This UK Bank Partners with Forcepoint to Outsmart Relentless Fraudsters Without Affecting the Online Customer Experience

Working with Forcepoint, this High Street bank discovered an ingenious new way to stop methods of fraud while keeping its consumer web application stable and trouble-free.

Headquartered in the UK, this bank is known for its forward-thinking approach to financial services as well as its IT infrastructure. With fraudulent activity costing banks millions of dollars every year, the financial institution took another progressive path—adding an extra layer of security to its online banking presence with Forcepoint Cloud Access Security Broker (CASB).

CUSTOMER PROFILE:
This UK bank serves more than one million customers with online banking and retail locations.

INDUSTRY:
Banking

HQ COUNTRY:
United Kingdom

PRODUCT:
Forcepoint CASB

Methods of fraud seem to stay one step ahead of banking applications, and with good reason. Fraudsters can change tactics as they develop them, but banking apps require constant stability. That means new threat intelligence is difficult to apply quickly, leaving the bank open to fraud's latest modus operandi. "You can't just make a change because something happened today," explains David Barnett, Head of CASB EMEA. "Fraudulent behavior is always changing, and the e-banking application itself can't react quickly enough."

As it eventually turned out, that's really not as big of a problem as everyone thought.

An application of CASB that thwarts even the most inventive fraudsters

The traditional use of CASB is to manage and control the use of cloud applications like Office 365 and Box by a company's workforce. One of the most powerful ways Forcepoint CASB sets itself apart is its behavioral analytics features, which detect behavioral anomalies and block or alert the team to suspicious activity. The bank could clearly see the value in this feature, but at a regular check-in with Forcepoint representatives, an idea was born.

What if Forcepoint CASB could be used to add an extra layer of security for customers versus just providing internal IT security?

3 wks

to deploy custom Forcepoint CASB configuration

4 mos

to realize ROI by stopping fraudulent users from stealing customer funds

> "Reducing fraud by even a small percentage can result in millions of dollars in savings."
>
> **DAVID BARNETT,** HEAD OF CASB EMEA

Forcepoint CASB provided an external layer of security that required no changes to their banking application, reducing the opportunity for potential downtime. This lets the bank keep pace with threats as they happen, while the banking application itself remains stable, ensuring a good customer user experience.

The CASB layer can identify anomalies like evidence of brute force attacks, repeated failed login attempts, login attempts from suspicious locations, and simultaneous access from distant locations. Best of all, deployment took just three weeks, for functionality that one competitor estimated could take up to a year to develop.

"Beyond the benefits that our behavioral analytics brings, our CASB technical reverse proxy was developed in such a way that we can support really any cloud application, including a customer's own custom app," said Barnett. "We don't look at our CASB as simply a technology—it's rooted in a new way of thinking."

Challenges

Safeguard customers and the bank against constantly changing, costly attacks on their online banking application.

Approach

Deploy a custom install of Forcepoint CASB to deliver a flexible security layer attuned to user behavior and anomalies.

Realizing full ROI in only four months

The bank reported a 100% return on their investment in just four months, simply by stopping fraudulent users from logging into customer accounts and stealing funds the bank would have been required to repay.

"Reducing fraud by even a small percentage can result in millions of dollars in savings. Wouldn't it be useful to know if somebody is trying to access their bank account from two highly unlikely, impossible-to-travel locations, or if they're trying to access an account in a way that is known to be a fraudulent method of attack?" asked Barnett.

The bank's security team can rely on Forcepoint CASB to keep pace with the latest security threats, leaving the banking application stable. This gives them the confidence to roll out new features to the application, take products to market faster, and accelerate their own digital transformation. But in the bank's world, it's really about the added value to the customer: a trusted environment where they can depend on seamless, invisible protection.

> "We don't look at our CASB as simply a technology—it's rooted in a new way of thinking."
>
> **DAVID BARNETT,** HEAD OF CASB EMEA

Results

- **Custom CASB configuration** deployed in just three weeks vs. up to a year for competitors.
- **Stopping fraudulent users** from stealing customer funds delivered ROI in four months.