Risk Engine-based Identity and Access Management

Risk is not something to be avoided. In your business, taking risks is what reaps the greatest rewards. But, risks must be carefully calculated and understood for greatest benefit. Risk metrics from AI driven risk engines, like the latest technology incorporated in Ilantus Compact Identity, allow you to monitor the different IAM related risks in your business IT environment.

Most IAM technologies provide tools for businesses to provision access for employees. But, whether an access request should be approved or denied is left entirely to approval authorities to decide. But, such decisions should be made with information, not based on policies. Ilantus' risk engine utilizes AI to record information such as past rate of approval for the access request for that employee's job role and presents the approval authority with risk metrics to assist in the decision making process.

Identity breaches are growing in scope and frequency, and affecting large and small customers alike. Insider threats are the number one threat because

a) Such threats are difficult to monitor and control
b) These threats pose a larger risk than outsider breaches because the breach can go undetected for months (or, in some cases, years)

But, relying on managers to authorize access requests based solely on their judgement is an accident waiting to happen. Integrated risk metrics enable managers to make educated decisions, and add an additional layer of security (managers can be shown responsible for breaches where they obviously ignored a clear warning from the system).

In 2020, when you shop for an IAM solution, seriously consider Ilantus Technologies. Our risk-engine driven technologies are the wave of the near future, and an essential for all sizes and types of businesses.