Arcon

Endpoint Privilege Management

Overview

Designed to enforce the Just-in-time privileges principle, ARCON | Endpoint Privilege Management solution offers a centralized framework to ensure a rule and role-based access to business-critical applications.

Excessive end-user privileges are extremely risky. Some of the costliest security breaches have happened due to misuse and abuse of endpoint privileges. Data leaks, cyber-attacks, cyber-espionage, zero-day threats – all such incidents happen when endpoint privileges are easily available in an uncontrolled environment.

Moreover, the outbreak of the pandemic and subsequent alteration in the work culture has meant that a large number of the workforces are accessing applications remotely. Every so often, the remote access happens from personal devices.

Resultantly, the multiple layers of applications and devices along with a high number of end-users makes business-critical applications extremely vulnerable to attack from malicious behaviour profiles.

Thus, granting the endpoint privileges 'just-in-time'/ 'on-demand' along with the end-user monitoring has become the cornerstone of robust IT governance for a modern-day enterprise.

In addition to fostering the just-in-time privileges practice, ARCON | Endpoint Privilege Management solution (EPM) detects insider threats, compromised identities, and other malicious attempts on the endpoints. It has a powerful User Behaviour Analytics component that takes note of the normal conduct of the end-users and identifies typical, atypical behaviour profiles and other entities in the network.

ARCON | EPM ensures there is adequate IT oversight and business-critical applications are accessed in a restricted and controlled environment.

ARCON | EPM

Offers a Unified Governance Framework

The solution enforces a centralized policy to regulate and govern all the end-users. The end-users' access to business-critical applications is rule and role-based. Thus, the solution strengthens the enterprise's overall compliance framework and prevents malicious activities.

arcon

ARCON | EPM

enhances IT administration and user experience

As the number of business-critical applications increases, the role of the IT administrators does become complex both from the IT security and operational standpoint. It's a tough ask for the IT help-desk to attend, manage and monitor every endpoint privilege request. Think about hundreds or thousands of endpoint privilege elevation requests on a daily basis. It is a complex IT operational challenge for the IT help-desk staff.

The ARCON | EPM solution will make the administrators' life easy. Every endpoint privilege request will flash instantly at the IT administrator's desktop. The request will be granted immediately based on the configured endpoint privilege elevation policies.

arcon

ARCON | EPM

Detects threats and raises red-flag on real-time basis

Granting access to business-critical applications is based on the end-users' risk-based assessments. The ML algorithms (UBA component) use the end-users' logged data to identify risky profiles. The ML algorithms clusters risky behaviour profiles and end-user anomalies. Subsequently, the AI analytics generate a risk-score based on each end-user profile.

arcon

Key Features of

ARCON | EPM

Centralized Governance

The endpoint privilege policies are automatically created by profiling all the on-boarded end-users' roles and responsibilities. The unified policy framework ensures a rule and role-based access to applications in the network.

Privilege elevation on-demand (just-in-time privileges)

ARCON | EPM offers seamless help-desk integration. Any on-boarded end-user in the network can request the administrator to grant an endpoint privilege for accessing a particular application. Based on the end-user role and responsibility, the administrator will then grant just-in-time endpoint privilege. After the privilege task is completed, the elevated privilege is revoked. The feature ensures robust implementation of the Least Privileges principle. The workflow Requests are approved/ rejected on-the-fly by administrators.

Priority-wise profiling

This feature enables the IT security staff to systematically grant access to the specific application/s based on the end-users' job profiles. Access priority is determined/set by the IT administrator.

Application Security

Malicious applications that run in the IT environment pose a serious security threat. The Application Security feature secures the endpoints by blacklisting malicious applications.

Fine-grained access control

All the on-boarded end-users' endpoint privileges are granularly controlled and restricted through time-based, day-based, and duration-based parameters. Likewise, the end-users' access to web browsers are also controlled and restricted.

arcon

End-user Behaviour Analytics

It detects anomalies and suspicious behaviour profiles on a real-time basis and generates risk-based scores with the help of Machine Learning and Artificial Intelligence.

Dashboard

The dashboard provides a real-time view of the endpoint privilege sessions. Thus, the tool offers an indispensable mechanism for IT oversight.

Audit Trails and Reporting

The audit trails are maintained of each and every endpoint privileged activity and the reports are generated for the audit purpose. It ensures compliance with the IT standards.

Data Loss Prevention (DLP)

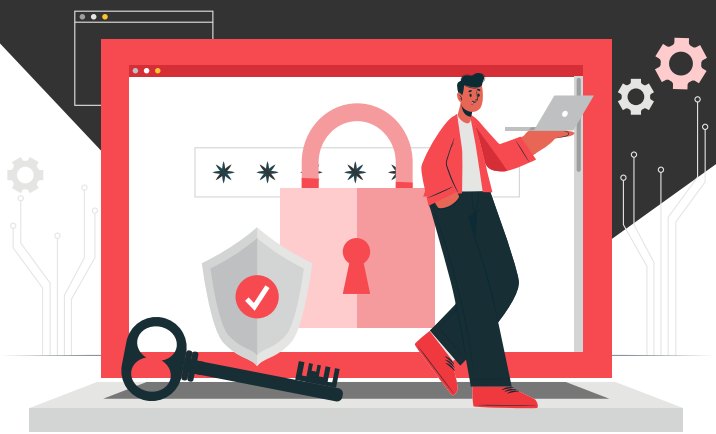
The endpoint security can be compromised if the end-users can easily target confidential information using any removable storage device. The EPM's DLP feature helps with mitigating the security vulnerabilities. ARCON | EPM assists the IT security team with USB restriction feature that ensures copying of any sort of information/file from the endpoint to USB and (vice versa) is restricted.

Facial Recognition

Facial Recognition mode of authentication is used to ensure authorized access to the critical systems and view logs of the number of users. These logs help the IT admins to show the total number of successful and failed login attempts done in a specified time-frame (both hourly & daily)

Alert Trends

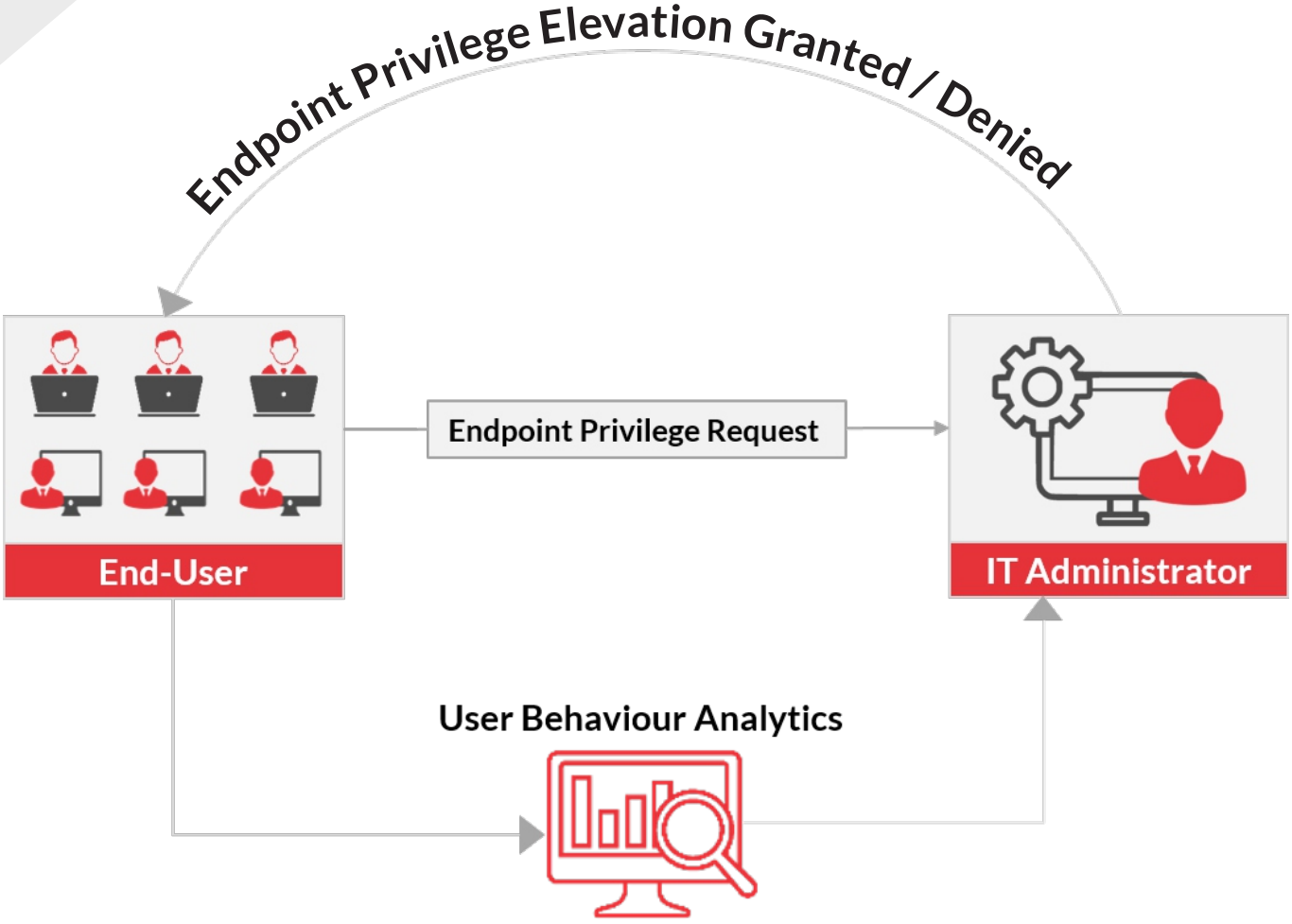
All the critical alerts that are displayed or notified during monitoring of endpoint privileges have categories as per the extent of seriousness. The patterns of anomalies and the importance of accessed accounts decide if the alerts are low, medium and high. With these alert trends, organizations can take necessary steps if any suspicion is triggered.



arcon

ARCON | EPM

How it works?



ARCON | EPM

Benefits

- Builds the framework to govern the end-users
- Elevates the endpoint privileges just-in-time
- Enforces application blacklisting
- Ensures the principle of the least privilege
- Detects suspicious end-user behaviour profiles in real-time
- Protects the endpoints
- Prevents granting elevated privileges to suspicious end-users
- Offers fine-grained access to all applications
- Enhances IT efficiency
- Helps meet the IT standards

arcon

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