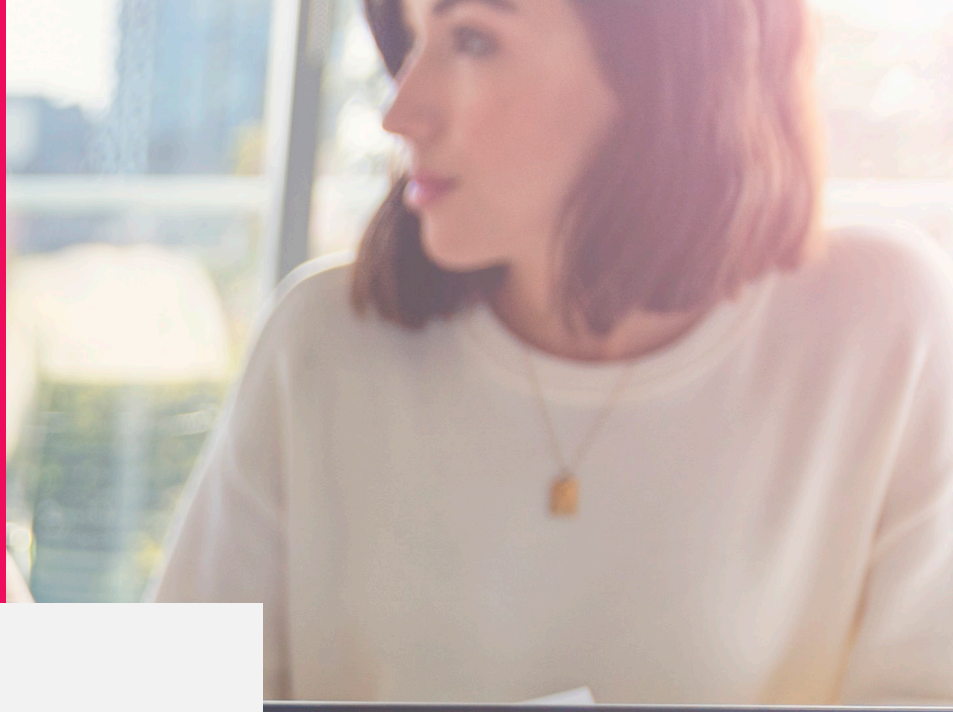

CHECK POINT™

SECURING AI INNOVATION IN FINANCIAL SERVICES

A Guide for the Future

Micki Boland - Technologist Global Team
Check Point Software Technologies - Office of the CTO

SECURITY IN ACTION

Financial companies are rapidly adopting artificial intelligence (AI) to stay competitive or risk falling behind. The banking, financial services, and insurance (BFSI) sector's AI investments are expected to grow at a compounded annual growth rate (CAGR) of 33.1% by 2032. JPMorgan Chase identified over 400 AI use cases, and their $600 million security investment led to an 85% improvement in their threat detection. Major banks are already leveraging this technology to transform their operations, from improving customer service to detecting fraud and optimizing investment strategies.

Top 3 Ways Financial Services Institutions Use AI

To address these challenges, financial institutions need security solutions that simplify regulatory compliance for security teams.

1. Personalized Customer Service

AI is transforming how financial companies serve their customers. Morgan Stanley uses an internal chatbot powered by OpenAI's GPT-4 to help wealth management advisors quickly find critical information. HSBC employs Contextual AI to provide research insights and process guidance by analyzing market outlooks and financial news. Advanced chatbots powered by large language models (LLMs) can process complex customer queries and simulate human centric interactions, dramatically reducing operational costs. AI can also deliver unique client experiences by generating individualized content from multiple sources including marketing materials, financial reports, and client communications.

2. Fraud Detection and Risk Investment

Financial companies face constant threats from fraudsters, but AI is helping fight back in increasingly sophisticated ways. Visa and Mastercard have leveraged GenAI for improved fraud detection by scoring transaction risks in real time and preventing fraudulent card use before it can impact customers. The systems analyze thousands of data points per second, from transaction locations to spending patterns, to flag suspicious activity. HSBC uses GenAI in its compliance processes to identify anomalies that might indicate financial crime. This real-time monitoring not only protects customers but also helps prevent problems that could result in regulatory fines.

3. Managing Investments

Generative AI can model various market conditions by simulating thousands of potential scenarios in minutes, helping customers and advisors make informed decisions. Goldman Sachs uses AI to improve its ability to predict investment risks and returns, making better decisions about where to invest money and how to manage risk. JPMorgan Chase has integrated AI into its trading platforms, using it to process huge amounts of data to develop better trading strategies. These AI systems help analyze market trends and make investment decisions faster than ever before, with some capable of executing trades in microseconds when opportunities arise. They also enable personalized portfolio recommendations by considering individual risk tolerance, investment goals, and market conditions. For institutional investors, AI systems can simulate complex market scenarios to stress-test portfolios and identify potential risks.

New Risks When Using AI

Data and Privacy Risks

As financial companies increasingly rely on AI, they face new challenges in protecting sensitive information and maintaining data privacy. AI systems need massive amounts of data to work effectively, but this increases exposure to cybercriminals and therefore the risk of data breaches. The EU's new AI Act classifies financial AI applications as "High Risk," requiring strict controls over data quality and security, along with regular audits of AI tools being used. Companies must be extra careful about how they collect, store, and use customer information, with continuous assessment and risk management. This requires implementing robust encryption protocols, strict access controls, and comprehensive audit trails for all AI-driven processes.

AI Risks

AI systems face unique security threats that need special attention. The OWASP Top 10 for Large Language Model Applications (2025) highlights key vulnerabilities including prompt injections that can lead to data leaks, unauthorized code execution, and AI model theft. These attacks can be particularly dangerous in financial settings where compromised AI systems could manipulate markets or expose sensitive customer data. Financial institutions must constantly evolve their security practices as new attack vectors are discovered and AI becomes more deeply integrated into critical operations.

Compliance Challenges

While financial regulations have usually focused on policy rather than technology, regulators are starting to provide detailed guidance for AI use in the financial sector. Companies must be able to explain how their AI systems make decisions and prove they're fair and unbiased. This includes documenting model development processes, conducting bias assessments, and maintaining detailed audit trails of AI decision-making. Many organizations are establishing dedicated AI governance committees to oversee these compliance efforts and ensure their AI implementations meet regulatory requirements. The increased regulatory scrutiny has led to the development of specialized tools and frameworks for testing AI fairness and explainability in financial applications.

Best Security Practices

Cybersecurity Mesh

A cybersecurity mesh creates a complete security network that protects all parts of a company's AI systems. JPMorgan Chase demonstrated the value of this approach when they invested $600 million in their zero-trust approach for securing remote worker access and cloud infrastructure in 2021. This led to an 85% improvement in threat detection speed and reduced successful breach attempts by 73%.

The mesh approach includes several critical components:

First, it provides advanced analytics and intelligence by collecting and analyzing security data from various tools across the organization. This helps quickly identify and respond to threats. The platform uses AI threat intelligence to evaluate real threats and trigger appropriate responses.

Second, it manages identity verification across the entire organization, which is absolutely required for a zero-trust architecture. This includes managing user directories, proving people are who they say they are, and controlling what they can access.

Third, it creates a unified approach to security policies. Instead of having different rules for different parts of the system, everything follows the same security standards. This makes it easier to protect data and control access, across the data center, network, cloud, and remote users.

Zero-Trust Security

In zero-trust, no user, device, or application is automatically trusted, regardless whethre they are inside or outside the network. Everything must be verified and authenticated before being granted access to any system. A leading financial services organization implemented zero trust principles by strengthening identity checks and segmenting their network. This resulted in a 40% reduction in unauthorized attempts to access restricted customer data.

The zero-trust approach includes several key strategies:

Strong Identity Management: Every user and device must prove their identity before accessing any resource. This includes using multiple factors for authentication, like passwords combined with security tokens or biometric data.

Network Segmentation: Systems are divided into smaller, protected segments. This means if one part is compromised, attackers can't easily reach other parts. For example, customer data systems might be separated from marketing systems, with strict controls on how information moves between them.

Least Privilege Access: Users only get access to what they absolutely need for their work. This access is regularly reviewed and updated. For instance, a financial advisor might only see their own clients' data, while a system administrator might have access for maintaining systems but no access to client financial details.

AI/ML Security Operations

Modern AI security operations combine traditional security practices with new approaches specific to AI systems. A great example comes from five Dutch banks that worked together to standardize their machine learning models to monitor payment transactions and detect signals indicating money laundering or terrorism funding. This initiative showed how financial institutions can work together to build stronger defenses across technology, business lines, and IT departments.

The project involved several approaches:

Standardized Model Development: The banks created common standards for building and testing AI models. This made it easier to ensure all models met security and performance requirements. They used MLOps (Machine Learning Operations) practices to automate many aspects of model development and deployment.

Cloud-Native Security: A cloud-native architecture enabled banks to weave security controls directly into its infrastructure, enabling automatic scaling of defenses in response to emerging threats. This allows real-time security updates to be deployed simultaneously and consistently across all instances.

Regular Testing and Updates: Banks rigorously penetration tested their AI models, probing for hidden vulnerabilities and attack vectors. As a result, they could rapidly deploy countermeasures and strengthen system defenses.

Steps for Success and Looking Ahead

The path to successful AI implementation in financial services begins with thorough planning and strong foundations. Organizations must start with a clear roadmap that aligns business goals with security requirements. This includes implementing comprehensive security tools, establishing monitoring systems, and ensuring all employees understand their role in maintaining security.

Success with AI security isn't a destination—it's an ongoing journey that requires constant vigilance and adaptation. Organizations must continuously monitor for new threats, evolve their security measures, and learn from their successes and challenges.

Financial institutions that thrive in the AI era will be those that create a culture of security awareness while innovating their technological capabilities. By learning from industry leaders and maintaining focus on both innovation and protection, companies can build AI systems that transform the way they do business while keeping their data and systems secure. The future of finance belongs to organizations that recognize security not as a barrier to progress, but as an essential foundation for trusted AI innovation.

Visit Check Point's financial services solutions page to learn how we can help protect your AI investments with industry-leading security that scales with your needs:

engage.checkpoint.com/financial-services

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com