Bravura Security

5 Point Checklist for Securing AI Assistant Identities

Artificial intelligence (AI) has become a critical component of many organizations' operations. AI can analyze large datasets and automate repetitive tasks to enhance decision-making processes. AI assistants, advanced software agents, aid in executing tasks and provisioning services in various environments. In educational and financial institutions or businesses they streamline information access, administrative tasks, and customer interactions. However, as AI becomes more integrated into our systems, the need for robust Identity and Access Management (IAM) strategies for AI assistants and their identities becomes crucial.

EXECUTIVE SUMMARY | SECURING YOUR DATA BY EFFECTIVELY GOVERNING AI

- ☐ Know what you have: conduct an AI policy review and add AIs to your Identity Inventories.
- ☐ Ensure Ownership: assign ownership with accountability or liability policy.
- ☐ Provision limited access accounts for use in AI Assistants.
- ☐ Certify AI Assistants periodically.
- ☐ Review AI Assistant transfers when people transfer or leave the organization.

1 INVENTORY INCLUSION

The first step in governing AI identities is to acknowledge their existence within your network.

- ☐ **Know Your AI Entities:** Create an inventory that includes all AI tools and assistants. Just as you would with human identities, ensure you have a comprehensive list detailing each AI's purpose, capabilities, and access levels.

2 OWNERSHIP & ACCOUNTABILITY

With AI identities inventoried, it's crucial to establish clear ownership.

- ☐ **Assign Responsibility:** Determine who within the organization is responsible for each AI identity. This could be a team or a specific individual.
- ☐ **Know Your AI Entities:** Create an inventory that includes all AI tools and assistants. Just as you would with human identities, ensure you have a comprehensive list detailing each AI's purpose, capabilities, and access levels.

3 ACCESS CONTROL

Once ownership is established, the next step is access control.

- ☐ **Provisioning:** Create limited access accounts, ensuring AI identities have only the access necessary to perform their functions. This limits the potential damage.
- ☐ **Principle of Least Privilege:** Implement the principle of least privilege for all AI identities, regularly reviewing and updating access as needed.

4 CERTIFICATION & COMPLIANCE

Like any component in your IT environment, AI identities must be certified and compliant.

- ☐ **Regular Audits:** Certify your AI assistants periodically to ensure they are operating within the established guidelines and have not been compromised.
- ☐ **Compliance Checks:** Ensure that AI tools comply with all relevant regulations and standards, which may include GDPR, HIPAA, or others depending on your industry.

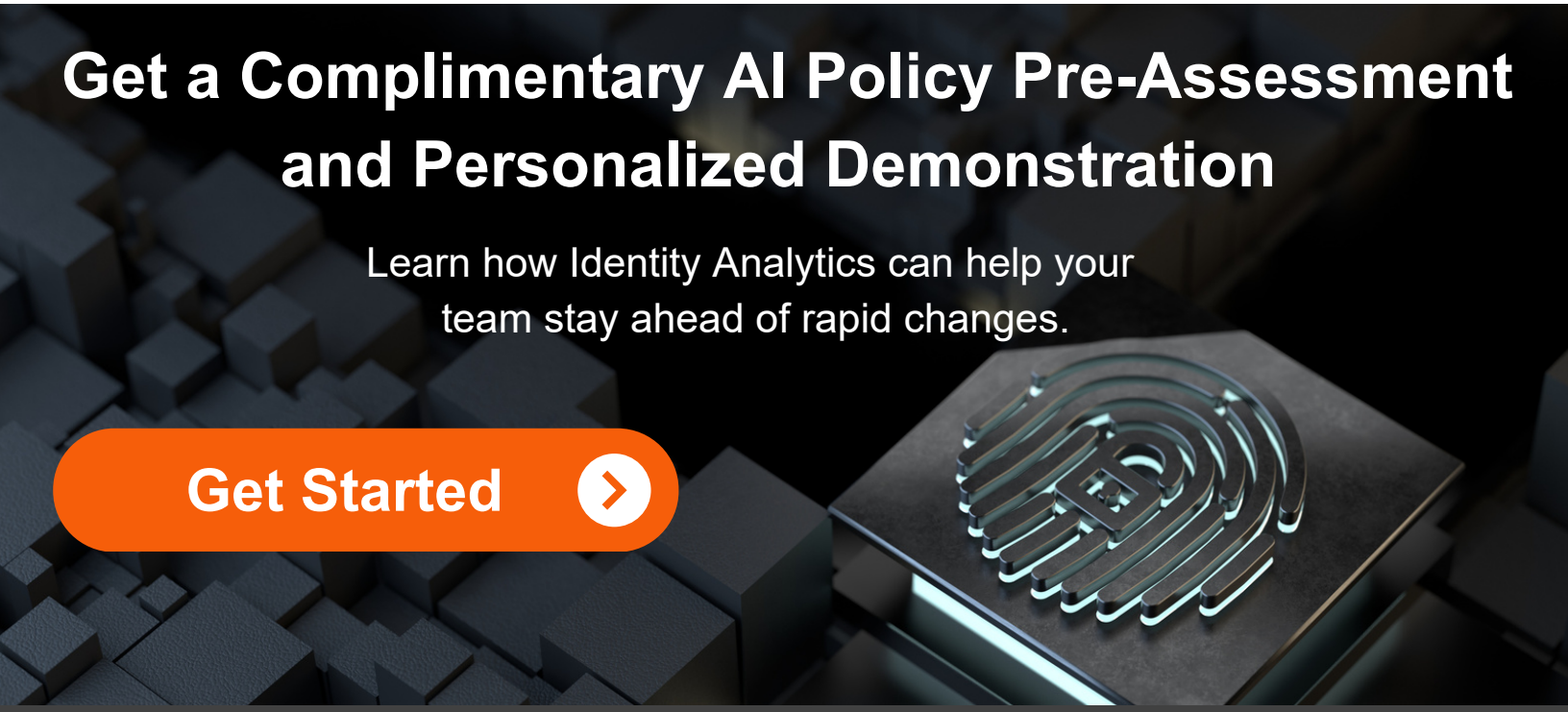
5 TRANSITION MANAGEMENT

AI identities require ongoing management, particularly when organizational changes occur.

- ☐ **Employee Movement:** When individuals leave or transition within the organization, review the AI identities they managed. Reassign ownership and adjust access as necessary to maintain security.
- ☐ **Continuous Monitoring:** Establish processes for continuous monitoring of AI activities to detect and respond to any anomalous behavior promptly.

EVOLVE YOUR IAM STRATEGY WITH THE CHANGING AI LANDSCAPE

An AI Policy Review can refine an organization's IAM and PAM strategies by identifying gaps and ensuring alignment with current security standards. Leveraging Identity Analytics enhances this process, providing data-driven insights for optimizing access controls and mitigating security risks efficiently. Stay informed, stay vigilant, and ensure your IAM strategy evolves with the changing landscape of AI technologies.



bravurasecurity.com
1-877-386-0372 / 1.877.495.0459
sales@BravuraSecurity.com

Bravura Security

© 2024 Bravura Security, Inc. All rights reserved. All other marks, symbols and trademarks are the property of their respective owners.