POINT OF VIEW

Cybersecurity for financial services organizations

An OpenText industry perspective

Contents

> “In 2024, roughly 65 percent of financial organizations worldwide reported experiencing a ransomware attack, compared to…34 percent in 2021.”
>
> Ani Petrosyan, Statista

> “The thing that we worry about a lot is cyber attacks. I think we have a great game plan for traditional issues like bad loans and things like that… [C]yber attacks are really the frontier where you worry.”
>
> Jerome Powell, Chair of the US Federal Reserve

Key cybersecurity challenges facing financial services organizations

Financial services organizations face relentless, evolving threats from cybercriminals seeking to exploit valuable assets through advanced techniques.

Here are their key challenges:

Preventing data breaches, insider threats, and fraud

Financial institutions are contending with increasingly sophisticated cybercriminal groups waging phishing and ransomware campaigns as well as launching account takeover, digital skimming, and payment fraud attacks.

Insider threats are also a significant issue in the financial sector. Rogue individuals within the organization, such as employees, contractors, or business associates, can misuse access to sensitive data and systems. The average annual cost of insider threats in the financial sector is around $14.5 million, which is higher than in any other industry.[1] To block and contain these threats, they must improve detection, accelerate incident analysis and response, and better protect customer and employee identities and credentials.

Frictionless and secure application deployment

Financial institutions are challenged to detect and reduce key vulnerabilities, misconfigurations, and other security issues in customer-facing applications without slowing development and deployment processes. Key best practices include security by design, automated software testing, and comprehensive screening of open-source and third-party code embedded in applications.

[1] DTEX, 2024 Insider Risk Investigations Report

More information on challenges facing financial institutions

- International Monetary Fund (IMF): Rising Cyber Threats Pose Serious Concerns for Financial Stability
- Forbes: Cybersecurity In Finance: Protecting Client Data And Mitigating Risks
- Forbes: Defending Against the Top Four 2024 Financial Services Attacks
- McKinsey & Company: The cyber clock is ticking: Derisking emerging technologies in financial services
- Statista: Cybercrime and the financial industry in the United States - Statistics & Facts
- Statista: Artificial intelligence (AI) in finance - statistics & facts
- Survey Report: STATE OF AI IN FINANCIAL SERVICES 2022 TRENDS
- Knowledge at Wharton: AI in Finance: The Promise and Potential Pitfalls
- Field Effect: The top cyber threats facing financial services firms
- UpGuard: The 6 Biggest Cyber Threats for Financial Services in 2024

Deliver seamless secure experiences

Providing seamless, secure experiences is crucial for maintaining customer trust, ensuring regulatory compliance, and enhancing customer loyalty.
It minimizes friction in transactions, protects sensitive financial data, and reduces the risk of fraud. This leads to increased customer retention, stronger reputation, and a competitive edge in a highly regulated industry.

Comply with expanding regulations

Regulators and standards bodies are continually escalating requirements for resilience, privacy, and governance. Organizations must comply with updated versions of GLBA, NYDFS, DORA, NIS2, Cyber Resilience Act, and NIST, as well as other state, federal, and international regulations and standards.

AI adoption

AI increases cybersecurity risks and data privacy concerns by relying on sensitive data, creating new attack opportunities, and complicating compliance with evolving regulations.

Preventing data breaches, insider threats, and fraud

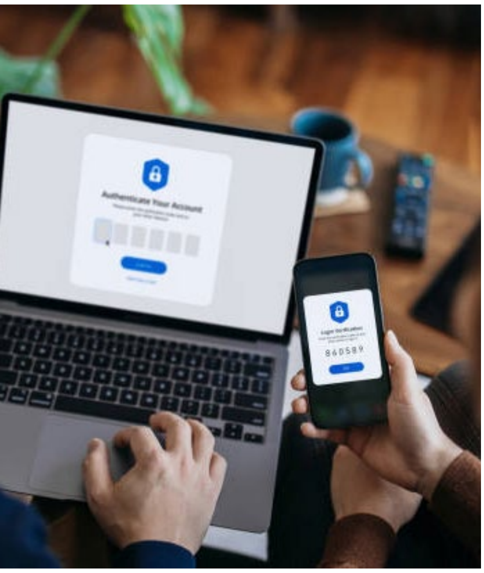
OpenText helps financial institutions strengthen their capabilities to protect identities and data while deploying secure applications.

Identity protection

Threat actors have discovered that the easiest way to circumvent security controls and anti-fraud measures usually involves exploiting legitimate customer and user credentials. To minimize the impact of identity-related attacks, financial institutions need to:

- Enforce policies that minimize unnecessary access to data and applications.
- Reduce the loss and theft of identity information and credentials.
- Detect threat actors attempting to impersonate employees, customers, and business partners using stolen credentials.

The OpenText identity and access management solutions (Access Management, Identity Governance and Administration, and Privileged Access Management) enable financial institutions to implement best practices to:



- Discover identity and credential stores across the enterprise, so they can be consolidated and protected.
- Streamline identity and access management (IAM) by using automated processes and intuitive workflows to define, manage, request, and approve identities, permissions, and credentials throughout their lifecycles.
- Leverage advanced identity governance to detect and address orphaned and inactive accounts, entitlement creep, over-privileged users, and unnecessary group memberships.
- Use rule sets to discover and retrieve various account details and help manage them. Discovery of privileged accounts also enables administrators to add multiple accounts to a preferred resource.
- Detect violations of separation of duties (SoD) policies.
- Ensure that non-human identities are who they claim to be and secure interaction between them.
- Ensure the validity of customer and remote employees with passwordless, attack-resistant multifactor authentication (MFA).
- Provide cloud infrastructure entitlement management (CIEM) to control access to SaaS applications, cloud file storage systems, and public and private cloud platforms.

The OpenText threat detection and response solutions can help detect anomalous behavior with integrated AI and analytics, delivering a faster incident response to effectively prioritize risk and reduce breaches and insider threats.

Data protection

Threat actors and fraud campaigns typically target customer and employee data. To safeguard that data, financial institutions need to:

- Accelerate threat detection and response.
- Discover and secure high-value data everywhere it resides.
- Consistently enforce security policies.
- Unlock deep insights that foster best practices for security and privacy.

OpenText data privacy and protection solutions help financial institutions implement best practices to:

- Find and control "shadow IT" applications and data repositories that increase the risk of data leakage and data breaches.
- Conduct global discovery, so all structured data stores and unstructured data repositories alike can be classified and protected with the appropriate controls.
- Employ AI to identify personally identifiable information (PII), financial account records, intellectual property, product designs, credentials, software, and other high-value information everywhere it is created, stored, and processed.
- Enforce access control and data access governance (DAG) policies consistently across the enterprise.
- Monitor and analyze data access events to uncover suspicious activities and unnecessary permissions, and identify data that should be moved, better secured, or retired.
- Facilitate secure testing, analysis, and data sharing through techniques for masking, tokenization, and anonymization.
- Identify opportunities to consolidate data repositories and reduce the data attack surface.
- Assess data-related risks to prioritize remediation activities, justify new data protection initiatives, and improve the organization's data security posture.

More information about identity protection and data protection

- Omdia 2024 Market Landscape: Data Security Posture Management (DSPM)
- IGA Buyer's Guide: Selecting the Right Identity Governance and Administration Solution
- Identity Administration Needs Governance
- Driving Efficiency and Optimization Helps Transform Your Business and Guides Data Privacy Preparedness
- Data Discovery: Key to Data Privacy and Cyber Resilience
- AI-Driven Analytics for Data Discovery
- OpenText Identity Governance and Administration web page
- OpenText Data Privacy and Protection web page
- OpenText Cybersecurity Aviator: Enable faster threat protection with AI and machine learning

More information about application security protection

- 2023 State of Code Security Report
- 2023 Gartner® Magic Quadrant™ for Application Security Testing
- OpenText Application Security web page
- Application Security Posture Management
- OpenText Fortify Aviator: Solution Overview

Deploying frictionless and secure applications

To prevent threat actors from compromising internet-facing software applications, those applications need to be "secure by design," with security requirements defined, developed, and tested throughout the software development lifecycle (SDLC).

OpenText application security solutions provide financial institutions the tools to implement best practices to:

- Integrate security testing of all types (including SAST, DAST, IAST, MAST, IaC, SCA, API, and penetration testing) into automated development, security, and operations (DevSecOps) processes.
- Drastically reduce the time developers spend remediating code security issues by leveraging AI-powered code fix suggestions.
- Improve the security of application programming interfaces (APIs).
- Shift left in the SDLC to swiftly identify vulnerabilities for both cloud-native applications and those being modernized for the cloud.
- Analyze the risks of application vulnerabilities and security issues to better prioritize remediation actions.
- Prevent software supply chain attacks by ensuring that open-source and purchased custom software has not been compromised and does not contain unlicensed proprietary code.
- Automatically scan open-source code bases for vulnerabilities and violations of licensing agreements.
- Provide visibility and analysis so the organization can monitor and improve its application security posture.

More information about frictionless customer experiences

- The Financial Brand: Go Beyond ROI With ‘Return on Experience’ in Banking
- What is Passwordless Authentication?
- Forbes: The Benefits And Risks Of AI In Financial Services
- Amplifying AI for banking: Your guide to accelerating digital transformation
- NetIQ Advanced Authentication for Your Business
- OpenText Advanced Authentication web page
- OpenText Experience Aviator web page
- OpenText Experience Aviator: Create unique content to cover all touchpoints with generative AI and image AI

Delivering frictionless secure experiences

A survey by industry analyst firm Forrester found that financial institutions are 180 percent more likely to see improved customer satisfaction when focusing on experience-driven engagements.[2]

Unfortunately, complex authentication processes and password-related issues have long frustrated customers and clients. In contrast, frictionless authentication and self-service enrollment and administration increase customer loyalty and improve security while reducing customer support costs.

OpenText identity security and data protection solutions enable financial institutions to adhere to best practices to:

- Improve customer experiences by deploying simple, passwordless, attack-resistant MFA (authentication processes that use biometric recognition rather than inherently insecure, difficult-to-support passwords and password management systems).
- Reduce support costs and customer frustration by providing self-service capabilities to enroll in online services and applications.
- Use adaptive authentication and contextual security data to dynamically create risk scores, provide frictionless authentication when possible, and create step-up validation requests when necessary.
- Use generative AI and AI image generation to gather insights from unstructured customer information, better understand customer needs and behaviors, and create contextual, personalized, and relevant content that transforms customers’ engagement with the organization.

[2] The Financial Brand, Go Beyond ROI With ‘Return on Experience’ in Banking, 2021

Complying with expanding regulations

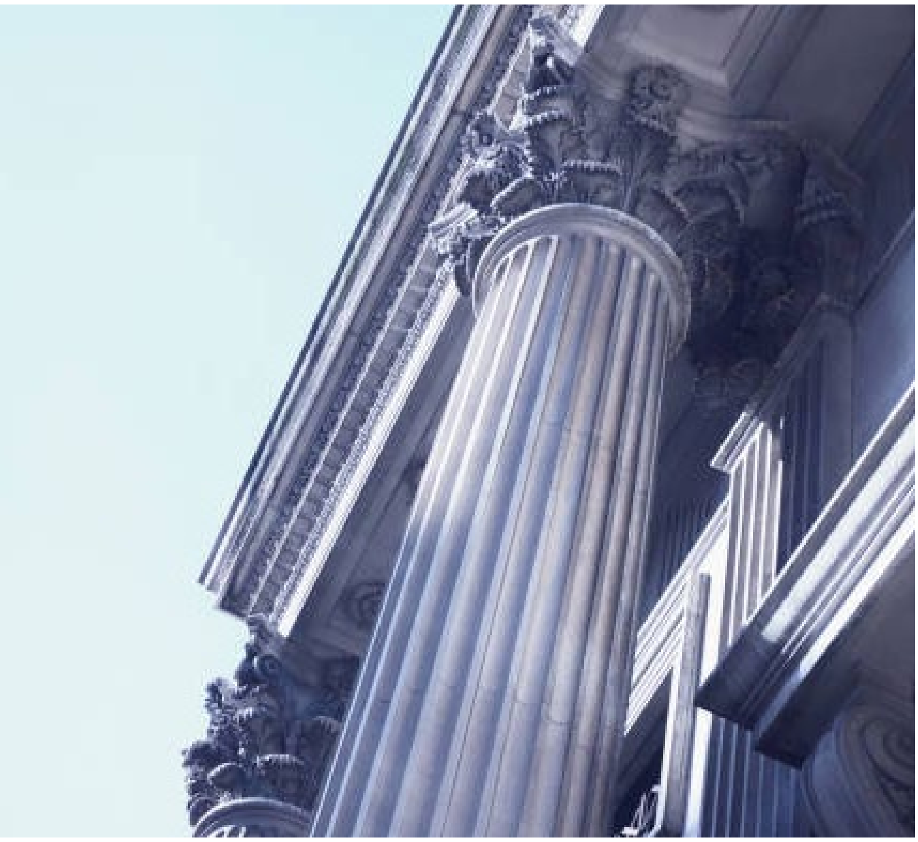
Numerous frameworks, regulations, and standards affecting financial institutions have either been updated and extended in 2024 or have new provisions going into effect during the year or soon after.

These include the Gramm-Leach-Bliley Act (GLBA), various NIST standards, and the New York State Department of Financial Services Cybersecurity Regulation (23 NYCRR Part 500) in the US, the Digital Operational Resilience Act (DORA), NIS2 Directive, General Data Protection Regulation (GDPR), and Cyber Resilience Act in the EU, and the Security of Critical Infrastructure (SOCI) Act in Australia, among others.

OpenText solutions for application security, data privacy and protection, IAM, and threat detection and response enable financial institutions to:

- Streamline the production of compliance reports, certifications, and micro-certifications.
- Meet requirements for data protection and business resilience by demonstrating visibility into all types of protected data at every level, consistently enforcing access policies for applications, databases, and data repositories, and managing effective data back-up and recovery processes.
- Implement best practices for retaining, archiving, and deleting data and for controlling the flow of data to third parties and across geographical boundaries.
- Implement best practices for enforcing role-based access control (RBAC), SoD, and the principle of least privilege.
- Comply with mandates to encrypt, mask, or anonymize data in motion and data shared with processors and service providers to maintain data privacy.
- Detect all instances of PII, payment card industry (PCI) data, account credentials and access keys, and words and phrases associated with specific regulations and standards so all information assets can be protected by the necessary controls.
- Support compliance with regulations governing personal information, including rights of access, rights to restrict processing of personal information, and “the right to be forgotten.”
- Create comprehensive audit trails of the creation, storage, access, and sharing of data.
- Employ artificial intelligence to collect, sift, analyze, and organize information for compliance reporting and to automatically prefill compliance reports.
- Perform and document all types of security testing during software development, including SAST, DAST, IAST, MAST, IaC, SCA, API, and penetration testing.

- Detect anomalous behavior and deliver faster incident response to effectively prioritize risk and reduce breaches with integrated AI and analytics.
- Use real-time contextual threat intelligence as the foundation for enabling unmatched threat insights as well as helping anticipate and adapt to meet new threats.
- Secure sensitive information from access violations and application vulnerabilities to establish a foundation for secure AI adoption.
- Improve security posture and integrate security across business functions, roles, and processes to drive governance.
- Prioritize threat investigations with automated and intelligent risk scoring.

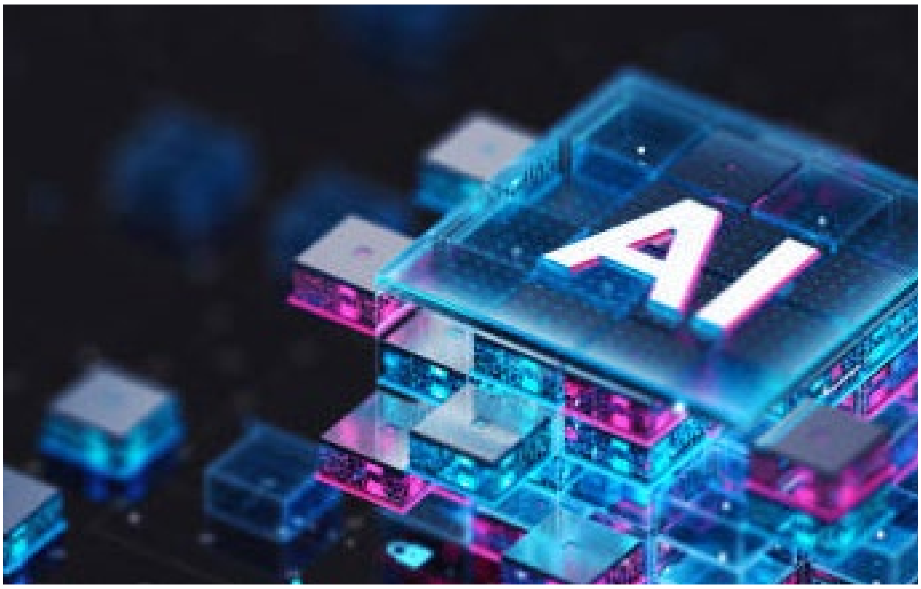


AI adoption

The potential of adoption of AI for security in the financial services industry is quite significant. Organizations must fully leverage AI and large language models (LLMs) to identify vulnerabilities and misconfigurations, detect suspicious activities, contain attacks, prioritize remediation activities, generate compliance documentation, recognize AI-based threats, and perform other key tasks.

OpenText security solutions can help you:

- Employ AI to identify PII, financial account records, intellectual property, product designs, credentials, software, and other high-value information everywhere they are created, stored, and processed.
- Use AI/ML and automation to continuously assess interactions that people and services have with sensitive information, enforcing stronger authentication or even blocking suspicious activities.
- Deploy artificial intelligence to collect, sift, analyze, and organize information for compliance reporting and to automatically prefill compliance reports.
- Leverage AI to recognize patterns and detect anomalies associated with attacks and fraud.
- Implement AI-powered threat detection to reduce the time it takes to identify suspicious activities and potential breaches, enabling quicker response and mitigation.
- Drastically reduce the time developers spend remediating code security issues by leveraging AI-powered code fix suggestions.
- Detect anomalous behavior and deliver faster incident response to effectively prioritize risk and reduce breaches and insider threats with integrated AI and analytics.



Conclusion

When it comes to digital security and privacy, financial services organizations are challenged in playing both defense and offense. You must counter increasingly advanced ransomware, insider threats, account takeover attacks, and fraud campaigns while also meeting expanding regulatory requirements. At the same time, you have opportunities to deliver more secure, lower-friction digital services to customers and to expand your use of AI and threat intelligence to anticipate, detect, and defeat threats.

You must also be prepared to seize the opportunities provided by AI as well as navigate new AI threats and risks.

OpenText can help you succeed with an extensive menu of cybersecurity and cyber resilience offerings, including solutions for identity and data protection, security by design and automated software testing, and attack-resistant MFA, and advanced security analytics. We are leaders in integrating AI and threat intelligence into our technology for automation and to improve productivity. Find out how we can partner with you to make your organization more secure, compliant, and resilient.

To learn more, go to: OpenText Cybersecurity Cloud