



Revolutionize your digital identity program with Bravura Identity. Easily enforce security and cross-platform access policies, while upholding the principles of least privilege.

DATA SHEET

Bravura Identity

Manage and govern identities, groups, and access to systems and applications all from one comprehensive solution — Bravura Identity. Implemented with industry-standard best practices including automation, self-service, certification, workflow, and analytics, Bravura Identity can revolutionize your identity and access management (IAM).

With more than 150 built-in reports, dashboards, and analytics, Bravura Identity can discover, detect, and proactively remedy entitlement and identity challenges like orphan and dormant accounts, segregation of duties (SoD) violations, out-of-band access accumulation, and more. It can keep your systems, data, and applications secure while proactively enforcing crossplatform access policies and upholding the principles of least privilege.

Bravura Identity moves access changes out of the IT department and into the hands of business users with a mix of automated business processes and request approval workflows so users can increase productivity and save time. It includes the industry's largest number of connectors to simplify integration applications and manage accounts, groups, and entitlements on-premises and in the cloud.

Bravura Identity is part of the Bravura Security Fabric. By enabling Bravura Identity, Privilege, and Pass within this security fabric, you can easily weave access patterns as your access management program evolves without having to install separate solutions.

Real-Time Automation to Govern Identity at Scale

The first step to digitally transform identity administration and manage access churn effectively is automation. Bravura Identity does so in real time as your organization administers and governs identities at scale. Automated identity administration turns access certification into a spot check to ensure Bravura Identity is operating as expected.

With Bravura Identity, intelligent automation grants access where the business need is predictable. A robust authorization workflow invites all of the right people to approve access requests, typically all at once rather than one at a time. This faster parallel authorization process shortens provisioning. Automated connectors provision and grant access without waiting for human intervention, so users have access before or as they need it. The result is anticipatory, revoked-on-time, and in-compliance access.

BEST-IN-CLASS SOLUTIONS. ONE MODULAR SECURITY FABRIC.

Automate compliance while managing identities, security entitlements, and credentials, for both business users and privileged accounts, on-premises and in the cloud. Our best-in-class solutions have helped banks, universities and Fortune 500 companies around the world protect their companies over the last two decades against increasing cybersecurity threats.

Bravura Pass Plus

Take back control of organizational passwords and give users the ultimate convenience of forgetting their passwords forever. Give organizations revolutionary control of all passwords with one-click re-secure for instant breach protection.

Bravura Pass

Simplify credential management across multiple systems and applications with password synchronization, self-service password reset, strong authentication, federated access and security questions.

Bravura Safe

Beyond SSO and privilege, safely vault and auto-fill decentralized secrets and password allowing seamless logins from all trusted devices. Detect weak passwords and safely share credentials.

Bravura Privilege

Frictionless, time-limited privileged access to reduce IT security risk and enhance accountability. Facilitate password randomizations and authorize access with a highly available, geo-redundant solution.

Bravura Cloud

More than a tool, it's a strategic partner to deliver security insights to enhance and maintain secure, efficient, and compliant security operations.

Correlate Access Rights to Business Responsibilities

All users should only have the access they need. More creates unnecessary risk. Less interferes with legitimate use of systems and applications. This precise balance, the principle of least privilege (PoLP), can be hard to accomplish.

Bravura Identity helps organizations link access rights to the appropriate business context and minimize the gap between the actual and minimum level of access individuals need. Access requests include a rationale as to why specific access is appropriate for a given user. In contrast, access certification can be used to review which access rights a user has or the role granting the access while removing entitlements that no longer make sense. The result is automatic access for users to do their jobs without additional hurdles.

Align Access Controls and Processes

Weak application access controls mean that entitlements may violate the segregation of duties (SoD), risk, or other security policies and can be challenging to trace. Bravura Identity strengthens application access controls, monitors both systems of record, including HR and integrated applications, such as Active Directory. It responds to changes by propagating them to other systems, requesting approval, or revocation. It enforces access policies, blocks violations at request time and proactively monitors for and detects violations that occur out-of-band. An access certification process invites stakeholders to review and correct entitlements, role definitions, and identity attributes. It enables organizations to define controls, prevent users from acquiring toxic combinations of entitlements, and detect pre-existing violations. This prevents malicious users from bypassing controls to commit fraud or data breaches.

Prevent Fraud and Data Breaches

Focus limited audit and control resources to have the most significant impact. Bravura Identity empowers organizations to rank users by how much risk their access rights pose. It adds controls and surveillance precisely on users that can cause the greatest harm.

The robust segregation of duties policy engine enables organizations to define controls, prevent users from acquiring toxic combinations of new entitlements, and detect users who had pre-existing violations. This prevents malicious users from bypassing internal controls to commit fraud or data breaches.

The focus of regulatory compliance legal requirements such as SOX, HIPAA, GLB, FDA 21-CFR-11, GDPR, and PIPEDA, and standardized security controls, such as ISO 27001/27002 are decidedly different. Nonetheless, they share common threads, such as the need for healthy internal controls for access to sensitive systems and data coupled with potent privacy protection.

While it is organizations, not software, that must comply with these regulations, Bravura Identity provides various capabilities that help organizations meet these objectives. It includes mechanisms that ensure access is business appropriate. It helps organizations manage identities, entitlements, and credentials securely so that authentication, access authorization, and audit functions can enforce the right rules at the correct times to support security, governance, privacy protection, and ultimately, regulatory compliance.

Empower Auditors to Answer Their Own Questions

Bravura Identity enables auditors to run reports without assistance from access administrators to expedite audits and reduce the IT administration workload. Access certification offloads individual user and entitlements review to managers and data owners, rather than auditors who may lack adequate business context to assess suitable access rights. With effective process automation, auditors can focus on how the process works, rather than on individual access rights.

Bravura Identity Reviews

By Bravura Security in Identity Governance and Administration

4.4 ★★★★★ 33 Ratings

"Easy interface to handle the product. Easy handling and user friendly experience. Love this product and want to work more on it."

"This product has allowed us to give access to a suite of tools across a huge fleet of remote workers. The ability to deploy policy based authentication has helped ease the burden of many user requests."

"Bravura Identity management suite is above average. Products effectively do threat identification, credential management, and identity protection across our organization. The deployment process was smooth and was completed as per committed timeline."