SECUREAD

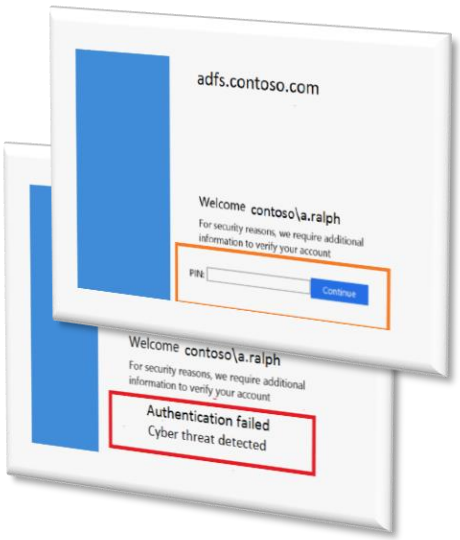
THEMIS
Enabling Trust

At-a-Glance

SecureAD is cloud based API service that allows organisations to add the next generation of access control to their existing ADFS estates, in doing so adding an additional layer of protection. No longer do you have to depend on the password to protect those important assets. You can now utilise a risk based service that makes intelligent authentication decisions based on real time context and business policies.

Advantages

- Improved security whilst keeping user experience impact low
- Policy driven ability to apply security where and when it's most needed
- Pre-configured security polices from industry experts
- Increases the lifespan & ROI on your existing ADFS investment
- Fast and simple to deploy, giving you faster time to your benefits
- Combat known bad sources using real time cyber threat intelligence



Secure Identity Management

Identity is playing an integral role in securing access to an organisations most important assets. With that being said can organisations rely on the password to protect those identities?

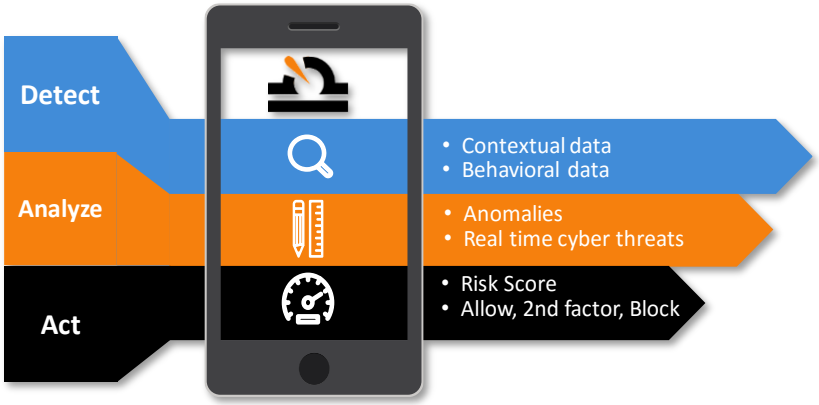
At Themis we believe the answer is no, especially with technology innovations that are driving different access sources and borderless destinations (Cloud, BYOD & IoT). Traditional methods of securing access have become obsolete.

Shield your ADFS

Hackers are becoming more sophisticated in their methods and therefore prevention techniques also need to be adaptive to deal with those threats. Themis SecureAD is an additional layer of security that can be applied to your existing ADFS identity estate. We recognise that many organisations have invested heavily in building ADFS and adding an additional layer of effective security would extend the lifespan of that investment.

RISK BASED AUTHENTICATION

The market is highly populated with new innovative methods of combating modem day threats but they lack the context to reliably distinguish an event from a non-event and prioritise protection based on business policies. Themis SercureAD utilises a policy driven risk based authentication engine.



Users can be resistant to adopting new security measures if it involves friction to the experience. The MyLogin risk engine self learns so as the frequency of use increases the service builds a history for that identity, fewer anomalies are found improving the user experience in terms of 2nd factor requests.

How it works

Start benefiting quickly as it's easy to deploy. There is minimal configuration on ADFS and we take care of rest by giving you an installer to deploy. It's a cloud based service so your ADFS instance will require HTTPS access to connect with SecureAD API service.

We require you to build your application policies allowing the service to understand the sensitivity of data within each application. We also provide pre-built policy templates which you can complete per application. These policies include parameters that can be set based on your requirements, for example:

- Identity reputation
- Cyber threat intelligence
- IP address
- Time of day
- Browser fingerprints
- Device fingerprint
- Geo-location

Cyber threat intelligence is a default security setting we apply to the service and it's a real game changer. It uses real time cyber data collected from our partners so if we see an attack from a known bad source the request can be blocked.

With very little fuss and effort SecureAD can really start helping you reduce your risk. You are able to apply the level of security you want based on the application, therefore allowing you to manage your risk more effectively. If a particular application holds sensitive data, select a high security template making SecureAD more responsive to any anomonlies. If an application holds less sensitive data, select a low security template. The power to manage the risk is in your hands as opposed to something like a password that can be easily compromised.