AI-Powered Security for Retail Banks

Cybersecurity, everywhere you need it

AI-Powered Security
for Retail Banks

Key Stats

In order to improve their services and protect themselves from these cyberattacks, banks are increasingly investing in AI:

$623 billion
investment in banking technology in 2022

(Source: Gartner)

$1 trillion of additional value to be delivered by AI

(Source: McKinsey)

The global market for AI-based security products is expected to reach **$133 million** by 2030

(Source: Acumen Research & Consulting)

Generative AI
will be commonly used in fraud detection, trading prediction and risk factor modelling

(Source: Gartner)

Authorize Payments

Digital payments are on the rise. The European Central Bank has reported that €114.2 billion of non-cash transactions were made in the Euro zone, totaling $201 trillion (€197 trillion) in 2021.

Today, consumers across EMEA are using a variety of different payment options, ranging from mobile payment apps to smartwatches, digital wallets and QR codes. Crypto payments are also becoming increasingly popular. By 2030, 47% of bankers believe customers will likely be using augmented reality or virtual reality (AR/VR) as a channel for making transactions.

When authorizing payments, banks must ensure they have the true identity of the customer – not an impersonator – and know when to request a second verification for added security. Identity and Access Management solutions can help banks to manage identity authentication and authorize policies against security breaches. This technology uses algorithms and machine learning to detect anomalies in the behavior of users in a corporate network.

Contactless
Cash Withdrawal

According to the European Central Bank, “in 2021, card payments accounted for 49% of the total number of transactions, while credit transfers accounted for 22% and direct debits for 20%.” Despite this, banks are still trying to provide a convenient experience for those who use cash, by bringing cash withdrawals into the digital age with contactless ATM machines.

Using their mobile banking app, customers can generate a QR code on a contactless ATM screen, which they then scan on their mobile device for user verification. This technology allows customers to safely withdraw large amounts of money by sending them notifications on their mobile device to securely verify their identity. This security also negates the risk of scammers conducting ‘drive-by’ cash withdrawals by scanning their card or device as they go past the customer.

Evolution of Branch Capabilities

These days, customers use their mobile devices for most of their banking needs and only 3% go into the branch. When opening a new product, 27% of consumers prefer to meet with the branch manager in person, while 22% use a mobile app and 21% go on the website, according to Accenture. Banks are meeting customer demands with a collective customer experience across various touchpoints – ensuring the seamless experience is always safe and secure.

The proliferation of mobile and Internet-of-Things (IoT) devices, the growing number of banking and payment apps, and the adoption of multiple cloud all heighten banking vulnerabilities. As the threat landscape evolves, consolidation and integration into a single cybersecurity platform is key. One platform enables network traffic to securely travel over multiple connections between branches and headquarters, to protect edge devices.

Protect Customers from Scams

In April 2022, researchers uncovered a new banking trojan, Fakecalls – a new form of vishing – which has the ability to ‘talk’ to victims and pretend to be an employee of the bank. Fakecalls mimic the mobile apps of popular banks. The trojan seeks to gain access to the victim’s contacts, microphone, camera, location, and call handling. Attackers then attempt to steal payment data or confidential information from the victim. Fakecalls also has a spyware toolkit, which continues to steal customer data undetected.

This is the latest addition to a tsunami of banking scams. In 2022, FortiGuard Labs detected that 23.71 million malicious files were distributed to financial institutions. Most of these were sent by phishing campaigns using malicious websites or office documents. The number of incidents involving cryptominers is also rising in tandem with trojans and InfoStealers.

Banks should be looking to use AI-powered threat detection services which provide advanced detection and response capabilities. These services offer protection across the entire network to quickly spot suspicious activities and prevent in-flight attacks.

Money Laundering-as-a-Service

The United Nations estimates the amount of money laundered to be between 2 and 5% of global GDP, or $800 billion to $2 trillion in one year. Cybercriminal organizations employ money mules to shuffle money through anonymous wire transfer services or through crypto exchanges to avoid detection.

Since recruiting money mules takes a lot of time and effort, cybercriminals are using automation services to move money through layers of crypto exchanges. Money Laundering-as-a-Service makes the process faster, less traceable, and more difficult for victims to recover stolen funds.

To combat this, banks need to utilize threat intelligence platforms to see what's coming in from outside their network and spot potential threats. The platforms use machine learning, automation and threat expertise to assess risk posture and advise actions for quick remediation.

For more information on how Fortinet can help banks to better understand the threat landscape and by providing them with real-time threat intelligence, and a framework for delivering a secure, high-performing user-to-application connection, visit our website: https://www.fortinet.com/. Or take our Cyber Threat Assessment to discover your organization's vulnerabilities.

FORTINET

www.fortinet.com

2141953-0-0-EN