See. Control. Secure.

Allot Traffic Intelligence Platform for the Financial Sector

Increases reputation, resilience and customer satisfaction

Worldwide Trends and IT Challenges

Digitalization and online services are already prevalent in the Financial Services Industry (FSI) and banking sector. To keep pace with technological expectations, there is an ongoing, increasing market demand for innovation.

Coping with the global pandemic has strengthened these trends tremendously, and has significantly impacted end-user behavior overall. Research shows that digital adoption was widespread across the industry: double-digit increases for online service consumption through portals and mobile apps, "overnight" virtualization of the workforce, and implementing new social distancing procedures within the workplace.

Another important trend that is reshaping banking and the larger FSI sector is adopting hybrid-cloud strategies to consolidate local data centers into private, cloud-based, centralized centers. Ideally, this trend is aligned with the desire to increase agility, resilience, scalability. Typically, these are fundamental characteristics of most any world-class financial institution's long-term vision and plans.

The Allot Traffic Intelligence platform provides the critical network visibility that Financial Service organizations require. It aligns application performance with business priorities, ensuring that critical services get top bandwidth priority while optimizing the end-user digital experience and assuring resilience and reputation.

This historic boost in digital transformation is having a revolutionary impact on IT in the FSI sector.

An excellent digital experience is the key to optimal productivity and a business reputation for banking and financial organizations. IT must ensure mission-critical applications and services get top priority while contending with hybrid work environments and the increased use of online services by customers. Moreover, **IT must gain visibility and control over the entire network while reducing operational costs** in the transition to consolidated cloud-based data centers. Additionally, in light of the increase in online service adoption, the number of digital interfaces increases, which significantly increases the attack surface leading to higher vulnerability to cyber disruption. **IT must be prepared to safeguard the network and minimize downtime caused by DDoS attacks and other cyber threats.**

Benefits

Fosters customers engagement and strengthens the organization reputation

- Assures an excellent digital experience for online services provided to customers and employees
- Enables IT to take prompt action, by synthesizing alerts and root cause analysis, before any degradation in end-user experience

Boosts FS organization productivity

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

Protects business reputation

- Detects and mitigates outbound DDoS attacks, on the spot, at Terabits/second
- Ensures that no network element is overwhelmed and that QoE is maintained throughout an attack

Reduces OPEX and CAPEX

- Scalable, centralized, streamlined 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

FSI Sector Use Cases

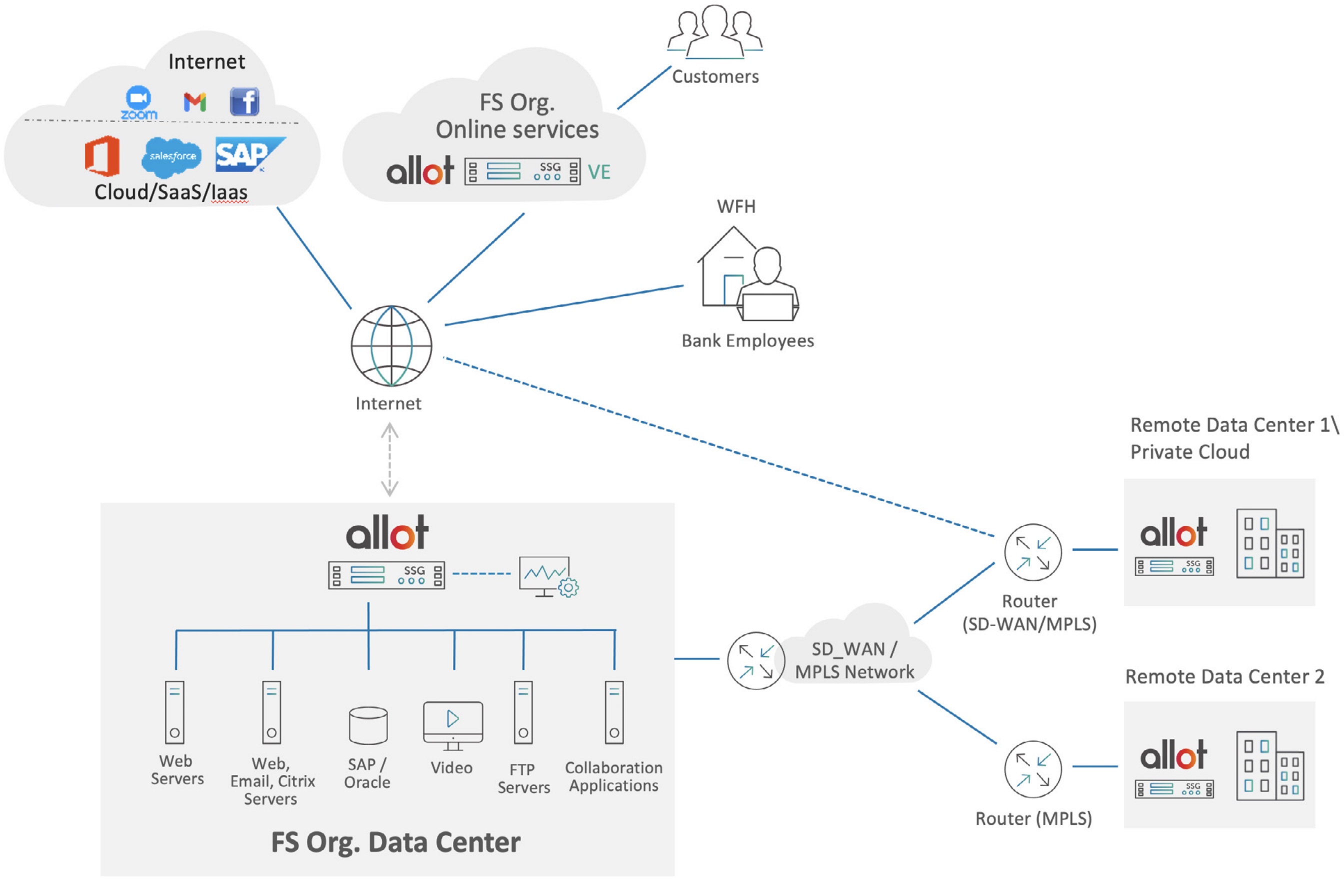
- Gain full visibility and control over both central and remote branches and data centers
- Assure a high-level digital experience for online services
- Assure sustained, high QoS of all ATM machines
- Assure mission-critical banking and financial service applications get top priority
- Minimize latency in remote branches
- Protect data by blocking anonymizers
- Protect IT infrastructure from DDoS attacks, cryptojacking, and other vulnerabilities

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 customers.

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. 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 uses powerful ML and AI engines, which constantly adapt to detect new applications and maintain up-to-date definition logic for Allot-empowered 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 FS organization deployments up-to-date with the latest application and web developments to ensure accurate traffic classification.

Complete Traffic Visibility

The Allot Traffic Intelligence and Assurance platform provides a 360° view of network traffic and the digital experience that employees, remote offices, and customers 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 the organizational unit, so IT personnel can better understand how employees consume corporate 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

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

The Allot Traffic Intelligence platform is ideally designed to support IT infrastructure at all types of FS organizations because it is scalable and enables smooth expansion when needed.

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. It identifies and then isolates possible threats originating from individual hosts, preventing outbound attacks that can disrupt the performance and integrity of network infrastructure and services.

August 2021

© 2021 Allot Ltd. All rights reserved. Specifications subject to change without notice. Allot and the Allot logo are registered trademarks of Allot. All other brand or product names are trademarks of their respective holders.