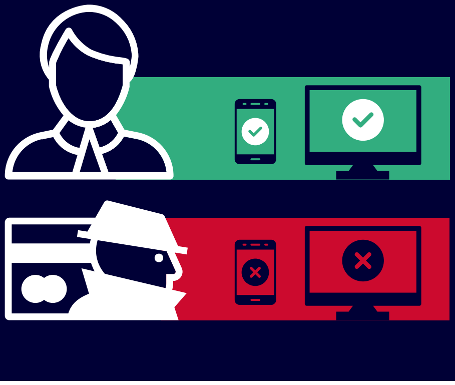
Arcot
by Broadcom Software

Arcot + ThreatMetrix

Combine the ThreatMetrix risk intelligence with Arcot risk assessment and flows.



ThreatMetrix Integration Overview

ThreatMetrix risk intelligence provides profiling of devices used by consumers during their online banking interactions. Their device intelligence can be layered upon the existing Arcot device intelligence to provide an advanced data point when trying to identify the reputation of a new device that may be used during a social engineering attack, and additional insight for other fraud types.

The Challenge

An issuer using different vendors across digital channels needs to be able to correlate device reputation and association across these channels to combat multi-channel fraud vectors, and to enhance the cardholder's journey by understanding a cardholder's genuine device profiles.

The Solution

The Arcot solution provides seamless integration with ThreatMetrix to allow device identification to occur during the 3-D Secure flow. During transaction processing, Arcot calls ThreatMetrix's application code to collect device data and sends it for processing.

This device data can then be used to allow ThreatMetrix to perform its risk intelligence profiling.

There are two options depending on the integration point:

A. The outcome can be passed back to Arcot during the challenge flow, and the flow can be routed accordingly — where heightened risk is identified, the transaction challenge flow can be 'failed' with an appropriate message.

B. The outcome can be passed back to Arcot during risk assessment (before a challenge occurs), and the flow can be routed accordingly — where heightened risk is identified, the transaction can be 'failed' with an appropriate message.

Key Benefits

- **Leverages cross channel device reputation**

In most implementations, the information gathered in each digital channel remains siloed, with no way to correlate the third-party device markers across channels. By deploying multiple device identification processes in the 3-D Secure flow these markers can be correlated and paired. Where the same device is being used, the 3-D Secure generated device identifier can be matched against the identifier created in an online banking session, and appropriate risk assigned.

- **Improves fraud detection**

Where a transaction is deemed medium to high risk in the 3-D Secure channel, an issuer may have made the decision to step up the transaction for authentication. The difficulty with multi-channel attack vectors (such as social engineering) is that a fraudster may already be in control of the authentication method. In which case, any step-up flow is immediately flawed. With this integration, the information shared about cross-channel device reputation can immediately increase the risk of the transaction from medium/high to high.

- **In-session decisioning**

If an authentication method has been compromised, a fraudster will be successful in completing the transaction authentication and may then benefit from a lighter authorization strategy - as the transaction will be seen as fully authenticated. With this integration, the issuer has the ability to fail a transaction for authentication

KEY BENEFITS, CONT.

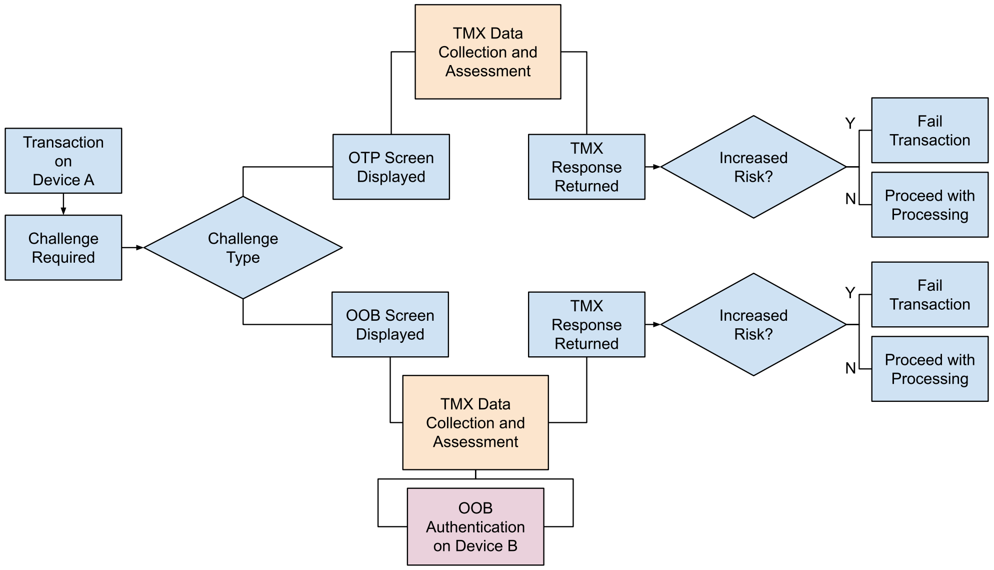
even when the authentication challenge may have been completed successfully - in-session, based on the shared cross channel device reputation.

Optimizes customer experience

If a device has not previously been used for 3-D Secure activity, it will have no reputation within the Arcot system. In which case, such a device can tend to be treated as a medium risk until its reputation is established. This integration allows devices that have previously been seen in an online banking session, and have a good reputation in that channel, to be treated more favorably in the 3-D Secure flow.

How Does It Work?

During the challenge flow, a call is made to ThreatMetrix to allow the collection of device data, whilst the challenge screens are being displayed. ThreatMetrix can use this device data, in combination with data already held and possibly data collected from the device used for authentication (where this is a banking app for example) to perform a risk assessment. The outcome of this assessment is passed back to the ACS to allow the transaction to proceed according to the risk identified. For example, transactions with elevated risk can be blocked; transactions with no elevated risk can be allowed to proceed and be authenticated as normal.



Learn More

Contact your Customer Success Manager to learn more about the Arcot and ThreatMetrix integration. If you do not have an assigned CSM, please email sales.arcot@broadcom.com.