Digital became the dominant way to get governmental & public sector services
Before COVID-19 appeared in our lives, digital was just one of the many options for public services. In light of social distancing, governments and public service organizations boosted their service delivery through digital channels. In many regions and countries, digital became almost the only way to get these services, and digital may remain the dominant channel.

‘Digital Citizen’ in mind approach
While government and public sector organizations were perceived for years as heavy bureaucratic entities, the Digital Transformation revolution significantly changed the public sector’s values and execution. The ‘Citizen’ is now in the center - new portals, applications, and digital services are deployed to increase accessibility; services are available from any device and at any time, and SLA is often defined to assure that government & public sector organizations deliver high quality of service.

Cloud adoption
In regard to privacy and other concerns, government & public sector information and data are very sensitive. Advanced data security and cloud protection technologies enable more and more governments and organizations in the public sector to consolidate their multiple, distributed data centers into centralized cloud-based IT centers. This digital transformation revolution is vital for governments worldwide as it strengthens the connection between the authorities and the public.

Strong impact on IT departments
An excellent Digital Experience is now, more than before, the key to productivity and public engagement for public sector organizations. As the new norm is composed of online services to the public, and a hybrid operations for public organization employees, IT must ensure mission-critical applications and services get top priority. Moreover, IT must gain visibility and control over the entire network while reducing management costs in the transition to consolidated cloud-based data centers.

As part of this increased public accessibility, the number of digital interfaces dramatically increases, and the attack surface vulnerabilities rise significantly. Therefore, IT must be prepared to safeguard the network and minimize downtime caused by DDoS attacks, hacktivists, and other cyberthreats.
Benefits

Fosters public engagement and strengthens governance
• Assures an excellent Digital Experience for online services provided to the population
• Corresponding alerts and root cause analysis enable IT to take prompt action before any degradation in end-user experience

Boosts government productivity
• True QoS for mission-critical applications is assured thanks to advanced traffic shaping and prioritization
• QoE score is calculated level to assure a consistent and high Digital Experience for employees

Safeguards government/public organization reputation
• Detect and mitigate outbound DDoS attacks, on the spot, at Terabits/second
• Scale-up to stop even the biggest attacks at Terabits/second
• DPI policies ensure no network element is overwhelmed and QoE is assured throughout an attack

Reduces OPEX and CAPEX for the organization
• Centralized management for efficient management and control
• Multi-tenant capabilities that enable independent, self-service control and management of any remote office
• Intuitive UI for quick set-up and deployment

Public Sector Use Cases
• Consolidation of distributed management centers into cloud-based centralized data centers
• Digital Experience assurance for remote government offices, utilizing multi-tenant capabilities
• Public network expansion
• Assuring high QoE and availability for Smart City services
• Election day protection
Features

Advanced Digital Experience Monitoring

Multiple performance metrics, including jitter, delay, packet loss, error, and many others are analyzed. The end user Digital Experience is quantified using the Allot Quality of Experience (QoE) score, which provides a real-time metric of the current Digital Experience of any online service provided to the public.

Graphical dashboards with advanced analytics and real-time troubleshooting inform IT infrastructure and operations (I&O) personnel about the Digital Experience story of the organization. Corresponding alerts and root cause analysis enable I&O personnel to take prompt action before any degradation in end-user Digital Experience.

Leading Traffic Classification

Allot’s Dynamic Actionable Recognition Technology (DART) engine, embedded in the platform, inspects every single packet and classifies traffic per application, user, IP address, location, and by any static or dynamic policy element. Allot’s extensive application and protocol classification logic consists of powerful ML and AI engines, which constantly adapt to detect new applications and maintain up-to-date definition logic to

Allot devices. The Allot Traffic Intelligence Platform contains a comprehensive signature library that identifies thousands of web applications and protocols and supports user-defined signatures. Automated DART protocol pack updates from the Allot cloud keep public organization deployment up-to-date with the latest application and web developments to ensure accurate traffic classification.
Complete Traffic Visibility
For governmental and public organizations, the Allot Traffic Intelligence and Assurance platform provides a 360° view of network traffic and the Digital Experience that employees, remote offices, and the public get from the data center, cloud applications, and online services. It also sheds light on shadow IT, BYOD, and mobile app usage, which might otherwise go unnoticed.

Integration with Microsoft Active Directory provides traffic intelligence per user and organizational unit, so IT personnel can better understand how employees consume organizational applications and network resources.

Key visibility features include:
- Layer 7 application visibility
- In-line SSL encrypted traffic visibility without decryption
- Web content and web threat visibility
- User and endpoint visibility with L4-L7 quality of Digital Experience KPIs
- Dashboard monitoring and analytics
- Live, self-refreshing performance metrics with down-to-the-second reporting granularity

Multi-Tenant, High-Resolution Traffic Control
Allot Traffic Intelligence Platform virtually partitions the public organization’s LAN, WAN, and internet resources so that users and applications no longer compete with one another for bandwidth and Quality of Service (QoS). Powerful policy tools, combined with multi-tenant capabilities, enable definition and enforcement of the Acceptable Use Policy as well as prioritization of mission-critical applications at office, user, and application level.

Key control capabilities include:
- Multi-tenant policy enforcement that enables independent management and control at the remote office level
- Support of hundreds of thousands of dynamic traffic policies
- Automated QoS policy propagation to all deployed appliances
- Asymmetric QoS policy synchronized in real-time across multiple datacenters
- Threshold-based enforcement (e.g., CER and live connections)
- Actionable alarms

Central Management, Scalability, and Superior Performance
The IT network of public organizations is usually enormous, potentially approaching 1Tbps in bandwidth. The Allot Traffic Intelligence platform is ideally designed to support such IT infrastructure because it is a scalable, carrier-grade, in-line appliance.

The Allot Traffic Intelligence platform comprises a central management layer that enables public organization IT personnel to effectively control and manage appliances located in the data center and remote units and offices from one central location, providing complete coverage over the entire network.

Leading DDoS Attack Protection
The Allot Traffic Intelligence platform protects against fast-moving, high volume, encrypted DDoS attacks as well as concise duration threats. It provides the first line of defense against both inbound and outbound attacks. Inbound DDoS attacks are automatically mitigated by discarding the DDoS traffic and allowing legitimate traffic to pass through. For outbound attacks, it identifies and then isolates possible threats originating from individual hosts that disrupt the performance and integrity of network infrastructure and services.