Enabling Smart Spaces: Strategies for Government

Smart spaces bring together universal connectivity and the potential of the Internet of Things (IoT) to enhance the places we live, work and play. They also help governments improve the constituent experience, accomplish more with limited resources and make good on the aspirational promise of smart cities. "Smart spaces connect citizens and enrich their lives," says Collin Averill, Cisco Meraki Solutions Marketing Manager.

This brief defines how smart spaces can transform government, the key components required to build out the underlying technology infrastructure, and strategies to begin connecting governments and the communities they serve.

Smart spaces and governments

Smart spaces represent a combination of technologies that, when integrated in intentional ways, enable greater interactivity in the places where people gather. Built on a foundation of networks and connectivity, they leverage touchpoints—smartphones or Wi-Fi devices, sensors, cameras and other connected technology—to help leaders understand and improve conditions in a physical location. "Smart spaces are about bringing together touchpoints and technology in ways that come together for an experience," says Averill.

For governments, those experiences can help better serve residents in public places such as schools, libraries, government offices, parks and high-traffic areas. For example, making public Wi-Fi available in libraries or other facilities can help meet constituent expectations and narrow the digital divide for those who lack internet access at home. But that's just the beginning of the potential of government smart spaces:

- **Cameras, smart IDs and device tracking systems can help governments understand how constituents and employees navigate public spaces to improve their design, ensure they remain secure, and provide personalized information and wayfinding.**
- **Data collected from smart spaces can help governments make wiser decisions about how facilities and public spaces are configured and when they should consider adding or reducing capacity.**
- **Once a connected infrastructure is in place, governments can rapidly create smart spaces to meet immediate needs, such as mass vaccination sites or polling places.**

Together, these capabilities improve constituent services, facility utilization, and, in the long run, the overall effectiveness of government and quality of life for residents.

Inputs and outputs: The building blocks of smart spaces

Smart spaces rely on an integrated ecosystem that brings together connectivity, intelligence and security. At the highest level, smart spaces require a network backbone that enables connected devices to collect data, or inputs, that can be aggregated and analyzed to generate outputs, which are data-informed insights that guide decision-making.

"You've got to have the inputs to have the outputs," Averill says. "Those outputs will drive better citizen experiences."

Intelligent cloud-based networks

Cloud-based networks are the foundation that enables smart spaces. They provide connectivity for IoT and constituent and employee devices. They ensure security of both physical and digital environments and enable the data collection and analytics that drive the full benefits of making spaces smart.

Connectivity for public Wi-Fi has become an expectation when people are in government facilities, and it served as a lifeline when schools were closed during the pandemic and libraries and community centers served as community hubs. As an integrated solution, networks must have sufficient bandwidth to securely accommodate a growing number of devices—constituent and employee computers, phones and tablets, but also the sensors, cameras and other IoT devices needed to make a space smart.

The new Wi-Fi 6E standard enables large numbers of connections to different kinds of devices. Capabilities such as cellular Wi-Fi and fluid mesh or wireless backhaul can provide fail-safes for critical services and allow governments to open polling stations or other short-term services within communities as the need arises.

In Miami-Dade County, Libraries Connect Communities

During the pandemic, the Miami-Dade Public Library System created smart spaces at all 49 of its locations, standing up 200 public Wi-Fi access points to ensure residents could connect. "People shouldn't be marginalized by lack of access to technology or bandwidth," says Ray Baker, Director of the Library System. "That's been central to everything we've been doing around the digital divide."

Connectivity was part of a broader refresh of the system's underlying network, which also added more than 1,000 smart cameras. Along with ensuring physical security, the cameras provided new insights into traffic flow, usage facilities, and where floor plans helped or hindered patrons. "It's our mission to interpret what happens when people visit the library," says IT Manager Julio Campa. Smart cameras also facilitate the sharing of information to other departments that help maintain facilities, and a unified dashboard allows the system to be managed by just two staff members.

In Colorado, Smart Spaces Provide Peace of Mind

The Marmot Library Network's six-person IT staff is charged with overseeing 1.2 million one-of-a-kind books, documents, maps and works of art focusing on Colorado's pioneer past in 35 libraries across the state's rural Rocky Mountains region.

As part of a network refresh that provided remote management of secure library Wi-Fi networks across all locations, Marmot added water leak detection sensors that allowed staff to monitor and protect both the artifacts and the network infrastructure remotely — critical for a small workforce in a region where weather can make travel difficult or impossible. "The historic collections they protect are irreplaceable," says Systems Administrator Jason Stow. "If one piece is damaged, it could be the only one like it in the world."

However, networks are only as good as an IT staff's ability to manage them. For governments with limited resources, it's essential that they are easy to administer and monitor. One critical component is having a single pane of glass for visibility into the entire system, letting staff manage all conditions from a single dashboard.

"The ability to manage everything in one place in the cloud is a differentiator that allows IT teams to solve for business-critical situations," says Chris Allen, Cisco Meraki Public Sector Marketing Manager. "You want to ensure you have that gateway and that your access points can handle tons of devices with a high level of security across all devices. But you also need to ensure you have the software that allows you to manage it and quickly provision new services."

Inputs: IoT and constituent and employee devices

IoT has evolved considerably in recent years, providing new opportunities to gather data that can help governments understand and improve facilities and services.

Security cameras, for example, have become smart sensors that provide capabilities far beyond visual monitoring for physical security purposes. They can also be used to track footfall and monitor capacity levels. This monitorization can help optimize the layout of heavily trafficked facilities, like libraries or motor vehicle departments, or assist with future planning for transportation hubs and city traffic signals. They can also ensure compliance with rules such as wearing badges or masks—an unanticipated need that smart technology was able to meet during the pandemic. "There are benefits you never thought you'd need to leverage," says Kelly Broadhurst, Cisco Meraki Marketing Manager.

Beyond cameras, connected sensors can identify changes in temperature and humidity, detect the presence of water, and alert staff when dangerous levels are reached or if a secure door is opened or closed. That's particularly helpful for government agencies managing a wide range of locations with a small workforce. Sensors can also monitor the network infrastructure itself, alerting IT staff when temperatures rise or moisture is detected in server rooms.

Intelligent networks also leverage user devices like smartphones and tablets to securely and anonymously track movement through public spaces to better understand how they are used.

Together, these connected devices generate the data and insights needed to make a space smarter and more efficient. Doing so requires a network with the capability to manage data from a wide range of connected devices through application programming interfaces (APIs) and other tools that ensure interoperability.

Outputs: Making sense of data

Connected devices generate large amounts of data. The challenge for governments, says Averill, is to "get actionable data and do something with it."

Platforms with analytics capabilities are essential to translate these inputs into actionable outputs. This includes everything from alerts or notifications signaling immediate issues such as a security breach or water damage to longer-term insights that allow governments to plan and maximize scarce resources. For governments, the key to generating meaningful outputs is to allow department or program leaders to understand the data through intelligent analytics and dashboards they can access and adjust to address changing needs.

"It used to be that IT had to pull the data and get data scientists to determine the needs," Allen says. "Starting with the network backbone, you have the ability to bring in the ecosystem, the APIs and the business partners to make decisions."

Strategies for smart spaces

For governments, smart spaces provide an opportunity to improve technology infrastructure in sustainable ways. They allow governments "to modernize while knowing they're up against constraints," Allen says.

“What is the problem you’re trying to solve? Ask yourself, what’s the challenge? Do you have the ability for the data inputs now, and is the data you’re collecting easily usable and digestible?”

Chris Allen, Public Sector Marketing Manager, Cisco Meraki

Those constraints may vary from locality to locality or department to department. Some are “ready to disrupt, wanting to innovate and provide these amazing outcomes,” says Katie Antonetti, Cisco Meraki Product Sales Specialist. Others, she adds, “are just trying to catch up,” in large part because of limited resources or previous budgetary challenges.

The benefit of the underlying network is that governments can start small and scale over time across multiple physical spaces or use cases. “It can start as simply as a few sensors to bring in IoT and understand how easy it can be to implement and how useful the data can be,” Allen says.

Among the strategies for government leaders:

Begin with challenges, not technology. Successful implementations rely on understanding government and resident needs. “What is the problem you’re trying to solve? Ask yourself, what’s the challenge? Do you have the ability for the data inputs now, and is the data you’re collecting easily usable and digestible?” Allen says. “Where I’ve seen success in some cases is not focusing on the newest bells and whistles but on using technology to meet the challenges in the moment. That’s how you solve those immediate problems.”

Ensure all stakeholders are involved in decision-making. Involving stakeholders in determining challenges and needs is critical for both the technology rollout—where historically siloed IT, facilities and security teams must collaborate on solutions for a specific space—and also to meet broader objectives.

Focus on gaps—data in particular. Once they identify objectives, IT leaders can help identify the gaps. This includes not only the devices and capabilities required to collect data, but also the ability to convert the data into actionable information.

“It’s not just which switches and ports you use and how you provision layered security, but how you make informed decisions that allow you to execute,” Allen says. “It’s about how you allow IT to become business decision-makers and generate insights.”

Emphasize cybersecurity. Smart spaces dramatically increase the number of endpoints accessing the IT infrastructure. “The more complexity you add to providing the services, the more difficult it is to deploy them in a safe way,” Allen says, noting that it’s critical that network infrastructure provides secure access and simplifies the process of onboarding and monitoring connected devices.

Identify available funding sources. Explore federal grants and programs focused on broader infrastructure improvements and sustainability. Some funding sources “may not necessarily have a specific line item that speaks to cloud network implementation, but there are things about sustainability,” Allen says. “There are ways to get into funding.” Vendors often have expertise in understanding funding sources that can support IT upgrades.

Plan with technology providers for growth. Vendors can provide advice on how to build from initial implementations and scale. “Push your partners to help you solve for these problems and simplify the parts of IT that may have bogged down groups in the past,” Allen advises.

Never stop looking for new partners and use cases. Initial implementations provide opportunities to demonstrate the benefits of smart spaces across departments or agencies. “The moment you have access to dashboards and features, you start to grow stakeholders across government who can help you advocate and stretch,” Averill says.

Conclusion

While smart spaces are anchored around individual facilities, the network backbone that enables them is the foundation for building a broader connected ecosystem over time. Doing so can help governments “work not in silos within agencies, but as a team to implement at a larger scale for increased benefits,” Broadhurst says.

One of those large-scale benefits involves sustainability. One study shows that enterprises that used IoT-enabled sensors and smart devices saw energy savings of 70% over three years.[1] When connected spaces become a pervasive part of how governments understand and improve constituent services, they can truly transform the safety, well-being and quality of life within a community.

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

1. https://www.forrester.com/report/Extend-IoT-Smart-Building-Solutions-To-Transform-The-Workplace/RES132901

Produced by: CENTER FOR DIGITAL GOVERNMENT

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.**

For: cisco Meraki

At Cisco Meraki, we create intuitive technologies to optimize IT experiences, secure locations, and seamlessly connect people, places, and things. Our cloud-based platform brings together data-powered products including, wireless, switching, security and SD-WAN, smart cameras and sensors, open APIs and a broad partner ecosystem, and cloud-first operations. We hope to connect passionate people to their mission by simplifying the digital workplace — making IT easier, faster, and smarter for our government customers. **Learn more at www.meraki.com/government**

IMAGES PROVIDED BY ADOBESTOCK & SHUTTERSTOCK.COM