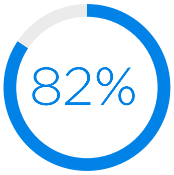
EXECUTIVE BRIEF

PUBLIC SAFETY TECHNOLOGIES

Your network is critical to mission success

Spectrum ENTERPRISE

Digital technologies like smart video and audio surveillance, smart street lights, body-worn cameras (BWCs), biometric monitoring systems and other Internet of Things (IoT) devices can help protect citizens and support public safety missions. They contribute to accountability, build trust within communities and provide real-time information on incidents in the field.



of police officers want to use body-worn cameras.[1]

IoT devices generate tremendous amounts of data that must be transported across a highly reliable, secure and high-capacity network. In this executive brief, you'll learn about the essential — and challenging — role that networks play in the public sector, as well as the solutions that support a successful public safety technology program.

Identify network challenges

Today's connected technologies make public safety more transparent. Their presence can also contribute to de-escalation and increase compliance during incidents. It's no surprise, then, that 82 percent of police officers want to use BWCs.[2] Studies show a 90 percent decrease in complaints against officers who wear the devices.[3] But, for all the potential they offer, public safety technologies are only as good as the infrastructure behind them. IT decision makers confront a range of network challenges to ensure IoT solutions are reliable enough for public safety officers:

Bandwidth

IoT devices' output can collectively generate hundreds of hours of video or audio daily that requires substantial bandwidth for storage and retreival. The Oakland Police Department, for example, transmits more than 7 TB of video footage per month from its BWCs alone.[4] Many agencies starting a public safety IoT program turn to cellular connections to mitigate the impact of new devices on their network traffic. However, an overreliance on cell network bandwidth can create latency issues during transport, sometimes resulting in low-resolution videos that may not hold up in court. Agencies need resources to scale their connectivity as IoT usage grows.

Public safety agencies can be required to store critical video footage and other data for five years or longer.[7]

Data storage

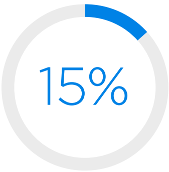
Public safety agencies can be required to store critical video footage and other data for five years or longer.[5] The amount of storage needed for BWCs can be immense, costly and time-consuming to manage on-premises. As a result, 88 percent of police forces are considering investing in cloud services to expand their storage and computing capabilities.[6]

Network operations

Transmitting video footage over an internet connection seems simple enough. But managing thousands of IoT-generated video files that need to be accessible on demand can require substantial upgrades to network architecture. This can grow to include multiple internet connections, private networks that move encrypted data among police stations and courthouses and increasingly sophisticated solutions for routing and traffic management. Complexity is a persistent challenge for public safety organizations that lack the in-house IT resources to keep pace with expanding demands on their networks.

324 days

is the average time it takes to detect and contain a data breach caused by a malicious attack on the public sector.[10]



reduction in IT costs, on average, can be experienced by organizations migrating to the cloud.[12]

Security

There's no shortage of stories detailing how hackers target high-value networks — including those that handle police records. On average, it takes 324 days to detect and contain a data breach caused by a malicious attack on the public sector.[8] At the same time, 56 percent of state IT leaders are not very confident in the cybersecurity practices at their state and local government organizations.[9] On top of daily management of the network, public safety IT teams must develop plans to protect sensitive data from IoT devices and other applications.

Find the right solutions

The equipment used in the field is only one component of an effective public safety program. Just as much scrutiny should be given to the networks that transmit, store and make footage accessible when it's needed. Public safety agencies need to adopt networking solutions to scale in a secure and manageable way.

High-capacity connectivity

Enterprise fiber solutions can handle even the most demanding public safety data traffic. Carrier-grade internet and Ethernet offer reliable connections between stored IoT data and investigators or courts. The best providers deliver security, reliability and throughput up to 100 Gbps with service-level agreements that meet the high standards of public safety organizations. Agencies can also establish private connections to cloud service providers for the secure transmission of sensitive data.

Connections to the cloud

Organizations can save an average of 15 percent of their IT costs by migrating to the cloud.[11] Connecting a network to the cloud offers scalability to meet evolving data storage needs. Going this route can also eliminate the upfront capital costs and ongoing maintenance associated with managing an on-premises data center.

Network technologies

A software-defined wide area network (SD-WAN) offers the ability to manage a complex multi-site network more easily from the cloud. It uses intelligent traffic routing to allocate bandwidth in real time to support changing network demands or to keep essential systems online in the event of a disruption. This helps networks scale to accommodate vast amounts of data, ensuring the ability to access video footage when and where it's needed.

Provider-managed security

A unified threat management solution with an advanced firewall can help protect the perimeter of a network. Meanwhile, distributed denial of service (DDoS) protection from a connectivity partner can identify and neutralize volumetric attacks. Managed security services from a nationwide network provider can help maintain and manage cybersecurity solutions for public-sector agencies with limited resources.

Managed solutions

In addition to security, public safety agencies can rely on managed services for other elements of their networks, such as routing, WiFi and SD-WAN. The right solutions provider can help free agencies from routine IT tasks like firmware updates, security patches and other network maintenance — allowing them to focus more on how best to protect and serve their communities. Working with a single partner providing multiple solutions can also simplify network management, strengthen security and give agencies one number to call for issue resolution.

Achieve your goals

Modernizing a network to support data-intensive applications can be a challenge for organizations navigating the daily demands of first responders. A trusted provider of network services with experience serving state and local governments can help them enhance network components like SD-WAN, WiFi, routing and firewalls. Agencies can also streamline IT operations by working with a partner to combine managed services and connectivity to meet their unique goals. The right provider will have local network experts who can manage and resolve issues as they arise — freeing up your team to focus on the critical work of public safety.

To learn more about strengthening your community through the power of connectivity, visit enterprise.spectrum.com/government.

1. James Careless, "How Body-worn Cameras Can Improve Police Transparency While Promoting Officer Safety," Police1, Jan. 19, 2021.
2. Ibid.
3. "7 Quick Stats About Police Body Cameras," 10-8 Video Systems, 2021.
4. Shridar Subramanian, "To Protect and Store: Body Cameras Place New Demands on Police," Evidence Technology Magazine, accessed Nov. 30, 2021.
5. Ibid.
6. Maham Zaidi, "Cloud Adoption is Essential for Law Enforcement," Vidizmo, accessed Nov. 30, 2021.
7. Shridar Subramanian, "To Protect and Store: Body Cameras Place New Demands on Police," Evidence Technology Magazine, accessed Nov. 30, 2021.
8. "Cost of a Data Breach Report," IBM, 2020.
9. "States at Risk: The Cybersecurity Imperative in Uncertain Times," Deloitte and the National Association of State Chief Information Officers, 2020.
10. "Cost of a Data Breach Report," IBM, 2020.
11. Kyle Turco, "4 Ways Cloud Computing Can Save Your Company Money," Technology Advice, June 24, 2021.
12. Ibid.

About Spectrum Enterprise

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions. The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. For more information, visit enterprise.spectrum.com.

Not all products, pricing and services are available in all areas. Pricing and actual speeds may vary. Restrictions may apply.