Improving Efficiency in IT Administration via Automated Policy Workflows in UNIX/Linux
# Table of Contents

- Executive Summary ........................................................................................................... 3
- Efficiency is the Driving Catalyst ......................................................................................... 3
- Key Advantages in Automating Policy Processes ................................................................. 4
- Recommended Steps toward Developing a Policy Automation Framework ......................... 4
- Unifying Platform to Automate Privileged Access Policy Processes across UNIX/Linux .......... 7
  - eWorkflow ....................................................................................................................... 7
  - Access Control Solutions Include: Internal Security through Delegation of Elevated Privilege .................................................................................................................. 8
  - Segregation of Duties (SoD) using Forbidden Commands .................................................... 9
  - Keystroke Logging and Playback Support Real-Time Attack Prevention .............................. 9
- About BeyondTrust .............................................................................................................. 10
Executive Summary

The last few years have lived up to the prophecy of a tough year for everyone, personally and professionally. With the economies of the world in turmoil and economic indicators illuminating a cautionary yellow, IT infrastructures have been forced to tighten budgets and reduce staff resources to insufficient levels. Yet the need for sophisticated privileged access security is arguably greater than ever before.

New creative business practices have led to increased efficiency and productivity; however, these new procedures have introduced an increase in security risks. For example, organizations are embracing the use of contractors, auditors and other outside partners with the goal of reducing costs. Outsourcing is creating IT security risks, which can affect an enterprise’s financial health and reputation. Outsourcing is ultimately enabling outsiders to, in effect, become insiders, increasing the risk of security breaches.

Since 2005, official reports of data breaches have been on a rapid ascent. Data breach incidents have not just begun to occur the past few years, rather the requirement to disclose those events have given the public a first view into the nature and severity of the problem facing every organization.

Data breach incidents prior to these laws going into effect were nearly all uncovered as a result of fraud committed using stolen data, or via media leaks. The reality is access to IT resources, originally available to vetted employees, are now open to a new workforce that has a much higher turnover and is less visible. The technological ability to store data such as customer and patient details, product designs and financial information online, and access it over the network, puts a greater part of corporate assets in danger. With increased risk, stringent regulations, applied by both industry and government agencies, have turned up the heat on IT professionals to develop sound security policies that protect data, reputation, and documentation of those controls.

So how can IT reconcile the need to improve security in the face of today’s financial downpour? Luckily, the latest IT security developments using access control and recommended privilege access lifecycle management deployments may provide an unexpected silver lining to the economic storm clouds.

Efficiency is the Driving Catalyst

The explosive growth in global networked communication has exposed IT resources to new resourceful attacks, creating an unprecedented challenge for enforcing information security fundamentals while minimizing downtime and increasing efficiency among enterprises. The key factor that has driven organizations to adopt role-based access control (RBAC) for IT administration is efficiency. Using access control, such as RBAC, helps achieve efficiency in these three areas:

1. **Efficiency in enterprise process**: Companies must minimize the time it takes new hires to access the applications needed to fulfill their job responsibilities. In addition, organizations want to ensure employees have proper access to perform job duties, but not have escalated access that could create critical mistakes and expose/release data due to negligence or maliciousness.

2. **Efficiency in IT operations**: RBAC gives organizations the ability to manage a smaller number of IT roles, rather than respond to a multitude of granular access requests.

3. **Efficiency in audits and compliance**: Standardized access for every job function using RBAC reduces the effort level for all of the players within the audit/compliance process.
Key Advantages in Automating Policy Processes

**Security:** Privileged access is critical for smooth ongoing administration of IT assets. At the same time, this access exposes an organization to security risks, especially with regards to insiders. The right solution will provide centralized visibility into policies, as well as actions taken related to privileged access control. This will ensure that there is complete awareness of the security position at each stage of the policy automation process.

**Compliance:** In relation to critical business systems, privileged access can bring significant regulatory compliance risks. For example, the right solution should address Segregation of Duties via automated workflows for policy approvals. Also, having the ability to provide an audit trail across all stages of the policy management and usage processes is essential for compliance, and is often difficult to realize within large complex heterogeneous IT environments. A proper solution will aggregate audit trails across multiple systems to simplify and automate the audit review process for compliance support.

**Lower IT Costs / Reduce Complexity:** Providing effective privileged access management in large multi-platform environments with multiple administrators, managers and auditors, is a challenging feat. The right solution significantly reduces an organization's complexity and IT costs associated with a Privileged Access Lifecycle Management. A suitable solution will use a centralized automation platform for policy creation and event reporting for each stage of the lifecycle.

**Investment Protection and a Single-Point Solution for a Heterogeneous Environment:** The right solution provides privileged access across a broad range of platforms including Windows, UNIX/Linux, AS/400, Active Directory, databases, firewalls, and routers/switches.

Recommended Steps toward Developing a Policy Automation Framework

Adopting an appropriate enterprise-wide framework can be a big change for organizations. The following recommendations cover essential goals for enterprises to follow in order to simplify the arduous process:

Assemble Appropriate Panel: Assembling an appropriate panel to identify the processes, roles, and responsibilities to standardize is critical to success. A basic panel should consist of:

- Business Process Owners
- IT Application Owners
- IT Implementation Team
- Internal Risk Management Team
- Business Process Analyst
- Technical Writers

New actors will be introduced beyond the normal application owners, process owners, data owners, and business owners that you already have been identified.

Establish Well-defined Goals: **Define measurable and focused goals, which are agreed upon by all stakeholders involved** in the deployment.

Perform a Role-mining Assessment: Begin with an assessment of the organization's current identity and access management (IAM) projects in place, and review the current level of “role maturity” that is in place to ensure segregation of duties. A role-mining assessment can assist an enterprise in aggregating, correlating, and cleaning existing data. During this project, it is important to implement base roles for existing, new, and contracted employees. This includes applying role definitions to users who cross organizational boundaries, but need similar access. This will allow an enterprise to successfully manage sensitive privileges within a network.
ESTABLISH STANDARDIZED ENTERPRISE IT OPERATING PROCESSES

A role’s lifecycle is the same as a user’s lifecycle. It gets taken over, transfers, changes, affects others, gets promoted, evolves, or terminates. Enterprises need to define and document the business processes for privileged access lifecycle management, and map this process to automate. Automation is essential to preventing stagnate or inaccurate roles, which expose IT assets to potential breaches. Crucial processes that should be identified for include:

- New role creation
- Role change management
- Disabling roles
- New certifications
- Entitlement certifications
- Assigning role ownership

SELECT A COMPATIBLE SOLUTION

Think Out-of-the-Box
Taking new perspectives on IT security administration will ultimately help IT traverse the tradeoffs among security, budget, risks and business needs. Research will produce examples of the latest developments in IT security intended to help the enterprise improve access control to protect critical assets without breaking the bank, exhausting employees or preventing the organization from operating effectively.

Be Open to Innovation
When a mature, successful IT infrastructure is already in place, it is easy to take the “why tamper with success?” approach. Many IT organizations use the same infrastructure vendors year after year, spending more money each year, without ever investigating alternative and potentially more cost-effective solutions.

The following chart depicts some typical roles and responsibilities within a privileged access management framework:

<table>
<thead>
<tr>
<th>New Actors</th>
<th>Responsibilities</th>
<th>Qualifications</th>
</tr>
</thead>
</table>
| Role Administrator| • Create, modify, and decommission roles  
|                   | • Generate Reports                                      | Application Administrator or possibly someone from your access admin team |
| Role Engineer    | • Review role consolidation and impact analysis reports 
|                   | • Submit recommendations to role governance committee   
|                   | • Schedule recurring role composition reports            | Business Process Analyst with great verbal and written communications; highly organized |
|                   | • Submit recommendations to role owner for review and certification |
**New Actors**

<table>
<thead>
<tr>
<th>Role Owner</th>
<th>Responsibilities</th>
<th>Qualifications</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Initiate request for new roles or modification of roles</td>
<td>A person that holds the greatest degree of understanding about roles and entitlements. Likely a person auditors would deem responsible for the associated business processes and/or data</td>
</tr>
<tr>
<td></td>
<td>• Approve / certify roles</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Committee</th>
<th>Responsibilities</th>
<th>Qualifications</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Review role creation, modification, and decommission requests</td>
<td>A good balance of business and IT employees. (Also: consider a leadership positing with reporting responsibility to CFO and CIO)</td>
</tr>
<tr>
<td></td>
<td>• Assign/replace role owners</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Review of roles to ensure roles still map to business processes</td>
<td></td>
</tr>
</tbody>
</table>

**Think Integration**

Since IT generally purchases multiple solutions from various vendors, it is important to realize that integrated IT security solutions can dramatically reduce capital outlay. Integration also improves IT’s efficiency and lowers the management overhead of running multiple systems.

Choosing the right vendor is an integral part of the process. Reviewing vendors to ensure proposed solutions match the enterprise needs ensures that the road to automation is mapped out correctly.

**STANDARDIZE IMPLEMENTATION PROCESS**

A first-rate vendor will be available to the enterprise implementation team to ensure the solution is properly integrated into the enterprise network. Since planning the implementation is so essential, consider the following steps:

1. **Phase the rollout**
   
   a) Phased deployment delivers incremental wins and demonstrates ROI

2. **Pilot the change**
   
   b) The reality is that this is a substantive change for the organization and the employees. This transformation needs to be tactically approached so strategic goals can be achieved.

3. **Recruit a business process analyst**
   
   c) Business process analysts can provide the documentation and defined processes that reflect uniform standardization. This standardization is important for ongoing compliance.

4. **Measure, reassess, and report**
   
   d) Document the number of entitlements, accounts, users, dormant accounts and sensitive entitlements within the enterprise. Analyze these metrics again and again while implementing the roles and associated certifications.

5. **Develop naming conventions**
e) Work with implementation and governance teams to develop a role-naming convention that can be easily identified by the end users and auditors.

6. Measure ROI

f) Evaluate ROI in terms of IT administration and the managing, provisioning, and de-provisioning certifications.

7. Get the Communications Department involved

  g) The communications team can help develop a unified message and communicate it in a way that is appropriate to the enterprise. When communicating the final message, deliver the information in as many different methods as possible (e.g., email, intranet, policy/executive memos).

8. Be prepared for change

  h) With a privileged access lifecycle management model, an organization and the business processes involved will change significantly.

Unifying Platform to Automate Privileged Access Policy Processes across UNIX/Linux

The PowerBroker Servers Management Console (PBMC) provides the platform for automation featuring centralized management capabilities, streamlined policy change management workflows and incident alert workflows for multiple PowerBroker Servers installations through a convenient web interface. PowerBroker Servers integrates with the PowerSeries Management console to deliver the following:

- Automated workflows for policy creation and change management to comply with segregation of duties and security best-practices
- Automated workflows for event and I/O log reviews and acknowledgements, and centralized audit trails, for streamlined audit support and heightened security awareness
- Centralized management of multiple PowerBroker Servers master servers through a single web based management console with automated policy propagation, to simplify administration and lower costs in complex IT environments
- Automated log centralization for multi-server deployments, to streamline audit and compliance support and to reduce costs through consolidation of logging resources.
- A graphical policy editor for PowerBroker Servers users that have limited UNIX expertise (e.g. helpdesk professionals), to reduce administrative costs and accommodate flexible workflows.

eWorkflow

eWorkflow is the umbrella workflow automation platform included with the PowerBroker Servers Management Console, which facilitates workflows for specific tasks. eWorkflow is built on a Role-based Access Control (RBAC) framework, and currently offers two workflow classes:

1. Policy eWorkflow
2. Event eWorkflow
POLICY EWORKFLOW

Policy eWorkflow is a workflow class offered with the eWorkflow platform. Policy eWorkflow provides automated workflows for the creation or editing of policies, review and approval of policy changes, and centralized deployment of approved policies for products integrated with the PowerBroker Servers Management Console. Policy eWorkflow utilizes a Role Based Access Control (RBAC) framework, is administered through an intuitive web interface, and offers configuration flexibility to adapt to organization-specific policy review and approval requirements.

Policy eWorkflow helps customers to achieve compliance through an automated framework for segregation of duties, and helps uphold security best-practices through enhanced controls for policy changes. Policy eWorkflow also drives accountability through detailed logging and audit-ability of all policy approvals.

EVENT EWORKFLOW

Event eWorkflow is a workflow class offered by the eWorkflow platform. Event eWorkflow provides automated workflows for the centralized aggregation of events (e.g. commands being issued) and actions being taken by privileged users on products integrated with the PowerBroker Servers Management Console. It also provides a detailed review of such events and actions by designated resources, and an archive of event and review data. Event eWorkflow utilizes a Role Based Access Control (RBAC) framework, is administered through an intuitive web interface, and offers configuration flexibility to adapt to organization-specific event and I/O review requirements.

Event eWorkflow helps customers to achieve compliance through an automated framework for Segregation of Duties, and helps uphold security best practices through enhanced controls over policy changes. Event eWorkflow also drives accountability through detailed logging and audit-ability of all event reviews.

PBMC VIEW LOG

eWorkflow is an extensible platform. In the future, eWorkflow will include additional workflow classes (e.g. System Management eWorkflow). Additionally, the PBMC will integrate with additional product lines, extending existing and future capabilities of eWorkflow beyond PowerBroker Servers.

eWorkflow provides customers with heightened security awareness and control, facilitates compliance through segregation of duties, and increases administrative efficiency while reducing costs.

The PowerBroker Servers Management Console lowers the cost of managing security, and simultaneously improves operational performance through enhanced application integration. With PBMC, IT administrators can now configure and manage hundreds-to-thousands of multi-platform systems in a fraction of the time it would usually take to perform traditional security implementations.

UNIX/LINUX ROOT ACCESS CONTROL

While limiting authorization, PowerBroker Servers provides access control through delegation of elevated privilege on UNIX/Linux systems. By binding each administrator's user ID to their assigned tasks, PowerBroker Servers allows system administrators to perform their duties without ever having the root/superuser password. PowerBroker Servers also protects systems and applications by only allowing them to be used by individuals who have been granted authority to use them. Using its flexible policy language, PowerBroker Servers can enforce access policies that apply to the entire organization. With PowerBroker Servers, enterprises can centrally manage authorization and privilege across complex multi-platform UNIX/Linux networks.

Access Control Solutions Include: Internal Security through Delegation of Elevated Privilege

Because PowerBroker Servers delegates elevated privilege by binding a task to a UNIX/Linux User ID, the password to
the elevated privilege account is never revealed. PowerBroker Servers thus enables a group of individuals to perform administrative tasks without using a shared account. Binding specific high-security tasks to User IDs in advance also disposes of the need to share passwords of superuser accounts in a “firecall” situation, or when the senior administrator is unavailable.

POLICIES ALLOW HIGHLY GRANULAR, CUSTOMIZABLE ACCESS CONTROL

A single PowerBroker Servers policy can implement a corporate security mandate across complex heterogeneous UNIX/Linux networks throughout the organization. Other PowerBroker Servers policies can be used to enforce access control with precise granularity.

PowerBroker Servers policies prevent insider attacks by limiting the route an access request can take. For example, a PowerBroker Servers policy could specify that requests to run a program that retrieves credit card data from a dataset could be submitted from a server in accounting, but not from any other server. This prevents an insider, with credentials for the database, from running the program from a server in his work area or any remote server.

**Segregation of Duties (SoD) using Forbidden Commands**

Insider attacks by senior administrators can be significantly reduced via segregation of duties. This is done by restricting access to the most powerful superuser commands through the creation of logical groups of these commands to one senior administrator, but unavailable to all other employees. This ensures no administrator has all the commands needed to perform a breach.

**Keystroke Logging and Playback Support Real-Time Attack Prevention**

PowerBroker Servers provides real-time keystroke logging and playback. This functionality allows senior administrators and internal auditors to do random “spot checks” of user activity, and play back any keystrokes that indicate inappropriate activity. Creating an environment of accountability is a good deterrent to insider threat.
About BeyondTrust

With more than 25 years of global success, BeyondTrust is the pioneer of Privileged Identity Management (PIM) and vulnerability management solutions for dynamic IT environments. More than half of the companies listed on the Dow Jones Industrial Average rely on BeyondTrust to secure their enterprises. Customers include eight of the world’s 10 largest banks, seven of the world’s 10 largest aerospace and defense firms, and six of the 10 largest U.S. pharmaceutical companies, as well as renowned universities. The company is privately held, and headquartered in Carlsbad, California. For more information, visit beyondtrust.com.

**CONTACT INFO**

<table>
<thead>
<tr>
<th>NORTH AMERICAN SALES</th>
<th>CORPORATE HEADQUARTERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.800.234.9072</td>
<td>550 West C Street, Suite 1650</td>
</tr>
<tr>
<td><a href="mailto:sales@beyondtrust.com">sales@beyondtrust.com</a></td>
<td>San Diego, CA 92101</td>
</tr>
<tr>
<td>EMEA SALES</td>
<td>1.800.234.9072</td>
</tr>
<tr>
<td>Tel: + 44 (0) 8704 586224</td>
<td></td>
</tr>
<tr>
<td><a href="mailto:emeainfo@beyondtrust.com">emeainfo@beyondtrust.com</a></td>
<td></td>
</tr>
</tbody>
</table>

**CONNECT WITH US**

Twitter: @beyondtrust
Facebook.com/beyondtrust
Linkedin.com/company/beyondtrust
www.beyondtrust.com