REPORT

Finance security trends and the impact of artificial intelligence

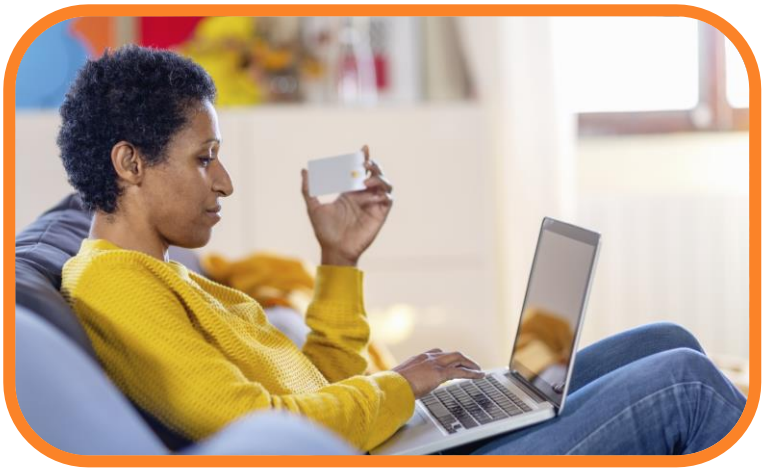
May 2025

LUMEN®

Contents

Introduction

The finance industry has increasingly relied on technology to improve operations, reduce risk, and enhance overall efficiency. Technology that was once considered innovative—like online banking, mobile payment systems, and financial management software—has become almost ubiquitous. This reliance on technology, however, has also made financial organizations prime targets for cyber threats—with two-thirds of financial institutions having experienced a cyber incident in the past year.[1]



It's easy to see why the industry is so highly targeted. Financial gain is the primary motivator behind cyberattacks, and financial organizations store vast amounts of sensitive data that can be exploited for identity theft, financial fraud, or ransomware if it falls into the wrong hands. Monetary rewards are not the only motivating factor. Some of the largest attacks on financial companies have been credited to nation-state actors who aim to gain economic advantages, destabilize economies, disrupt vital infrastructure, or steal valuable data and intelligence—a so-called "digital Pearl Harbor."

To complicate matters, financial services organizations typically have IT infrastructure with numerous connected devices and third-party vendors, as well as physical branches, which increases the potential attack surface and makes it harder to secure. Emerging technologies such as cloud, the Internet of Things (IoT), and generative artificial intelligence (GenAI) further proliferate the attack surface and can complicate security stacks, reducing visibility.

Recently, AI integration in finance has brought both opportunities and challenges from a cybersecurity perspective. AI has emerged as a powerful tool in finance, offering solutions for predictive analytics, fraud detection, and credit risk assessment. Simultaneously, AI has introduced new vulnerabilities, regulatory uncertainties, and ethical concerns that must be addressed.

In this report, we explore the state of cybersecurity and compliance in finance, along with the impact of an AI-driven future. By understanding these dynamics, financial organizations can be better prepared to avoid and mitigate risks.

Security trends in finance

Below are some of the latest security trends in finance—from vulnerabilities to increasing cyber threats, rising costs, and a fluid regulatory landscape. Later in this report, we will dig into some of the ways AI could impact the future of finance.

Vulnerabilities

Hacking financial organizations is lucrative, so the industry has always been vulnerable to cybercrime. And now AI is changing the game both for threat actors and cyber defenders. Some of the trending vulnerabilities in financial services include:

Quantum decryption

AI is now, but the financial world is well aware that quantum computing is the future. The up-and-coming technology promises innumerable benefits; however, like AI, quantum computers are a double-edged sword. Quantum algorithms can factorize large numbers exponentially faster than classical computers, rendering current encryption methods that are foundational to securing financial transactions and sensitive data obsolete.

To counteract the threat posed by quantum computing, the finance industry must transition to quantum-safe cryptographic algorithms to protect sensitive financial data.

Endpoints and IoT devices

The proliferation of connected financial devices has further compounded security challenges. While these devices allow for remote account access and automated transactions, many lack basic cybersecurity protection. Devices such as ATMs, point-of-sale systems, and mobile payment terminals can be exploited to disrupt transactions or gain access to broader financial networks. Fifty-two percent of financial organizations reported endpoints as a common attack vector in 2024.[1]

Cryptocurrency and fake digital assets

While hackers often target unpatched software and endpoints to breach financial networks, many cyberattacks on financial companies involve fake digital assets meant to scam victims. Fake digital assets can take many forms, such as fake cryptocurrencies or investment opportunities in fake initial coin offerings (ICOs) that promise high returns with no actual technology to invest in.

Crypto crime is trending upwards according to the FBI and is a huge vulnerability in the finance industry, with losses related to cryptocurrency fraud estimated at over $9.3 billion in 2024, a 66% increase year over year. Seventy percent of those losses were connected to investment fraud.[2] Cryptocurrency is a murky and shifting landscape, with the currency's anonymity and irreversible, decentralized transactions making it an attractive vehicle for bad actors while making it near-impossible to recover funds.

Figure 1

The FBI estimates a 66% increase year-over-year in losses related to cryptocurrency fraud, with $9.3B losses in 2024.[2]

Source: FBI, IC3 Cryptocurrency Fraud Report 2024, April 2025

Fraud and impersonation threats

It's becoming easier and easier for bad actors to commit fraud. With AI-driven deepfakes, synthetic identities, and voice cloning, fraudsters can pose as trusted individuals, making it difficult to distinguish between legitimate and fraudulent communications. One financial firm made headlines in 2024 for accidentally giving cybercriminals $25 million after being duped by a deepfake of the company's CFO.[3]

Human risk and phishing

Human risk management is nothing new, and as attacks grow more sophisticated and frequent, employee security awareness is an essential defense against cyber risks. One avenue that fraudsters use to exploit financial employees is targeted phishing attacks, whereby bad actors may send a fake email to trick employees into providing their credentials. According to IBM's latest research, 24% of breach root causes in 2024 in the finance sector were tied to human error.[4]

Later in this report, we will look at the latest trend that is increasing threat actors' ability to create more sophisticated phishing scams, more realistic fake digital assets and synthetic identities, and harder-to-detect endpoint attacks: artificial intelligence.

Increasing cyber threats

As financial companies seek to mitigate the above-listed vulnerabilities, threat actors continually look for opportunities to launch catastrophic attacks and steal data. Some of the trending attack types for the finance industry include:

Ransomware

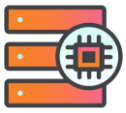
Ransomware continues to be one of the most pervasive threats for financial companies, with payments trending higher, increasing 500% across all industries in the last year.[5] Many ransom-seekers have targeted finance for a lucrative payout. In November 2023, for example, the world's largest bank, Industrial and Commercial Bank of China, suffered a ransomware attack that made headlines for disrupting Treasury markets.[6]

Supply chain attacks

The finance industry is highly interconnected and increasingly digital—considering mobile banking, third-party APIs, open-source tools, digital wallets, and interconnected systems, it's no wonder that the software supply chain is vulnerable to cyberattacks. In fact, over 52% of financial organizations said their organization was impacted by a supply chain attack in 2024.[1]

Cloud compromise and API attacks

As endpoint protection has advanced and become harder to bypass, attackers have switched focus to applications as a gateway to infiltrate financial systems, exploiting an increasingly complex hybrid and multi-cloud architecture environment. In 2024, cloud environments and APIs were the top two attack vectors in financial organizations.[1]



Nation-state-sponsored cybercrime

In recent years, the Russian-Ukraine war has demonstrated the profound impact that nation-state cyberattacks can have on the global economy. These attacks often target critical infrastructure, such as banks, with the intent to destabilize national economies.

The finance industry is particularly vigilant about geopolitical developments, as these factors significantly influence global markets. With the current volatility in global markets due to shifting economic sanctions and tariffs, this trend is top of mind for the industry, as there is a heightened risk that nation-state-affiliated hackers might engage in retaliatory cyberattacks.

Cost of being breached

The cost of data breaches continues to be a serious issue for finance companies. According to the IBM Cost of a Data Breach 2024 report, the average global cost of a data breach has surged to US$4.88 million, marking a significant increase from last year's US$4.45 million and representing the largest jump since the onset of the pandemic.[7]

For financial enterprises, the stakes are even higher, with the industry suffering the second-highest breach cost of any industry. The average cost of dealing with data breaches in this sector has escalated to US$6.08 million, which is 22% above the global average.[4]

Additionally, financial enterprises face intense scrutiny from regulatory agencies, meaning that breach costs go far beyond the price of identification and remediation. Any delays in addressing threats could mean regulatory fines that outstrip initial expenses.

24%

Of GenAI initiatives are secured, showing a lack of security that could expose data and data models to breaches.

1 in 3

Breaches involved shadow data, showing the proliferation of data is making it harder to track and safeguard.

$6.08M

Average cost of a breach for financial enterprises, which is 22% than the global average.

$2.22M

Average cost savings for organizations using extensive security AI and automation in prevention versus those that didn't.

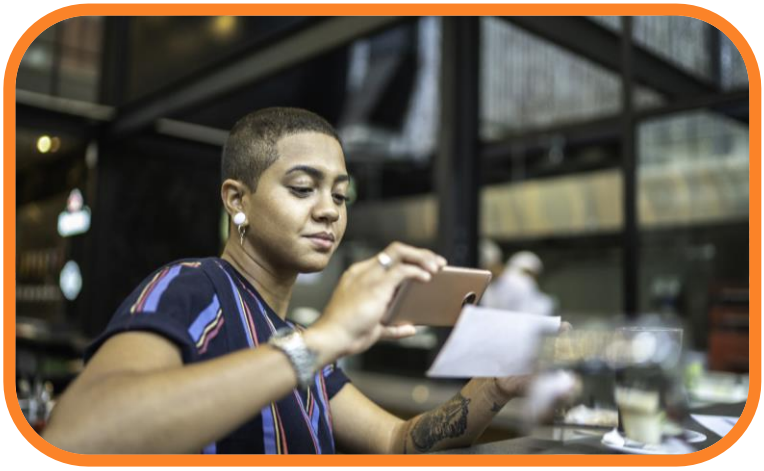
Source: IBM, Cost of Data Breach Report 2024, July 2024

Emerging technologies and regulatory considerations

Speaking of the financial regulatory landscape, which has always been under a microscope, cryptocurrencies and the adoption of advanced technologies such as AI have introduced new regulatory challenges. Regulators are increasingly focusing on the security implications of these technologies and implementing new frameworks to manage associated risks and compliance requirements.

AI and GenAI governance

The integration of AI and GenAI in financial services offers promising opportunities for personalized customer engagement and operational efficiency. However, these technologies also introduce significant risks, including biases, data privacy concerns, and the potential for misuse. To mitigate these risks, regulatory bodies are emphasizing the importance of AI governance frameworks like AI TRiSM, which ensure trustworthiness, fairness, reliability, robustness, efficacy, and data protection. Banks are required to adopt these frameworks to comply with regulatory standards and safeguard customer interests.[8]



Cryptocurrency and digital assets

The adoption of cryptocurrencies and digital assets is gaining momentum, driven by regulatory changes and increasing client interest. The EU's Markets in Crypto Assets (MiCA) regulation and the U.S. Securities and Exchange Commission (SEC) enabling individual investors to purchase spot exchange-traded funds (ETFs) are notable developments.[8] These regulations aim to provide a clear and comprehensive framework for crypto assets, enhancing investor protection and fostering market stability. Financial institutions must navigate these regulatory changes to safely integrate digital assets into their offerings and meet client demand.

Data privacy and protection

With digital-first banking and AI-driven insights, data privacy and protection have become critical concerns. Regulatory bodies are enforcing stringent data minimization requirements and transparency standards to ensure that customer data is handled responsibly. Financial firms are investing in customer data platforms (CDPs) to unify and manage data from various sources, optimizing customer engagement while complying with data privacy regulations.[8]

In conclusion, the regulatory landscape in the finance industry is adapting to address the complexities of emerging technologies and cybersecurity threats. Financial institutions must stay abreast of these changes and invest in compliance measures to protect their operations and maintain client trust.

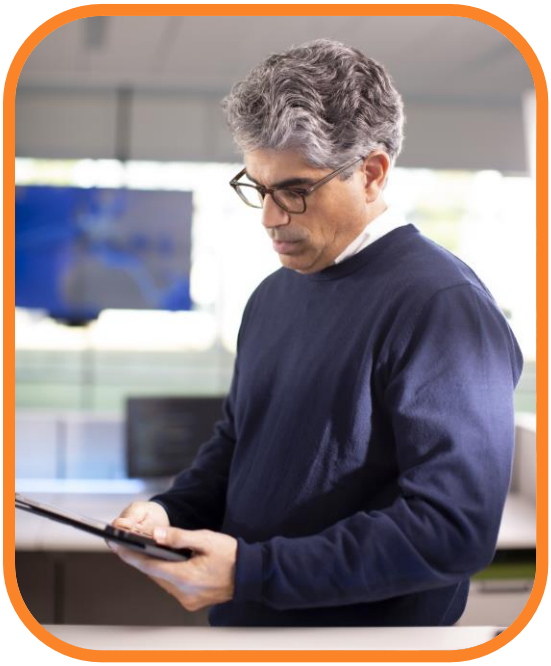
Artificial intelligence in finance

AI and machine learning are transforming the finance industry. These technologies are being integrated into various applications such as chatbots, transaction monitoring, fraud detection, trading algorithms, and more to enhance innovation, efficiency, and financial services. While AI can save money for financial firms, it can just as easily become an additional attack vector for cybercriminals, costing millions. In fact, just 24% of generative AI initiatives are secured according to IBM.[4]

Given the ongoing vulnerabilities in financial technology, the continued rise of cyber threats, and the regulatory changes described above, it's important to look at the impact that AI has on the finance industry.

Benefits of AI in finance

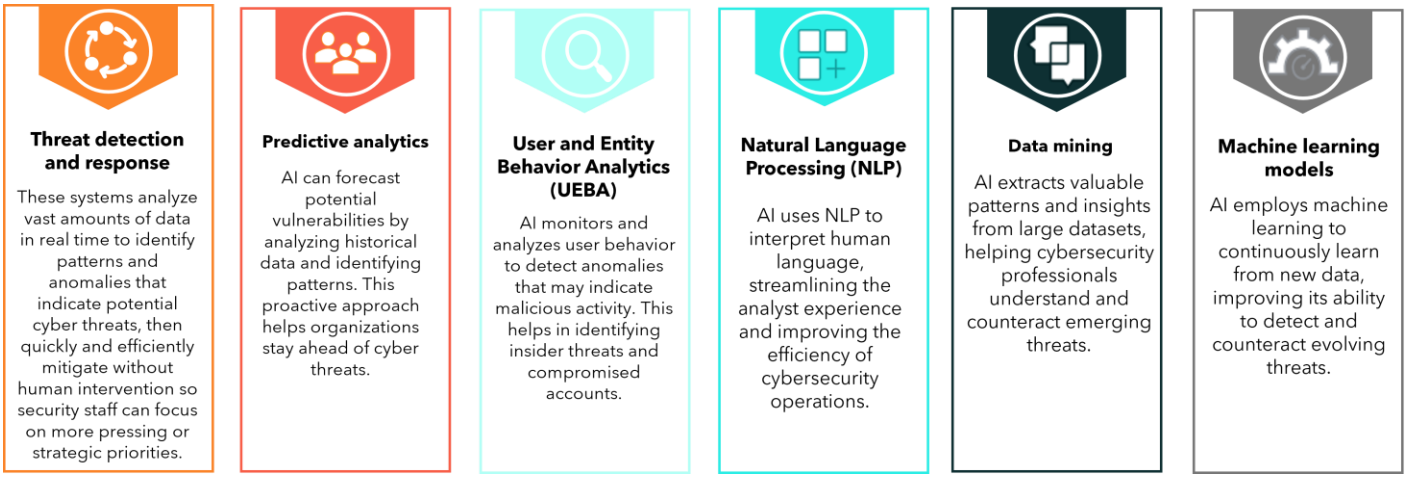
AI offers numerous benefits to the finance industry, including:



- **Improved fraud detection:** AI algorithms can analyze large volumes of transaction data in real-time to detect suspicious activities and potential fraud. By identifying patterns and anomalies, AI enhances the security of financial transactions and protects against cyber threats.
- **Personalized financial services:** AI enables personalized financial services by analyzing customer data to predict the most effective products and services. For example, AI-driven robo-advisors offer automated investment advice, while AI-powered lending platforms provide personalized loan offers based on individual credit profiles. This approach improves customer satisfaction and reduces trial-and-error in service offerings.
- **Predictive analytics:** AI allows financial institutions to leverage predictive analytics for better decision-making. By analyzing historical data and identifying trends, AI can forecast market movements, assess credit risk, and optimize investment strategies.
- **Risk management:** AI enhances risk management by providing real-time insights into potential risks and vulnerabilities. Financial institutions can use AI to monitor market conditions, assess the impact of economic changes, and develop strategies to mitigate risks.
- **Streamlined administrative tasks**: AI automates repetitive and time-consuming tasks such as data entry, transaction processing, and compliance checks. This reduces operational costs and minimizes the risk of human error. Gartner predicts that by 2026, more than 70% of frontline tasks will leverage GenAI capabilities to financially empower banking customers.[8]
- **Enhanced customer service:** AI-powered chatbots and virtual assistants provide 24/7 customer support, handling routine inquiries and transactions efficiently. This helps improve customer satisfaction and enables human agents to focus on more complex issues.
- **Regulatory compliance:** AI assists financial institutions in complying with regulatory requirements by automating compliance checks and monitoring transactions for suspicious activities. This ensures adherence to regulations and reduces the risk of penalties.

AI-driven security solutions

As financial organizations implement AI to innovate, discover new products, and improve efficiency and customer service, they're also exploring ways to secure their enterprises with AI. Some of these solutions include:



AI-driven attacks

When it comes to cybersecurity, AI is a double-edged sword. As financial organizations employ AI to stop attacks before they occur, threat actors weaponize AI to create highly targeted campaigns and launch sophisticated attacks. Gartner predicts that by 2027, 17% of all cyberattacks will involve GenAI.[9]

Some of the AI-driven tactics cybercriminals use today include:

- Sophisticated phishing attacks: AI can craft highly convincing phishing emails that lack common red flags, making them harder for employees to detect.
- Targeted spear phishing: Threat actors use AI to analyze stolen data to create personalized spear-phishing emails, increasing the likelihood of successful attacks.
- Automated data analysis: AI tools can quickly process and organize large amounts of stolen data, aiding cybercriminals in identifying valuable targets.
- Accelerated brute force attacks: AI can accelerate brute-force password cracking, allowing even quicker access to systems.
- System vulnerability analysis: Threat actors have used AI to identify and exploit vulnerabilities, making the attacks more efficient and damaging.

Recommendations for IT security in finance

Recent research from IDC reports that the top three cybersecurity gaps are detection, talent, and visibility.[10] Given the vulnerabilities, threats, regulatory changes, and AI-powered attacks impacting the finance industry, immediate proactive steps are necessary to close these security gaps and mitigate overall risk.

Invest in AI-driven threat intelligence

Investing in advanced, AI-driven security tools is essential. AI-backed cybersecurity technologies can protect sensitive patient data by quickly identifying fraud and blocking bad actors, thereby maintaining safe experiences and building trust between healthcare companies and their stakeholders.

The threat intelligence arm at Lumen, Black Lotus Labs, has been using proprietary machine learning models for years to automate threat detection and response across the Lumen internet backbone. Our success in this region earned Lumen the Cybersecurity Breakthrough Awards Threat Intelligence Company of the Year in 2024.

Secure the edge

In addition, real-time data processing requires faster speeds to offer real-time trading and personalized financial service recommendations. This is why edge solutions integrated with AI can enhance financial operations and customer service by keeping data close to the source and reducing latency.

Foster a culture of security

Continually training staff in cybersecurity best practices and encouraging collaboration between IT and financial professionals can significantly enhance the security posture of financial organizations. A culture of security ensures that all stakeholders are aware of and actively engaged in protecting financial data. Financial organizations should implement AI- and cloud-ready technologies to support scalable and secure data management.

Prepare your network

As we have seen, AI is transforming finance in profound ways. But an AI-enabled future requires preparation, and financial companies must ensure their networks can handle the increased data demands. This is because AI applications process vast amounts of data in real-time, which can quickly overwhelm outdated systems and cause them to struggle to efficiently process and store data. The subsequent delays and operational errors can lead to financial loss and poor customer outcomes, and the reliance on legacy infrastructure can expose critical weaknesses, which makes it easier for cyber attackers to exploit vulnerabilities and gain unauthorized access to sensitive information.

Upgrading to modern, secure systems is essential to handle the data-intensive requirements of AI technologies effectively. Without modernized network infrastructure, financial organizations risk facing data bottlenecks, delays in critical diagnostics, and potentially compromised customer service.

By upgrading their networks, financial companies can help ensure seamless data flow, which can improve customer experiences while helping decrease costs and minimize risks.

Leverage managed and professional services

- **Enhanced security**: Reduce threat management overload, minimize attack surfaces and enhance defense alertness with certified consultants and engineers to help protect sensitive financial data in real-time. This is crucial as AI applications require real-time data processing, which can expose vulnerabilities if not properly secured.
- **Incident Response**: Proactive threat monitoring and incident response services provide comprehensive protection and rapid resolution of security incidents.
- **Regulatory compliance**: Managed services assist financial organizations in staying compliant with evolving regulations through assessments, compliance programs, and readiness assessments.

- **Pen testing and assessments**: Regular audits and penetration testing identify and address vulnerabilities, helping to ensure resilience and risk management even as AI workloads expand the attack surface.

By leveraging managed and professional services, financial companies can effectively prepare for an AI-enabled future, ensuring that they can harness the benefits of AI while minimizing risks and maintaining compliance.

How Lumen can help

Networking and security solutions

With the integration of AI into finance, the demand for high-capacity, low-latency networks has never been greater. Lumen's networking solutions are designed to support financial companies as they prepare for this AI-enabled future. Our robust infrastructure, including our extensive fiber network and advanced AI-driven security solutions, helps ensure that financial organizations can leverage AI technologies to enhance customer service, streamline operations, and improve fraud detection accuracy.

Lumen provides AI-enabled connectivity, AI-optimized data/cloud, and AI-automated security, and includes the following suite of networking and security solutions:

- **Flexible network connectivity:** Lumen® Network-as-a-Service (NaaS) provides real-time, self-service, scalable control over network connectivity, enabling businesses to manage, bandwidth, path, and latency dynamically.
- **Minimize downtime and enhance customer experiences:** Lumen® DDoS Mitigation services provide comprehensive protection against DDoS attacks by rapidly filtering malicious traffic and returning clean traffic to customers, leveraging a multi-layered scrubbing architecture and advanced threat intelligence from Black Lotus Labs.
- **Minimize risk:** Lumen Defender℠ powered by Black Lotus Labs® offers proactive network protection by automatically blocking traffic from risky sources before it breaches internal networks, leveraging comprehensive threat intelligence.
- **Simplify networking and security:** Lumen® SASE Solutions unify network and security management through a centralized, cloud-based experience, simplifying the design, purchase, deployment, and orchestration of software-defined network infrastructure and information security.
- **Minimize costs and scale on your terms:** Lumen® SD-WAN solutions support secure, scalable, and cost-efficient deployment and management of hybrid networks, providing complete visibility, control, and security across various connectivity types.

BLACK LOTUS LABS® by Lumen

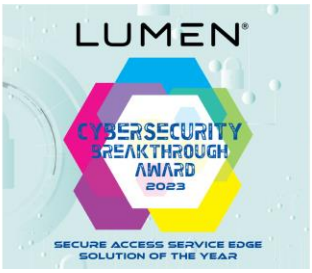
Black Lotus Labs® is the award-winning, in-house threat research arm of Lumen. The team of data scientists, reverse engineers, security engineers, and threat analysts leverages their unmatched visibility into the Lumen network to protect businesses and help keep the internet clean.

Black Lotus Labs use advanced threat technology to identify and eliminate threats quickly, employing machine learning algorithms to automate protection and neutralize threats. The team has been involved in the identification and takedown of some of the most high-profile malware of the past decade.

- **Optimize efficiency for customers and employees:** Rapid Threat Defense integrates Black Lotus Labs intelligence to proactively block known malicious traffic, enhancing operational efficiency and reducing the burden on IT staff.
- **Focus resources, minimize expenses:** Lumen Security Operations Center as a Service (SOCaaS) offers fully managed cybersecurity threat detection, incident management, and response support, providing visibility across an agency into cyber activity.
- **Reduce costs and risks:** Lumen Incident Reporting system provides prompt reporting and management of risk-related incidents involving company employees, vehicles, and facilities, facilitating rapid response and resolution.
- **Reduce workloads while defending critical apps and data:** Lumen's managed and professional security solutions provide comprehensive protection through proactive threat monitoring, incident response, penetration testing and tailored advisory services, providing robust security and compliance for businesses.

By providing secure, high-speed connectivity and real-time data processing capabilities, Lumen helps to enable financial organizations to implement AI applications such as predictive analytics, robo advisors and chatbots, and automated administrative tasks. This helps improve patient outcomes, minimize security and compliance risks, reduce costs and increase revenue.

Lumen has won three consecutive Cybersecurity Breakthrough Awards including the 2022 Network Security Provider of the Year award, the 2023 SASE Solution of the Year award, and the 2024 Threat Intelligence Company of the Year award.



The bottom line

The integration of AI into finance presents both opportunities and challenges in the realm of cybersecurity. By understanding current security trends, vulnerabilities, regulatory changes, and the impact of AI, financial organizations can better prepare for and mitigate cyber threats. Implementing robust security measures, staying updated with regulations, and fostering a culture of security are essential steps in safeguarding financial data and ensuring the continued advancement of financial technology.

Your network infrastructure is the cornerstone of your AI efforts

The Lumen network supports the dynamic demands of AI-powered technologies and enhances patient care by providing high-capacity connections, deep IP peering and AIOps to leverage AI/ML apps without the constraints of a traditional network.

View secure solutions

Footnotes

[1] Contrast Security, Modern Bank Heists Report 2025, March 2025
[2] FBI Internet Crimes Complaint Center (IC3), 2023 Cryptocurrency Fraud Report, April 2025
[3] CNN, Finance worker pays out $25 million after video call with deepfake 'chief financial officer', February 2024
[4] IBM, Cost of a data breach 2024: Financial industry, August 2024
[5] Sophos, State of Ransomware 2024, April 2024
[6] CNBC, China's ICBC, the world's biggest bank, hit by cyberattack that reportedly disrupted Treasury markets, November 2023
[7] IBM, Cost of a data breach report 2024, July 2024
[8] Gartner, Top Business Trends in Banking for 2025, March 2025
[9] Gartner, Gartner Forecasts Global Information Security Spending to Grow 15% in 2025, August 2024
10 IDC, The New Cybersecurity Equation: Risk, Response, and Business Outcomes, February 2025

Why Lumen?

Lumen is your single provider to enable digital transformation. With a comprehensive portfolio and experienced talent, we can help safeguard your customer experience, protect your confidential data, and manage threats. Backed by the extensive and deeply peered Lumen global network, Black Lotus Labs® threat intelligence, and our skilled and experienced team of security experts, Lumen is a trusted partner to help improve your security posture.

866-352-0291 | lumen.com | info@lumen.com

LUMEN®