Arcon

User Behaviour Analytics

Overview

Malicious end-users are one of the biggest IT threats. Early detection of the malicious end-user activities is another challenge that today's organization go through frequently.

And adding to the woes is the fact that it's impossible to monitor a growing number of end-users in a typical IT set-up. As a result, end-user behaviour anomalies remain undetected amid ever-expanding IT set-up.

Was a certain end-user entitled to access a specific application? Why is a certain end-user downloading so many files all of a sudden? Or, are the end-users adhering to the configured baseline activities or straying away from the mandated tasks? These are some of the critical questions that need to be addressed.

Growing IT complexities, however, has meant that malicious end-users can easily exploit the security gaps, resulting in a data breach, application misuse/abuse among other IT frauds.

Therefore, monitoring end-user behaviour patterns in complex environments requires a robust solution capable of detecting threats posed by anomalous end-user profiles on a real-time basis.

ARCON | UBA

Information Security and Access Control are the two most essential components for a robust IT ecosystem. However, enterprises are dynamic and ever-evolving, which has led to complexities. The general approach is to restrict the end-users as much as possible. There is a general belief that “Close as many doors as possible,” which has led to a restrictive practice and all the investments made in automation and information technologies to create efficiencies are now challenged.

We believe that ARCON | UBA will transform the way Information Security is approached in the next decade. It will essentially be “do what you want", but we will assess and monitor you as and when required. ARCON is a pioneer in self-learning end-user behaviour analytics. ARCON |UBA is a comprehensive solution that is capable of crunching a huge amount of data, spot suspicious end-user profiles and trigger alerts on a real-time basis.

arcon

ARCON | UBA

features

The key features of ARCON | UBA have been developed and enhanced based on practical enterprise use-cases. The following are some of the robust features of ARCON | UBA:

Analyze User Behaviour

Configure and Identify user behaviour based on their roles and daily activities

Granular Level Monitoring

Seamlessly monitors end-users' behaviors granularly throughout your enterprise

Manage Application Access Criteria

Manage application inventory and access criteria

Role-based groups

Auto-create and assign end-users to groups based on roles, rights and responsibilities

arcon

User Authentication

Use ML algorithms to determine user authenticity and alarm admins of anomalous security risks

Manage elevated end-user rights

Assign, elevate, expand and revoke admin rights; ensures compliance

User-Friendly UI Dashboard

Making administrators jobs easier

Facial Recognition

Authenticates end-users

Provision role-based access

Provision end-users with Role Based Access Control (RBAC) and easily analyze login attempts

Enhance Productivity

Detailed productivity reports for any/ all end-users

Reporting

Detailed reporting of tasks performed including minute-by-minute details per end-user

Assign Temporary Rights

Quickly assign privileged rights specific to temporary needs or requirements for internal users, vendors, analysts and/ or contractors. Just-In-Time access adds elevated rights for urgent tasks and be set to expire or reviewed after the timeframe allocated

ARCON | UBA

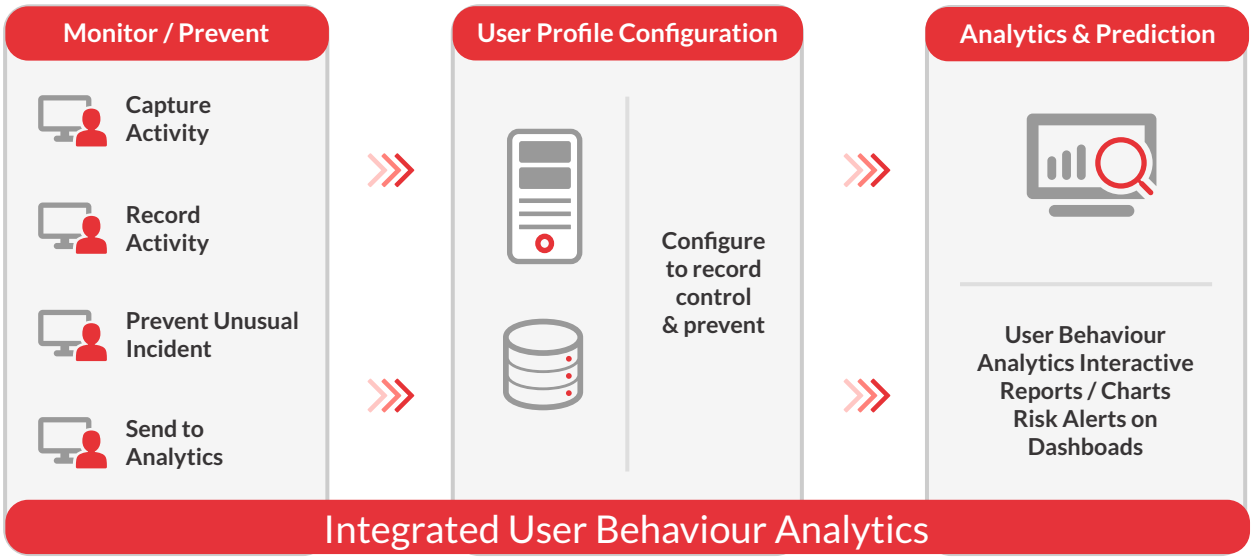
Benefits

- Leverages AI/ ML to solve a range of distinct use-cases related to end-user behaviour monitoring and data exfiltration
- Helps to configure baseline for end-user activities
- Detects end-user behaviour anomalies and profiles that deviate from the configured baseline in real-time
- Offers unified governance framework for both IT visibility and mitigating insider and zero-day threats
- The product can be deployed as a discrete solution or can be embedded with ARCON | PAM and ARCON | EPM
- When embedded with ARCON | PAM, ARCON | UBA enables to detect anomalies in privileged access environment, thus mitigate data breach threats

Product Architecture

ARCON | User Behaviour Analytics (UBA) is an effective solution when it comes to detecting insider threats. The solution essentially nips threats in the bud before they maneuver and execute malicious activities through the endpoints. The robust solution provides a secure IT set-up in an enterprise by isolating anomalous activities in real-time. With the help of AI/ ML algorithms, the solution configures baseline IT security policies for every end-user in day-to-day IT operations. Thus, it reduces the endpoint attack vector while helping enterprises to comply with the international IT security standards.

User Behaviour Analytics



About ARCON

ARCON is a leading enterprise information risk control solution provider, specializing in Privileged Access Management (PAM) and continuous risk assessment solutions. Our mission is to help enterprises identify emerging technology risks and help mitigate them by robust solutions that predict, protect and prevent.

PAM: ARCON | Privileged Access Management (PAM) is a highly effective solution that helps in managing, controlling and monitoring privileged user activities. The solution provides IT security team with a centralized policy framework to authorize privileges based on roles and responsibilities ensuring rule-based restricted access to target systems.

UBA: ARCON | User Behaviour Analytics (UBA) is a highly effective risk predictive & analytics tool built for daily enterpris e use cases. It breaks the traditional approach of 'restrictive' access and is capable of crunching large lakes of enterprise data, spot anomalous activity and trigger alerts in real-time.

SCM: ARCON | Security Compliance Management (SCM) allows an enterprise to prioritize security and compliance efforts based on risk level. The tool enables continuous risk assessment for critical technology platforms and ensuring desired compliance levels.

Connect with us