if only to ensure that shared responsibilities between enterprises and service providers have been addressed.

When selecting a cloud option, an organisation needs to consider to what extent they can assume the risk and responsibility required to maintain proper security compliance and on-going operational continuity. With private solutions, systems need to be maintained, logs rotated, file systems cleaned, backups performed, operating systems patched and around-the-clock monitoring of security posture and system health. With a qualified cloud partner, all compliance and operational risks are managed for you. This includes better controls to manage and monitor permissions, access, use and data administration, while also providing the highest level of protection from security threats, which frees your staff to focus on strategic initiatives and community safety. All of, this can be accomplished while retaining 100% control and ownership of your data.

### ARE YOU READY FOR THE CLOUD? SOME QUESTIONS TO ASK...

- Are you looking to improve operations that can lower crime rates?
- Is your staff experiencing increased time processing case data?
- Are officers spending more time with administrative reports impacting time available for patrol?
- Are you effectively using all of the information stored on location (e.g., fully automated)?
- Do you have redundant protection to all of the applications and data you currently use?
- Do you have the means to ensure full government security compliance of all personnel hired to manage your data and network operations?
- Do you find maintaining compliance to the latest regulatory standards a growing challenge?
- Are you experiencing inconsistent network quality of service across your organisation?
- Have you invested large amounts of time and money into programs that no one uses?

### AUGMENTING CONTROL ROOM OPERATIONS IN THE CLOUD

When data is unified and integrated onto a secure, cloud platform, rapid correlation and analytics engines begin extracting actionable intelligence in real-time. This ensures the right information is delivered to the right users at the right time. By breaking down data silos with a flexible platform design, you can easily scale applications throughout your organisation as future needs evolve and data requirements grow.

Once data is centralised in the cloud, realising value is simple in control room workflows. With applications designed to common police workflows, agencies can quickly onboard users without a difficult learning process.

#### PLAN

- Analytics dashboards can automate CAD/RMS data to visualise information through heat maps, graphs and geospatial views for customised roll call and trend casting reports. This enables users to quickly view criminal activity by shift and across jurisdictions.
- Predictive analytics can make public safety agencies more accurate and efficient in deploying patrol officers in specific areas where crime is likely to occur using targeted area predictions derived from historical data — ultimately reducing crime activity.

## SUPPORT

- True real-time situational awareness can be achieved unifying video, data and voice for a common operating picture providing critical intelligence to control room operators in seconds to quickly aid responders and investigators on site.
- Faster decision-making by responders on the scene is achieved by disseminating geospatial intelligence using data layers to show locations of people, events, alerts and historical details pertinent to the situation at hand.
- Effectively used analytics, sensors and video data with bufferless, real-time video streaming capabilities sent from the control room to dispatch and to responders to provide vital information about crimes in progress and dangerous situations as they unfold.

## INVESTIGATE

- Quickly aggregate social media data and customise analysis by defined queries that alert users to the most critical, relevant information to aid in tactical response and investigations.
- Fuse rich datasets together automatically and easily analyse massive amounts of data to resolve cases faster — and more accurately — to prevent future crimes. Browser-based access helps users generate actionable intelligence from anywhere — any time.

## COLLECT

- Efficiently manage rapidly-growing digital evidence as body-worn camera programs are adopted to reduce administrative overhead and simplify digital storage challenges. Video evidence management is streamlined from capture to storage with automated uploads, tagging, content grouping and rapid redaction. Easily maintain policy and compliance with chain-of-custody controls that automate security and content integrity.
- Instantly connect with the community to aid in policing efforts by receiving crime tip submissions and citizen video evidence improving police response and overall safety.

## SOURCES

1. "Facts and Stats About The Big Data Industry," CloudTweaks, March 17, 2015, <http://cloudtweaks.com/2015/03/surprising-facts-and-stats-about-the-big-data-industry/>
2. "The Zettabyte Era—Trends and Analysis", Cisco, <http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/>
3. "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>
4. "Steve Kavanagh Blog: Policing the digital age," NPCC, December 2, 2015, <http://news.npcc.police.uk/releases/steve-kavanagh-blog-policing-the-digital-age>
5. "Crime soars 107% as cyber offences included for the first time - as it happened" <http://www.telegraph.co.uk/news/uknews/crime/11932670/Cyber-crime-fuels-70-jump-in-crime-levels.html>
6. "Inadequate Data Hampers Law Enforcement in Fight Against Rising Crime," The Wall Street Journal, October 8, 2015, <http://www.wsj.com/articles/inadequate-data-hampers-law-enforcement-in-fight-against-rising-crime-1444331310>
7. "PwC: Millennials at Work" <https://www.pwc.com/gx/en/managing-tomorrows-people/future-of-work/assets/reshaping-the-workplace.pdf>
8. "Using IOT to Create Opportunity for Software Monetization," Gartner, <https://www.gartner.com/user/registration/webinar?resId=3099417&commId=166777&channelId=5501&srclId=1-3478922244>
9. "Three Ways to Improve Millennial Recruitment," October 2015, Hendon, [https://www.hendonpub.com/law\\_and\\_order/articles/2015/10/three\\_ways\\_to\\_improve\\_millennial\\_recruitment](https://www.hendonpub.com/law_and_order/articles/2015/10/three_ways_to_improve_millennial_recruitment)
10. IDC "Safer in the Cloud" White Paper, July 2015
11. [http://www.policeforum.org/assets/docs/Free\\_Online\\_Documents/Technology/implementing%20a%20body-worn%20camera%20program.pdf](http://www.policeforum.org/assets/docs/Free_Online_Documents/Technology/implementing%20a%20body-worn%20camera%20program.pdf)

Smart Public Safety Solutions from Motorola Solutions embrace cloud-based operations and can transform your ever-growing data sources into a force multiplier enabling fast, accurate emergency response and crime prevention. Learn more at [motorolasolutions.com/spss](http://motorolasolutions.com/spss).

Motorola Solutions U.K., Ltd. Viables Industrial Estate, Jays Close, Basingstoke, Hampshire RG22 4PD, United Kingdom [motorolasolutions.com](http://motorolasolutions.com)  
MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylised M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2016 Motorola Solutions, Inc. All rights reserved. 05-2016

## 24K HOURS OF BODY WORN CAMERA VIDEO GENERATED PER OFFICER OVER 5 YEARS<sup>11</sup>

By harnessing the cloud, public safety agencies have a flexible data platform where security, compliance and performance can all be configured to meet specific service requirements and is easily upgraded to keep pace with future requirements. Moving to cloud-based data management solutions can help police agencies manage and store large volumes of sensitive data with more control, better security, and greater flexibility to enhance crime-fighting capabilities.

### CLOUD ADVANTAGES

- OPEX model and cost savings with reduced IT overhead
- Rapid deployment of critical resources
- Off-site storage and disaster recovery
- Dynamic provisioning of new applications when needed
- Full security compliance
- Dedicated management of security risk posture
- Full mobile functionality
- Faster data sharing and collaboration
- Easier to implement and integrate
- System updates when needed are automatically managed
- No additional hardware investments
- Flexible subscription plans
- Future-proof
- Increased uptime

