

## IDENTITY MANAGEMENT THAT WORKS

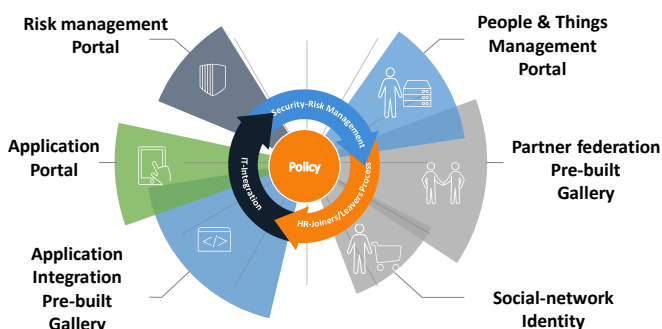
Traditional methods of users accessing applications have become obsolete. An individual has too many different identities to manage. Cloud computing, BYOD and IoT are changing the security landscape and the communities of users requiring access to the applications is growing. Themis MyLogin is a cloud based identity management service that offers employees, partners and customers secure access to any application on any device. It provides single-sign-on, directory integration including social, risk based authentication, multi-factor authentication, reporting and much more.

### MYLOGIN - SINGLE SIGN-ON (SSO)

Password fatigue is affecting us all, whether you are a user trying to remember passwords or if you deal with password reset requests. The number of apps being utilised is growing and having multiple credentials just isn't sustainable. MyLogin utilises industry standard federation to provide SSO, meaning users only need to remember one set of credentials to access your enterprise applications.

Mylogin provides an app gallery with a list of pre-built app connectors, this means with a few clicks you can enable SSO to your existing apps. If the app you want doesn't exist in the gallery you can use our wizard to build the connector or contact us and we will build the connector for you.

Cyber security is a major challenge for organisations, MyLogin utilises a risk based security engine that scores each login attempt and then makes intelligent authentication decisions based on business policy. This innovative method truly means you no longer have to rely on the password for security.



### Enables Flexibility - App On-boarding

Faster integration of new applications using the federation tools which enable faster time to value. No need for complex integration projects, use the app gallery for pre-built connectors or use the wizard to build your own.

### Cost Reduction – Efficiencies

Reduce the helpdesk password reset volumes through enabling single sign-on and social sign-on. Using the pre-built connectors saves on expensive integration projects.

### Increased Productivity – User Portal

Your users will no longer have to suffer from password fatigue, making them productive. The user portal will display the apps they are authorised to use, giving them a single access point across all their devices.

### Improved Security – Risk Based Authentication

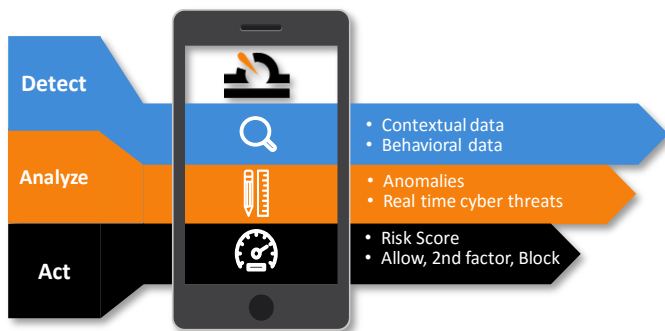
The cyber security challenge is growing, improve your security and reduce risk with MyLogin's Risk Based Authentication, it is adaptive to tackling modern day threats.

### Compliance - Reporting

Enforce authentication policy compliance through a single tool making it easy to report on who has access to what and their usage.

## RISK BASED AUTHENTICATION

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



When login behaviour is normal, a simple password is acceptable. When a login is attempted under usual or suspicious circumstances, like via an unknown device or unusual location, the user is prompted for a 2nd factor to respond to a challenge. When login behaviour is very suspicious the user access is blocked. Security is maintained without the hassle of a passcode unless it's necessary.

The risk engine self learns so as the frequency of use increases the service builds a better understanding of that identity, fewer anomalies are found and user experiences improves with less 2nd factor requests. These policies include parameters can be set based on your requirements, including:

- Identity reputation
- Cyber-threat Intelligence
- IP address
- Time of day
- Browser and device fingerprint
- Geo-location

## CYBER THREAT INTELLIGENCE

Cyber threat intelligence is 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 authentication request can be blocked. It's a method of proactive security with alerting functions that allow you to take further actions if required.

## PEOPLE & THINGS – DIRECTORY

Using identity bridges integrate your existing directory, we have many pre-built connectors for Active Directory, LDAP, Azure, Google Apps or many more including social. Once integrated you can simply manage your identities, provisioning users and what they can access.

## SOCIAL AUTHENTICATION

Social authentication on ecommerce websites has been very successful, increasing registration rates, reducing password reset requests and user friction. Should businesses be adopting social login for their enterprise applications? At Themis we believe you should. With risk based authentication protecting user access, you are simply using the credentials as a verification step. What is better than their social identities that they use daily and remember.

