Designing a Public Safety Ecosystem

When designing and implementing technology environments, it's important for public safety organizations to think about the entire ecosystem: applications, services and network infrastructure. Before they can truly benefit from emerging technologies such as next-generation 9-1-1 (NG9-1-1) — which can enhance the speed, accuracy and efficacy of first responders by enabling citizens and public safety answering points to send and receive voice, text, photos and video communications over an internet protocol (IP) network — they need to have a robust ecosystem in place.

Without an adaptive, scalable and robust foundation, these solutions likely won't perform at their best. In addition, if security isn't a key part of the ecosystem, data transmission could be vulnerable to cybercriminals and other bad actors. This issue brief describes some of the key components public safety organizations need to consider when planning their ecosystems to support NG9-1-1.

Deploying the Right SD-WAN

One of the most important components of the public safety ecosystem is the network that supports a variety of communications options. Deploying a high-quality software-defined wide area network (SD-WAN) is essential to operating a public safety ecosystem in today's digital world.

An SD-WAN accelerates network agility by dynamically routing traffic, managing user policies and setting security controls in near real time. It can also help public safety agencies prioritize applications, mitigate performance issues and deploy application-aware failover to ensure continuous access to critical cloud-based resources.

In addition, SD-WAN offers enhanced resiliency and a high level of security. Public safety agencies can protect their networks by deploying active/active connectivity that is balanced under normal conditions and automatically reroutes traffic if one connection goes down.

Among the key security features agencies should look for in an SD-WAN offering are authentication, key exchange and encryption, firewall with content filtering, URL filtering, IP filtering, intrusion detection/protection, and real-time as well as historical analytics and reporting.

Ideally, public safety agencies should not have to manage the entire SD-WAN on their own, but should look to leverage outside expertise when needed through a managed services provider with highly skilled experts to help design, configure, deploy and manage the network. This frees up internal IT resources for other strategic projects.

Bolstering Security

The cybersecurity landscape is constantly evolving, so real-time threat information has to be incorporated into NG9-1-1 networks on a regular basis.

New digital services being offered by public safety providers are IP-based, which means they are vulnerable to a large number of potential threats, including distributed denial-of-service (DDoS) attacks. One recent study conducted out of North Carolina found only 6,000 bots are sufficient to significantly compromise the availability of a state's 911 services and only 200,000 bots can jeopardize the entire United States.[1] Public safety operations are natural targets for cybercriminals and other bad actors, and agencies need to take appropriate action by creating a defense-in-depth strategy.

A cybersecurity program needs to include components such as global threat intelligence that's capable of finding and stopping DDoS attacks, web application firewalls to safeguard individual applications and managed firewalls that protect network perimeters from external threats. It also requires professional security services that include ransomware assessment, cybersecurity awareness training and other offerings.

Data analytics capabilities have advanced enormously in recent years, and agencies can apply this to threat management

efforts. Automated tools can proactively identify and respond to potential security issues before they cause serious problems.

Providing Power at the Edge

Edge computing is enabling public safety agencies to more easily leverage Internet of Things (IoT) applications and speed the delivery of services to citizens. Data on the edge will help emergency control centers (ECCs) share data, which is particularly important in certain emergency situations where multiple groups of first responders have to work together and exchange information.

With edge computing, organizations can move computing power, storage and data analytics much closer to where they are actually collecting the data, including a variety of devices equipped with sensors. For instance, first responders can assess video surveillance feeds in real time for facial recognition and alert a community immediately if a perpetrator is in the area.

This capability eases or eliminates the problem of network latency, and can enable faster decision-making based on findings gathered in the field. Public safety providers can see benefits such as increased performance of high-bandwidth applications, faster software updates, access to location-based analytics and increased security.

Edge platforms can serve as extensions of on-premises environments, providing a seamless infrastructure that allows public safety organizations to take advantage of their existing data centers, cloud services, and mobile devices and apps as needed.

Utilizing Public Safety as a Service

The market is moving toward a public safety as a service model that reflects the larger move to the cloud underway across virtually every facet of government and type of business. This lets agencies move to a predictable, monthly operating expense model instead of a one-time capital expense model. For some agencies this is a better financial model. Organizations that provide safety services within their communities need to consider and prepare for this eventual shift — whether it's near term or long term.

When they deploy managed solutions, public safety providers do not need to own, manage and maintain their own network equipment. That frees up time for technology professionals to focus on delivering better services to the community.

With this new model, service providers manage the entire infrastructure for an organization, providing a team that offers various levels of support. Public safety agencies can make changes in network, security or application configurations as they see fit, or can have the support team make these changes for them.

With edge computing, organizations can move computing power, storage and data analytics much closer to where they are actually collecting the data, including a variety of devices equipped with sensors. For instance, first responders can assess video surveillance feeds in real time for facial recognition and alert a community immediately if a perpetrator is in the area.

Some of these service offerings also provide cybersecurity resources, including the necessary tools to defend against attacks. This is especially useful for smaller organizations that might not have the resources or expertise they need to deal with these risks on their own.

Embracing the Digital Age

The emergence of digital services and tools presents public safety entities with unprecedented opportunities to better serve their communities. But to take full advantage of these new offerings, they need to think about the ecosystem that makes these new capabilities possible.

That means having modern networking technology in place, leveraging edge computing and building a strong cybersecurity program. And as the internet and cloud services play an increasingly large role in the delivery of public safety services, agencies should consider bringing in an outside expert to provide the necessary expertise and support.

Moving to a services model to design, manage and maintain the technology ecosystem does not mean giving up control. Rather, it's an opportunity to enable experts to help an organization transform more quickly into a digital enterprise – and better serve their communities.

This piece was developed and written by the Center for Digital Government Content Studio, with information and input from Lumen.

ENDNOTES:

1. https://www.hstoday.us/subject-matter-areas/cybersecurity/study-next-generation-911-services-highly-vulnerable-to-cyber-attack/

Produced by: CENTER FOR DIGITAL GOVERNMENT

For: LUMEN®

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

Lumen is guided by our belief that humanity is at its best when technology advances the way we live and work. We deliver the fastest, most secure platform for applications and data to help government deliver amazing experiences. Learn more about Lumen's network, edge cloud, security and communication and collaboration solutions and our purpose to further human progress through technology at **www.lumen.com.**

Photo provided by Shutterstock.com