Indeed Privileged Access Manager Benefits

Potential benefits:

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

Table A. Cost reductions

Feature to consider	Problem	Solution
Cost of work performed by the contractors	You have no way to determine the actual volume of work performed by the IT contractors. Payments are made for volume claimed by the contractor, while the actual amount of work may be different.	You can use special mechanisms to capture the duration of work (sessions), which will allow you to determine and cover only the actual labor costs.
Quality of services provided by privileged users and contractors	Even if the declared and actual amount of work are the same, the quality of services may be lower compared to SLA metrics on account of intentional or unintentional actions. But whatever the quality, the cost of work will remain the same.	Specialists can review activity logs to perform expert assessment of the contractors' skills. If the results are unsatisfactory (if the quality of work is substandard), you have the option to reduce the fee due to the contractor.
Remote access to critical IT infrastructure	Certain limitations may apply for remote connections to critical resources since your company may not be able to control the activity of contractors, administrators, APCS (automated process control systems) engineers, and other privileged users. In this case, the preferred option is local access, which requires additional spending on logistics.	You can use a specialized solution that enables privileged remote access to critical resources, captures user activity, and serves as a single-entry point for all connections to such resources. This means that local access will no longer be required to perform relevant work. This will reduce your logistics costs.

Table B.1 Increased labor productivity

Feature to consider	Problem	Solution
Centralized privileged access management	Companies need to take various technical security measures to enable safe privileged access to target resources. They also need to set up user accounts to personalize connections and control password renewal.	You can use a single tool for managing privileged access rules for all connections to target resources and enable end-to-end authentication based on saved accounts. This will allow you to optimize labor costs related to setting up privileged access to the existing target resources. You can also use integration with Service Desk to minimize labor costs related to configuring access rules.
Fast identification of root causes of failure (incident)	Finding the exact causes of failure or incident may prove quite hard, especially if the resource performance has been downgraded and its stable operation has been disrupted, making the event log unavailable.	All administrative sessions are logged, and additional data that may be useful for investigation is captured. This will allow you to determine the root cause of failure or incident and the responsible person in any case.
Control over the performance of typical tasks	Managers, auditors, and leading specialists may find it hard to control the	A manager or auditor can always analyze employee activity to give them advice and

	quality of work performed by the company's employees.	help them handle typical tasks. This is especially useful for new hires or young professionals.
Remote access to critical IT infrastructure	Certain limitations may apply for remote connections to critical resources since your company may not be able to control the activity of contractors, administrators, APCS engineers, and other privileged users. In this case, the preferred option is local access, which requires additional spending on logistics.	You can use a specialized solution that enables privileged remote access to critical resources, captures user activity, and serves as a single-entry point for all connections to such resources. This means that local access will no longer be required to perform relevant work. This will reduce your logistics costs.
Finding and adding privileged accounts to the protected PAM storage vault	Relevant administrative accounts are used for connections to target resources. Your team needs to manually maintain a complete list of such accounts and manually add them to the secure PAM storage vault for future use.	The system can automatically find privileged accounts on controlled resources and enable their oversight. These accounts are then used for end-to-end authentication without password disclosure.

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

Feature to consider	**Increased labor productivity**			
	Information security administrators	Auditors and managers	In-house privileged users	Outsourced privileged users
Centralized privileged access management	+			
Fast identification of root causes of failure (incident)	+		+	
Control over the performance of typical tasks		+		
Remote access to critical IT infrastructure	+		+	+
Finding and adding privileged accounts to the protected storage vault	+			

Table C. Reinforced information security

Feature to consider	**Problem**	**Solution**
Scheduled access and access upon approval	Your company may face risks on account of violation of security requirements related to uncontrolled use of privileged sessions outside of business hours or at other unauthorized time intervals.	You can use a single tool to manage time-sensitive access policies, that includes locking and access negotiation mechanisms. In critical situations (in case of emergency or failure), internal tools can be used to bypass these restrictions.
Audit and activity analysis tools	Your company needs to use local audit mechanisms, such as logs and agency solutions.	The system uses alternative points to capture user activity in different formats that do not depend on the state of the controlled resource and can be quickly enabled and disabled with minimal impact on the IT infrastructure.
Account password updates	Passwords to user accounts are changed manually. With multiple accounts, it may be difficult to update passwords in a	You can enable automatic password rotation for privileged accounts (including passwords for local administrators) at

	timely manner and comply with the security requirements.	predetermined intervals and with due regard to the security requirements.
Non-personalized accounts for administration of target resources	Privileged users may use non-personalized administrative accounts in their daily work. Yet, pinpointing the user of an non-personalized account may prove almost impossible.	The single non-personalized administrative account is stored in a secure database. It can be used for end-to-end authentication on the target resource without password disclosure, and the user of the non-personalized account will be recorded in the event log.