ACTI - Allot Cloud Traffic Intelligence for the Public Sector

Fosters Governance & Productivity

Securing mission-critical digital public services in the cloud era

Government and public-sector organizations are undergoing rapid digital transformation as essential citizen services, authentication systems, government portals, and back-office operations migrate to hybrid and multi-cloud environments. Today's digital-first public expects government services to be always available, responsive, and secure—regardless of traffic load, cyberthreats, or infrastructure complexity. These changes reflect broader trends that are fundamentally reshaping government and public-sector digital ecosystems.

Accelerated migration to centralized & public cloud environments for government portals, identity systems, tax platforms, e-government services, and internal operations.

Growing adoption of AI-driven citizen-facing systems such as chatbots, fraud detection tools, automated claims processing, and risk scoring models.

Reliance on latency-sensitive services such as e-voting, real-time authentication, video-based remote citizen services, and emergency communication platforms.

Rising cyber risk & political DDoS campaigns, often targeting public portals, election infrastructure, and essential services.

Complex multi-cloud and remote office environments are increasing management burdens across ministries, agencies, municipalities, and remote government branches.

As cloud adoption accelerates and critical public services become distributed across data centers, SaaS platforms, and public clouds, IT teams face rising pressure to maintain service continuity, ensure digital experience quality, and protect against increasingly sophisticated cyberattacks, especially large-scale DDoS campaigns targeting public-facing digital assets.

Delivers unified observability, granular traffic control, and precise mitigation of DDoS & Botnet attacks across cloud-hosted public services, ensuring service continuity, operational resilience, and an optimized digital experience for citizens and public-sector employees. ACTI helps public organizations with right-sizing their public cloud resource usage, thereby curbing cloud costs.

Allot Cloud Traffic Intelligence (ACTI) for Government & Public Services

Public Sector Use Cases

- Ensuring granular observability for cloud-hosted government portals (E.g.: tax services, licensing, benefits systems, government platforms).
- Providing cloud observability into the public sector organization's cloud-hosted applications, identity systems, remote offices, and data center traffic.
- Guaranteeing digital experience for video-based remote citizen services (E.g.: tele-government, remote hearings, consultations).
- Protecting critical public-facing services from terabit-scale DDoS attacks, including:
  - National or municipal portals
  - Voting/election systems
  - Emergency services & first responder platforms
  - Public facing websites & open data APIs
- Maintaining performance for government AI workloads and large data exchange systems.

Benefits

Fostering governance

- Detects digital experience degradation across cloud-hosted sensitive public service and triggers corrective action.
- Ensures service level adherence and fair share bandwidth allocation across branches.
- Ensures uninterrupted access to citizen services during peak load or cyberattacks.

Boosts the public sector organization's productivity

- AI-driven observability enables proactive troubleshooting.
- Automated cloud traffic policy enforcement for mission-critical cloud-hosted applications, across ministries, agencies, and remote branches
- Assures an optimized Digital Experience even under attack or congestion

Curbing the public organization's cloud costs

- Providing QoE-based rightsizing of public cloud resource utilization
- Assures optimized utilization of existing public cloud resources

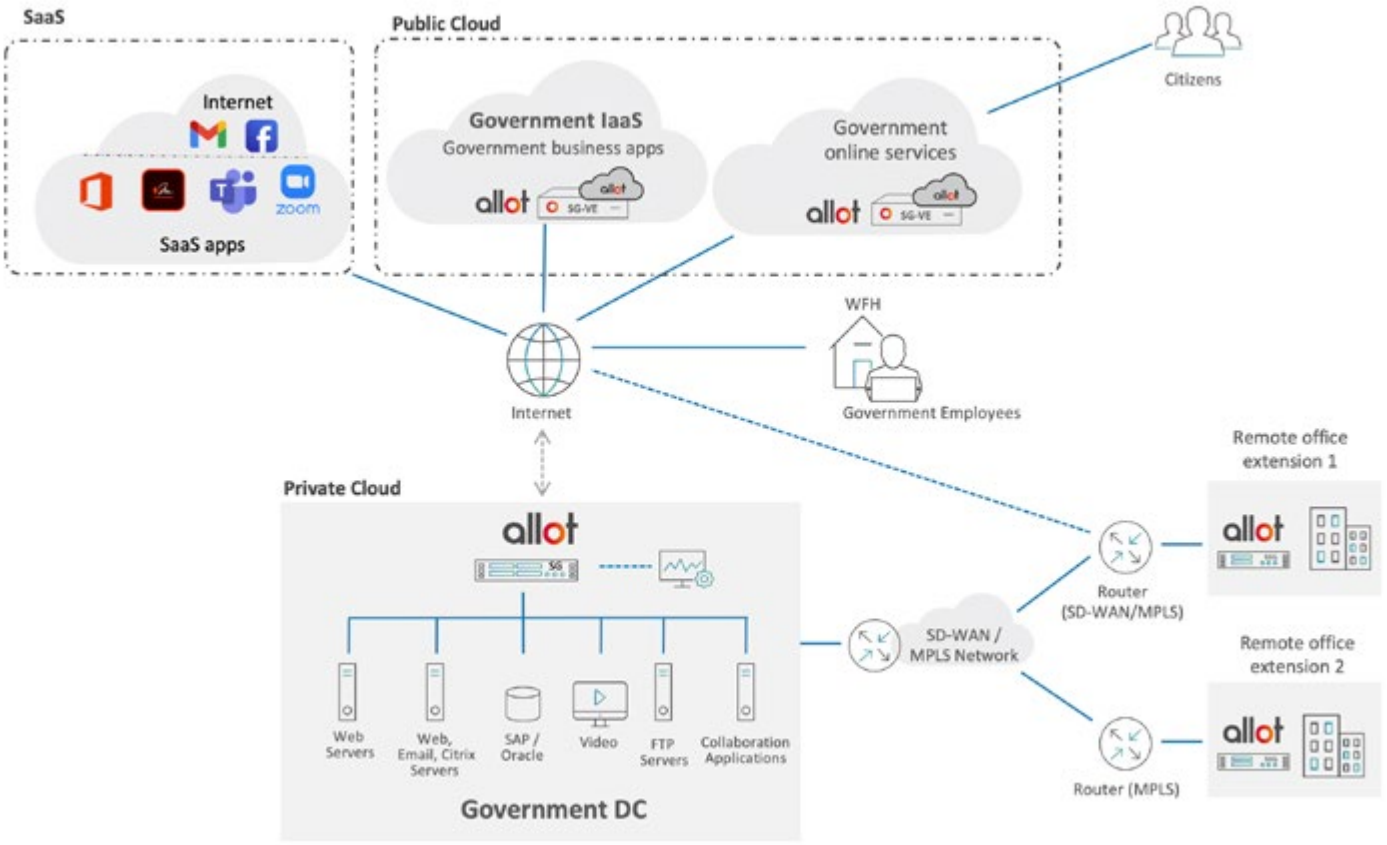
Features

AI-based Observability for Cloud-Hosted Government Applications

ACTI leverages Allot's 30 years of experience in internet traffic analysis and visibility along with expertise in the Public Sector and the Government's public cloud environment. Using advanced AI algorithms to analyze encrypted (which is becoming more common) and unencrypted traffic, ACTI provides holistic observability into the performance of the public sector organization's cloud-hosted applications and digital public services. ACTI covers both Ingress and Egress traffic, as well as the internal cloud traffic. Intuitive, actionable dashboards enable the public-sector organization's IT team to quickly troubleshoot and take appropriate action.

Advanced cloud-based traffic control

In light of its advanced observability capabilities, ACTI provides IT professionals at public-sector organizations with a centralized control plane to govern cloud traffic, ensuring that sensitive digital public services and mission-critical cloud-hosted applications receive the required priority. A dedicated, HTML-based, intuitive UI, programmable via the CLI (Command Line Interface), enables IT professionals to monitor Data Transfer Out (DTO) and enforce required traffic policies, such as priority-based policies. It ensures critical online public services receive the necessary resources and supports fair-share bandwidth management, ensuring equal distribution across all the organization's branches, ideal for maintaining balance and avoiding monopolization of cloud resources.



ACTI deployment within the Government IT environment

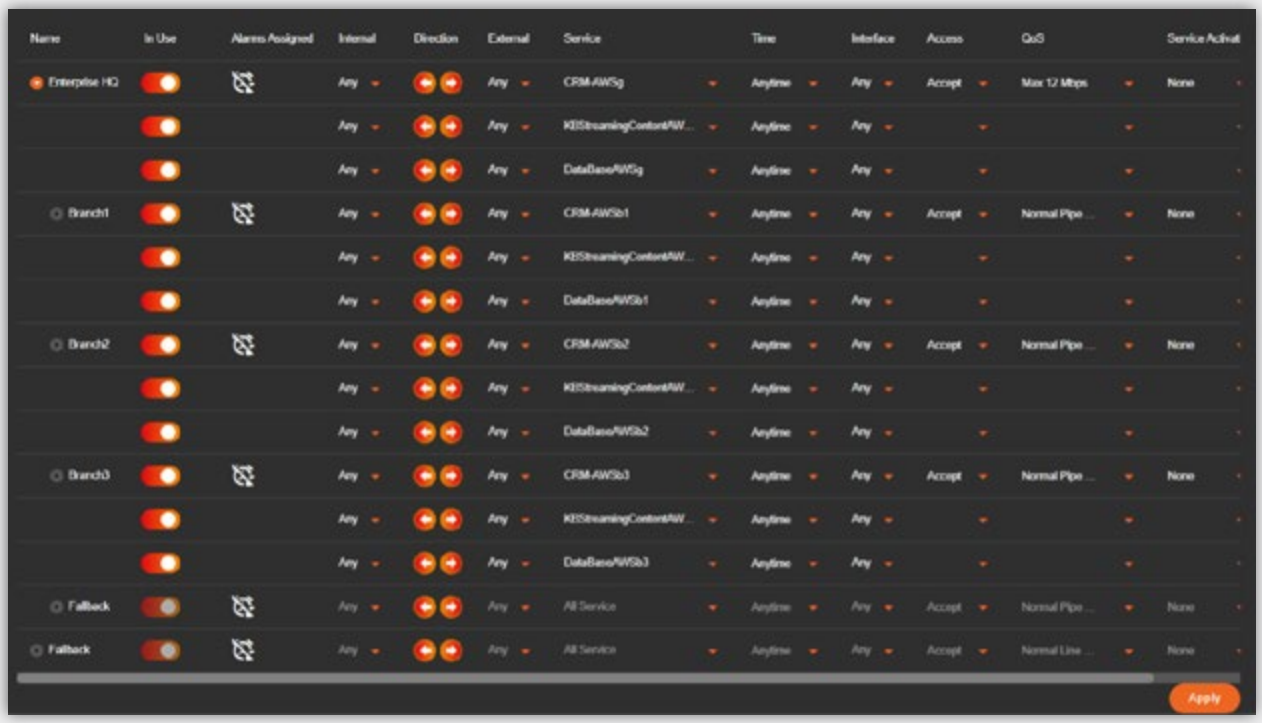
UI-based policy scheduler for optimizing cloud resource usage

An intuitive graphical UI gives IT professionals in public-sector organizations access to the ACTI policy scheduler, where they can set timers to trigger cloud pipe policies and time-based policies (timeslots) and apply troubleshooting and policy changes.

The policy scheduler optimizes cloud slicing capabilities and policies, triggers "softer" policies (e.g., Weighted Fair Queues), and deploys KPI-based dynamic policies.

Precise DDoS and Botnet mitigation

While public cloud vendors protect their entire cloud ecosystem against DDoS and Botnet attacks, volumetric attacks still occur across various public cloud deployments. Public cloud service providers offer a blunt DDoS mitigation capability: an all-or-nothing approach. If the public cloud mitigation system is deployed, it blocks all traffic to the public sector organization's public cloud environment whenever it detects a volumetric DDoS attack. This also affects legitimate traffic to online public services and the public organization's cloud-hosted administrative applications. ACTI offers precise DDoS mitigation against inbound and outbound attacks, blocking only malicious traffic and not legitimate traffic. In the event of a Botnet attack, ACTI quarantines the infected servers. Additionally, ACTI ensures users' optimized Digital Experience even during volumetric attacks



ACTI – Traffic policy rules UI

March 2026