ACTI – Allot Cloud Traffic Intelligence for Higher Education

Ensures Learning Continuity & University Reputation

Higher Education in the Cloud Era

Higher education institutions are rapidly transforming as learning, research, and student services move to cloud-based platforms and hybrid digital environments. Universities now rely on distributed, multi-cloud ecosystems to deliver online learning, AI-powered academic tools, collaboration services, and mission-critical administrative systems. In this new landscape, maintaining learning continuity, safeguarding institutional reputation, and ensuring a consistently excellent digital experience for students, faculty, and staff are essential. These changes reflect broader industry trends that are fundamentally reshaping higher education ecosystems.

Acceleration of cloud migration
Universities are shifting Learning Management Systems (LMS), Student Information Systems (SIS), research workloads, collaboration suites, and identity systems to public and hybrid clouds.

AI-driven learning systems
The increased use of AI tutoring, proctoring solutions, and analytics platforms is placing greater real-time demands on connectivity and cloud services.

Mass adoption of SaaS education platforms
Google Classroom, Canvas, Blackboard, Coursera, Zoom, Teams are all cloud-based and latency-sensitive.

Rising cyber risk for education
Higher Education has become a top target for ransomware and DDoS attacks globally, driven by valuable data and often outdated security systems.

Edge and multi-cloud complexity
Distributed campuses, dorms, research centers, remote test sites, and BYOD environments broaden the attack surface and management burden.

As universities accelerate their transition to cloud-based learning platforms, academic applications, and administrative services, IT teams face significant challenges in maintaining operational continuity and a consistent, optimized digital experience. While public cloud providers offer basic logs and infrastructure-level metrics, they do not provide the end-to-end observability needed to understand how cloud-hosted LMS, SIS, research workloads, and collaboration tools perform for students and staff. Universities require a comprehensive view of service-level performance and observability, with the ability to detect when cloud-hosted educational services fall below expected service thresholds and to enforce granular, per-application or per-user policies to restore service quality.

At the same time, the rapid growth in online learning and digital interfaces dramatically expands the cyber-attack surface, increasing exposure to disruptions such as DDoS and Botnet attacks that can cause downtime for critical academic services, admissions portals, and online exams. Public cloud DDoS protection mechanisms are often blunt, blocking entire traffic flows and unintentionally impacting the university's learning continuity and reputation.

ACTI - Allot Cloud Traffic Intelligence for Higher Education

Allot Cloud Traffic Intelligence (ACTI) ensures learning continuity and a consistently excellent digital experience across the university's cloud hosted applications and services. ACTI helps higher-education institutions right-size their public cloud resource usage, thereby curbing cloud costs.

Higher Education Use Cases

- Providing **cloud observability** for university cloud-based applications, portals, university remote branches, and internet traffic
- Guaranteeing **digital experience for video-based remote learning** (Zoom, Teams, Webex).
- Detecting **shadow cloud applications** used by students and staff.
- Protecting academic operations from **terabit-scale DDoS attacks** targeting:
  - Admissions portals
  - Exam platforms
  - Research data centers
  - Public-facing university websites
- Maintaining performance for **research cloud workloads** (e.g., high bandwidth data transfers).

Benefits

Safeguards the University's reputation

- Ensures optimized digital experience for critical online learning and administrative services.
- Provides unified observability across campus, remote sites, and cloud platforms.
- Proactively detects digital experience degradation and facilitates corrective action

Boosts the University's productivity

- AI-driven observability enables proactive troubleshooting.
- Automated cloud traffic policy propagation across all academic sites.
- Assures QoE and optimized Digital Experience even under attack.

Assures learning continuity and strengthens resilience

- Precise mitigation (inbound & outbound) that blocks only malicious traffic.
- Ensures the Quality of Experience (QoE) of legitimate traffic is maintained throughout an attack

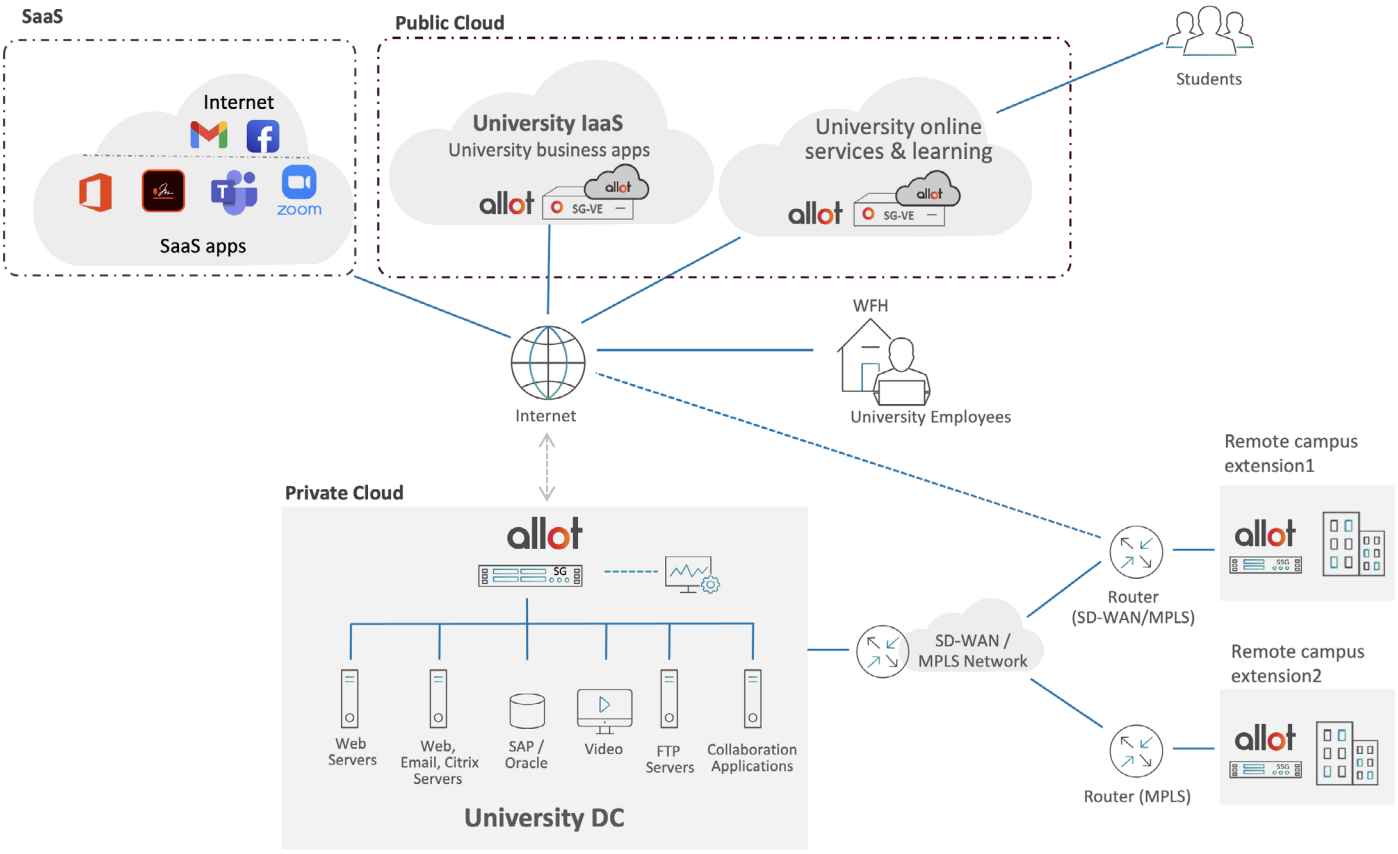
Curbing cloud costs

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

Features

AI-based Observability for Higher Education Cloud-Hosted Applications and Services

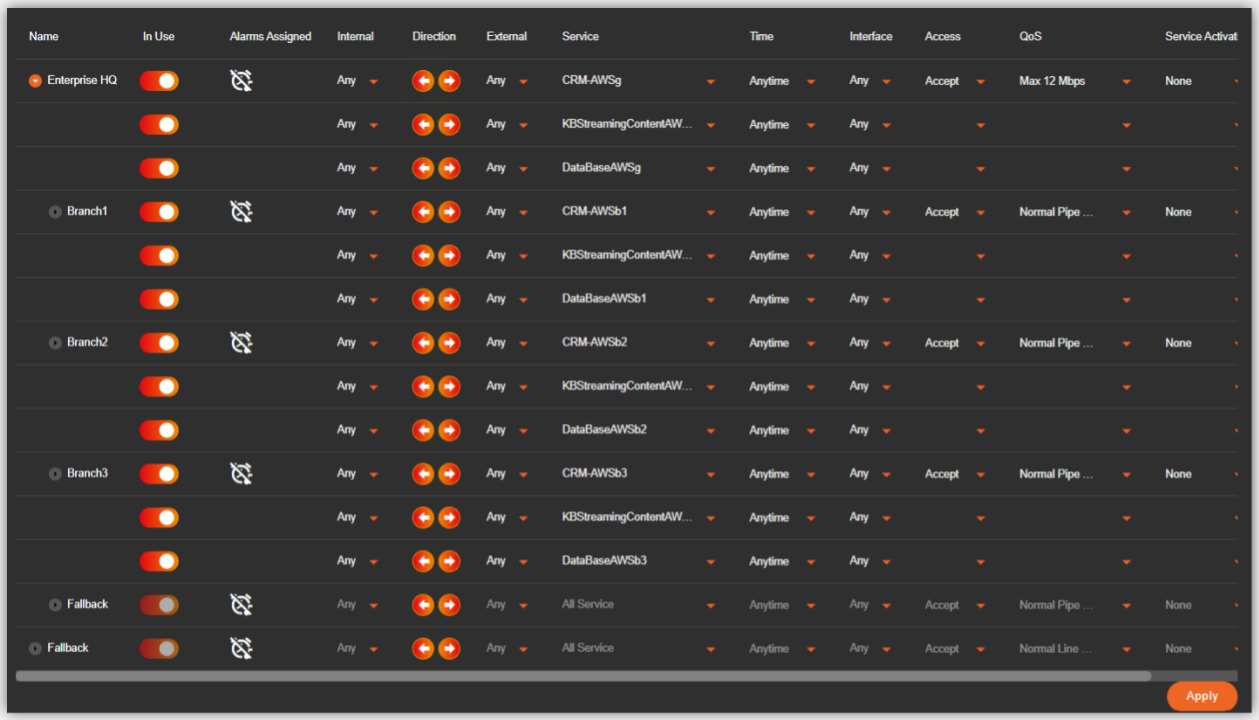
ACTI leverages Allot's 30 years of experience in internet traffic analysis and visibility, along with its expertise in the Higher Education sector and its various public cloud environments. Using advanced AI algorithms to analyze encrypted (which is becoming more common) and non-encrypted traffic, ACTI provides holistic observability into the performance of university cloud-based applications and services. ACTI covers both Ingress and Egress traffic, as well as internal cloud traffic. Intuitive, actionable dashboards enable the university IT team to quickly troubleshoot and take appropriate action when needed.



ACTI and Allot deployment architecture

Advanced cloud-based traffic control

In light of its advanced observability capabilities, ACTI provides IT professionals at universities and other higher education institutions with a centralized control plane to govern cloud traffic, ensuring that SLA-based educational services and applications receive the required priority. A dedicated, HTML-based, intuitive UI, which is also programmable via CLI (Command Line Interface), enables IT professionals to monitor cloud pipe status and enforce required traffic policies, such as a priority-based policy that ensures critical educational services receive the necessary resources or fair share bandwidth management that ensures equal bandwidth distribution across all the university's branches: ideal for maintaining balance and avoiding cloud resources monopolization.



ACTI – Traffic policy rules UI

UI-based policy scheduler for optimizing cloud resource usage

An intuitive graphical UI provides IT professionals in higher education institutions with 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" cloud pipe policies (e.g., Weighted Fair Queues), and deploys KPI-based dynamic policies.

Protection against DDoS and Botnet attacks

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, whenever it spots a volumetric DDoS attack, it blocks ALL traffic toward the university cloud environment. This also affects legitimate student and university personnel traffic. The ACTI DDoS protection for inbound and outbound attacks provides precise mitigation that blocks only malicious traffic, not legitimate traffic. In the event of a Botnet attack, ACTI quarantines the infected servers. Additionally, ACTI ensures users' QoE remains consistent even under volumetric attacks.

Feb 2026