

# TOP TEN GLOBAL BANK TAPS INTO BEHAVIORAL BIOMETRICS FOR IMPROVED FRAUD PROTECTION

## Appgate's behavioral biometrics service seamlessly strengthens online banking authentication, improves customer satisfaction

### Background

With more online interactions comes increased global fraud as threat actors continually innovate new ways to target customers. This global banking institution, that serves millions, is committed to continually increasing security to prevent fraud as well as deliver an improved experience for its customers.

### Challenges and Requirements

The bank's online customers were under constant attack from banking trojans and fraud attempts using social engineering techniques to bypass existing device and token-based security, resulting in financial losses. Key challenges included:

- Complex corporate customer business needs made accurate authentication difficult using legacy systems alone and forced the bank to maintain a high authentication threshold
- Increased ability by fraudsters to bypass other controls such as username, password and step-up authentication methods
- Legacy fraud detection solutions that undermined the customer experience due to a high level of false rejections, expensive manual verification calls and cumbersome authentication steps

These challenges highlighted the urgent need to verify online sessions beyond a one-time password and identify the actual customers rather than their devices. The institution sought a frictionless behavioral biometrics solution to improve its banking platform, increase user confidence and alleviate authentication complexities without interfering with or reducing adherence to strict security and privacy rules.

### Solution

After evaluating several vendors, the bank chose Appgate's behavioral biometrics service because it was "30% more effective" than the others they tested in the areas of accuracy, features and ease of integration. Key benefits to the bank and its customers include:

- **Unique customer profile:** By capturing unique user characteristics and how they interact with devices, the bank gains a profile that is as unique as a fingerprint
- **Customer loss prevention:** By layering Appgate behavioral biometrics in its existing infrastructure, the bank was able to detect and stop almost all potential fraud loss events
- **Invisible authentication:** After initial set up, the service runs without additional action by customers
- **Fewer attacks attempted:** Fewer overall attacks attempted against customers as most of the attacks were blocked and the chances of a successful attack fell dramatically.
- **Increased customer confidence:** The solution is so successful in preventing attacks that customers have far greater confidence in the bank's ability to protect them and their funds and are more confident in using online banking

### INDUSTRY

Financial services

### THREAT TYPES

Social engineering, credential theft, account take over, session hijacking

### CHALLENGES

Increased fraudster sophistication

Many customers lack sufficient awareness to protect themselves from socially engineered fraud schemes

Taxing authentication steps adds friction to customer experience

High level of false rejections and need for expensive manual verification calls

### BENEFITS

- Integrates with existing solutions
- Enhance effectiveness of current fraud protection solution resulting in overall detection rate of over 90%
- Reduces the use of additional authentication factors
- Adapts to organization risk tolerance
- Improves user experience with less friction

***"Appgate behavioral biometrics ensures that our customers are protected from the security risks posed to them and their business. Since launching the service, the results have been impressive, including more attacks caught and prevented, fewer attacks attempted, increased customer satisfaction and reduced costs."***

### - Head of security and info risk

### About Appgate

Appgate is the secure access company. We empower how people work and connect by providing solutions purpose-built on Zero Trust security principles. This people-defined security approach enables fast, simple and secure connections from any device and location to workloads across any IT infrastructure in cloud, on-premises and hybrid environments. Learn more at [appgate.com](https://appgate.com)