pathlock

Elevated Access Management

Audit-ready, Time-Bound Privileged Access Via Automated Workflows

Introduction

Granting elevated access to production systems is a high-risk activity that many auditors will identify as a significant deficiency if not appropriately controlled. Pathlock allows organizations to streamline their elevated access management (EAM) processes while meeting audit and security requirements. The automated process with built-in workflows reduces the need for additional IT resources while adding additional layers of security.

Remove the Burden of Manual Provisioning and Ensure Auditability

Sometimes, employees or contractors need temporary privileged access to business applications to troubleshoot a problem, respond quickly to a business issue, or perform administrative functions. But, granting elevated access is risky, so it is crucial to put measures in place to minimize the risk. For example, you may need to:

- Ensure that requests are appropriately approved.
- Restrict the duration of the access to the amount of time needed to complete the task.
- Remove the privileged access at the end of the allotted time.
- Log and review all activities performed during the access period.

In some cases, such as troubleshooting, the access may be required urgently, so it's also important to be able to provision the access quickly and efficiently when needed.

EAM empowers you to automate the processes of managing temporary access requests, approvals, provisioning, deprovisioning, and activity logging.

Respond Quickly and Safely to Requests for Temporary Elevated Access

Pathlock's Elevated Access Management allows you to grant urgent or scheduled temporary privileged access rights to a user who does not typically have that type of access. It enables you to swiftly and easily authorize access for a specific duration, automatically revoke the access at the end of the specified period, and monitor and review the actions performed by the user during the access period.

This solution supports the requirement for sensitive and elevated access to be authorized only on an as-needed basis while complying with the principle of least privilege access. This approach guarantees that access is granted only for essential daily tasks and adheres to an approved process for temporarily granting elevated access.

Business Benefits

Ensure access requests are appropriately approved:

Pathlock incorporates a robust approval process into the provisioning workflow. This ensures that each access request is thoroughly vetted and only approved by authorized personnel, reinforcing accountability and reducing the chances of unauthorized access.

Automatically remove privileged access when due:

By automatically deprovisioning access after a specified period, Pathlock eliminates the risk of lingering permissions that may be exploited maliciously. This automated process also reduces manual tracking and follow-ups, increasing the efficiency of your IT operations.

Review privileged access activity to identify misuse:

Pathlock's logging and monitoring capabilities allow you to closely monitor the activities performed during the access period. This facilitates early detection of any misuse or suspicious activities, enabling swift remedial actions and reducing potential damage.

Complete audit trail of privileged user activities:

Pathlock provides a comprehensive audit trail for each privileged access session, making it easier to meet compliance requirements and conduct internal audits. This audit trail includes details such as who requested access, who approved it, and when and what actions were taken during the session, providing a transparent record of all privileged activities.

Module Features and Functions

Supports Two Types of Elevated Access Management

- Role-based EAM: a predefined role, including EAM privileges, is assigned to the requestor for a specified duration if approved.
- ID-based EAM: the requestor is assigned to an appropriate EAM/Firefighter account for a specified duration if approved.

Customizable Elevated Access Request Forms

You decide what information to include on the request, for example, reason for request, type of access needed, and duration. You can also add a disclaimer to the request and require the requestor to accept appropriate access and usage policies. You can create as many request forms as needed to cater to different types of requests.

Request for Self or Others

Users can submit requests for access to be assigned to themselves or to other people, such as members of their team.

Configurable Approval Process

Pathlock Cloud's configurable workflow engines give you enormous flexibility to tailor the processing of your requests to suit different scenarios, including pre-approved requests, auto-approval or multi-stage, multi-approver requirements.

pathlock

Automatic Provisioning / Deprovisioning

Once the access has been approved, it will be provisioned automatically immediately or at the time designated on the request. At the end of the allotted time, the access is automatically removed.

Logs All Activities

For every successful request, EAM logs all activities that are performed during the access period. At the end of the access period, the log is automatically sent to a designated user for review.

Audit Trail

All requests, approvals, provisioning and deprovisioning of access, as well as all actions performed during the access period, are recorded. This includes before and after changes of any deleted materials. This comprehensive audit trail is available to management and auditors to ensure compliance with all policies and regulatory requirements.

Integration with Ticketing Systems

EAM can be integrated with ticketing systems such as ServiceNow or Jira to trigger elevated access requests and workflows as appropriate.

Manage Elevated Access Management Requests Quickly and Efficiently While Minimizing Risk

With Elevated Access Management, enterprises can respond quickly and safely to urgent needs, planned absences, or project-based requests for privileged access while ensuring the auditability of activities performed.

A Complete Application Access Governance Product

Access Risk Analysis
Identify role conflicts and manage separation of duties (SoD) for all of your critical business applications

Compliant Provisioning
Onboard, manage, and remove user access efficiently to maintain regulatory compliance

Certifications
Reduce the effort - and cost - needed to manage access reviews

Elevated Access Management
Audit-ready privileged access via automated workflows

Role Management
Automate the manual efforts required to design, update, and maintain roles

About pathlock

Pathlock Cloud protects leading ERP systems and enterprise business applications and the critical transactions they power. Our Application Access Governance product helps companies enforce GRC controls and take action to prevent loss. Enterprises can manage all aspects of application governance in a single platform, including access risk analysis, user provisioning and temporary elevation, ongoing user access reviews, and audit preparation.

Take Action: Empower your organization with Elevated Access Management to secure privileged access effortlessly. Request a Pathlock Cloud demo today.

REQUEST DEMO

For more information, visit **www.pathlock.com »** or **get in touch »** with us for a demo.