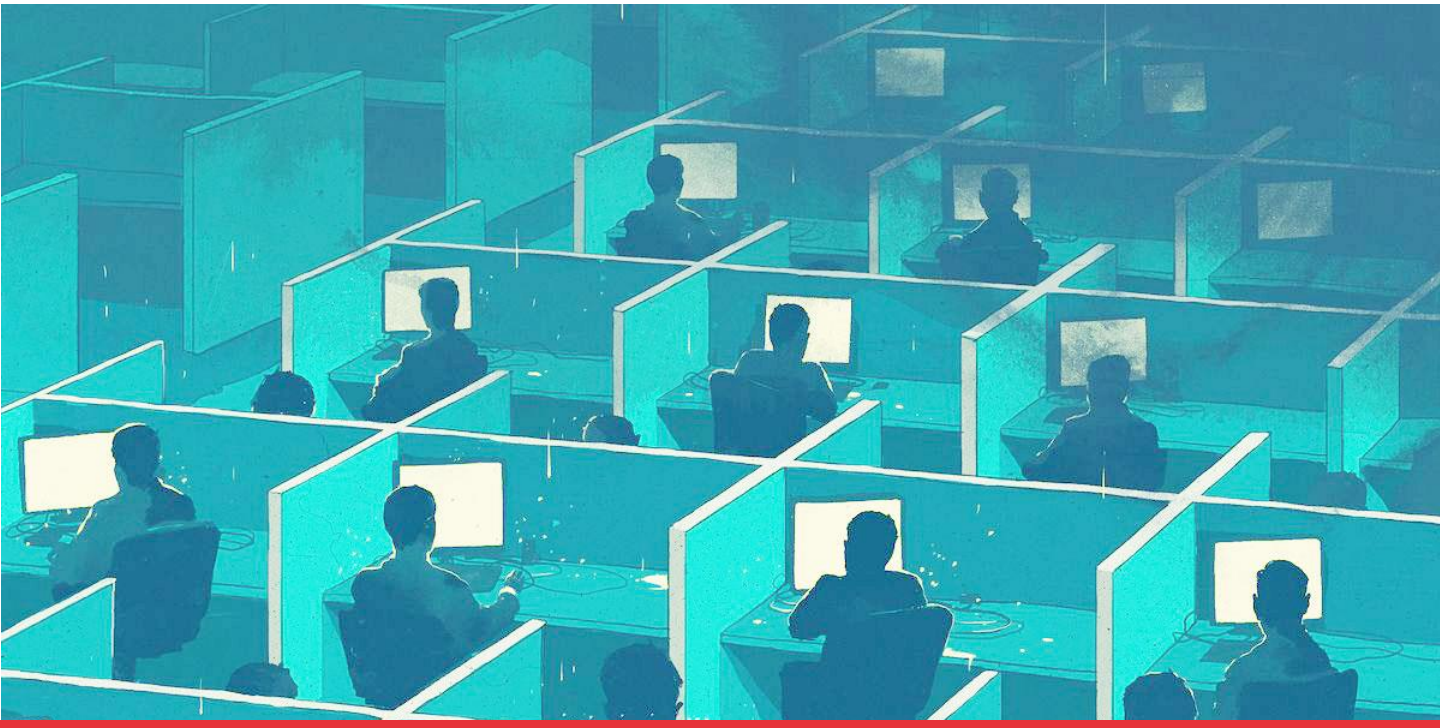


ARCON | Endpoint Privilege Management (EPM)

Why an enterprise requires endpoint privilege management (EPM)?

The endpoint privilege threat vector is expanding

At an enterprise level, some of the most costly security breach incidents such as theft of credentials, espionage, and pilfering of data assets stem from unprotected laptops and desktops. The challenge arises due to lack of privilege endpoint management, which is essentially due to the nature of complexities involved in managing a large number of elevated privileges accessing underlying applications. As the number of endpoints for typical mid-size and large-scale enterprises are exploding due to the rapid pace of digitization, security vulnerabilities have also expanded. IT security managers often find it difficult to keep a tab on every activity performed from endpoint privileges, resulting in lack of IT oversight. Thus business-critical applications are accessed in an unrestricted and uncontrolled environment.

Controlling and containing enterprise IT threats requires robust endpoint protection

ARCON | Endpoint Privilege Management (EPM) reinforces protection for endpoints through a rule based restrictive privileged elevation to critical applications. The robust solution fosters the best privilege endpoint practices in an enterprise IT environment. An end user's access to business-critical application is subjected to risk-based assessments of individual behavioral profiles. ML algorithms use end users' logged data to identify risky profiles. As soon as ML clusters risky behavior profiles and users' anomalies, AI analytics generate risk-score based on each end-user profile. Further, the tool offers access only on "need-to-know" and "need-to-do" principle to control spiraling of excessive privileges. ARCON EPM ensures that an end user privilege to any application is instantly revoked after the task is completed. Thus it helps implementing the principle of Least Privileges, the cornerstone to form a robust identity and access control framework.

ARCON | EPM enhances IT operational efficiency and user experience

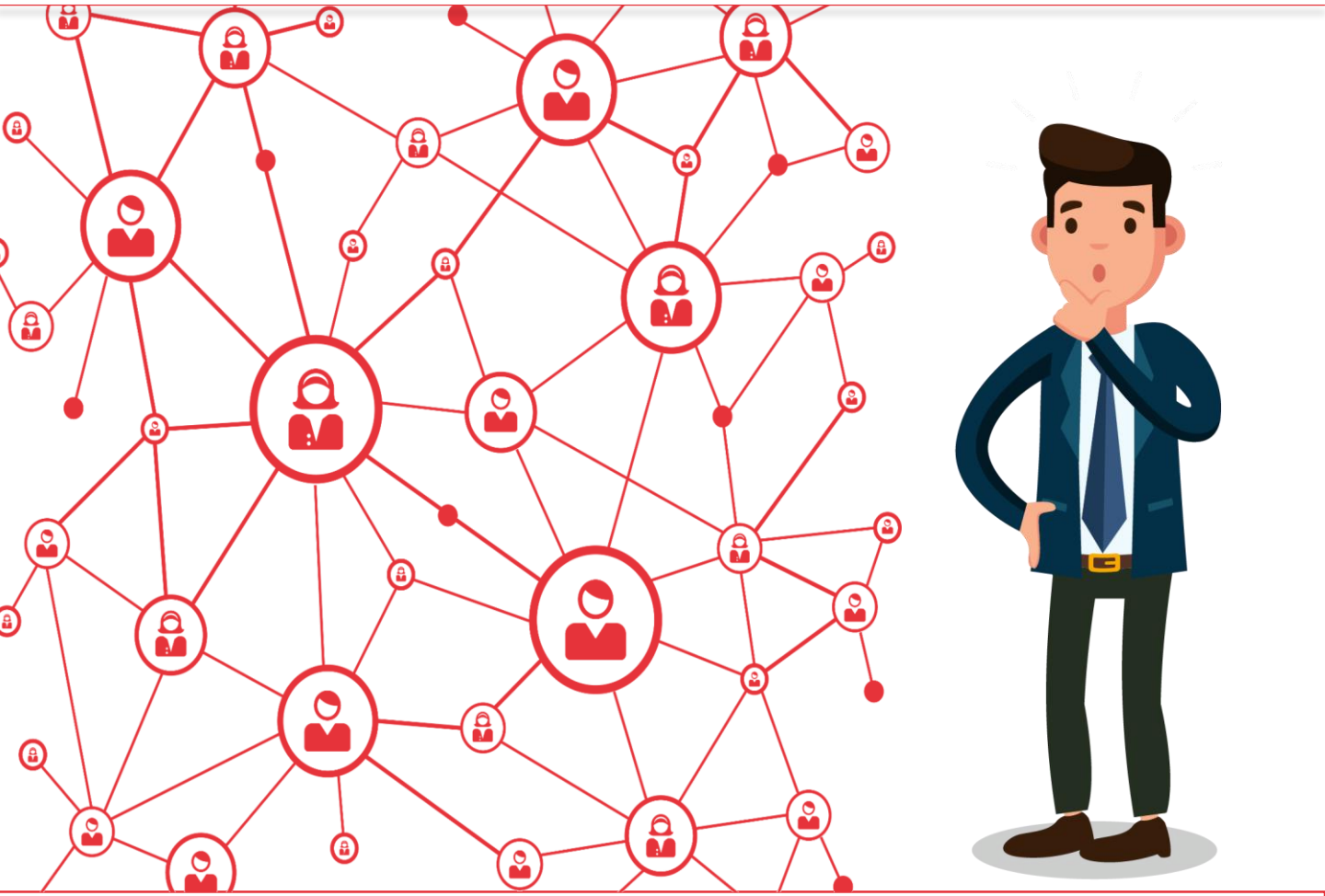
Further, as the number elevated privileges increases, the role of IT administrators do become complex both from IT security and operational standpoint. It's a tough ask for IT Help Desk to attend, manage and monitor every endpoint privilege request. Think about hundreds or thousands of endpoint privilege elevation requests on a daily basis. It is a complex IT operational challenge for IT help desk staff when they have to attend requests from one desktop to another. EPM makes administrators' life simple. Every endpoint privilege request will flash instantly at IT administrator's desktop. Request will be granted immediately based on the risk profile and according to the configured policies. Thus it reduces the burden for the IT Help Desk staff and limits the number of tickets raised. Likewise, end-users expect a user experience that enhances productivity and efficiency. With the help of a single right click, an end user can raise the endpoint privilege elevation request and finish off the task subject to endpoint privilege approval.

ARCON | EPM provides a unified endpoint governance framework

The solution's centralized policy engine regulates and governs all endpoint privileges. It acts a pivotal security component by enforcing endpoint privileged security through rule and role based endpoint privileges. Thus it strengthens an enterprise's overall compliance framework and prevents malicious activities such as data theft, data encryption and corporate espionage.

ARCON | Endpoint Privilege Management (EPM)- A stepping stone to build a robust Zero Trust Framework

The Zero trust framework is a radical shift from conventional perimeter-centric security outlook to a data-centric security approach. The basic requirement to attain a Zero Trust framework is building a robust data protection mechanism. Thus the essence of Zero trust framework lies in endpoint security as most cyber-attacks are initiated from the endpoints. Secondly, according to Forrester, The Zero Trust model never assumes 'trust' but it continuously assesses 'trust' using risk-based end-user analysis collated from information gathered.
Thus, in addition to network security, the Zero Trust framework argues for an urgent need to develop a unified data security policy for all endpoints. ARCON | Privilege Endpoint Management provides security managers with the best Zero trust practices as this robust tool ensures greater privilege endpoint visibility wherein every elevated privilege is continuously assessed and governed, which helps in containing and preventing attacks on endpoints.



ZERO TRUST FRAMEWORK

ARCON | Endpoint Privilege Management Features in Details

Centralized Policy Enforcement

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

Privilege Elevation on-Demand

ARCON | EPM offers seamless Help Desk integration. Any on-boarded user in the network can request the Administrator to grant endpoint privilege to access a particular application. Based on the user, the Administrator will then grant just- in-time endpoint privilege. After the privilege activity is finished, the elevated privilege is revoked. The feature ensures robust implementation of Least Privileges principle. Workflow Requests are approved/ rejected on-the-fly by administrators.

Priority wise Profiling

This functionality enables the IT security staff to systematically grant access to specific application/s based on job profiles of the end users. Access priority is determined/set by the IT security team.

Application Security

Secures endpoints and helps preventing malicious applications running in the environment by application blacklisting.

Fine-Grained Control

All on-boarded end users' endpoint privilege is granularly controlled and restricted through time-based, day-based, and duration-based rules. Not only that, ARCON offers deepest level of granular control. For instance, endpoint privilege will be granted only for a specific application for which the request has been raised. Likewise, end users' access to web browsers is also controlled and restricted.

Privilege Behaviour Analytics

Isolates anomalies and suspicious behavior profiles in real-time. Generates risk-based scores through AI & ML.

Dashboard

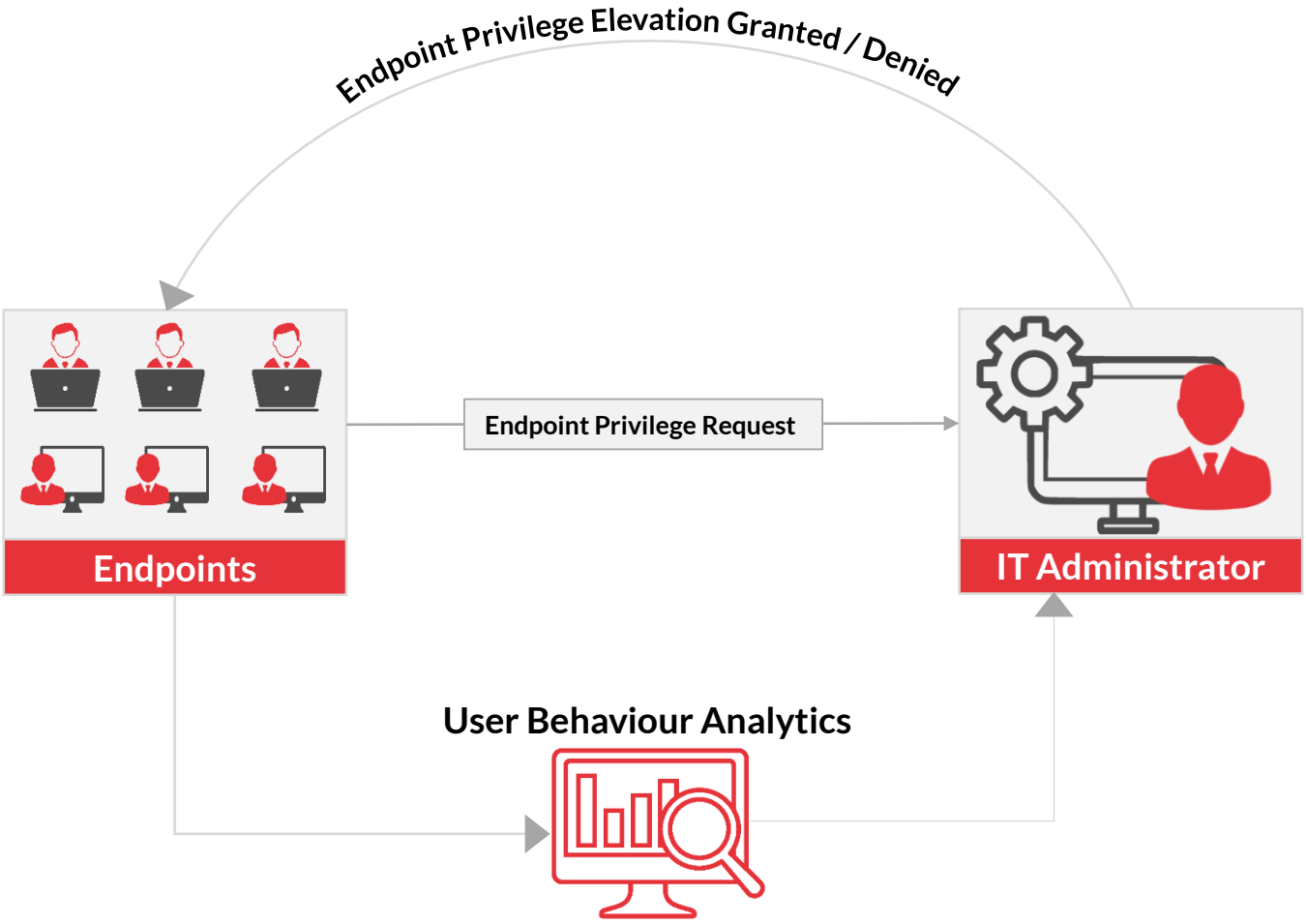
It provides real-time view of endpoint privilege sessions. Thus it provides an indispensable tool to control and govern users helping meeting regulatory compliance standards.

Audit Trails & Reporting Monitor real-time endpoint privilege activities and generate reports for audit purpose and compliance with the regulatory standards.

Data Loss Prevention

Endpoint security can be compromised if end-users can easily target confidential information using any removable storage device. EPM's DLP feature helps containing security vulnerabilities as security staff can administer specific hardware example USB and content based filtering and blocking

ARCON | EPM Architecture



Benefits of ARCON Privilege Endpoint Management (EPM)

Builds an end-user governance framework

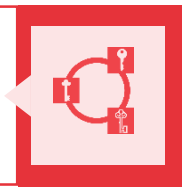
Prevents granting elevated privileges to suspicious users

Protects endpoints

Continuous assessment of end-users' behaviour

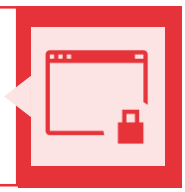
Prevents escalation of privileges by adopting least privileges principle

Fine-grained access control over all applications



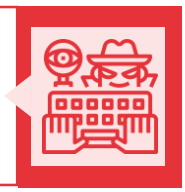
Elevates endpoint privilege just-in-time

Application black listing

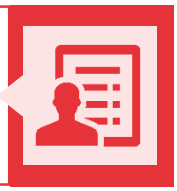
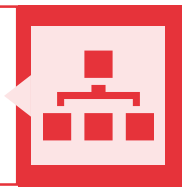
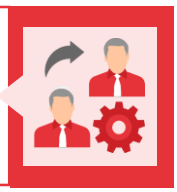


Increases IT oversight

Data Loss prevention



Benefits of ARCON Privilege Endpoint Management (EPM)

- Enhances User productivity 
- Audit and Reporting 
- Reduces help desk calls 
- Helps meeting compliance standards 
- Reduces Help Desk Tickets 
- Builds the foundation for Zero Trust Architecture 
- Harnesses the practice of least privileges 
- Real-time threat analytics through Dashboard 
- Enhances IT efficiency 
- Helps meeting compliance 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