BANKING INDUSTRY PAPER

Asurvio Shield: Advanced Threat Defense for the Online Banking Industry

Protecting customers from fraud, phishing, account takeover, impersonation, and emerging digital threats before losses occur.

Overview

Financial institutions face an expanding range of cyber threats, including phishing attacks, account takeover attempts, malicious websites, credential theft, social engineering campaigns, and digital fraud. Traditional security solutions often struggle to keep pace with rapidly evolving attack techniques and increasingly sophisticated threat actors.

Asurvio Shield's Advanced Threat Defense delivers real-time protection by continuously evaluating digital interactions, identifying suspicious activity, and preventing threats before customer accounts, credentials, or sensitive financial information can be compromised.

Designed for modern banking environments, Asurvio Shield seamlessly integrates across online banking platforms, payment systems, customer communications, and mobile banking experiences to reduce fraud, strengthen customer trust, and improve operational resilience.

The Banking Industry Challenge

Cybercriminals are becoming increasingly sophisticated, targeting financial institutions and their customers through phishing, account takeover, impersonation, social engineering, and fraud campaigns. Modern attacks are designed to evade traditional defenses, exploit customer trust, and rapidly adapt to avoid detection.

At the same time, financial institutions must balance strong security measures with seamless digital experiences. Protecting customers requires a proactive approach capable of identifying threats before they become financial losses.

The Evolving Threat Landscape

Common Threats

- Phishing and credential harvesting
- Account takeover (ATO) attacks
- Business email compromise (BEC)
- Fraudulent payment requests
- Malicious websites and spoofed portals

- Social engineering scams
- SMS phishing (smishing)
- Brand impersonation attacks
- Malicious links and fraudulent communications

Business Impact

- Financial losses from fraud and unauthorized transactions
- Increased account takeover incidents
- Customer trust and reputational damage
- Higher operational and support costs
- Greater regulatory and compliance pressure
- Resource-intensive fraud investigations and recovery efforts

The Solution: Advanced Threat Defense

Asurvio Shield delivers comprehensive threat protection through continuous evaluation of customer interactions, digital channels, websites, email links, login pages, payment workflows, and online communications.

By identifying suspicious activity before sensitive data is exposed or accounts are compromised, Asurvio Shield helps financial institutions reduce risk, prevent fraud, and strengthen customer confidence.

How It Works

1. Continuous Monitoring

Asurvio Shield monitors customer interactions across online banking, mobile banking, payment portals, websites, and digital communications.

2. Threat Evaluation

Multiple risk indicators are analyzed, including suspicious domains, impersonation attempts, unusual behavioral patterns, malicious content, and known threat intelligence.

3. Risk Assessment

Threat signals are evaluated in real time to determine the likelihood of fraud, account compromise, or malicious activity.

4. Protective Response

When a threat is identified, Asurvio Shield can trigger warnings, block access, escalate alerts, or activate institution-defined response actions before harm occurs.

Banking Industry Applications

Account Protection

Detect fraudulent login pages, credential theft attempts, and account takeover campaigns before customer accounts are compromised.

Benefits

- Prevent unauthorized account access
- Reduce account takeover incidents
- Protect customer credentials
- Strengthen authentication security

Fraud Prevention

Identify fraudulent payment requests, deceptive payment portals, invoice scams, and social engineering tactics designed to facilitate financial fraud.

Benefits

- Reduce fraud-related losses
- Improve transaction security
- Prevent payment scams
- Minimize recovery costs

Digital Banking Security

Protect customers across online banking platforms, mobile banking applications, digital payment channels, and customer communications.

Benefits

- Consistent protection across all digital channels
- Improved customer confidence
- Enhanced digital experience
- Reduced exposure to online threats

Brand Protection

Identify and disrupt attempts to impersonate financial institutions, trusted partners, and banking brands.

Benefits

- Protect organizational reputation
- Reduce successful impersonation attacks
- Preserve customer trust
- Strengthen brand integrity

Customer Threat Protection

Help customers avoid malicious websites, fraudulent communications, and scams designed to steal personal or financial information.

Benefits

- Improve customer safety
- Reduce support calls related to fraud
- Enhance customer experience
- Build long-term digital trust

Advanced Detection Capabilities

Asurvio Shield evaluates multiple threat indicators simultaneously to identify known and emerging risks.

Behavioral Analysis

Identifies suspicious activity patterns commonly associated with fraud, account compromise, and malicious behavior.

Domain & Infrastructure Analysis

Detects typosquatting, spoofed websites, suspicious domains, and malicious infrastructure.

Brand Impersonation Detection

Recognizes unauthorized use of banking brands, logos, messaging, and visual identity.

Content Analysis

Evaluates websites, emails, messages, and digital content for indicators of deception, fraud, or malicious intent.

Threat Intelligence Correlation

Compares observed activity against known threat indicators, fraud trends, and emerging risks.

Adaptive Threat Identification

Recognizes evolving attack techniques and new threat patterns targeting financial institutions and their customers.

Value for Financial Institutions

Reduce Fraud Losses

Prevent threats before they lead to account compromise, unauthorized transactions, or customer financial losses.

Strengthen Customer Trust

Demonstrate a proactive commitment to protecting customers and safeguarding sensitive information.

Lower Operational Costs

Reduce fraud investigations, account recovery efforts, support center workloads, and incident response expenses.

Enhance Regulatory Readiness

Support cybersecurity, fraud prevention, consumer protection, and risk management initiatives through proactive threat monitoring.

Improve Security Effectiveness

Enable faster threat identification and response while reducing dependence on reactive security controls.

Future-Proof Digital Banking Security

Protect against evolving threats with capabilities designed for today's rapidly changing cyber risk environment.

Why Asurvio Shield?

Asurvio Shield provides financial institutions with a proactive approach to defending customers, accounts, and digital banking services from an expanding range of cyber threats.

Through continuous monitoring, intelligent threat evaluation, and real-time protection, institutions gain greater visibility into risks while reducing fraud exposure and improving customer confidence.

Financial institutions can focus on delivering exceptional digital experiences while maintaining strong security and operational resilience.

Conclusion

Asurvio Shield's Advanced Threat Defense helps financial institutions stay ahead of an increasingly complex threat landscape by identifying and stopping malicious activity before harm occurs.

Through continuous threat evaluation, real-time protection, and proactive risk analysis, organizations can reduce fraud, protect customer accounts, and strengthen digital trust.

As cybercriminals continue to evolve their tactics, financial institutions need a defense strategy capable of protecting customers wherever they engage. Asurvio Shield delivers the visibility, protection, and confidence required to secure today's digital banking environment.

Protect Customers. Reduce Fraud. Defend Trust.

Contact us to learn how Asurvio Shield can help safeguard your customers, strengthen digital trust, and reduce fraud risk.