

## **Reduce Security Risk with Compact Identity**

Identity Management is associated with improved convenience, better authentication, and improved security. It is popularly thought of as Single Sign-on and, perhaps, Password Management. Identity Governance and Administration (IGA) is also a critical component that is lesser known. Even this is usually associated just with compliance reports and administrative functions. But, today, Identity Management is also expected to be an avenue for reducing risk. Compact Identity enables such possibilities.

The solution enables this process by allowing you to categorize risks for your assets. You can calibrate risk values for apps, roles, entitlements and accounts. You can assign values of low risk, high risk, and so on. This sets the ground for the solution to help you manage your risks.

When managers are approving access requests, they know whether they are dealing with a high or low risk access. This is the most basic way in which Compact Identity helps you manage risk. If the access is high risk, you can choose a multi-level approval feature to increase security. Not one but multiple approvals from different tiers of managers are required for an access to be granted. This ensures that risky accesses are gated behind a tiered approval process.

Then there is the Identity Administration function of Access Recertification. Periodically, and for compliance reasons, accesses should be reviewed for appropriateness. This is especially true for risky accesses. It is possible within Compact Identity to exert the principle of exception (rather than the principle of rule) by choosing only to require recertification for high-risk accesses. This saves managers time by excluding less risky accesses from the recertification process.

Compact Identity sports context based authentication. You can set up what context you want to implement. For instance, perhaps a large number of employees in your organization use mobile phones to access apps. Perhaps they hail from different geographies, travel a lot, or login at unusual hours. The solution allows you to choose more complex authentication protocols for such login attempts. This improves security on a contextual basis.

A relatively new feature in Access Management is 'forced single sign-on'. Traditionally, employees can either use the SSO dashboard to sign in to all apps, or even sign in to an app manually. Businesses are beginning to recognize the risk of such procedures, and want employees to be forced to use the SSO solution only, for improved security. Compact Identity offers this feature.

Risk Management exists outside of Identity Management as well. Solutions like CASB (Cloud Access Security Broker) and SIEM (Security Information and Event Management) offer powerful ways of reducing security related risk in your organization. Compact Identity flawlessly integrates with such solutions. UEBA (User Entity and Behaviour Analytics) is also

something that helps you reduce risks, in a different way. It helps detect insider threats, targeted attacks, and financial fraud. Compact Identity integrates perfectly with these solutions too.

More features which help manage security related risks are in the roadmap of Compact Identity.

Our powerful risk-engine will be available soon. This feature computes Residual Risks (risks that are based on recorded data) as well as Runtime Risks (risks that are based on ongoing activity.) These risks are translated into specific actionable events – that then direct user behavior and actions, as well as trigger system actions to mitigate these risks or intimate them to relevant parties through escalation.

Passwordless Authentication is also in the roadmap. Passwords pose a number of problems such as password fatigue, and can be hacked rather easily. Passwordless authentication enables multi-factor authentication with biometrics, soft tokens, hardware tokens, and through other means, to authenticate users without passwords entirely.

In today's security environment, managing risk is critical to success. It's no longer about absolutes or single-form preventative measures, proactive involvement is necessary. It's not enough to have a system for access requests, access approvals, and access recertifications, the process must be guided by risk metrics. Compact Identity offers all this and more...