arcon

Predict | Protect | Prevent

ARCON | Endpoint Privilege Management

Overview

Too many end-user privileges bear risks of unwanted access. Endpoint privilege abuse is the reason behind many costly and infamous security breaches across the globe. Data thefts, insider-attacks, cyber-espionage, application misuse or abuse – all such incidents happen when endpoint privileges are easily available and accessible in an uncontrolled environment. Moreover, there are sudden changes of work environments such as shift from on-prem to cloud or hybrid work environment, forces employees to access critical applications remotely from personal devices.

Resultantly, multiple layers of applications and devices along with many end-users make business-critical applications vulnerable to malicious activities. Thus, granting the endpoint privileges 'just-in-time'/ 'on-demand' along with the end-user monitoring and role-based access has become the cornerstone of robust IT governance for a modern-day enterprise.

In addition, 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 (ab)normal/anomalous conduct of the end users and identities typical, atypical behaviour profiles in the network.

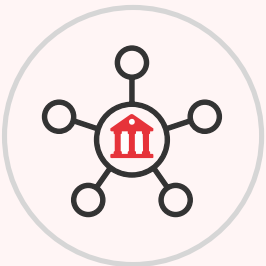
Data contextualization is another key functionality provided by ARCON | EPM solution. As organizations of all shapes and sizes generate a huge volume of data every day, IT security pros require a mechanism through which actionable insights can be generated to make well-informed decisions. Data Intellect, a critical component of EPM, builds a ring-fence around data and provides a contextual security layer around the data. File Integrity Monitoring (FIM) is an added layer of security that enables IT security pros to identify and take necessary actions against unapproved changes in device configuration.
Briefly, ARCON | EPM ensures that there is adequate IT oversight and business-critical applications are accessed in a restricted and controlled environment.

ARCON | EPM

Key Features

The features of ARCON | EPM have been segregated into unique features and generic features.

Unique Features



Centralized Governance

ARCON | EPM offers a centralized admin console for managing various endpoints such as Windows, Linux and MacOS. Centralized engine ensures rule-based access to applications. Built-in automated profiling allows administrators to create and segregate profiles of the users based on their roles.

Application Restrictions

The threat vector created by unrestricted usage of harmful applications can be significantly reduced through classifying applications based on risk levels associated with them. Application Restrictions helps to secure all the endpoints in the network by blacklisting and whitelisting applications.

Privilege Elevation and Delegation Management (PEDM)

This feature enables IT administrators to grant temporary elevated privileges to end users that need to perform specific project-based tasks on Windows, MacOS, Linux and Unix environments. The PEDM functionality allows IT security teams to adhere to the principle of “Least Privileges.”

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

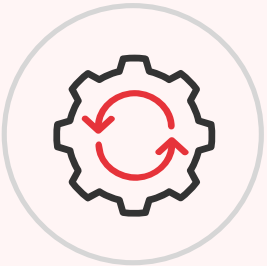
Any on-boarded end-user in the network can request the administrator to grant an endpoint privilege for accessing a particular application. Based on the end-user roles and responsibilities, the administrator grants just-in-time endpoint privilege. After the privilege task is completed, the elevated privilege is revoked. This feature ensures robust implementation of “Least Privilege” principle and follows Zero Trust architecture. The workflow requests are approved/ rejected on-the-fly by administrators.

File Integrity Monitoring

It provides an added layer of security to IT security pros. FIM helps to identify unapproved or unauthorized changes made on files in end-user devices and take necessary actions (rollbacks if needed) while keeping track of file history.

Independent workflow

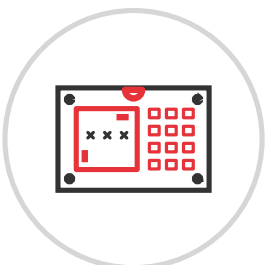
EPM offers dynamic workflow management to ease end users' experience and enhance administrative efficiency. End users out of the network can easily raise requests for elevated access to get things done promptly and seamlessly.



Audit Trails, Reporting and Alert Trends

EPM provides audit trails of each endpoint privileged activity, and the reports are generated whenever there is any audit requirement. It ensures compliance with the global IT standards. In addition, it monitors endpoint privileges and triggers alerts in case of suspicious activity.

Generic Features



Password Vaulting

ARCON EPM's password vaulting ensures that the endpoint passwords are stored and managed in a highly secure environment by providing a secure and single point of control. It eliminates the need to remember and share passwords, thus lowering the risk of password misuse. It also provides an audit trail of all privileged account password access, including who accessed the password, when, and for what purpose, thereby improving the overall security posture of the organization.

Multi-Factor Authentication (MFA)

ARCON EPM supports MFA options for end-users who intend to access critical applications during any given point of time. It includes options such as ARCON Authenticator App, Email OTP, SMS OTP, hardware tokens, Google and Microsoft Authenticator, biometric authentication, Facial Recognition, and many more. Organizations opt for MFA to meet their security needs and integrate with their existing IT infrastructure seamlessly.

Automated Profiling

Deployment of EPM could be tedious and time consuming if there are many users in an IT environment. With the help of auto-profiling, administrators can create, and segregate profiles of the users based on their roles. It reduces administrative tasks by providing relevant suggestions of profiles that can be assigned to individual users or user groups based on the activities performed regularly.

SIEM Integration

With the help of this logging tool, IT administrators can identify, understand, and address potential security threats and vulnerabilities before they have a chance to disrupt business operations. It prevents misuse of endpoint access and ensures log management.

AD Integration

Active Directory tool in ARCON | EPM allows organizations to use LDAP as an industry-standard application protocol that accesses and manages the distributed directory information services over any network. Once the users are created and authenticated post-AD integration, it starts supporting different operating systems, such as Microsoft, Linux, and Unix.

ServiceNow Integration

With this feature, any file access request made by any end-user is assessed and allowed based on the role of the user and the relevancy of the task for which the request is made. Even if the administrator approves the request through ServiceNow, it remains a time-based elevation, hence security is ensured.

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 is also controlled and restricted seamlessly.

Data Loss Prevention (DLP)

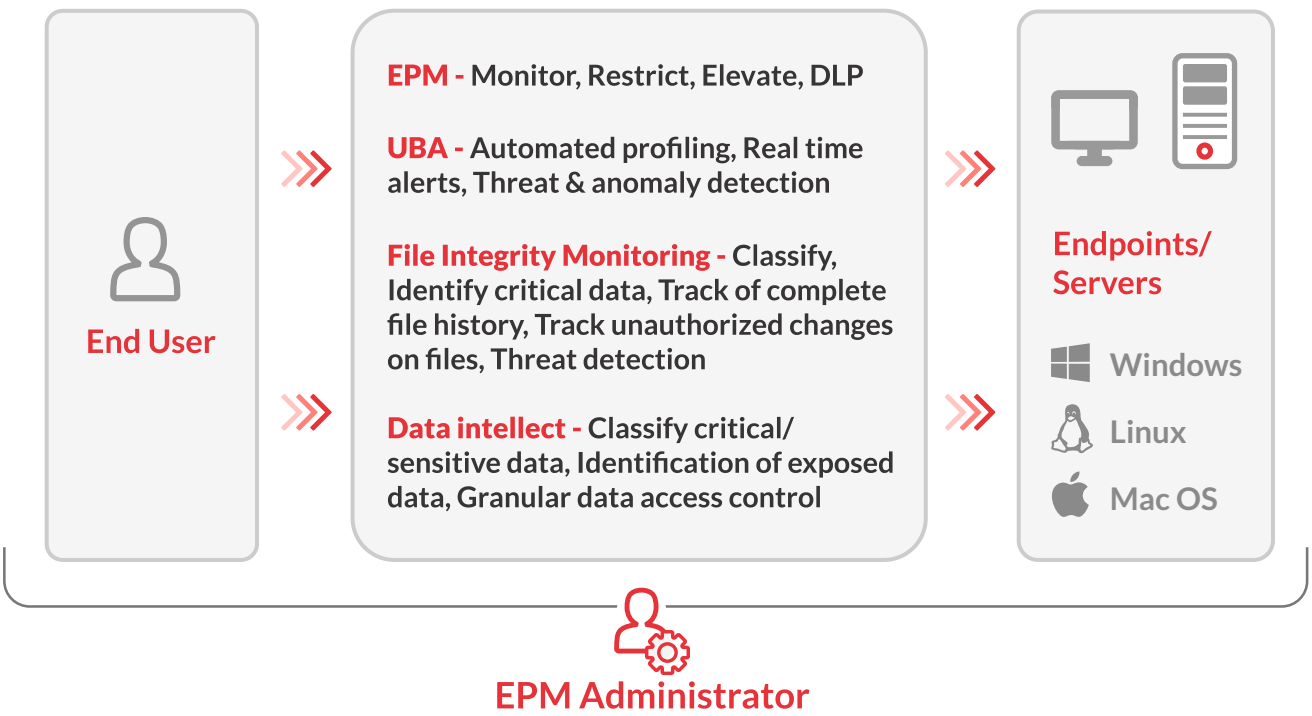
The endpoint security can be compromised if the end-users can easily target confidential information using any removable storage device. The EPM's DLP feature helps mitigating security vulnerabilities by restricting mobile devices or even mobile Bluetooth connections and Bluetooth transfers. ARCON | EPM assists the IT security team with USB restriction feature that ensures copying of any sort of information/file/folder from the endpoint to USB and vice versa.

ARCON | EPM

Benefits at a glance

- Builds the framework to control, monitor and govern the end-users
- Elevates the Just-in-Time (JIT) privilege practices
- Enforces application blacklisting/ whitelisting
- Ensures the principle of the “Least Privilege”
- Detects suspicious end-user behaviour in real-time
- Protects the endpoints based on Zero Trust security model
- Prevents granting elevated privileges to suspicious end-users
- Offers fine-grained elevated access to all applications
- Enhances IT efficiency
- Easy deployment based on automated and role-wise segregation of users
- Helps to meet with IT standards and regulatory compliances

Product Architecture



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.