Trellix

SOLUTION BRIEF

Driving Cyber Resilience in Financial Services

The global financial services sector faces a surge in sophisticated cyber threats, with 45% of financial institutions experiencing AI-powered cyberattack attempts in 2025.[1] Supply chain compromises, identity-based attacks, and the blurring of the lines between cybercrime and geopolitical objectives have all contributed to a perilous landscape, as has the expanded attack surface introduced by open banking APIs and fintech integrations. With the average cost of a data breach in the financial sector reaching $5.56 million, having a proactive security strategy is paramount.[2]

To reduce risk, reinforce customer trust, and safeguard sensitive data, organizations require robust cyber resilience. Trellix® provides such cyber resilience by combining AI-native threat intelligence, endpoint security, network detection and response, data security, and security operations with expert consulting services and strategic partnerships.

Integrating security controls across endpoints, networks, data, cloud, email, and third-party applications to correlate signals and data-access events, Trellix empowers financial services organizations to proactively detect attacks and secure their operations. Trellix also helps customers improve visibility and control in support of strict regulatory and standards-driven requirements, such as faster investigation and response for SEC, DORA, CIRCIA, and NYDFS 500 cyber incident disclosure readiness, to name just a few regulations.

Countering AI-powered attacks with integrated solutions

Generative AI (GenAI) has fundamentally altered the threat landscape. AI agents are now the enterprise's fastest-growing exposed attack surface.[3] As teams use tools like LLMs and coding agents, the agents are

1 Axios, Exclusive: Financial sector most susceptible to AI-powered cyberattacks, 2025
2 IBM, Cost of a data breach: The financial sector, 2025
3 Infosecurity Magazine, AI Agents Now the Enterprises Fastest Growing Exposed Attack Surface, 23 July 2026.

given privileged access to essential infrastructure. Cybercriminals then target these AI identities, taking aim at the trust, credentials, and access permissions granted to them.

For example, a bank deploying an internal LLM connected through model context protocol (MCP) to CRMs, customer databases, identity access management, configuration management databases, or cloud services is no longer just deploying a chatbot. It is potentially creating a new privileged access and data aggregation layer.

Attackers also now deploy highly scalable and realistic social engineering and phishing campaigns that perfectly mimic internal corporate language, operational communications, and vendor correspondence. Deep-fake audio and video challenge the reliability of traditional verification and operational decision-making.

According to recent Trellix research, for example, the Scattered Lapsus$ alliance sustained highly focused voice phishing operations, employing real-time AI voice synthesis to impersonate internal IT staff during live support calls, successfully bypassing multifactor authentication (MFA) to access enterprise cloud environments. In addition, GenAI attacks can specifically target ATM operations teams to steal privileged credentials and manipulate maintenance workflows.

Trellix addresses these challenges by delivering integrated cybersecurity capabilities, with a strong focus on endpoint security, network detection and response, data security, email security, and security operations. Trellix solutions protect fully on-premises deployments, including highly restricted or air-gapped environments, while also extending protection across hybrid and cloud-connected architectures.

This empowers financial services organizations to improve visibility, strengthen protection, detect threats earlier, and respond faster across multiple environments without compromising the availability and stability requirements of critical operations. For example, equipped with Trellix solutions, Arab National Bank integrated siloed tools, eliminated redundancies, and cut down on operational error, simplifying security operations.

Providing AI-native detection and response

Unlike fragmented point solutions, Trellix provides an integrated security architecture designed to strengthen uptime, operational control, and cyber resilience. The core of this defense is a layered detection and response framework that brings together endpoint security, network visibility, threat intelligence, and security operations.

- **Endpoint Security:** Trellix endpoint security solutions protect endpoints across complex environments. These capabilities include prevention, detection, investigation, containment, and recovery, while reducing the attack surface through controls such as application control, device control, allow/deny lists, host firewall policies, and forensics-driven response.

  AU Small Finance Bank, for example, has deployed Trellix Endpoint Security across the enterprise, spanning tens of thousands of endpoints. The solution incorporates next-generation antivirus protection and data encryption, providing proactive defense against intrusion. In addition, the bank has deployed Trellix Endpoint Detection and Response for AI-guided threat investigation, along with Trellix ePolicy Orchestrator for centralized endpoint security management.
- **Network Detection and Response:** Trellix Network Detection and Response (NDR) improves visibility across financial services environments. By monitoring network communication patterns, identifying suspicious behavior, detecting anomalies, and supporting asset visibility, Trellix enables security teams to identify lateral movement, unauthorized access attempts, and advanced threats targeting financial services organizations.
- **Security Operations:** Trellix connects endpoint, network, data, threat intelligence, and security operations telemetry through an integrated security platform. AI-assisted capabilities such as Trellix Wise allow analysts to prioritize critical alerts, reduce alert fatigue, and accelerate investigation and response, improving operational efficiency. Trellix also provides on-premises and disconnected deployment models where cloud connectivity is limited or restricted.

Together, these capabilities empower financial services organizations to move from isolated detection to coordinated defense, improving visibility, reducing response times, and strengthening resilience against ransomware, unauthorized change, lateral movement, and targeted attacks.

Protecting sensitive data

Financial services companies handle large volumes of sensitive information, including customer records, commercial contracts, trading information, and regulated data.

Trellix protects this information through Data Loss Prevention (DLP) and Database Security capabilities that secure data across endpoints, networks, cloud repositories, and databases. These solutions monitor sensitive data movement, detect unauthorized access, audit database activity, monitor privileged users, and minimize the risk of data leakage.

By protecting data both at rest and in motion, Trellix enables financial services organizations to safeguard intellectual property, maintain compliance, and reduce the risk of exposure.

Strengthening security with Trellix consulting and partnerships

Technology alone cannot fully secure highly complex, mission-critical financial services environments. Many organizations face gaps in specialized cybersecurity expertise, architecture design, deployment readiness, operational governance, and incident-response planning. These challenges become even more critical when security controls must be implemented without disrupting business operations.

Trellix bridges this gap through experienced Professional Services, advisory support, and a broad ecosystem of technology and industry partnerships. Trellix Professional Services collaborates with customers to assess their current security posture, design practical deployment architectures, validate segmentation and visibility requirements, support implementation, tune detections, and align security operations with business and operational risk.

Through consulting-led engagement and partner collaboration, Trellix enables financial services organizations to achieve measurable security outcomes, including improved visibility, stronger control of critical assets, faster threat detection, reduced operational risk, and more resilient business operations.

Trellix Professional Services

Trellix Professional Services allows financial services organizations to maximize the value of their Trellix investments through custom scopes of work, deployment expertise, and specialized methodologies. These services enable customers to assess risk, design resilient architectures, implement controls, and operationalize security without compromising uptime or business continuity. Key services include:

- **Incident-response Readiness:** Trellix experts develop incident-response playbooks, escalation models, and response templates aligned to business operations requirements and applicable regulatory obligations. This allows security and operations teams to respond faster while minimizing disruption to critical systems.
- **Data Security Rollouts:** Trellix Professional Services provides expertise for data classification initiatives, database risk assessments, and DLP policy design for sensitive financial services data, including customer data, commercial contracts, and operational records. These services reduce the risk of intellectual property exposure and unauthorized data movement.
- **Continuous-monitoring Deployments:** Trellix consultants assist with the deployment and configuration of endpoint, EDR, NDR, and security operations capabilities across complex environments. Services may include detection tuning, integration with SOC workflows, threat-hunting enablement, and operational handoff to internal SOC teams or managed service partners for ongoing monitoring.

Strategic OEM partnerships

Trellix collaborates with technology partners, OEMs, and managed service partners to extend security across complex financial services environments.

Trellix works with technology and infrastructure partners to align security controls with financial services requirements. Where supported by the customer's architecture and vendor ecosystem, Trellix capabilities strengthen endpoint protection, access control, data protection, encrypted communications, and monitoring across critical operational infrastructure. This improves resilience while supporting operational integrity and compliance requirements.

Together, these partnerships empower customers to move from an isolated technology deployment to a coordinated security model across financial services operations.

Conclusion

By combining a unified security architecture with deep consulting expertise and a strong partner ecosystem, Trellix enables financial services leaders to protect their operations, data, and reputation. Trellix provides the visibility, protection, threat detection, and response capabilities needed to strengthen operational resilience and protect customer trust.

With Trellix, financial services organizations can reduce cyber risk, improve security operations, protect sensitive customer data, and support safer, more resilient business operations.

To learn more, contact us or visit trellix.com.