IDC

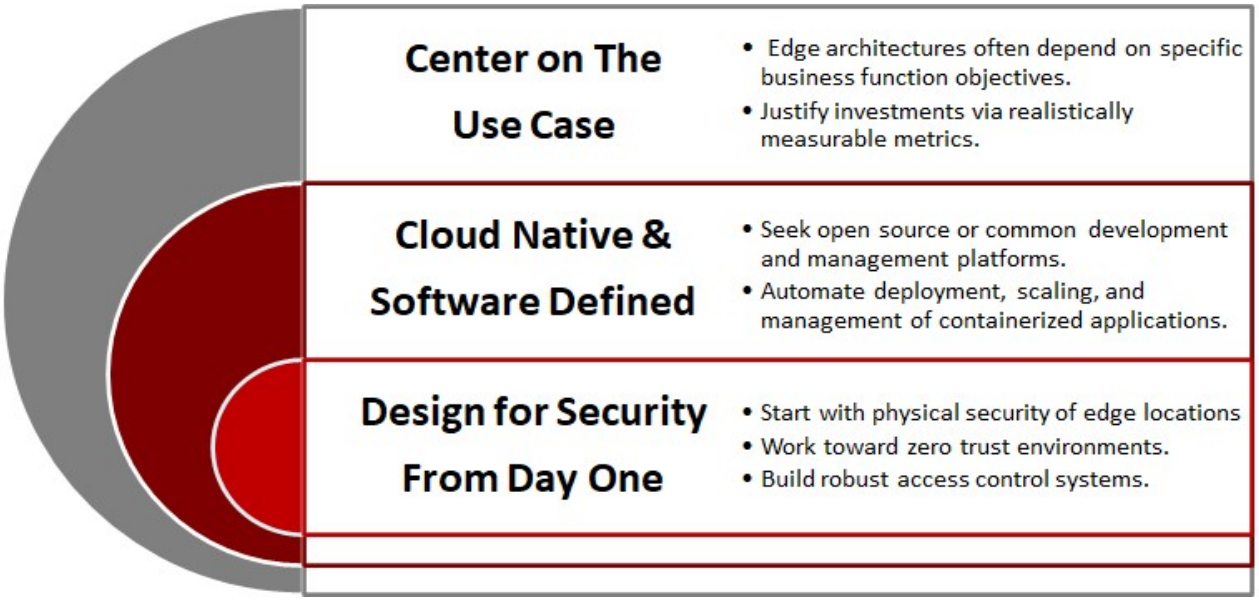
IDC Government Insights

Guidelines for Successful Government Edge Computing

Edge computing centers on processing and technology actions performed outside of centralized datacenters and closer to the network edges. For government, the term especially refers to systems that serve as intermediaries between connected endpoints and the core IT environment.

Modern government edge systems are distributed, software defined, and flexible. Government is in a unique position to offer edge-based services across a set geographic area. Both gov employees and citizens can potentially interact.

- Current and future needs of edge security must be integrated into each agency's security strategies.
- 5G will be the lead connection technology to leverage growth in outdoor spaces. Wi-Fi will continue to lead for indoor spaces, parks and business hubs.
- Data-driven edge initiatives will be transformational for both local and national governments in the coming years. Agencies that invest now can build a solid foundation for long-term edge processing options. This will transform citizen interactions, anticipating needs and shepherding user experiences to where services can be found quickly, essentially driving the evolution of new data-driven services.



Trends Driving the Future of Edge Computing for Government

- Data-driven edge initiatives will be a transformational effort for local and national governments in the coming years
- Agencies that invest now can build a solid foundation for long-term edge processing options. This includes transforming the citizen experience, anticipating needs and shepherding user experiences to where services can be found quickly.
- Agencies are making more investments in analytics and AI at the edge, to streamline data-driven decisions and to deliver logical choices based on data.
- Data analytics, controlled by an AI solution, helps for such missions. While analytics applications can be run from edge-based servers and can be a key part of how an edge-based system is used, one or more AI applications also can reside there, preprogramed to conduct data analysis at set times, depending on available processing power.
- Security is a key part of edge system development. Many agencies are moving toward zero trust environments for connectivity. Large agencies will need to seek broad sub-agency alignment with enterprise zero trust plans, including partner access, external collaboration and risk management. Agencies' identity management systems need to adapt to a broader range of participants. A data-centric approach can be coupled with device-agnostic trust scoring.

Initial Edge computing Checklist

DATA INVENTORY

- [ ] **What data lives within your current facilities?** Chances are you already are collecting some edge data. Understand collecting points and timing. Study data formats. Have the inventory details available when planning, including expansion plans.

- [ ] **How much time does it take** for those data collections to traverse your networks? Use network tools to study data loads, transit times and bottlenecks. Decide if basic network improvement can solve any data flow issues. If not, then you may find evidence that edge computing is a next step.

- [ ] **Decide if edge computing will better serve your needs** when working with that edge-collected data. Video analytics is often a starting point for edge processing, because video produces a lot of data that may not need to be transferred back to a central data center. Other uses can include distributed blockchain calculations and connected vehicles (in preparation for an eventual increase in semi-autonomous vehicles).

- [ ] **What data do you want that exists at other locations?** Some edge computing focuses on a single collection point and data type. Other systems integrate multiple types of data from multiple locations. Understanding what may need to be imported, and volumes of data to be analyzed, should be an early step.

IDC

Analytics at the Edge

- [ ] **Evaluate whether your agency needs advanced analytics** – to help uncover details, trends and correlations. Analytics, running at the edge, is a logical extension of edge processing and accelerated decisions.

- [ ] **Determine whether data processing and analytics will grow in importance** and if there is a sustained interest in gaining real-time insights, related to citizen services, priority setting, cost control, security and more.

- [ ] **Invest in analytics that can continuously process incoming data** to highlight changes, anomalies, security threats or anything else a government deems valuable and actionable.

Artificial Intelligence at the Edge

- [ ] **Is AI needed to help make decisions** near where the data lives? AI can be used to make decisions based on what the analytics uncovers.

- [ ] **Evaluate whether your agency has internal capability** and staff to handle the training of the AI system - so that it makes appropriate decisions. Or will this be delegated to temporary or contract workers who have such training?

- [ ] **Review what other agencies are doing.** The National Artificial Intelligence Initiative maintains the AI.gov website, which offers government use cases and details of infrastructure.

- [ ] **Look for guidance documents** that can help with the planning process for Edge computing and AI. For example, *Edge Computing, 5G, and AI: Government's Exponential Perfect Storm*.

Security at the Edge

- [ ] **Review and make decisions about edge security**, while keeping in mind government edge usually is part of a larger set of systems. Coordinated protection is needed tor the data center, the cloud, the network edge and a range of virtualized environments.

- [ ] **Set security policies that protect** every application, provide secure connections for APIs, microservices, and containers that access government applications. Zero trust is often the best approach for broader security needs.

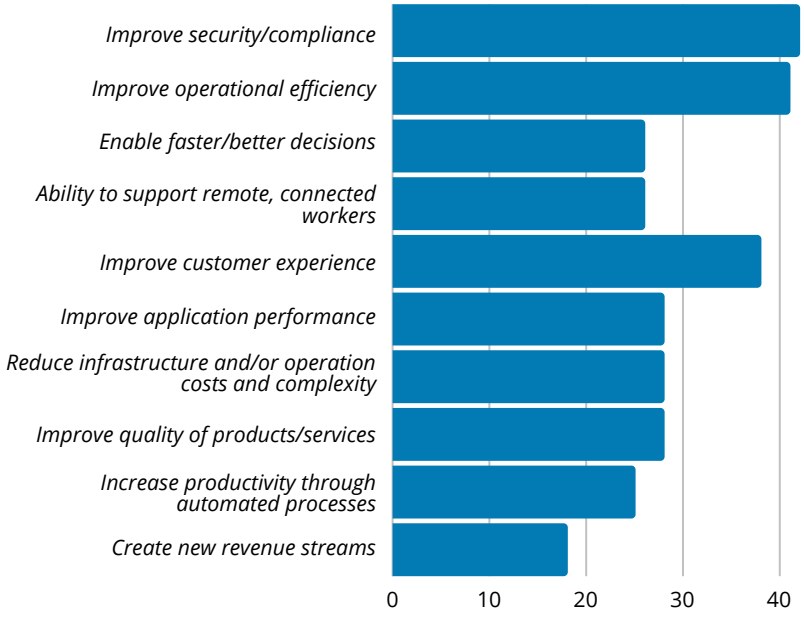
- [ ] **Consider setting micro-perimeters** for users, devices, and application traffic. Most also provide detailed logs, reports, and alerts to help detect and respond to threats.

Future Needs

- ☐ **Once edge systems are in place**, work on the overall long-term coordination of the system, including data feeds, data sharing and reporting requirements
- ☐ **Will your system design require powerful, fault-tolerant and ruggedized servers** at the edge? This can drive up costs, but that may be necessary in military situations, or when the edge data facility is located in a harsh environment.
- ☐ **Determine if compliance be one of the duties** for your edge computing installations. Some zero trust control planes can help set and enforce security-related compliance rules.

Benefits Government Expects Edge to Bring

What benefits do you expect edge adds/will add your organization?



Unified threat management at the edge is moving toward automated zero-trust

- AI-Controlled connections
- Dynamically application of security policies,
- zero-trust connections for devices and end users

Adding edge-based data analytics and AI

- Helps improve the citizen experience
- Fast decisions - immediate citizen impact

To learn more about Government Edge computing, read IDC's new eBook, ***Extending Missions & Finding Business Value In Government Edge Computing***.

For more information on Edge Computing and other government systems and integration issues, see the IDC Research program **United States Government Infrastructure and Systems Optimization Strategies.**