Indeed Access Manager Benefits

Potential benefits:

- Cost reductions
- Increased labor productivity – you can reduce workforce (man-hours) costs required for handling standard and non-standard work tasks
- Reinforced information security – Indeed AM will improve your company's capacity to withstand cyberattacks on information resources

Table A. Cost reductions

Feature to consider	Problem	Solution
Accessibility of strong authentication technology	Manufacturers of strong authentication software and devices offer secure access solutions that often do not support products made by other manufacturers. This means you may have to buy additional products.	A single solution supports strong authentication software and devices offered by a wide range of vendors.
Support for different categories of corporate resources	Strong authentication solutions are only available for specific scenarios, for example, remote access only or local access only. This means you may have to buy additional products.	You can use a one-size-fits-all solution that supports diverse categories of corporate resources.

Table B.1 Increased labor productivity

Feature to consider	Problem	Solution
Centralized access management for corporate resources	You need to set up various technical security mechanisms to control access to your corporate resources.	You can use a single security and access control tool that includes a shared access event log.
Administration and utilization of user passwords	You may often need to reset user passwords, for example, to enable remote access or access to corporate applications.	Thanks to one-time password generators, hardware tokens, and biometric technology, you no longer need to reset passwords.
Access to corporate applications and services	Users have to memorize individual passwords to each corporate application and web application.	You can use a single set of authenticators to access all controlled corporate resources.
Response time for access incidents	You need to study the audit logs of various technical tools to find out what caused the incident.	You can use a single tool available in one window to monitor access events across all controlled corporate resources.
Initializing and assigning authenticators	Authenticators cannot be centrally assigned to users: each authenticator is initialized and assigned separately.	You can use a single solution to initialize all required authenticators and assign them to users.
Keeping track of assigned authenticators	There is no single tool to monitor all authenticators issued to users.	The user's card contains information about all issued authenticators.

Table B.2 Increased labor productivity (by user category)

Feature to consider	Increased labor productivity		
	System administrator	Information security administrators	Other users

Centralized access management for corporate resources	+	+	
Administration and utilization of user passwords	+	+	+
Access to corporate applications and services			+
Response time for access incidents		+	

Table C. Reinforced information security

Feature to consider	Problem	Solution
Authentication for corporate resources and applications	As a rule, authentication in various systems and applications is based on passwords that can be disclosed. And you will only find out that a password was compromised after an incident involving unauthorized access.	Strong authentication eliminates the threat that your credentials can be compromised and used for gaining unauthorized access to confidential documents and corporate services. If a device has been lost, this will be quickly detected and brought to the attention of responsible employees.
Password compliance	Even when the same password is used for gaining access to all corporate resources and applications (which is a rare case), more often than not, password security requirements are disregarded. Compliant passwords are hard to remember, and users normally write them down, which makes it much easier to have them compromised.	Password management is automated, and users don't know their passwords. To mitigate vulnerability to brute-force attacks, passwords are generated automatically in line with the security requirements.
Integration with Access Monitoring and Control System (AMCS)	To avoid additional criteria linked to an employee’s geographical location in the logical access management, logical and physical access control systems normally operate separately.	Users need to physically visit the company’s premises to work with critical workstations and terminals.
You can set up various strong authentication scenarios in line with the access format and resource criticality.	Regardless of the access format (remote or local) and resource criticality, users are forced to use authentication methods suggested by the developer (usually passwords) even if such methods can only offer weak protection against cyberattacks.	Each user receives a single set of authenticators. You can set up individual authenticators for all access formats, as well as for resources and applications with varying degrees of criticality.
Blocked domain accounts after external access attempts	If your company uses public resources, attackers may apply brute-force techniques to block domain accounts, which will stymie the work of your staff.	If any attempt to guess one-time passwords to public resources is detected, only password authentication will be blocked instead of the actual domain account. This means that you can use other strong authentication methods to gain local access to this resource and continue working with it.
Account password updates	Passwords to user accounts are changed manually. With multiple accounts, it may be difficult to update passwords in a timely manner and comply with the security requirements.	You can enable automatic password rotation for privileged accounts at predetermined intervals and with due regard to the security requirements.
Sharing user accounts	A user may need to provide a colleague with access to their account, for example, to ask them to send an email or view a document. Such situations are extremely difficult to track.	You can enable deputy mode: the administrator will assign a deputy for the employee who is currently away from work. The deputy can use their own authenticator to log in on behalf of their colleague and do

		what needs to be done. This activity will be recorded in the general log.