BlackBerry

Securing the **Enterprise of Things** in the Public Sector

Table of Contents

The Enterprise of Things Is Here – Are You Ready?

The Enterprise of Things (EoT) is the network of people, endpoints, and digital assets owned by and connected to the enterprise (or public sector organization, in this context). It casts a wide net, to include content, communication, collaboration, transportation, and facilities – that is, anyone and anything connected to the internet.

The EoT represents a powerful opportunity to transform existing public sector processes and create entirely new ones. Governments are moving on these initiatives because policymakers are legislating it, constituents are demanding it and because it presents an opportunity to do more with less.

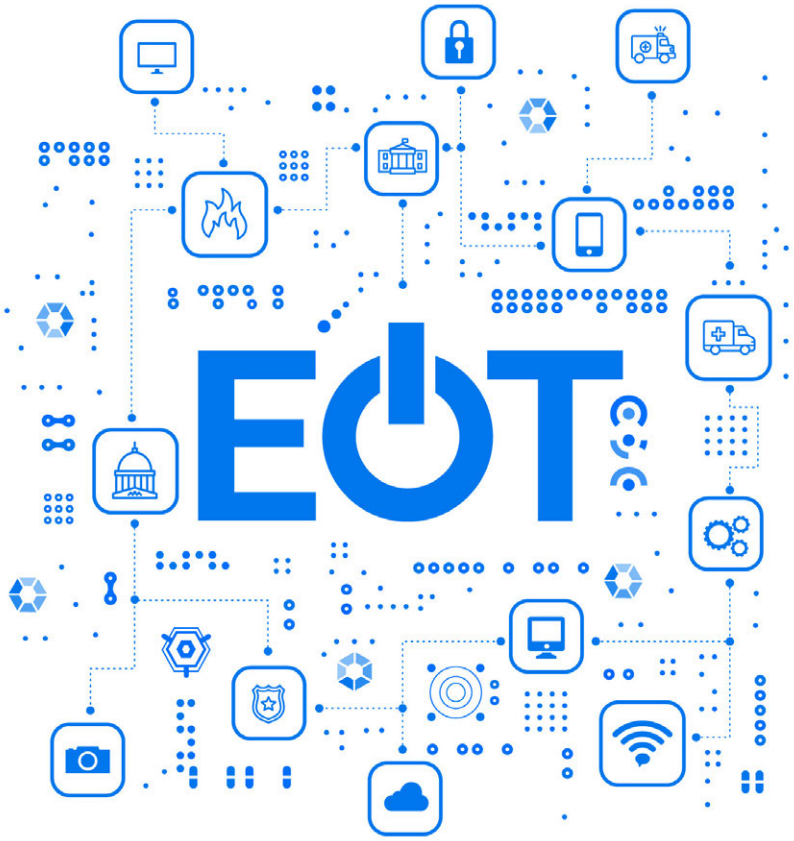
But with those opportunities come challenges, especially when it comes to security.

In the public sector, a comprehensive, integrated approach to security is all the more important as digital transformation imperatives are bringing more people and things online across government, defense, and public safety organizations.

Yet, so far, while governments are making some great strides in digital transformation, and leveraging "things" in the process, they've tended to adopt point solutions, or a patchwork approach, to secure these innovations. That must change if they want to save money, enhance services for citizens, and reinvent processes; because every new, connected endpoint exponentially increases the security risk of a network.

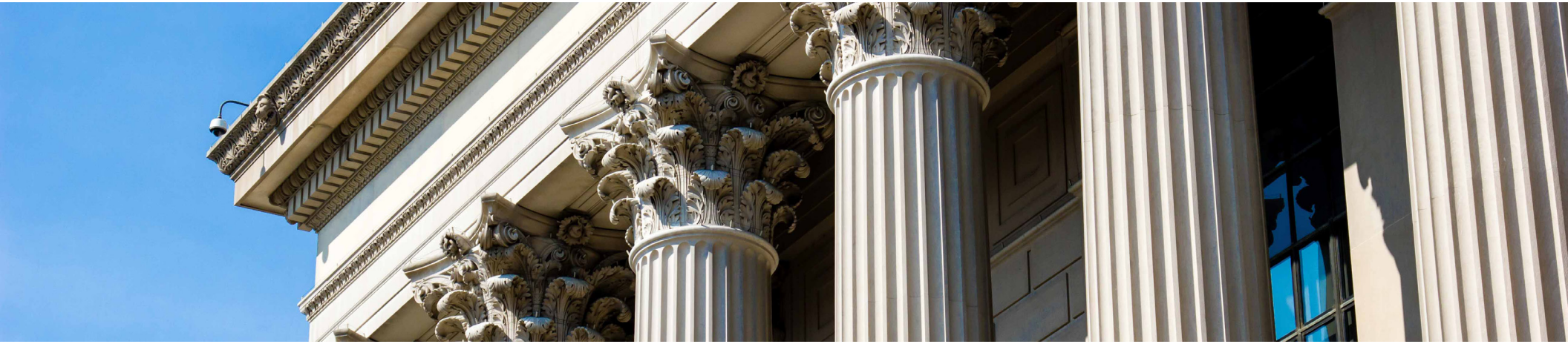
When you consider that the public sector encompasses military units, first responders and public safety policymakers, in this fast-rising wave towards hyperconnected digital and physical 'things', early decisions to prioritize safety and security are literally going to save lives.

In this eBook, we'll look at the opportunities that EoT brings to government, defense, and public safety organizations and we'll explore EoT challenges that must be addressed too. You'll see the ways in which BlackBerry is already deeply involved in shaping how the EoT unfolds in the public sector and learn about solutions that can help your public sector organization provide better outcomes for everyone you serve.



How the **Enterprise of Things** is Transforming Government

In this section:

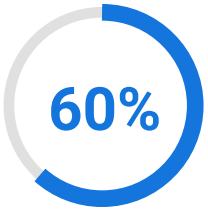


A Better, Faster Way to Serve the Public

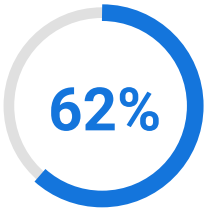
Government agencies, like their counterparts in the private sector, are adapting to sweeping changes in their workplaces, workforces and workflows. And everything (and everyone) that connects to the internet from government networks must be secure.

While expectations from all stakeholders are high, budgets are tight, and tightening further. As a result, headcounts are shrinking, and human resources are expected to deliver maximum productivity with maximum efficiency.

With increasing demands for transparency in government, every dollar is scrutinized and must be rationalized. And, while saving money is critical, so too is increasing revenue. Governments, with taxpayers in mind, are enticed by the potential gains: digital transformation in government stands to generate over $1 trillion annually worldwide, according to McKinsey estimates.[1]



of citizens think increased use of technology by police, border agencies and government as a whole will make them more secure.



of citizens are less confident today than 12 months ago in government's ability to protect against cyber threats and attacks.

2018 Accenture Public Service Citizen Survey[2]

What Governments Can Achieve with Digital Transformation and a Secure EoT

While there are hundreds of goals in government digital transformation, most fall into one of the following groups: Improving services for citizens; re-envisioning business processes; using data analytics to drive better decisions and improve safety; and sharing data to overcome siloes. Let's explore each of these opportunities in depth.

Improving services for citizens

Many government transformation initiatives begin with a mandate borrowed from the private sector: improve the customer experience, or in this case, the constituent experience.

While citizens are demanding an improved experience, legislators around the world are insisting on it, too. For example, in the US, the Customer Experience Act of 2017 bill outlines "the sense of Congress that all agencies should strive to provide high-quality, courteous, effective, and efficient services and seek to measure, collect, report, and utilize metrics relating to the experience of persons interacting with them to continually improve services."[3]

Digital tools are the ideal way to accomplish these goals because citizens have come to expect self-serve interactions with businesses and now expect the same from government agencies.

This is why the United Kingdom initiated its transformation strategy by digitizing 25 basic services, such as voter registration, while in China, some provincial governments now accept passport and visa applications through WeChat, a widely used mobile app.[4]

Mobility is key, because in the business world, 'digital' now means anywhere and on any device. And that doesn't just apply to customers or citizens. To deliver better service, government workforces need secure access to devices, apps and information they can use to serve citizens from anywhere – whether those workers are in the office, at a project site, carrying out a home visit, or on-scene during a rescue or recovery operation. As mobility for government workers improves, agencies will increasingly turn to IoT devices and cloud-based applications to serve citizens with better efficiency.

This is good news for everyone involved. According to 2018 Accenture Public Service Citizen Survey, citizens worldwide support governmental adoption of emerging technologies to provide better, faster service: "2 in 3 citizens support artificial intelligence for faster tax refunds, virtual reality to better manage retirement, cross-agency data sharing to increase border safety, and a single online portal to access all their public services on one platform."[5]

Streamlining operations

Government processes are often mired in red-tape or driven by the requirements of decades-old technology. With systems and practices that are deeply entrenched, government organizations (and employees who must carry out these activities) can be slow to accept and agree to change. But innovators in government see how much efficiency there is to be gained by using digitization and the EoT to streamline or fully reinvent cumbersome processes, and continue to make strides.[6] For example, after updating tax laws, government innovators in Denmark created an algorithm for classifying newly registered businesses. Now, "more than 98 percent of the tasks involved in registering companies take place in seconds, with no human intervention." And Sweden's social security organization began its digitization program by overhauling five products that accounted for "60 percent of all manual processing work and more than 80 percent of the agency's call-center volume."[7]

With many government processes at least digitized by now, the focus is shifting to using digital technologies to re-envision those processes from the ground up. In the near future, these technologies will likely replace any and all manual, outmoded and inefficient processes, across all levels of government.

Improving decision making and safety

Digital technology produces vast amounts of data, and if harnessed properly and securely, this data can help governments predict outcomes and make smarter decisions about many things, including health and safety. But with so many potential sources of data, governments need the ability to synthesize information from these various feeds, and then use algorithms to trigger real-time reactions.

In Singapore, for example, individual agencies already use sensors to collect data on air quality, traffic patterns and more. The government is now setting up a nationwide network of sensors that will stream all the available data these devices produce into a single online repository accessible by all agencies.[8] When that data is used to trigger automatic changes to the physical environment (such as traffic lights), securing the entire process is critical. Singapore is a global leader in government transformation, but its recent healthcare data breach, the country's worst ever, serves as a reminder that even the most technologically advanced agencies are vulnerable.[9]

Los Angeles, too, is using data and IoT to create new ways to protect citizens. The city has many connected things, including 145,000 streetlights and 4,500 intersections. While they draw basic data from these devices today, the plan is to move from a Smart City 1.0 approach to something more advanced: exchanging information between both city-owned sensors and the sensors that exist in citizens' devices (e.g. smartphones, wearables), too. Smart City 2.0 is about gathering "streams of data, then laying them atop of each other and getting situational awareness and location intelligence," explains Ted Ross, the City of L.A.'s general manager and CIO.[10] But of course, connecting constituents' devices with government-owned platforms can only be done when privacy and security are optimized across the EoT landscape.

In the EoT, wearables are indeed important data collection and access tools. When they're connected to smart home technology, for example, they can help governments improve the safety of elderly or homebound constituents who lack support systems and connections to the wider community. This way, they can remain in their homes safely for longer, and require less physical intervention by public health workers, which also saves money.[11] These applications must be properly secured on all sides, as they involve life or death scenarios as well as patient health information.

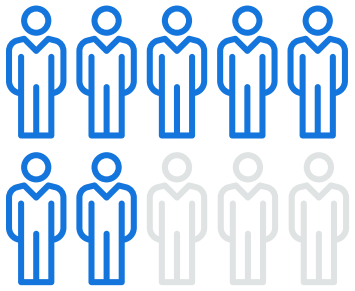
Workplace safety is another EoT application that governments are exploring right now. In some regions, legislators are mandating the use of IoT devices and applications that can monitor work environments for potential risks, alert workers and connect them to outside resources for guidance or rescue. For example, firefighters will soon be outfitted with not only connected cameras, but devices to monitor for falls, vital signs, air tank capacity and more.

With a secure, comprehensive approach to EoT, all kinds of data can be collected, analysed and used to alter outcomes in people, processes or things. And if data is successfully and securely stored and analysed, it can even be used to inform workplace safety regulations.

Enabling and securing data-sharing

Governments agencies have long struggled with how to work together given disparate technologies, unlinked chains of command, and different regulatory compliance requirements. However, when these challenges are overcome, the potential gains are huge. For citizens, the benefits take the form of faster, better, more convenient service. For government organizations, one of the most tangible benefits is in cost savings, through streamlined process and the elimination of duplicated data and effort. For example, agencies are saving money while improving safety by unifying emergency communication systems so that workers get alerts anywhere, anytime. That doesn't have to mean ripping and replacing existing systems; new solutions create interoperability where it simply couldn't exist previously.

A first step in sharing data is to unify registries of public information, such as real-estate records, contact details, company information, citizen profiles and infrastructure logs. The UK tax authority, for example, has succeeded in linking a billion data items from 30 sources, including government land and vehicle registers, social media sites and trade associations. Since its launch, the technology has allowed the agency to identify tax evasion and claim an additional £3 billion in tax revenue. [12]



7 in 10

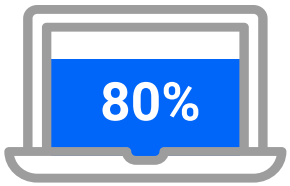
citizens seek guidance from government on a range of topics, from how to manage healthcare costs in retirement, to how change will affect them, to how artificial intelligence will improve

2018 Accenture Public Service Citizen Survey[13]

In another example of how interagency collaboration and data sharing is already having an impact, the US Department of Homeland Security is using inexpensive sensors and IoT-based approaches to facilitate evacuations, flood monitoring and the maintenance of critical infrastructure. Collaborating with the Lower Colorado River Authority, FEMA and the National Weather Service in flood-prone areas of Texas, the program will share real-time data so first responders and local authorities can respond faster when a flood hits, to safeguard infrastructure and even save lives.[14]

Using this scenario, it's possible to see how a single datum flows through a huge array of touchpoints, triggering changes along the way. A sensor detects that water levels are rising in an aqueduct where government scientists are collecting samples. The threat data is fed in real time to a system at one agency, which is responsible for assessing the risk. The risk is deemed severe enough to warrant an immediate extraction of the team. An automated system must alert the workers immediately; an agency must approve the mission to airlift them out; field workers and rescue teams and third-party experts must be engaged and deployed.

After the successful rescue, records of the cost and outcomes must be retained and shared by all parties and analysed by regulators. One datum has triggered hundreds of interactions between people, processes and things. Many of the human interactions involve files, records, phone calls and video links. The ability to quickly and effectively share data across all these moving parts can change and save lives. But all of this must be secured.



of citizens want to give government permission to share their data across agencies to enable better, more convenient services.

2018 Accenture Public Service Citizen Survey[15]

Digital Transformation Demands More Focus on Security

Even with their advances in service offerings and investments in mobile security solutions, governments are not in the clear when it comes to securing the Enterprise of Things. In fact, by undergoing digital transformation and thereby rendering government information accessible in the IoT, agencies are accepting a new set of challenges that must be considered.

Increasing cyber threats
As government agencies collect and share more digital information, the number of cyber attacks is on the rise, too. Threats against public safety, citizen privacy and national security will continue to emerge due to more data being stored online and the increasing cost of an attack. In 2017, public sector organizations experienced 53 attacks per week on average costing an average of $8.2 million, up from $6.77 million in 2016, according to the Ponemon Institute.[16]

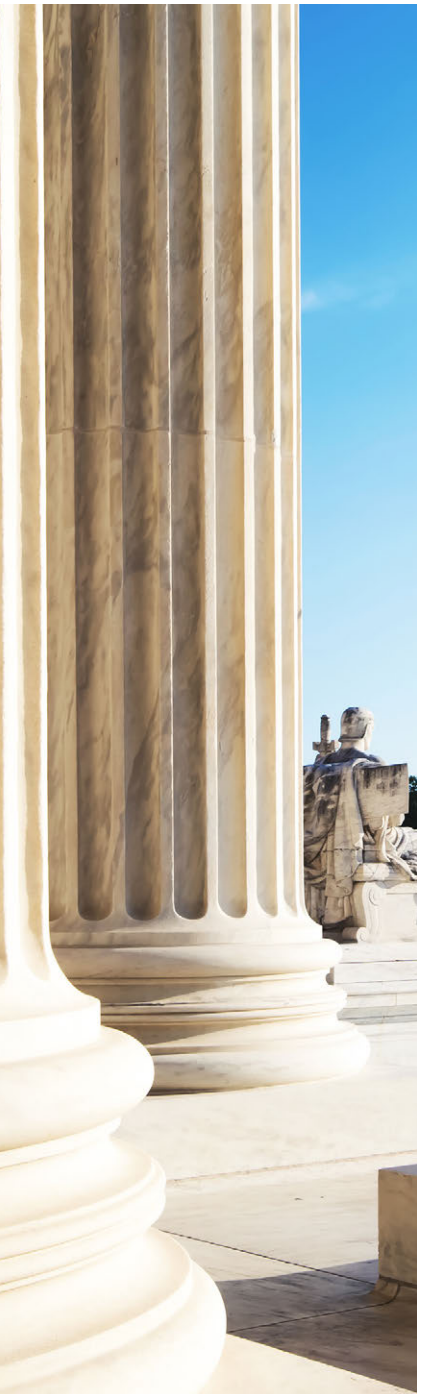
Evolving threat tactics
All the while, cyber attackers are honing their craft and finding new ways to hack high-value targets. Electronic eavesdropping and call tapping are easier than ever, due to an organization's lack of technical and financial resources to implement appropriate defenses. Plus, with advances in artificial intelligence, increasingly, bad actors will have even more tools at their disposal and be able to find vulnerabilities in hyperconnected systems and craft attacks in much less time.

Pressure from the public
Government entities are also under pressure to fill security gaps that leave them vulnerable to even the simplest attacks, like ransomware. Citizens expect that their personal data is handled with a high degree of privacy and care. This can present a challenge for Chief Information Officers at government organizations who are already struggling to balance organizational productivity, user satisfaction and security.

Insider risk
Government employees can also compromise security. Common in today's digital workplace, knowledge workers expect rich, consumer-like tech experiences and bring a variety of preferred apps and tools to work. In a recent survey, nine out of 10 law enforcement officials reported using mobile phones for work-related communication, yet only 17% had an agency-issued phone.[17] Evidently, many workers are using personal devices to exchange private or classified information across networks that are not monitored or secured by the government.

Government leaders identify the following as their key challenges in digital transformation:[18]

- Security concerns
- Insufficient technical skills
- Lack of an overall strategy
- Lack of understanding
- Lack of collaborative, sharing culture
- Legislative and legal constraints
- Lack of organizational agility



How BlackBerry is Helping Government Secure the EoT

Securing the Enterprise of Things requires that every access, every interaction, and every communication with every person is singularly secure from any endpoint and any location. Securing the EoT means that government operations can be more productive, safe and secure.

For government workers
BlackBerry is empowering the transformation from a less productive silo culture to agile Government as a Platform; improving collaboration in policy research and development; and improving productivity with faster information flow and convenient mobile workflows both within a department and between government agencies and external stakeholders. BlackBerry solutions are increasing employee satisfaction and enabling productivity beyond laptops and corporate-owned devices, enabling core office workflows over any mobile device, and decreasing total cost of ownership (TCO) for remote access. Unified crisis communication enabled by the EoT makes it easy to share information across personal devices and connected devices such as speakers and digital displays.

For Government to Civilian (G2C) & Business (G2B) interactions
In support of interactions between governments and their business partners and citizens, BlackBerry is enabling secure and effective G2C and G2B document-sharing over mobile and desktop, and empowering C2G and B2G service workflows through secure chat on web portals and mobile devices.

For government IT teams
Behind the scenes, BlackBerry is enabling secure and cost-effective choose-your-own-device (CYOD)/corporate-owned, personally-enabled (COPE)/bring-your-own-device (BYOD) models, empowering app development, lowering complexity and costs with a single management pane for multiple services. 70% of US federal government agencies choose BlackBerry to protect their people, offering the first and only FedRAMP authorized crisis communication solution.

For Government to Government (G2G) exchanges
BlackBerry is securing document collaboration, increasing information velocity in G2G with secure real-time chat, and lowering the risk of security breaches in data and voice communications. BlackBerry's ability to deliver a federated emergency platform enables agencies to meet federal interoperability mandates by extending emergency notifications between agencies.

For government leadership
For government decision-makers, up to the highest levels, BlackBerry is securing mobile document approval workflow, enabling the dissemination of sensitive documents, and transforming committee collaboration with secure real-time chat and secure file sync and share.

How BlackBerry Cybersecurity Consulting Helped This Agency Secure, Connect and Protect Its Data

Challenge

This government agency manages huge quantities of critical data and had recently established a new data portal to foster better access to public sector information. The agency also outsourced its IT department. In response to these significant changes and a changing regulatory environment, decision-makers enlisted the help of BlackBerry® Cybersecurity Consulting to evaluate and renew their security posture.

Solution

The BlackBerry team examined the agency's systems to identify weaknesses in their technical defenses and security processes (like patching and updates). They also assisted in developing strategies to reduce the cyberattack surface and improved employee security training.

Results

Today, there is increased security awareness across the whole organization, and data loss is no longer a significant threat. Compliance with strict data security regulations is also much easier.

How a Tragedy Prompted this Government to Solve Emergency Communication Challenges

Challenge
In 2014, this government experienced an active shooter event which resulted in the death of an employee and wounding others. The incident and its subsequent investigation resulted in the development of an emergency notification system, which is designed to deliver immediate emergency communications to all employees, contractors and visitors to keep them informed and safe. One major challenge was to ensure crisis communications were easily understood by every stakeholder in a bilingual work environment.

Solution
BlackBerry® AtHoc provided ready-made "building blocks" to supplement their existing crisis communication system. By integrating BlackBerry AtHoc, they now have a single unified solution system to manage sharing critical information, offering a flexible and adaptable way to manage crisis communication, including the ability to inform specific stakeholders and delivered in multiple languages to employees. The enhanced solution automated their crisis communication process and expanded the methods used to reach the right people at the right time, improving the safety of their workforce.

Results
With BlackBerry AtHoc, this government created a secure unified emergency communications platform that greatly enhanced the ability to share critical safety information to protect employees.

Mobility Solutions for Improved Services and Security

Government organizations were among the first to invest in secure mobility solutions to enable critical workflows, communication and decision making from anywhere, at any time. With significant workplace improvements already underway, including smarter, better, and faster workflows for workers and services for citizens, government organizations are indeed making progress, but must be prepared for a host of security challenges to come.

The **EoT** in Defense: Securing the Networked Battlefield

In this section

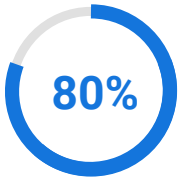
The Battleground Has Changed

The defense sector is turning to digital transformation, or the "networked battlefield," as a way to improve operational efficiency and effectiveness. While the private sector currently drives IoT applications, the defense sector traditionally takes a more conservative approach in adopting the available innovations.[19] This slow pace of adoption could be due to the unique regulatory and security demands, along with fragmented, outdated IT infrastructure.

The EoT is already re-shaping warfare, workflows and workplaces in the defense sector. Fighter jets, battleships and tanks are outfitted with numerous connected sensors, all feeding data back to central command. Ground soldiers are wired, too, through "smart clothing" – that can detect and alert team members or dispatchers if an officer has been shot – and connected devices that give them additional intelligence about their surroundings, and at the same time, transmit information back to decision-makers.

On or off the battlefield, defense personnel need to be able to quickly, easily, and confidently access and share files from their computers or mobile devices. They need to be able to maintain control of those files, especially in the event that a device is lost or stolen and it needs to be remotely wiped clean. Monitoring the status of every "thing" that's connected to the network in real time, and being able to manage it remotely, is where EoT security comes into play.

In the defense industry, downtime is simply not an option - especially when lives are at stake. Network connectivity is essential, but defense organizations must be able to attribute and authenticate data so it can be trusted as it crosses the network. All forms of data and communication must be encrypted and restricted to only those with proper clearance.



of aviation and defense executives acknowledge that the benefits of digital transformation apply to forecasting, integration across operations, and internal/external collaboration

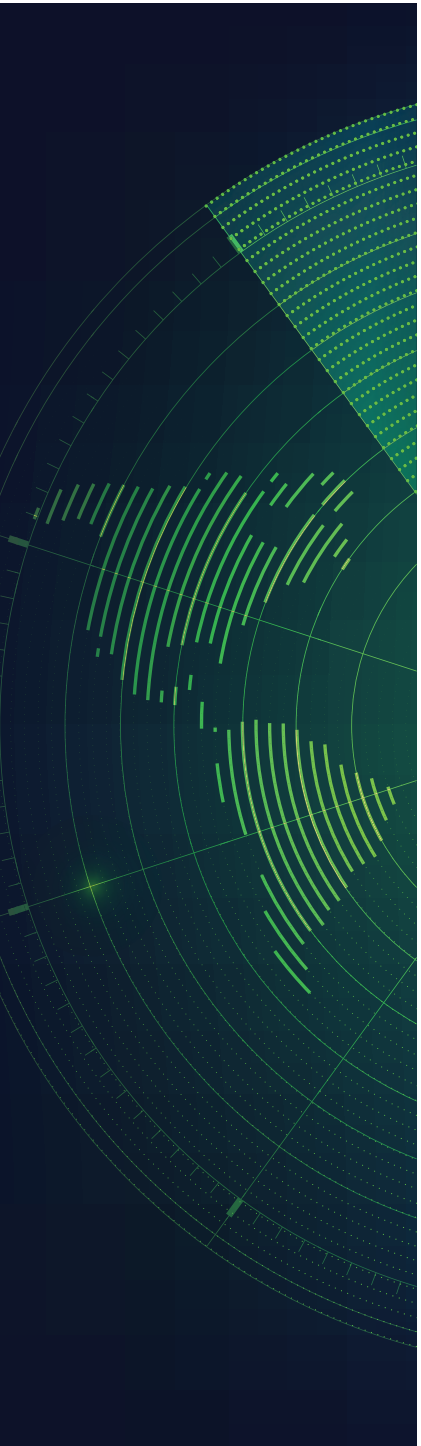
How Digital Transformation is Reshaping the Defense Industry, Aviation Week [20]

EoT off the battlefield

- Just in time delivery of supplies, such as fuel and equipment
- Use of Radio-frequency identification (RFID) tags for tracking shipments and manage inventories
- Better tracking of assets to ensure they are deployed efficiently and don't fall into enemy hands

EoT on the battlefield

- Improved situational awareness beyond what soldiers can see, hear, smell and sense
- Use of overhead UAVs, ground and chemical sensors, and intelligence from online banking activity, transportation logs, cameras and other sources
- Real-time data back to operations command posts



What the Defense Industry Can Achieve with Digital Transformation and A Secure EoT

Today's military operations occur in complex, ever-changing environments, including the evolving cyber frontier. At the same time, defense organizations are under pressure to maintain a high level of security for citizens while reducing spending.[21]

Any deployment of EoT technologies requires investment in technologies, connectivity, interoperability and security. Any EoT solution must address stringent requirements protecting public safety and national security. The massive international human resources infrastructure, including many outsourced contractors, must also be considered.

Let's examine a few key objectives defense leaders can achieve by leveraging a new state of hyper-connectivity.

Improving operational agility

Intelligence is everything on the battlefield, and always has been. Informed decision-making depends on the speed, agility and accuracy of information exchange between command and field operators. Hyper-connectivity, in this sense, can revolutionize intelligence by enhancing the availability of timely, accurate data.[22] It can enhance and unify situational awareness in two specific arenas: on the battlefield and in the command center. On the battlefield, networked personnel can use and transmit critical data related to the physical and human environment, equipment conditions and availability of supplies, for example. Today, individual apps allow soldiers to view streaming video from unmanned aerial vehicles, see ammunition status of nearby soldiers, even allow command to look through a rifle scope.[23]

In the command center, as it follows, this critical data received from the networked battlefield provides command personnel with enhanced awareness of real-time operational performance. For example, the Department of Homeland Security uses Blue Force Tracking Systems to track personnel and assets and offer dynamic situational awareness.[24] The system hasn't been elevated to full IoT functionality, however, with data bottlenecks often occurring due to many distinct networks.[25]

Saving time and money with predictive maintenance of assets and people

Mission readiness hinges on readiness of equipment and personnel. Connected sensors in aircrafts, ships, land equipment and people serve to detect potential failure or fatigue, enabling preventive response and reducing downtime. The sensors are also connected to maintenance operations, so that parts and supplies can be stocked and ready. This represents the potential for improved availability of equipment and personnel, as well as significant long-term cost savings.

The most advanced example is the Autonomic Logistics Information System (ALIS) of the F-35 joint strike fighter, which uses sensors embedded throughout the aircraft and sophisticated analytics to detect performance and predict maintenance needs, then communicate with maintenance staff.[26]

Enhancing interoperability
Today's defense organizations are a complex patchwork of discrete technologies, data models and standards.[27] Because of this complexity, it can be difficult to design a model that leverages connectivity to improve communications, security and collaboration. There are multiple different systems for battle-tracking within NATO, but many are not interoperable.[28]

Striving for complete interoperability across all branches of defense will allow everyone, from headquarters to the battlefield, to benefit from connectivity and the increasing flow of data across all sources.

Increasing health and safety of personnel
Wearables that track the physical and psychological health of personnel (e.g. hydration, heart rate, blood sugar) produce data that can help assess risk of injury and/or trauma in the field. For training, wearable technology makes it possible to mimic live combat, using motion and acoustic sensors, then sending data to a trainer who can provide coaching in real time.

Another example is autonomous systems (e.g. armoured vehicles) with embedded sensors that can provide situational awareness and send supply/ammunition requests, resulting in reduced exposure of personnel to dangerous environments.

Crossing Digital Transformation Barriers in Defense

Commercial IoT applications still pose many challenges across industries, including security, standardization and interoperability. But these obstacles are more intense in the defense sector, and compounded by many others, including:

Security & Privacy
The defense industry is dealing with higher stakes than in regular enterprise, since growing cybersecurity threats can affect public safety and national security. Every day, the Pentagon thwarts 36 million emails full of malware, viruses and phishing schemes from hackers, terrorists and foreign adversaries trying to gain unauthorized access to military systems.[29] This extreme level of risk requires organizations to have the right people, equipment, and capabilities to counter known threats and respond to contingencies that arise, both now and in the future.[30]

Budget Constraints
Defense budgets are under intense scrutiny. A survey conducted by the University of Maryland's Program for Public Consultation (PPC) in 2017, found that while US President Donald Trump proposed a $54 billion boost to federal spending for the military in 2018, a majority of Americans preferred a cut of $41 billion. When public opinion favours transparency and reduced spending, investments in new, advanced technologies can often be shelved.[31]

Mobility, Availability & Reliability
With the dispersed nature of military organizations, it can be difficult to deploy solutions to users on the move in remote areas, with uncertain networks.

Interoperability
The military has been on the forefront of machine-to-machine communications (e.g. radio) on distinct channels, but still there are multiple internal and external systems that have yet to be enabled for connectivity. Digital workplace technologies have the power to gather unprecedented amounts of data from disparate systems and—by weaving systems, data and people together – fundamentally change how a defense organization operates.[32]

Internal Knowledge & Education
In general, there is a lack of critical mass in specific skills and knowledge for digital transformation. Without the right talent, no transformation project can succeed. Defense organizations have to assess their current needs, but also plan for the future, including how to retain good talent. The US Air Force Digital Service (AFDS), for example, is already taking steps to meet its skills needs by recruiting engineers from the private sector for short-term stints working for the service.[33]

Culture & Pace of Change
The rapid pace of digital transformation outstrips the sector's internal capacity to adapt and innovate – and can especially be difficult to adopt for an organization with a risk-averse culture.[34] Many organizations shy away from developing new operating models in favor of maintaining the status quo. While resistance to change is common, most defence organisations spend all their time and funding on technological rather than cultural transformation.[35]

How BlackBerry is Helping the Defense Sector Secure the EoT

Defense and military organizations can now digitize a wide spectrum of use cases, including secure maintenance checklists on tablets and phones, digitized weapons inspections, digital training instructions and communication, secure document and contract workflow with partners and contractors, and near-real time tracking of container shipments and monitoring of assets.

By partnering with BlackBerry, defense organizations are leveraging connectivity and optimizing the flow of rich data to achieve digital transformation and EoT objectives in the following areas.

For command & management
BlackBerry is helping military leaders improve safety for people with rapid incident alerting; speed up workflows in scenarios where every second counts; share and debrief on sensitive documents, wherever officers are stationed; and facilitate secure communication in foreign missions.

For external stakeholders
Defense organizations rely on outside parties. BlackBerry secures those interactions, whether it's document collaboration between procurement decision-makers and suppliers; real-time chats with contractors and vendors; incident coordination where private sector partners are involved; or federation of alerting so there are no gaps in emergency communications.

For field operations & mobile staff
Electronic flight bags (EFBs) have been in use for years, but militarized versions today contain features and functionality that demand advanced security, such as data and fuel calculations, flight plan details, payload information, and more. BlackBerry is protecting EFB devices and ensuring this sensitive material doesn't fall into the wrong hands. Similarly, BlackBerry makes it possible for weapons technicians to carry out secure inspections using mobile devices, and for maintenance crews to assess even the most sensitive equipment and weaponry using secured mobile apps.

For IT & security
Like any enterprise-grade organization, the defense industry grapples with a range of device ownership models, and BlackBerry helps secure every one of these scenarios: corporate-owned, personal-enabled (COPE), corporate-owned, business only (COBO), choose your own device (CYOD), bring your own device (BYOD) – and most often, a mix of these approaches. BlackBerry® Spark™ apps (off-the-shelf, bespoke, and via ISV partners) allow defense IT teams to monitor and manage their high-availability EMM platform (BlackBerry® UEM) from wherever they need to, securely.

For the academy
In defense, even learning environments are highly sensitive – as troops learn how to use weapons, as trainers convey how to react tactically to enemy advances, as battle plans are reviewed and dissected. Like all learning environments, military "classrooms" are increasingly digitized and mobilized. BlackBerry is securing learning by protecting training content and media, enabling remote document collaboration between students and instructors (who may be stationed off-base), and supporting teamwork with real-time chat and video links.

For logistics

In the EoT, getting the right equipment to the right place at the right time is increasingly automated. Sensors can determine when supplies are low and trigger a re-order without a human ever intervening. While early military efforts to transform logistics in this way are aimed at non-essentials, work is underway to extend this kind of automation to mission-critical supplies. The stakes are high: imagine hackers interfering with an automated shipment of ammunition or medical supplies to a warzone. BlackBerry is helping defense logistics teams re-envision processes through near real-time tracking of shipments and asset optimization with remote equipment monitoring.

How an Armed Services Organization Deployed a Unified Front with a Single Secure Platform

Challenge

A major armed services organization made up of multiple departments each using its own mobility solution was seeking a single secure platform to increase efficiency and save money. The organization had dual priorities: ground personnel wanted ease and efficiency to access information such as mission parameters and navigation details, while headquarters needed to comply with policy and data security regulations.

Solution

With BlackBerry, the organization met both goals. BlackBerry® UEM consolidated and unified their mobile strategy with central mobile management, and BlackBerry® Dynamics™ provided a secure container for existing apps in addition to enabling the development of new secure custom apps using BlackBerry® Dynamics™ SDK.

Results

Every command is now centrally-managed, which has improved both security and efficiency. The organization can support BYOD with confidence, knowing there is a clear separation between personal and work-related data. Most important, sensitive information is protected and in compliance with relevant regulations.

How a DoD Security Agency Implemented a Complex Threat Response System

Challenge

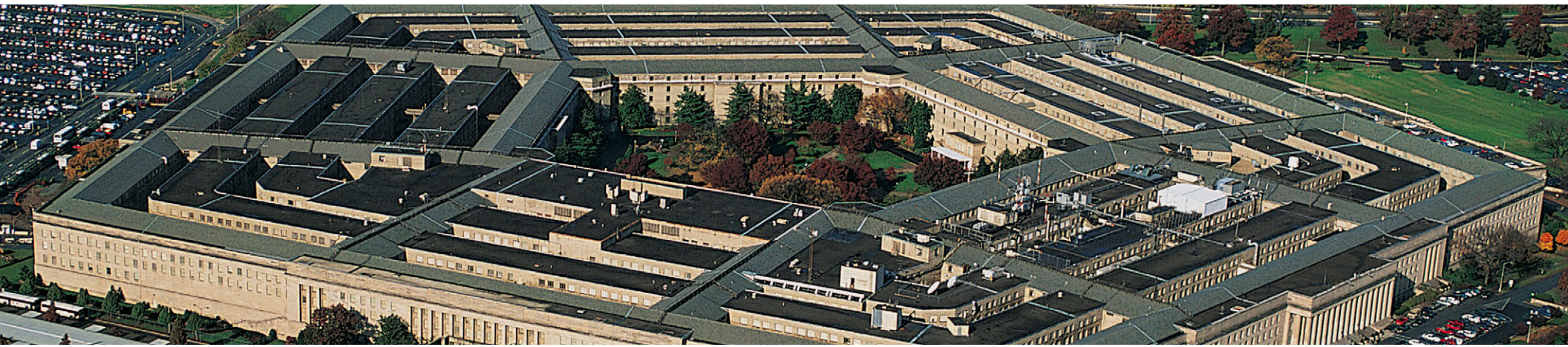
The Pentagon Force Protection Agency (PFPA) was created as a direct response to the terrorist attacks on the Pentagon on September 11, 2001. The agency lacked a common internal network and was unable to effectively communicate directly with organizations outside the Pentagon. It also needed the ability to monitor receipt of communications and emergency alerts.

Solution

By implementing BlackBerry® AtHoc® Connect , the PFPA broke down existing communications barriers within the Pentagon and created a permissions-based network of external organizations for interoperable crisis communication. It enabled secure, real-time collaboration with anyone on the network, anytime, on any device.

Results

All external organizations on AtHoc Connect can decide which of their personnel should receive PFPA alerts, while the PFPA has full control over messages received and sent. After-action reports capture every activity on the system.



Investing in End-to-End Security

Digital transformation goes far beyond ensuring every soldier has a smartphone in hand. Rather, it's about creating a secure flow of high-quality data up and down the chain of command, and across external partners and allies. To that end, defense organizations should focus their investments on interoperable, scalable platforms with end-to-end security that can increase readiness while decreasing long-term costs.

Every Second Counts: Why a Secure **EoT** in Public Safety Will Save Lives

In this section:

New Threats, New Opportunities

Public safety agencies, including law enforcement, first responders and border control, confront constantly evolving threats from both the physical and digital realm. The digital era has created an entirely new arena for lawbreakers. Cybercrime was virtually unknown 20 years ago, but now 30 per cent of citizens report being victims of some type of cyber attack.[36]

But digital disruption has also ushered in opportunities for digital transformation in public safety: to improve real-time incident coordination, reduce operational costs, enhance inter-agency collaboration, and better predict or prevent crime.

Trust is Key

Building end-to-end security is vital in maintaining public trust.

Enabling the IoT securely in public safety sphere has direct outcomes for citizens. It involves highly sensitive personal information, not to mention life-and-death situations. Many public safety organizations have taken steps toward digital transformation through discrete projects and technology investments. With a secure, coordinated approach, public safety can become more intelligent, collaborative and connected.[37]

What Public Safety Organizations Can Achieve with Digital Transformation and a Secure EoT

Enabling the EoT securely in public safety has direct outcomes for citizens, often life or death. The speed with which first responders can react, how much visibility remote supervisors have into incidents, how well agencies can collaborate to solve crimes and use data to prevent incidents – these are the kinds of opportunities that exist.

Behind the scenes, as with their counterparts in defense and government, public safety agencies are using digital transformation to re-envision existing processes, develop new operating models and redesign traditional workforces. Doing so means they can deliver proactive, preventative responses that are aligned to citizens' expectations. But it all needs to happen with security built in.

First responders, law enforcement agencies, national security, customs, immigration and border control agencies can leverage the EoT to achieve the following:

- Better incident coordination and situational awareness
- Better evidence gathering, criminal investigation collaboration, and data sharing across agencies
- Process efficiencies and cost reduction
- Mobilizing staff for faster action and better community engagement

In this next section, we'll explore some of the ways the public sector can benefit from adopting digital-driven methods of connecting and leveraging data.

Improving situational awareness and incident coordination

An effective incident response requires officers and command to have the right information at the right time. Forward-thinking agencies worldwide are moving toward "connected officers" using IoT technology (sensors, video, body cameras) to support mobility while gathering real-time information and communicating with supervisors.[38]

More than half of all medium-to-large police departments in the U.S. now use (or are testing) body-worn cameras, and the body camera market is expected to soon reach $1 billion.[39] This allows field officers to stay in the field, rather than returning to vehicles or desk, while providing both officers and command with rich, immediate situational awareness for better decision-making.

In fact, over 3,500 police departments use small, battery-operated body cameras that offload footage via Wi-Fi and upload it to Evidence.com, a cloud-based repository that already stores over 3.5 petabytes of crime data.[40] The United Kingdom government even launched a secure online portal called Facewatch, which enables police, businesses and communities to work together toward reducing crime. This provides officers an opportunity to access the data they need or solve crime quickly.[41]

Enhancing inter-agency collaboration

Many forms of 21st century crime have no borders; the lines between local and global crime are blurring, especially in the digital world. Successful apprehension of criminals requires information-sharing and open communication between all types of public safety organizations, intelligence agencies, military and other stakeholders. [42]

There is a growing need for secure, real-time, anytime interoperability with both internal and external partners. Public sector organizations, like Mexico City for example, are recognizing that need and piloting new initiatives that serve to connect data across public entities. Through its Ciudad Segura, or Safe City initiative, Mexico City implemented a unified command-and-control center for all security forces. [43]

In Contra Costa County, California, 1.1 million people live within striking distance of six oil and gas refineries. When the county's cutting-edge warning system, driven by BlackBerry technology, receives an alert from any one of these refineries, it can deliver detailed information to 25+ law enforcement and fire departments, plus the county's public health, hazmat and public works departments. In near real-time, alerts or warnings can reach thousands of homes, nearby schools, and healthcare providers. And refineries are linked to each other so they can respond quickly and share tools and resources in the event of any public safety issues. [44]

Improving intelligence with data analytics

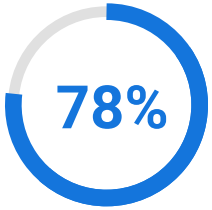
The Internet of Things is generating an ever-increasing flow of all types of data to public safety agencies, from body-worn cameras to surveillance cameras in smart cities to environmental sensors, data from smartphones, social media posts, and beyond. This involves capturing, storing and analyzing data in a way that produces valuable insight for more effective policing and public safety.

The Sacramento Police Department Real Time Crime Center aggregates data from Police Observation Devices or PODs (cameras located throughout city) and other streaming video feeds. The department also monitors radio traffic, social media feeds and tools like ShotSpotter (gunshot location service) – all to provide real-time information to officers during city events, investigations and critical incidents.[45]

Saving money and enhancing safety through prediction and prevention

As we know, IoT supports different, smarter, ways of operating versus conventional reactive approaches in public safety such as responding to calls for service. With data-driven insight, the strategic application of IoT data shifts to intelligent intervention, not just incident response. For example, a predictive and preventative model enables a department to detect fraud or identify crime hotspots, resulting in more effective resource deployment.[46]

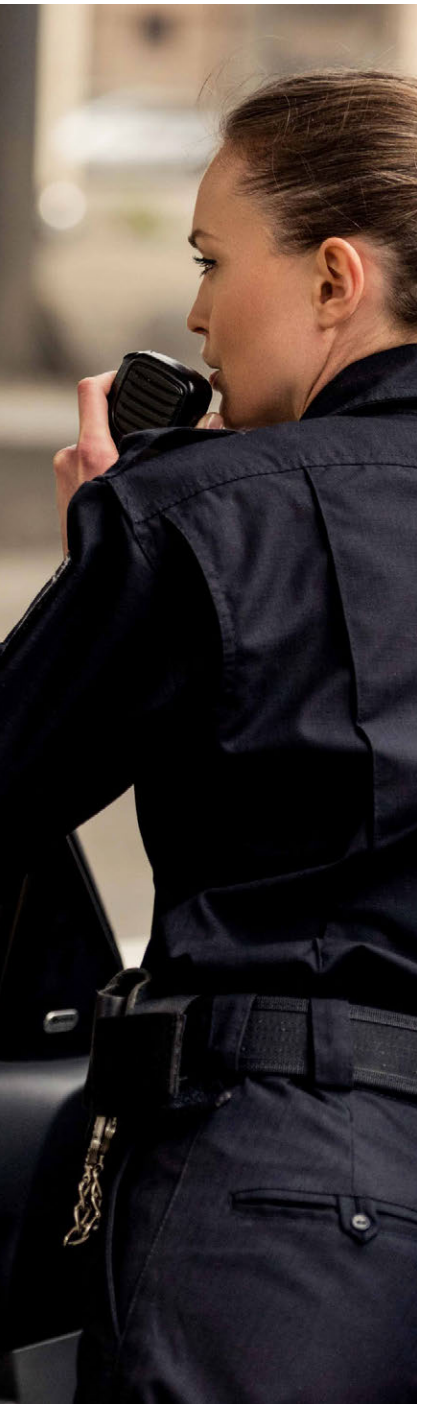
A study of this type of predictive policing based on advanced analytics in relation to robberies in Milan, Italy, concluded that predictive policing significantly improves police patrolling, and the benefits appear to outweigh the cost by a factor of five. [47]



Collaboration Against Crime

of police officers surveyed said their top communication need is inter-agency collaboration.

How Technology and Collaboration Can Help Create Smart and Safe Cities, BCG [48]



Digital Transformation Challenges in Public Safety

While 90% of public safety leaders have a high awareness of what digital transformation can enable, only half of public safety respondents have adapted their organizational models to take advantage of new technologies. [49] The following are just some of the obstacles slowing the pace of digital transformation in the public sector.

Financial constraints
Public safety operations are becoming more expensive due to increased personnel costs, growing public demand for police services, rising complexity of public safety work and operational inefficiencies. [50] Leveraging secure mobile technology that is easily deployed and managed can span this divide between ability and cost. Public safety agencies overcome the barriers of limited budgets and technical support to implement secure EoT solutions across the continuum of emergency response.

Outmoded systems and siloed operations
A large part of the public sector relies on legacy solutions that are not agile enough to meet today's intense, dynamic operational requirements. For example: desktops or laptops are used to access Records Management Systems, which can severely limit mobility and interoperability. Agencies realize they can achieve greater real-time collaboration by connecting across all platforms – including private, public, P25 and Public Safety (PS) LTE – and all devices, from Land Mobile Radios (LMR) to Mission Critical LTE handhelds to consumer-grade smartphones and tablets.

Shared connectivity is more critical than ever in ensuring that personnel from various agencies using different devices can interoperate and coordinate together.

Rising citizen expectations
Digital citizen culture demands faster, more personalized service that is accessible and responsive 24/7. More than two-thirds of citizens believe that the effectiveness of police services would be increased by greater use of digital technologies. [51]

Privacy
While citizens want to know about threats as quickly as possible, they're concerned about how their personal information will be used. For example, using a smartphone to message police services about a crime may turn a citizen into a witness, and that witness needs to trust that their identity won't leak through unsecure digital channels. Likewise, citizens who grant permission for public safety organizations to access their personal wearables (such as the elderly or vulnerable) need to know that agencies won't abuse those privileges or unwittingly expose their data to hackers, or even to third parties, such as insurance companies.

Skills gap
Old roles, such as the traditional beat police officer, lack the skills needed in hyper-connected environment (e.g. data analytics, digital investigation) In a recent survey, one-third of agencies say that, beyond budget, a lack of resources and technical support was their biggest challenge. This will increase as more data pours in to command and dispatch centers from other agencies, jurisdictions and from the public. Agencies must prepare to handle all of the data – and turn it into actionable intelligence – before it overwhelms them. [52]

Public education
Citizens need to understand what digital transformation initiatives public safety organizations are making and why – and of course, how these programs are being secured – so they can join in with confidence. That takes an investment in ongoing communication with the public, something that isn't always accounted for in public sector budgets. But in the EoT, public safety improves with each new node in the network.

Security
Last, but perhaps most important, there is the challenge of securing the whole connected public safety ecosystem. Existing solutions do not allow officers to securely and efficiently collect sensitive information such as interviews and interrogations, and arrest and booking details, and there is no secure method to share data and files with internal and external partners either.

How BlackBerry is Helping Public Safety Organizations Secure the EoT

Public safety agencies have already adopted a wide spectrum of IoT technologies to improve intelligence, surveillance, inter-agency collaboration and predictive policing. Here's a brief look at some of the ways BlackBerry is helping them move toward a trusted EoT.

For criminal investigations
BlackBerry provides officers with a secure and easy to use system to communicate, consult and collaborate with other parties both internal and external to their agency (such as social workers, lab techs, and forensic experts). They can do so while at the crime scene, and in the aftermath, through text, photos, voice notes, and videos. This kind of fast, secure teamwork in a missing persons case, for example, can save lives.

For records management
BlackBerry technology helps officers easily create and file documents from anywhere, then share those documents with external collaborators without fear of losing control or exposing content to unauthorized parties. This capability creates dramatic improvements in the speed and convenience of filing statements and other forms. It also improves the quality of data with less re-keying or double-keying of officer-supplied data. And it makes critical information available virtually immediately, without compromising security.

For incident coordination
To effectively respond to incidents, law enforcement must communicate and coordinate with their own officers, as well as other first responders, regardless of location. This includes bringing in personnel whether they are on or off duty. BlackBerry's networked crisis communication system provides a secure way to unify critical communications within and between organizations, their people, devices, and external entities.

This technology enables organizations to gain real-time visibility into their personnel's safety and status, send emergency mass notifications to anyone and anywhere on any device, communicate and collaborate with other organizations, and gather critical information from people for situational awareness. For example, Contra Costa County needed a fully integrated warning system to evacuate residents from a forest fire on Mount Diablo. BlackBerry provided this system, helping first responders get information quickly and securely to the public. [53]

For evidence gathering

With communication and first responder apps directly on their devices, officers can quickly and securely gather all types of media on the scene and file reports. This allows them to be more self-sufficient, without waiting for someone else to do checks or find information for them. BlackBerry's unified endpoint management system offers trusted end-to-end security and support for a wide range of devices, with enhanced collaboration tools and secure file sharing. This type of secure, reliable access to data is essential, especially in emergency scenarios.

To speed up complex criminal investigations, police officers need to share documents with other agencies, the prosecutor's office, and social workers, while remaining in complete control of sensitive information. BlackBerry's content collaboration platform addresses the challenge of securing the exchange of sensitive information, by applying a combination of FIPS 140-2 validated encryption and integrated digital rights management.

BlackBerry's networked crisis communication system empowers public safety agencies to make better decisions by enabling field personnel to be the eyes and ears of the operations center. For the first time, an operations center can see what's happening at the incident scene, enabling rapid mobilization for a more effective response.

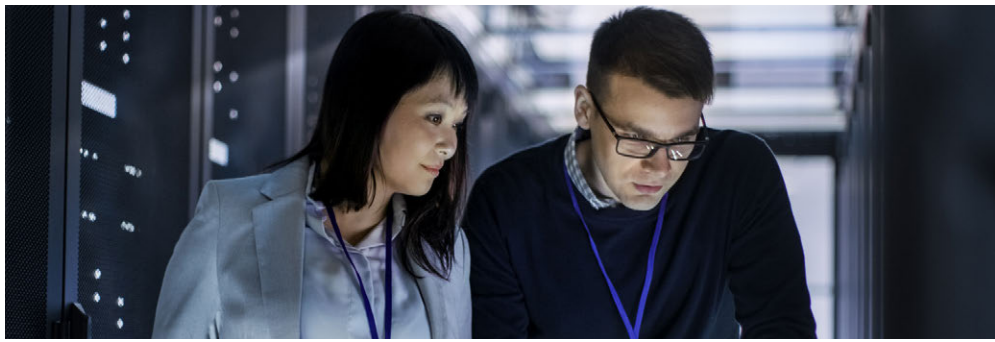
For supervisory awareness
Officers need a reliable secure instant messaging solution on their devices to allow those outside of a patrol vehicle to communicate with one another, without having to tie up the Land Mobile Radio (LMR). This can be especially valuable during busy call periods when the radio system can be congested. BlackBerry technology enables officers to communicate securely via text, voice, or video, with end-to-end encryption. BlackBerry crisis communication solutions allow organizations to gather critical information from their people for situational awareness, [54] and to gain real-time visibility into personnel location and status for effective crisis handling and response. [55]

For the prosecutor's office
Public sector agencies face strict requirements to carefully manage and control sensitive information. However, this information often needs to be shared internally and externally. As prosecutors embrace mobility, new challenges emerge for providing information to any mobile device, computer or tablet, anywhere in the world. Lawyers and support staff need the ability to work with and share files while mobile, but device-centric security fails to address data security requirements when information is accessed on unmanaged devices.

BlackBerry addresses the challenge of securing critical information while enabling seamless sharing and collaboration. This allows for cross-agency collaboration as legal teams can set permissions to access, download, view, edit, copy, or print. Prosecutors stay in control of content even after external collaborators have downloaded it.

For civilians
BlackBerry technology provides unified crisis communications with mass alerts across internal and external channels. In Iztapalapa, Mexico, for instance, an earthquake warning system issues public alerts, and allows users to share pictures of damaged buildings after the incident, pinpoint where those buildings are located and indicate whether they're habitable. This empowers every person in the organization to report events, work progress and operational status using geo-tagged multimedia information – from the field. [56]

For IT
Using BlackBerry's technology, operators from any location in the organization can activate alerts to virtually any device, track responses and view accountability reports. Through a single web-based console, IT teams can launch and manage all communication channels simultaneously. This real-time response tracking provides accountability and visibility into the safety and status of personnel.



How a Major Police Service Modernized Emergency Communications

Challenge

Incident Command and Traffic Services Operators in a large municipal police force relied on group text messages and emails to alert and distribute information to first responders during critical events. The operators created manual distribution lists that required constant updating, and text messages had limited space for detailed information. Even worse, officers often missed the alerts when their phones were in silent mode.

Solution

The police force implemented BlackBerry® AtHoc® in a pilot project involving 80 first responders who received alerts based on automated workflows and predefined templates. The new system included notification capabilities on phone, email, SMS and mobile, while allowing operators to track replies in real time.

Results

Operators gained the ability to notify officers via multiple channels, instead of text messages alone, and no longer wasted time updating distribution lists. The police department benefited from the capacity to audit all alerts and responses. Based on the pilot project's success, the police force is expanding their use of BlackBerry AtHoc across the organization.

How a Law Enforcement Agency Enabled Secure Mobility for its Officers

Challenge

One of the largest police agencies in the U.S. needed to provide its field officers – intelligence officers in particular – with simple, quick access to its central database. Strict security regulations required two-factor authentication, so the department used costly, inconvenient hardware tokens. They needed a more affordable, user-friendly solution for remote connectivity.

Solution

The department deployed BlackBerry® UEM for cross-platform management of all mobile endpoints, in addition to BlackBerry® 2FA, which allows field officers to authenticate with critical systems using only their device.

Results

Since the move to BlackBerry UEM and 2FA, the department has lowered its security costs and gained greater control over its mobile fleet. Field officers can easily access critical information, and the IT department spends less time on helpdesk requests.

Bringing it All Together

From terrorism and human trafficking to gun violence and cyber attacks, new and growing threats in the physical and digital world demand innovative, data-driven approaches to keeping citizens safe. Many public safety organizations that have started on the path toward digital transformation with discrete IoT solutions and siloed communication strategies for maximum effectiveness and efficiency, instead need a unified approach that gives every stakeholder the ability to securely access, capture, analyze and share the right data at the right time.

Addressing Yesterday's Issues, Today

Securing the Enterprise of Things requires that every access, every interaction, every communication with every person is singularly secure from any endpoint and any location. Securing the Enterprise of Things means that public sector operations are productive, safe and secure.

To make it happen, you need the most secure and comprehensive software platform to connect people, devices, processes, systems and organizations.

Today	Tomorrow
Disparate security solutions in place to address rising threats	Public sector agencies are resistant to malicious attack with holistic security solutions
No standard automated process for emergency communications	Unified critical communications connect and protect people, devices and external organizations
One-off projects underway for digital transformation that may not integrate with others (in security, especially)	An EoT and digital transformation environment that's unified, integrated and secure from top to bottom
No secure access to corporate systems from outside the office	Secure remote access for any Windows® 10 or macOS device
Multiple logins	Microsoft® mobile apps can be used seamlessly and securely from every endpoint
Endpoints that aren't secure, unsecured BYOD, and accidental content leakage – despite multiple MDMs	Confidence that all endpoints can be secured, whatever the ownership model, and managed through a unified platform
A wide variety of file sharing solutions	Security travels with files wherever they go
No standard for EoT and wearables connectivity	Wearables and other IoT devices a connect using the same standards as other endpoints
Consumer messaging use for public sector business	Collaboration (with coworkers and external partners) happens inside a secure managed app environment
Disconnected workplaces, closed workforces, siloed workflows	Secure connectivity that unifies and enhances workplaces, workforces and workflows. Instantaneous control and response in complex autonomous systems

About BlackBerry

BlackBerry is an enterprise software and services company focused on securing and managing IoT endpoints. The company does this with BlackBerry® Spark™, an end-to-end Enterprise of Things platform, comprised of its enterprise communication and collaboration software and safety-certified embedded solutions.

Learn more at: www.blackberry.com

Sources

1. https://www.mckinsey.com/~/media/mckinsey/industries/public%20sector/our%20insights/transforming%20government%20through%20digitization/digital-by-default-a-guide-to-transforming-government-final.ashx
2. https://www.slideshare.net/accenture/what-do-citizens-want-10-key-insights-for-public-service
3. https://www.congress.gov/bill/115th-congress/senate-bill/1088
4. https://www.mckinsey.com/~/media/mckinsey/industries/public%20sector/our%20insights/transforming%20government%20through%20digitization/digital-by-default-a-guide-to-transforming-government-final.ashx
5. https://www.slideshare.net/accenture/what-do-citizens-want-10-key-insights-for-public-service
6. http://www.govtech.com/dc/digital-cities/Digital-Cities-Survey-2017-Winners-Announced.html
7. https://www.mckinsey.com/~/media/mckinsey/industries/public%20sector/our%20insights/transforming%20government%20through%20digitization/digital-by-default-a-guide-to-transforming-government-final.ashx
8. https://www.mckinsey.com/~/media/mckinsey/industries/public%20sector/our%20insights/transforming%20government%20through%20digitization/digital-by-default-a-guide-to-transforming-government-final.ashx
9. https://www.cnbc.com/video/2018/07/22/singapore-experiences-its-worst-data-breach.html
10. http://www.govtech.com/network/practical-uses-of-the-internet-of-things-in-government-are-everywhere.html
11. https://www.sap.com/cmp/dg/sapleonardo-public-sector/index html?resource=%2Fcontent%2Fsapdx%2Fwebsite%2Fnam%2Fusa%2Fen_us%2Fcmp%2Fdg%2Fsapleonardo-public-sector%2Ftyp.html&j_reason=unknown&j_reason_code=unknown#pdf-asset=2ac218fb-b97c-0010-82c7-eda71af511fa&page=10
12. https://www.mckinsey.com/~/media/mckinsey/industries/public%20sector/our%20insights/transforming%20government%20through%20digitization/digital-by-default-a-guide-to-transforming-government-final.ashx
13. https://www.slideshare.net/accenture/what-do-citizens-want-10-key-insights-for-public-service
14. http://www.govtech.com/network/practical-uses-of-the-internet-of-things-in-government-are-everywhere.html
15. https://www.slideshare.net/accenture/what-do-citizens-want-10-key-insights-for-public-service
16. https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
17. https://www.policeone.com/communications/articles/69229006-First-look-2016-tech-trends-cops-need-to-know/
18. https://www2.deloitte.com/content/dam/insights/us/articles/digital-transformation-in-government-summary/DUP_1424_Journey-to-govt-digital-future_EXEC-SUMMARY.pdf
19. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5087432/
20. http://aviationweek.com/aviation-maintenance-and-support-software/how-digital-transformation-reshaping-defense-industry
21. https://www.mckinsey.com/industries/public-sector/how-we-help-clients/defense-and-security
22. https://www.accenture.com/gb-en/blogs/blogs-five-steps-creating-your-first-line-defense
23. https://www2.deloitte.com/insights/us/en/focus/internet-of-things/iot-in-military-defense-industry.html
24. https://www.dhs.gov/publication/blue-force-tracking-systems
25. https://www2.deloitte.com/insights/us/en/focus/internet-of-things/iot-in-military-defense-industry.html
26. https://www2.deloitte.com/insights/us/en/focus/internet-of-things/iot-in-military-defense-industry.html
27. https://www.accenture.com/gb-en/blogs/blogs-five-steps-creating-your-first-line-defense
28. https://www.nato.int/docu/review/2015/also-in-2015/enhancing-interoperability-the-foundation-for-effective-nato-operations/EN/index.htm
29. https://www.nextgov.com/cybersecurity/2018/01/pentagon-thwarts-36-million-email-breach-attempts-daily/145149/
30. https://www2.deloitte.com/us/en/pages/public-sector/articles/national-security-industry-outlook.html
31. https://www.publicintegrity.org/2017/03/23/20778/public-favors-cutting-defense-spending-not-\adding-billions-more-new-survey-finds
32. https://www.defenceiq.com/defence-technology/articles/digital-transformation-first-line-of-defence
33. https://www.defenceiq.com/defence-technology/articles/digital-transformation-first-line-of-defence
34. https://digit.hbs.org/submission/digital-transformation-and-the-dod/
35. https://www.defenceiq.com/defence-technology/articles/digital-transformation-first-line-of-defence
36. https://www.mckinsey.com/industries/public-sector/our-insights/policing-a-vision-for-2025
37. https://www.accenture.com/t20170224T045610Z__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Local/PDF/Operations_2/Accenture-Web-Connected-Public-Safety-Pov.pdf
38. https://www.nytimes.com/2017/01/06/us/police-body-cameras.html
39. https://www.nytimes.com/2017/01/06/us/police-body-cameras.html
40. https://www.networkworld.com/article/3105045/internet-of-things/holy-batman-look-at-how-iot-has-transformed-police-cars.html
41. https://www.accenture.com/t20170224T045610Z__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Local/PDF/Operations_2/Accenture-Web-Connected-Public-Safety-Pov.pdf
42. http://goldenstateinc.com/downloads/motorola/whitepapers/motorola_public_safety_survey.pdf
43. https://placesjournal.org/article/inside-mexico-citys-c4i4-surveillance-center/
44. https://www.athoc.com/ccc-video.html
45. http://www.govtech.com/em/safety/Sacramento-real-time-crime.html
46. https://www.mckinsey.com/industries/public-sector/our-insights/policing-a-vision-for-2025
47. https://www.mckinsey.com/industries/public-sector/our-insights/policing-a-vision-for-2025
48. http://goldenstateinc.com/downloads/motorola/whitepapers/motorola_public_safety_survey.pdf
49. https://www.accenture.com/_acnmedia/PDF-41/Accenture-Public-Safety-Digital-Disruption.pdf
50. https://www.ncjrs.gov/pdffiles1/nij/231096.pdf
51. https://newsroom.accenture.com/subjects/research-surveys/majority-of-us-citizens-feel-safe-in-their-neighborhoods-but-want-police-to-increase-community-collaboration-and-their-use-of-digital-communication-tools.htm
52. https://www.motorolasolutions.com/content/dam/msi/docs/2015_public_safety_survey_white_paper.pdf
53. https://www.athoc.com/ccc-video.html
54. https://www.blackberry.com/content/dam/blackberry-com/Documents/pdf/athoc/br-athoc-collect.pdf
55. https://global.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/wp-athoc-smarter-personnel-accountability.pdf
56. http://bizblog.blackberry.com/2016/06/how-athoc-is-helping-keep-mexico-city-residents-safe-from-earthquakes/


BlackBerry®