# Shaping Banking's Next with Security and Privacy Tech

Security and privacy are cornerstone in banking today as these aspects have now transformed from afterthoughts to top priorities. As banks embrace innovations and new technologies – most of which revolve around data, traditional security approaches no longer suffice. These factors are driving banks to rethink their security strategies — moving from reactive measures to proactive, embedded privacy-first approaches. In 2025, these imperatives are expected to reflect in banks' technology investments and strategies as well.

Banks will increasingly embed security and privacy considerations at core of their strategies. Two key areas of focus will be cybersecurity mesh and privacy-preserving technologies. Cybersecurity mesh will help banks secure distributed environments by creating dynamic micro-perimeters around devices and users, improving threat detection and response. Meanwhile, privacy-preserving technologies like homomorphic encryption and federated learning will allow banks to innovate with data while preventing data security breaches. These technologies will enable secure collaborations, better fraud detection, and personalized services while keeping customer data secure.

## Industry Trendline

90% banking executives foresee threats and budgets more than doubling in cybersecurity space by 2030
Innovation in Retail Banking Report 2024

In last 12 months, homomorphic encryption moved from "innovation trigger" to "peak of inflated expectations" in Gartner Hype Cycle
Gartner

Federated machine learning offers business value in enhanced data privacy and compliance; better use of edge data through local data processing.
Forrester

## In 2025, Security- and Privacy-First Technologies will become vital

Headless Banking Architecture to ensure customer-centricity

Cybersecurity mesh to help improve overall security posture

Privacy-preserving technologies in focus: Homomorphic encryption and federated learning

# Cybersecurity mesh to help improve overall security posture

The traditional “castle and moat” approach to cybersecurity, with a single perimeter around the network, is no longer sufficient in today’s dynamic and distributed environments. The rise of remote work, cloud computing, and the Internet of Things (IoT) has blurred the lines of the network perimeter, making it increasingly difficult to defend. According to Innovation in Retail Banking survey by Infosys Finacle and Qorus, 90% banking executives foresee threats and budgets more than doubling in cybersecurity space by 2030.  Cybersecurity mesh is expected to emerge as the go-to option for banks to respond to this challenge.

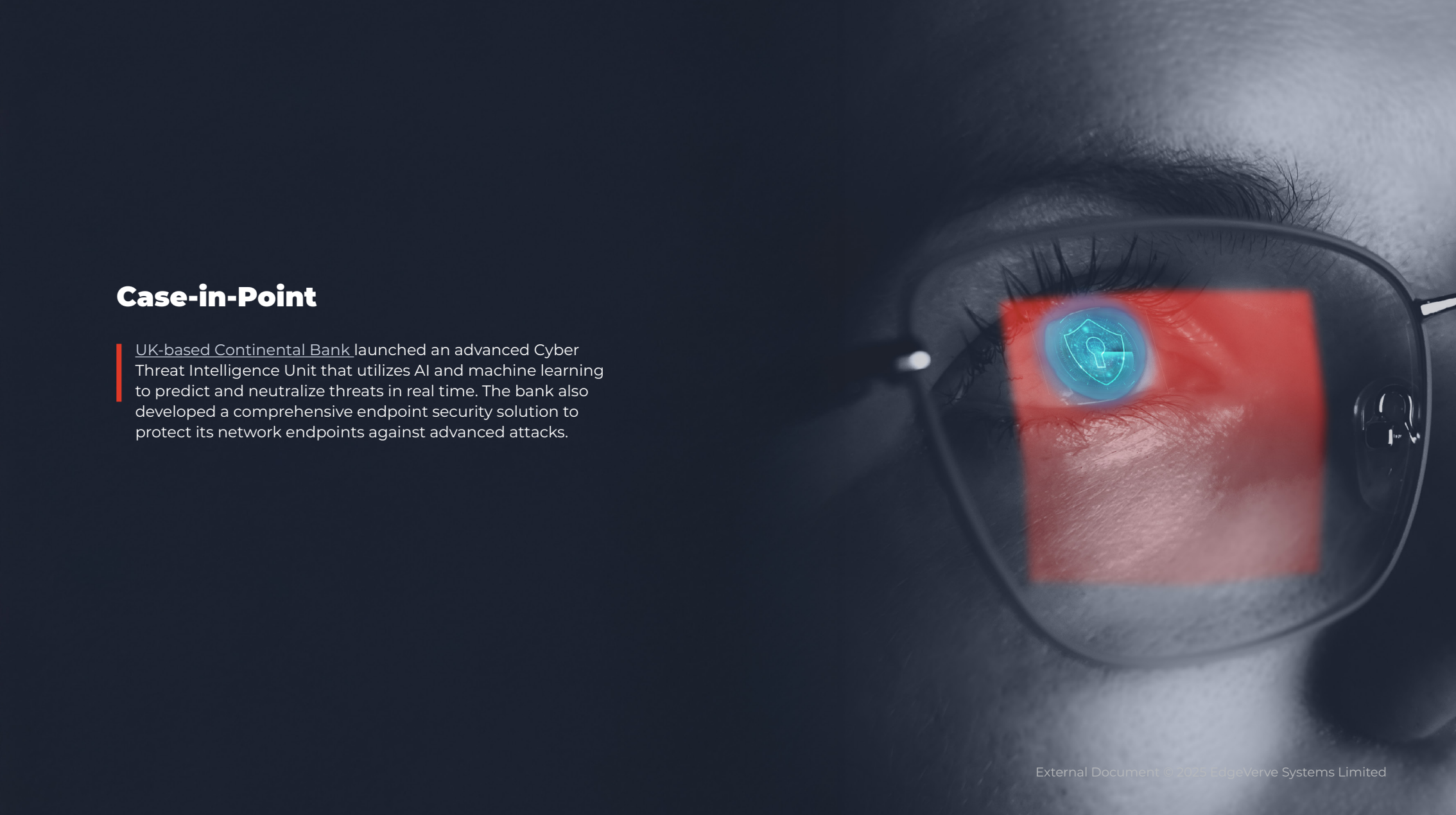
A cybersecurity mesh is a decentralized security architecture that focuses on securing individual devices and users rather than relying solely on a centralized network perimeter. It leverages a distributed identity fabric and dynamic security policies to create micro-perimeters around each entity. By securing individual devices and users, banks can better protect sensitive data and mitigate the risk of cyberattacks. The mesh provides granular visibility and control over devices, users, and data flows, enabling proactive threat detection and response. The decentralized nature of the mesh allows banks to adapt quickly to changing threats and business needs.

In 2025 and years thereafter, interest in this space is expected to grow significantly in upcoming years. Banks will focus on integrating mesh-based solutions with their existing security infrastructure after conducting pilot projects and evaluate the effectiveness. Automation will play a critical role in scaling and managing the complexity of the mesh. Collaboration between banks, technology vendors, and security experts will be essential for driving innovation and best practices.

Integrating mesh-based solutions with existing systems can be complex and time-consuming. There may be a shortage of skilled professionals with the expertise to design, implement, and manage mesh-based security solutions. To ensure success in this journey, banks must adopt a phased approach to implementation and gradually expanding the scope. Investing in training programs and partner with technology vendors will help augment the existing capabilities. Addressing these challenges while embracing the principles of the cybersecurity mesh will enable banks to significantly enhance their security posture.

## Case-in-Point

UK-based Continental Bank launched an advanced Cyber Threat Intelligence Unit that utilizes AI and machine learning to predict and neutralize threats in real time. The bank also developed a comprehensive endpoint security solution to protect its network endpoints against advanced attacks.



# Privacy-preserving technologies in focus: Homomorphic encryption and federated learning

The banking industry faces increasing pressure to protect sensitive customer data while simultaneously leveraging it for innovation and competitive advantage. Traditional data sharing and analysis methods often involve centralizing data, which raises significant privacy and security concerns. This is where privacy-preserving technologies like homomorphic encryption and federated learning are coming into play.

Homomorphic Encryption is a powerful cryptographic technique which allows computations to be performed directly on encrypted data without the need to decrypt it first. This means that sensitive information remains protected throughout the entire processing chain. In the last 12 months, the technology has moved from “innovation trigger” to “peak of inflated expectations” in Gartner Hype Cycle, signaling significantly growing interest.

Federated learning is another technology of interest in this domain. It is a decentralized machine learning approach enabling multiple organizations to collaboratively train a shared model without sharing their raw data. Each participant trains a local model on their own data and only shares model updates with a central server, preserving data privacy. According to Forrester, “Federated machine learning offers business value in enhanced data privacy and compliance; better use of edge data through local data processing; and access to richer and more diverse data sets.”

As data privacy becomes bigger priority than ever, banks will focus on these privacy-preserving technologies in 2025. Both these technologies offer robust protection for sensitive customer data, mitigating the risks of data breaches and unauthorized access. Federated learning enables banks to collaborate on advanced analytics and AI models without compromising data privacy, fostering innovation and improving services. Homomorphic encryption and federated learning can help banks comply with stringent data privacy regulations like GDPR and CCPA.

While still in early stages, some banks are experimenting with these technologies for specific use cases, such as fraud detection and risk assessment. Banks are expected to develop highly personalized financial products and services based on aggregated customer data without compromising privacy. Banks are expected to collaborate to identify and prevent sophisticated fraud schemes without sharing sensitive customer data. Federated learning will also help improve supply chain risk management and optimize lending decisions.

These technologies can be computationally expensive, which may limit its scalability for certain applications. Implementing and managing these technologies requires specialized expertise and can be technically challenging. The lack of standardized protocols and frameworks can hinder interoperability and widespread adoption. Continued investment in research and development is crucial to improve the performance and efficiency of these technologies. Collaboration between banks, technology providers, and regulators alongside training programs can help to develop best practices and address common challenges. Adoption of these privacy-preserving technologies will not only ensure privacy and compliance with regulatory requirements but also allow for responsible use of data.

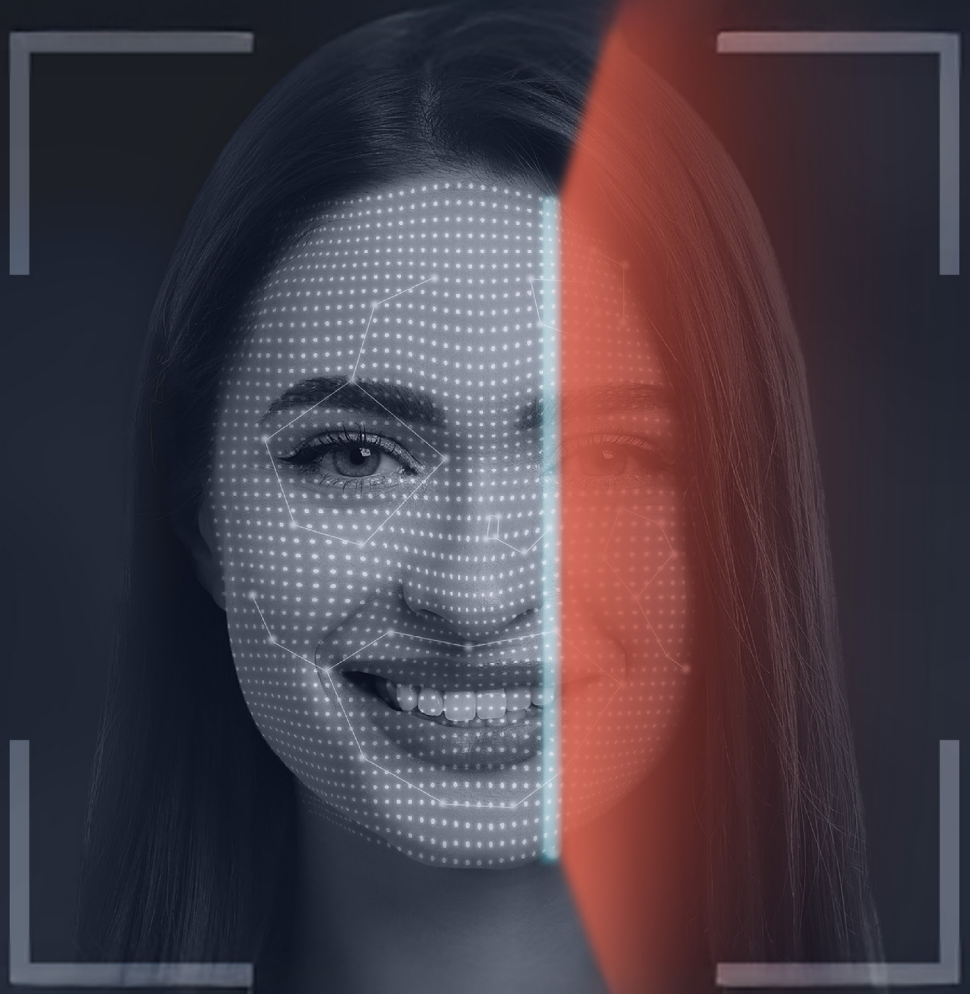
## Case Examples

HSBC is one of the banks exploring privacy-enhancing technologies like homomorphic encryption. The bank has launched projects to enable secure data sharing, tackle financial crime, and carry out in-depth investigation of real-world, regulator-approved applications.

China's WeBank has developed a federated learning model for credit rating. The co-developed model is strictly restricted to measuring the credit risk of small and micro-enterprises. This has halved the number of defaults among WeBank's loans to these customers.

# Mastering Security and Privacy Tech Will Be Crucial

As data security and privacy takes centerstage even further in 2025, cybersecurity mesh and privacy-preserving technologies will be crucial for banks to tackle emerging threats and safeguard sensitive information in distributed environments. By embedding these technologies at the core of their operations, banks can move from reactive to proactive security strategies, ensuring compliance and protecting customer trust. Mastering these innovations will be crucial for banks to secure future success in an evolving regulatory and threat landscape.



## Why we exist

To inspire better banking so that billions of people and businesses can save, pay, borrow, and invest better.

## How we do it

Our solutions and people help banks to engage, innovate, operate and transform better, so that they can improve their customers' financial lives, better.

## What we offer

A comprehensive suite of industry-leading digital banking solutions and SaaS services that help banks engage, innovate, operate and transform better.

Infosys® | Finacle

Finacle is an industry leader in digital banking solutions. We are a unit of EdgeVerve Systems, a wholly-owned product subsidiary of Infosys (NYSE: INFY). We partner with emerging and established financial institutions to help inspire better banking. Our cloud-native solution suite and SaaS services help banks engage, innovate, operate, and transform better to scale digital transformation with confidence. Finacle solutions address the core banking, lending, digital engagement, payments, cash management, wealth management, treasury, analytics, AI, and blockchain requirements of financial institutions. Today, banks in over 100 countries rely on Finacle to help more than a billion people and millions of businesses to save, pay, borrow, and invest better.

**For more information, contact finacle@edgeverve.com** **www.finacle.com**