Bravura Security

Reduce IT security risk and enhance authorized access and accountability with the frictionless, time-limited privileged access of Bravura Privilege.

DATA SHEET

Bravura Privilege

Provide frictionless, elevated, and time-limited access to reduce IT security risk and enhance accountability with Bravura Privilege. Our privileged access management (PAM) solution supports millions of daily password randomizations and facilitates access for thousands of authorized users, applications, and systems through a highly available, geo-redundant architecture. Use Bravura Privilege to create accountability through an audit trail of privileged sessions for every account. Access and session data can be surfaced through custom reports to gain valuable insight.

As part of the Bravura Security Fabric, a singular IAM platform and framework, Bravura Privilege can integrate with every client, server, hypervisor, database, and application, on-premise or in the cloud. Working within a singular security fabric, you can easily weave access and privilege patterns by combining services as your access management program evolves without installing separate solutions.

Enable Robust Access Control Policies

Bravura Privilege provides access to shared accounts and elevated group memberships based on flexible, robust, and easily managed access control policies. High-frequency users can be pre-authorized based on group memberships or identity attributes without waiting for approvals, while infrequent users might require approval from their supervisor or other stakeholders.

Securely Store Credentials

When passwords are changed regularly, an encrypted vault prevents unauthorized disclosure and ensures maximum availability when faced with a site outage. Bravura Privilege includes a unique, geographically distributed active-active architecture that replicates this critical data set in real time across all instances for high-availability and disaster recovery scenarios.

Randomize Privileged Account Passwords

As the scope of an organization’s IT assets grows — sometimes with thousands of privileged accounts across a wide variety of platforms — it can become increasingly difficult to securely manage those assets. Coordinating password changes or tracking changes back to individuals can be even more painful without a privileged access management (PAM) system. Bravura Privilege replaces shared and static passwords tied to privileged accounts with periodically new and random values based on robust password policy controls. It can enforce multiple scheduled or event-triggered password policies on fixed IT assets, laptops, and rapidly provisioned virtual machines.

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

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

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 Safe

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

Bravura Identity

Identity administration and access governance with full process automation, on-premises and in the cloud.

Get Just-in-Time Access

Bravura Privilege customers can take just-in-time (JIT) access to the next level incorporating create, read, update, and delete (CRUD) operations and group elevation as part of a privleged access session strategy. Bravura Privilege supports creating, updating, and deleting privileged accounts and groups to help customers achieve the principle of Zero Standing Privileges (ZSP) where and when it makes sense.

Ensure Administrator Accountability

IT staff often manage the highest privilege accounts using generic login IDs without administrative change auditability and accountability. Bravura Privilege randomizes administrator passwords frequently, so each password is different, changes over time, and is not known. It mediates logins to these accounts, requiring that users be personally identified, strongly authenticated, and specifically authorized for access. Shared account use with elevated privileges is linked to individual IT staff to create strong accountability.

Generate Forensic Audits of Privileged Logins

In rare instances, staff may be suspected of causing harm. When this happens, it is helpful to see what the user did while connected to privileged accounts. Audit logs can support forensic analysis where policy may dictate that login sessions be recorded for vendor access, to high-risk systems, or to systems in certain jurisdictions or processing certain kinds of data. Bravura Privilege can record keyboard input, take a picture with time and day stamp info, and collect other data keys for forensic audits, internal knowledge sharing, and training. Session recording, search, and playback provide a high level of accountability. Recorded sessions are secured through a combination of access control policies and workflow approvals, designed to safeguard user privacy.

Discover SSH Trust Relationships

Discover and analyze existing SSH trust relationships and create temporary access to build a trust graph to prevent unauthorized access. Trust graph analytics, in turn, can identify high-risk accounts and disable unnecessary trust relationships.

Gartner
Peer Insights™

Bravura Privilege Reviews

By Bravura Security in Privileged Access Management

4.4 ★★★★★ 21 Ratings

"Very helpful to eliminate static passwords and great to manage Elevated Windows admin passwords. The user interface is easy and robust."

"I loved the ease and speed at which we were able to deploy this."

"Bravura Security has been a good partner. They are very responsive to support requests, provided a strong partner resource to assist us with the implementation, and make a good product with a considerable number of features."

"Bravura Security Privileged Access Manager secures access to elevated privileges. It is very useful to eliminate shared and static passwords for privileged accounts. Also, it enforces strong authentication and reliable authorization prior to granting access."

"Bravura Privilege creates strong accountability, strong authentication with strong authorization prior to granting access. It provides very good reliability while ensuring continuous access to shared accounts and security groups."

Easily Scale Up

In large organizations with rapid account turnover, manual configuration is impractical. Bravura Privilege offers advanced infrastructure and auto-discovery monitor systems of inventory, apply management rules, and probe for accounts, groups, and services. Organizations can set policies for account management and classification, enabling effortless scaling.

Manage Personal Administrator Accounts

Many organizations assign secondary accounts to administrators who have elevated privileges. These accounts are used to carry out administrative tasks and minimize excessive privileges on regular accounts. However, these accounts must also be managed. Bravura Privilege ensures that personal admin accounts are assigned to their rightful owner and can be restricted to their intended purposes without getting in the user's way.

Delegate and Maintain Tight Policy Control

Designed with empowerment in mind, Bravura Privilege features a team-centric framework that enables resource owners to onboard and offboard servers, accounts, and colleagues for whom they are responsible.

Learn more about Bravura Privilege