Allot Traffic Intelligence Platform for the Financial Sector

Increases reputation, resilience and customer satisfaction

Worldwide Trends and IT Challenges

Digitalization and online services are widespread in the Banking and Financial Services Industry (FSI) . To keep up with technological expectations, there is a growing market demand for innovation. Research shows that digital adoption is common across the industry, with double-digit growth in online service usage through portals and mobile apps, as well as the adoption of new work habits, including remote work (WFH). Another key trend transforming banking and the broader Financial Services sector is the adoption of public cloud computing and hybrid-cloud strategies, where a public cloud layer is added to the existing local datacenters or private cloud facilities. This change is driven by the need for greater agility, resilience, scalability, and cost efficiency – all essential for staying competitive, providing seamless digital experience, and successfully transitioning applications and services to the public cloud.

The transition to the public cloud is complex and comes with notable challenges, which could potentially lead to disastrous repatriation scenarios, and costly migration failures.

> Allot Cloud Traffic Intelligence (ACTI) aligns the financial organization's mission-critical applications with its business goals, reduces cloud costs, and minimizes repatriation scenarios, ensuring reputation, productivity, and resilience.

While public cloud vendors provide foundational observability tools like logs and metrics for financial institutions and banks on their purchased cloud infrastructure, they often lack a comprehensive view of the performance of their cloud-based financial applications and services. A public cloud typically offers single hardware-instance visibility, but IT teams require full observability and control over cloud applications and network performance – allowing them to gauge the SLA and Quality of Experience (QoE) metrics delivered to their users. Monitoring the cloud-deployed services SLA and QoE metrics is essential to ensure bank and finance institute's business continuity and reputation. Hence, whenever these metrics are not met, IT teams need to react: they require the ability to enforce granular policies per service, per branch, or per user. Managing the overall cloud traffic is also a key requirement of IT teams, allowing them to optimize their cloud resource use and control costs as growth occurs.

Consumers and partners access online payment gateways and open-banking services on a daily basis, requiring split-second SLA to API calls and online operations.

Additionally, as more online services are adopted, the expanding digital interfaces increase the attack surface, heightening the risk of cyber disruptions. IT must be prepared to protect public and private cloud networks to minimize downtime caused by DDoS attacks.

Benefits

Fosters customer engagement and strengthens the organization's reputation

- Assures an excellent digital experience and QoE for cloud-based online digital services provided to customers, partners, and employees
- Enables IT to take prompt action by synthesizing alerts and troubleshooting capabilities, before any degradation in end-user experience

Boosts Financial Services organization productivity

- Assures QoS for mission-critical applications through advanced traffic shaping and prioritization
- Delivers a consistent and high-quality digital experience for employees

Assures business continuity

- Provides precise DDoS mitigation that blocks only malicious traffic
- Ensures the Quality of Experience (QoE) of legitimate traffic is maintained throughout an attack

Reduces cloud expenses growth

- **Up to 25% average savings** on annual cloud expenses*- leveraging QoE-based measurements to right size cloud resources and optimize cloud utilization

  *Based on market benchmarks

Financial Services Sector Use Cases

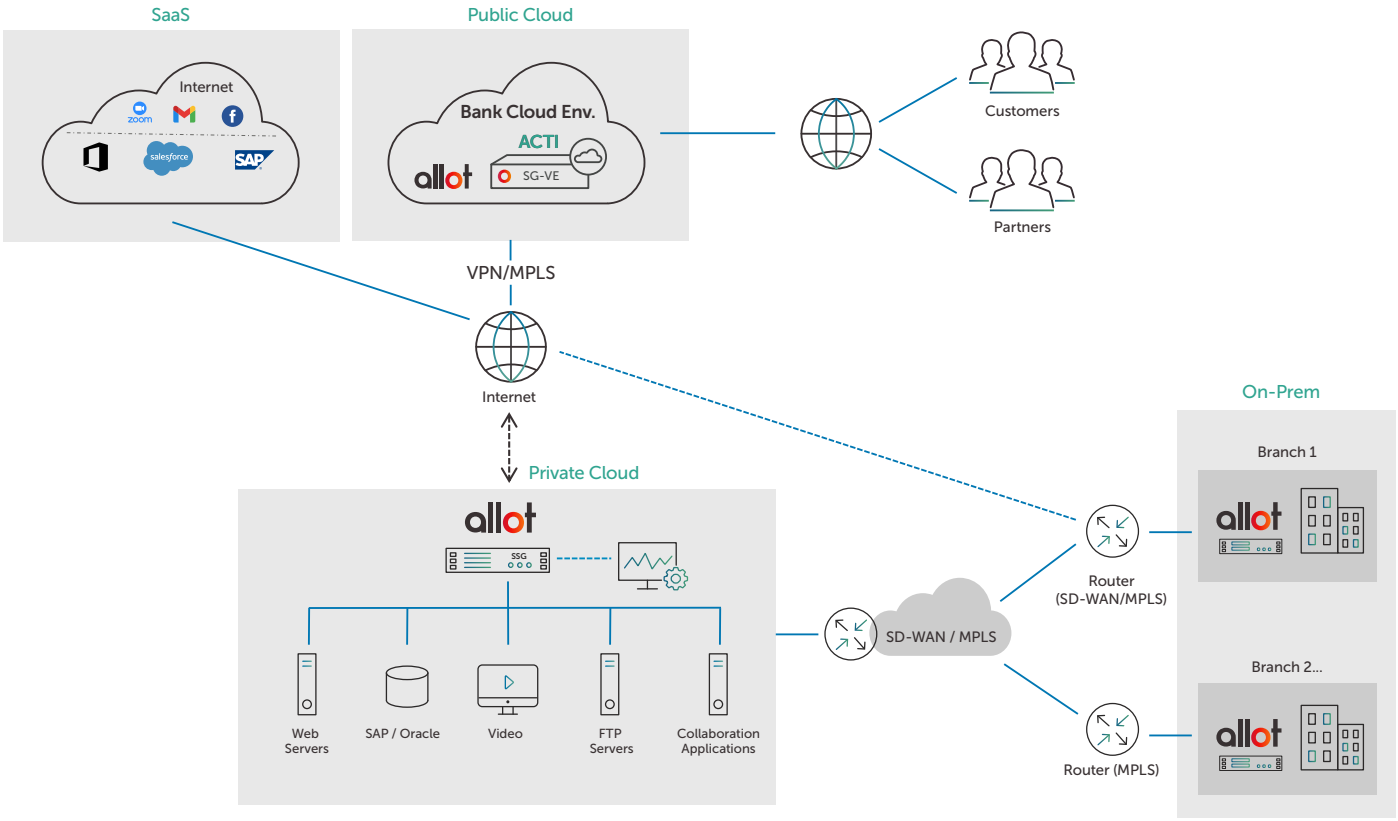
- Gain complete observability and control over public cloud and private cloud traffic and applications performance.
- Assure a high-level digital experience for online services, APIs, payment gateways, open-banking services, and more.
- Assure sustained, high QoS of the nationwide network of ATM machines, connecting to cloud-based banking backend.
- Assure mission-critical banking and financial service applications get top priority over non-critical services.
- Protect cloud infrastructure from DDoS and botnet attacks.

Features

Advanced cloud-based digital experience monitoring

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 cloud-based online service provided to customers.

Allot's Dynamic Actionable Recognition Technology (DART) engine, embedded in the solution, analyzes all cloud-based traffic and categorizes it based on application, user, location, and any static or dynamic policy element. Allot's extensive application recognition logic employs powerful ML and AI engines that continuously adapt to identify new applications and keep definition logic up-to-date. Graphical dashboards with advanced analytics and real-time troubleshooting provide IT with insights into the organization's cloud-based digital experience for online services and applications. Alerts and root cause analysis enable IT to respond quickly before any degradation occurs in the end-user digital experience.



ACTI deployment architecture

Granular observability into cloud workloads, services, and cloud pipe traffic

ACTI provides granular observability into cloud workloads, applications, resources used, and their Key Performance Indicators (KPIs) – it serves the Allot DEM (Digital Experience Management) function.

Graphical dashboards highlight SLA-based applications and services that fail to meet their SLA commitments in terms of performance and the expected digital experience.

Dedicated dashboards show your cloud-slicing computing resource use over time, enabling you to understand if you need to extend your slice or free some of your assigned resources.

Advanced cloud-based traffic control

In light of the advanced observability capabilities, IT professionals in financial organizations are looking for a centralized control plane where they can define their cloud pipe policies and ensure that SLA-based financial services and applications get the required priorities accordingly. The Allot HTML-based intuitive UI, also programmable via CLI, enables IT professionals to monitor the cloud pipe status and enforce the required cloud slicing priorities.

Dashboards that facilitate the optimization of cloud resources

An intuitive graphical UI provides IT professionals in financial organizations with access to the ACTI policy scheduler, where they can set timers to trigger cloud pipes policies, timeslots (time-based policies), and apply troubleshooting and policy changes. The policy scheduler allows for optimization of the cloud slicing capabilities (and policies), and triggering "softer"cloud pipes policies (e.g., Weighted Fair Queues), or deploying KPI-based dynamic policies – this is typically achieved only when the IT professionals have obtained a clear understanding of how their cloud-slicing resources are used, what the financial implications are, and how to optimize cloud resource usage.

Protection against DDoS and Botnet attacks

While public cloud vendors protect their entire cloud ecosystem against DDoS and Botnet attacks, volumetric attacks still occur within various deployments within the public cloud. Public cloud service providers deliver a blunt DDoS mitigation capability: it's an all-or-nothing type of action. If the public cloud mitigation system is deployed, whenever it spots a volumetric DDoS attack, it blocks ALL traffic toward the FSI cloud environment. This impacts the consumer's legitimate traffic as well. The ACTI DDoS protection system protects the financial organization against these attacks. ACTI offers precise DDoS mitigation that blocks only malicious traffic, but not legitimate traffic. In addition, ACTI ensures users' QoE can be protected, even during DDoS attacks.

Oct 2025