ARCON | User Behaviour Analytics (UBA)

ARCON | UBA packs a punch when it comes to detecting looming insider threats. The solution essentially nips threats in the bud before they maneuver and execute malicious activities through endpoints. In this paper we also discuss three case studies to demonstrate how it helped each global enterprise to mitigate IT and insider threats.

synopsis

Think about today's enterprise's complex IT infrastructure, which is constantly expanding with multiple layers of applications, devices and technologies. Managing IT risks becomes a daunting task in this set-up. After all it's not easy to keep a check on every bit of information and activities happening in the IT network. Is the end user authorized to access a certain application? Are risky behaviour profiles under examination? If such critical questions are not answered swiftly, data misuse among other harmful activities can cause an IT disaster.
It is fair to say that today's IT risk management dynamics have altered. Amid constantly evolving technologies, the attack vector has enlarged. Any IT ecosystem urgently requires robust threat detection and mitigation capabilities. The faster a threat is identified, lesser will be the damage and vice-versa. For a modern-day enterprise IT infrastructure, predicting and detecting risks is at the core to maintain robust IT security.

ARCON | UBA :
a robust threat detection and prediction tool

At the heart of the conventional IT security posture, restricting users has been a trusted approach. 'Close as many doors you can to mitigate risks' is the standard line of action.
That approach has three flaws, which are as follows:

- It never provides analytics and insights into the risky behavior profiles
- Data is not collected from all endpoints thus leading to ambiguity over application access
- All investments made into technologies, automation and internet doesn't yield results due to restrictive IT practices

ARCON | UBA is a highly effective risk predictive & analytics tool built for daily enterprises use cases. It breaks the traditional approach of 'restrictive' access. Even better, it takes a modern approach, which is based on: 'do whatever you want to do but we will assess the trustworthiness as and when required'. The tool predicts threats on a real-time basis. A self learning user behavior analytics tool, ARCON | UBA is capable of crunching large lakes of enterprise data, spot anomalous activity and trigger alerts in real-time. By deploying the solution enterprises get value for money. It boosts workforce productivity by creating a configured baseline on endpoints whilst it secures access to critical systems and applications.

case study 1

One of the Big Four Audit and Accounting firms reduces attack vector and enhances productivity by deploying ***ARCON | UBA***

the challenge

Hundreds of auditors access several applications on a daily basis. Therein lies the complexity and need to have a sophisticated analytics methodology. Practically, end users require access to only specific applications. In other words, every end user does not require access to every enterprise application. Lack of role-based 'need-to-know' and 'need-to-do' application access control not only expands the attack surface but also mar productivity. It incentivizes end users to deviate from baseline activities.

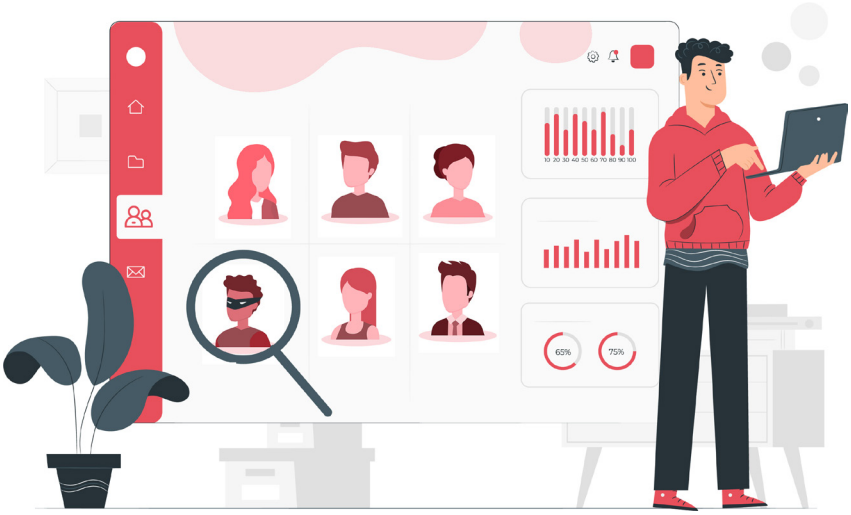
the solution

ARCON UBA enabled its Client to overcome these challenges through following solutions:

- The tool centrally collects all enterprise data
- The insights provided by data analytics helps the security and risk management team to implement application access control
- Application access is granted based on daily use cases
- Access to application other than permitted is granted by UBA Admin through an elevation request
- Application access through an elevation request is granted for a specified period of time (Read ARCON whitepaper 'Leverage Just-in-time Privileges with ARCON | Privileged Access Management to learn how this functionality helps in reinforcing the overall privileged access security posture)

case study 2

*One of India's largest financial institutions deploys **ARCON | UBA** to configure end user baseline activities and spot risky behaviour profiles*



the challenge

Remote workforce is the new norm especially at the time of pandemic. The security risk assessment team wanted to capture details of all the end user activities. It wanted to record video of all user activities happening with critical applications.

the solution

The tool enabled our Client to keep a check on risky behavior profiles through the following mechanism:

- Our Client acquired comprehensive threat detection capability through ARCON | UBA
- The tool enabled our Client to configure baseline activities on machines as per the centralized policy
- Unified data analytics helped our Client examine anomalous activities deviating from configured baseline policy
- Implementation of video recording for critical applications used by end users
- Dynamic reports enabled our Client to make better IT security decisions

case study 3

*One of India's leading consulting firms ensures compliance with CERT-India guidelines by deploying **ARCON | UBA***

the challenge

CERT-IN, which stands for Computer Emergency Responses Team – India, is responsible for any computer security related issues in India. CERT-IN provides guidelines on securing endpoints. Our Client wanted a robust threat detection tool.

the solution

ARCON | UBA helped our Client to build a robust endpoint security framework. It offered the following solutions:

- It enabled our Client to do data profiling and anomaly detection
- Unified governance framework supported better visibility
- It mitigated insider and zero day threats
- It offered advanced risk analytics capabilities
- Provided endpoint privilege 'on-demand' to critical applications reinforcing the overall privileged access security posture)

conclusion

ARCON | UBA is a robust tool which can provide an enterprise a secure IT set-up by isolating anomalous activity in real-time. The tool aligns IT security policies with day to day IT operations. It thus reduces the endpoint attack vector whilst helping complying with international security standards.

about ARCON

ARCON is a leading Information Risk Management solutions provider specializing in Privileged Access Management and Continuous Risk Assessment solutions.

ARCON Privileged Access Management (PAM) is a leading global product and a robust solution that mitigates risks arising out of privilege identity and access management

Connect with us