WHITE PAPER

THEFENCE™ Access Risk Control

TheFence Cross Application SoD & Least Privilege Access Control (Software)

To enforce the "need-to-know" principle, ensuring that individuals have access only to the data and functions they require for their job/role within a system, and to enable compliance with the relevant legislation and security standards, XS Matrix have developed a unique security software. With TheFence organizations can measure the access risk of the identities, users, and their profiles within business applications and IT infrastructure layers. Companies can detect who the riskiest identities are and which risky access right elements can be **sensitive or conflicting** in their access profiles. Based on the results, unnecessary yet risky functions can be detected and removed in order to prevent incidents.

TheFence supports the IT Security team in discovering the riskiest employees, third parties, technical users, service accounts as well as the poor decisions of data owners in the access approval process, wrongly planned or tested access profiles, and the misuse of user management and external hacks using privilege elevation techniques.

How the product works

The discovery process is based on a granular analysis of the access profile content. TheFence automatically connects to the monitored systems and collects user and authorization data down to the deepest entitlement objects within roles or profiles. The software connects the users with the identities recorded in the HR systems to determine which user belongs to which identity. TheFence has a base sensitive access or conflicting risk collection built into the software that is defined at the **deepest access object level.** The **risk patterns** have individual **risk scores**. This is a quantitative, scoring-based risk calculation method, where risk scoring is determined by the potential impact of the incident. Risk patterns are editable, customizable and expandable.

Conflicting (SoD) access risks can be set between different business applications or IT technologies. The software collects, stores and analyzes user and access data at an automated, pre-scheduled frequency and creates reports and alerts on the results. These reports can be further analyzed with drill-down capabilities. The **reports** can be customized and automatically distributed to the configured organizational units' emails in Word or PDF format attachments. Based on the reports, recurring IT security access monitoring processes can be created. Risk-based decisions can be made, and the risk-proportional protection can be provided to internal or external auditors. Additionally, based on the drill-down analysis, unnecessary risky objects can be identified and removed or reengineered.

TheFence is not an IAM (Identity Access Management) or PIM/PAM (Privileged Identity/Access Management) solution, as it does not cover or administer the request-approval-implement-removal cycle typical of IAM systems and does not handle privileged users' credentials or record their sessions for control.

Product architecture and integrations with applications

For the monitored system and HR integrations, TheFence uses both agent-based and agentless connections. The agent-based connections (e.g., SAP, S/HANA) use secured, encrypted file transport communication, while agentless connections (e.g. Active Directory, Azure AD) go through technical users to access the monitored systems. For custom applications, we can use DB View-based data retrieval or REST APIs. These connections and technical users only require read access to the monitored systems. These connections can be scheduled and run automatically with the desired frequency, typically once/day.

THEFENCE AI-Powered User Access Review (UAR) (SaaS)

The Periodic User Access Review process is typically orchestrated by the IT Security team. They need to connect and prepare HR employee data, organizational structure data, data owner information, system data, user and access profile data. The merged data must be sent to the data owners directly, and they need to review the identities' accesses under their authority. Most of the time, the IT Security team does not have a proper tool for managing the whole preparation and review process. It can easily become a manual (or semi-automated) task that is time-consuming and poorly administered. Besides, the data owners do not get any meaningful help for their review decisions, therefore the outcome can be poor and unacceptable for internal or external auditors, authorities.

TheFence provides a SaaS-based User Access Review solution that includes **AI-based decision-making support** for the data owners.

How TheFence UAR works

Comprehensive functionality is provided for the entire User Access Review process. This includes source data preparation, administration, notification, ticket creation, and post-review activities.
The IT Security professional logs into their own tenant in the SaaS environment. A central management screen displays an overview of the current and previous UAR tasks. They can open a new UAR process and select which integrated systems need to be included. HR employee data with organizational data is needed and can be uploaded from a CSV file when there is no HR connection.

User and access profile level data can automatically be loaded when there is already an integration, or this data can be uploaded manually from any custom app in CSV format. The uploaded identity and access data will automatically be prepared, and data cleaning (e.g. missing data owner information) can be executed. Once finished, the review requests can be sent to the approvers.

Data owners are informed and can log in to see their employees' data for approval. They are supported with an **AI co-pilot** that provides proposals for approval or denial decisions, thereby saving a significant amount of time. AI proposals are based on the user's status, activity and riskiness.

User removal/access modification tickets based on these decisions can automatically be generated and tracked, along with the execution of access or user removals. The IT Security professional can manage the **entire process end-to-end**, from initial data preparation to checking the removal of revokable accesses.

The UAR process we have implemented in our SaaS solution aligns with best practices and adheres to international security standards and regulations.

Product architecture and integrations with applications

The SaaS environment for the AI-powered UAR is built on AWS, with separate environments in the US data center and EU data center. We can provide shard-level segmentation in case of special enterprise needs. The SaaS includes a multi-tenant environment, even groups of companies can use it in a separate but centrally managed way.
Integrations of TheFence UAR are based on cloud-to-cloud REST APIs or manual, custom file uploads on secure web protocols.