Unified Application Delivery, Security, and AI Protection for Financial Services

One platform. One architecture. Built for flexibility, performance, and control across modern financial environments.

Simplified High Performance and Flexible Application Delivery

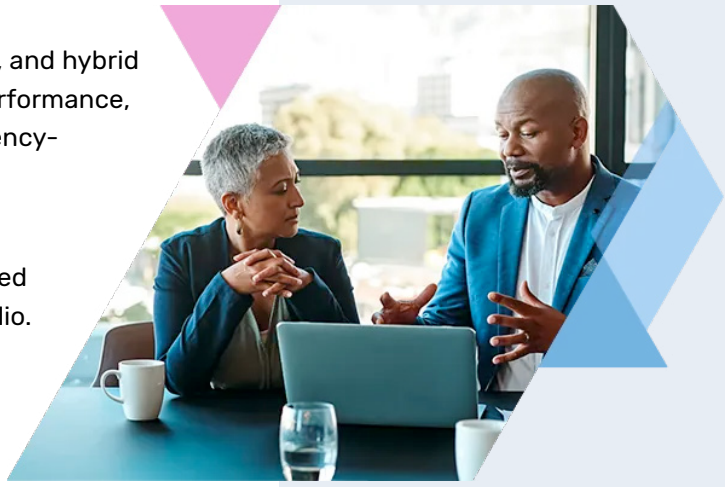
Modern financial services applications demand flexibility in both deployment and scale. Applications run on-premises, in public or private cloud environments, or across multiple locations at once. These environments shift quickly, requiring infrastructure that can scale on-demand without introducing performance bottlenecks or inefficiencies. This is particularly critical in mobile banking, payments, and real-time transaction processing.

A10 Networks helps financial organizations deliver consistent application performance while adapting to changing infrastructure needs. By combining flexible consumption models with high-performance application delivery, organizations can scale efficiently while maintaining responsiveness across digital banking platforms and transaction-heavy systems.

Unified Application Delivery for a Complex Financial Landscape

Financial infrastructure now spans data centers, cloud platforms, and hybrid environments. As this footprint grows, maintaining consistent performance, visibility, and security becomes more difficult, particularly for latency-sensitive applications such as trading platforms, APIs, and customer-facing banking services.

A10 brings application delivery, centralized management, advanced security, and AI protection together as a cohesive solution portfolio. This unified approach simplifies operations while maintaining control across all environments, helping ensure consistent user experiences even during periods of high transaction volume or market activity.



Modernize Application Delivery, Security, and AI Protection

A10 helps financial institutions scale dynamically, reduce latency, secure applications and APIs, and support modern banking, trading, and payment environments with confidence.

How It Works

Flexible Licensing and Dynamic Scaling

Application demand fluctuates constantly based on user activity, transaction volume, and market conditions. Traditional licensing models can make it difficult to respond quickly when demand spikes.

FlexPool is a flexible licensing model that allows capacity to move where it is needed most. This supports scaling across on-premises and cloud environments. By aligning licensing with real-time demand, organizations can maintain performance without overprovisioning.

Simplified Management, Automation and Control

Managing application delivery infrastructure at scale requires automation, visibility, and consistency. This includes understanding application traffic patterns and managing the lifecycle of SSL certificates that secure application traffic, both of which become increasingly complex in distributed environments.

A10 Control is a unified management and control platform for managing application delivery controllers, configurations, and certificates across distributed environments. It gives teams a clear view of traffic patterns, application performance, and infrastructure health while enabling automated policy enforcement and simplified certificate management. A10 Control also helps streamline operations and eliminate manual, error-prone tasks across large and complex environments with intent-driven automation.

Ultra-low Latency Performance

In financial services, latency directly affects outcomes. From everyday banking transactions to trading workflows and FIX protocol routing, even small delays can have measurable impact. A10's **low latency** and **ultra-low latency** capabilities are designed to minimize delay and deliver consistent performance across time-sensitive applications and services. This helps improve execution timing, maintain responsiveness under load, and support systems where speed and precision are critical.

Advanced Protection for Applications and APIs

With the advent of mobile banking in financial services, applications aren't just part of the business anymore — they are the business. Modern banking and fintech platforms run on APIs and backend application logic where transactions are initiated, processed, and approved, making them the prime target for attackers. From AI-enhanced bot and fraud attacks, business logic API exploits, and Layer 7 DDoS, protecting where money moves has become critical.

ThreatX protects the application layer from the inside out, securing the **backend systems, the web applications, APIs** — the communication channels from mobile banking apps to the web applications, and transaction flows, which are all opportunities for bot and L7 DDoS attacks to disrupt. **ThreatX:**

- Protects the backend applications and APIs, which are where transactions are now executed and sensitive financial data is accessed
- Detects and mitigates automated fraud, credential stuffing, and account takeover attempts through behavioral analysis
- Stops malicious API activity and Layer 7 DDoS attacks before they disrupt critical financial services
- Uses inline protection and adaptive risk scoring to identify abuse of application logic and anomalous transaction behavior, securing the systems where the money moves

AI Security and Governance

Applications are the core and operational backbone of modern financial enterprises, and their security, integrity and performance are foundational to business resilience. As AI is becoming a core part of financial applications, enabling smarter transactions, recommendations, and customer experiences, it is introducing new risks related to data exposure, misuse, and lack of transparency.

The A10 AI Firewall is an enterprise guardrail solution that protects AI applications from AI-native threats in real time, enabling custom policy enforcement in natural language, ensuring governance, built-in governance, and delivering deep visibility across both inputs and outputs.

- Deploy anywhere — on-premises on A10 or customer hardware, or in the public cloud as Kubernetes pods on any GPU-enabled platform
- Inspect every prompt and response for intent and context using a proprietary unified semantic reasoning model
- Out-of-the-box protection against OWASP, NIST, and MITRE framework LLM threats, zero-day AI attacks, and custom policy violations
- High detection accuracy and industry leading low false positive rate, powered by continuous red teaming testing and adversarial model training
- Reduce risk and enforce compliance with use-case-specific custom policies, defined in natural language
- Real-time observability into AI interactions with audit trails and reasoning behind each violation

Chat with Us

Schedule a consultation today and learn how A10 can support your business needs at A10Networks.com/contact-us/contact-sales

About A10

A10Networks.com

Contact Us

A10Networks.com/contact

Part Number: A10-BR-20127-EN-01 May 2026