

Protect identities, systems and data from malicious attacks with resilient, automated processes paired with a singular identity, privileged access and password platform with built in threat detection and response.

DATA SHEET

Bravura Security Fabric

Compromised passwords remain the top cause of breaches and attacks. Reduce the risk in shadow IT by securing the hundreds of employee passwords, secrets, and files outside your onboarded IAM program. Bravura Safe centrally and securely manages decentralized passwords, secrets, and files, including time-bound passwords and encryption keys, for everyone in your organization.

The Bravura Security Fabric empowers organizations to better navigate this difficult terrain with a resilient, flexible, single identity and access management (IAM) platform and framework. The Bravura Security Fabric has the technological and architectural building blocks with decades of proven reliability to protect, manage and govern your entire digital identity and access infrastructure from malicious attackers.

The Bravura Security Fabric is a singular, powerful framework and platform that brings together all of the layers of Bravura, including Identity, Privilege, Pass and Group plus a threat detection and response (TDR) layer: Bravura Discover.

The Bravura Security Fabric creates a centralized view to weave patterns of functionality your organization needs so it's protected against continual threats and all aspects of your identity and access security program are covered. As you uncover new identity and access threats or your roadmap evolves, turn services on or off as needed without installing other products to improve IT security, support internal controls and regulatory compliance, and lower access administration and costs.

Move Faster Against Cyber Threats

Progressively sophisticated hacking makes it more difficult to defend your organization against fast moving attacks. Cyber-criminals now share tools, software and frameworks within global hacking communities. The new kind of hacker uses software to scrape publicly available information and create a structured overview of an organization's vulnerabilities. Automated tools let hackers move faster to exploit your organization's vulnerabilities.

Instead of manual methods, combat automated attacks with security automation to win against hackers. Automated and tested processes will result in fewer mistakes and lower risk to your organization.

The Bravura Security Fabric automation-first approach gives you agility and flexibility to accurately configure your identity and access solution. Provide continual protection with a singular platform and an automation-first approach to secure your systems faster and more effectively than access certification and individual products.

Bravura Identity

Revolutionize your digital identity program with Bravura Identity. Implement the best-in-class solution to enforce security, cross-platform access policies, and uphold the principles of least privilege.

Bravura Privilege

Reduce IT security risk and enhance accountability with frictionless, time-limited privileged access. Bravura Privilege facilitates millions of daily password randomizations and authorizes access with a highly available, geo-redundant solution.

Bravura Pass

Improve login security processes and simplify credential management for passwords, tokens, smart cards, security questions and biometrics management across systems and applications with Bravura Pass.

Bravura Safe

An easy-to-implement enterprise password safe that centrally, consistently, and securely manages decentralized passwords, secrets, and files to protect against cyberattacks. Employees can securely send time-bound passwords for new accounts, encryption keys for files, or entire files without them being leaked or intercepted.

Bravura Discover

Bravura Discover delivers a powerful risk and threat assessment for both IAM and PAM solutions to get your organization on the right track—quickly. Its automated discovery analysis takes just a day to provide the most accurate data to close identity and privileged access security gaps with confidence by removing the potential for human error or intervention.

Discover Risks Below the Surface and Automate Solutions to Strengthen Governance

Security is an ongoing process that begins with discovering weaknesses and automating the repairs to potentially exploited areas. Implementing automation enables quick protection for your identity and access solution, while focusing on discovery helps you detect potential attacks before they even happen.

The Bravura Discover TDR, an integral layer of the Bravura Security Fabric, reveals your changing risks and threats (including the ones below the surface) with the most accurate, fastest, and in-depth TDR report for both identity and privileged access.

When implemented as part of your Bravura Security Fabric, it also helps to structure your existing services, show the gaps and reveal duplicated services. This helps optimize investments and improves security on a continual basis. It provides Managed Detection & Response (MDR) by identifying all of your systemic risks upfront and providing a holistic recommendation.

Invest In an Open, Flexible and Unified Security Fabric

With cybersecurity protection challenges constantly emerging, your organization will require a flexible approach to IAM. Bravura Security Fabric offers sturdy and mature automation and detection; governance and compliance; analytics and reporting capabilities are expertly designed for organizations with even the most complex requirements.

Leveraging the Bravura Security Fabric as the central structure for all IAM solutions simplifies vendor selection and program deployment. It also streamlines service level agreements and lowers overall cost to create a reliable identity and access program. The Bravura Security Fabric offers a single platform with open architecture and shared connectors across all products allowing flexibility to easily scale. has the industry's largest organically grown portfolio of connectors and a robust API platform to integrate any system to complete a robust security strategy.

Use Proven Patterns for Faster Time to Market

With more than 20 years of deep domain experience and countless custom deployments for Fortune 500 companies around the world, the Bravura Security team has honed in on how to deliver faster time to value. Bravura Security has used these best practices to develop the Bravura Security Fabric Patterns. These patterns are strengthened with tried and true best practice processes, policies, and metadata common to particular industries and solutions. They reduce time, cost and risk for IAM deployments from months to days.

The Bravura Security Fabric Patterns lets organizations automate a more comprehensive set of identity lifecycle processes up front, such as onboarding, deactivation, access reviews, transfers, leaves of absence, name changes, rehire detection, and more. This allows more flexibility than starting with one or two processes and building over time. The Bravura Security Fabric Patterns are optimized for fast service and robust internal controls to improve on the legacy processes to create a more efficient implementation.

MINIMUM REQUIREMENTS

Type	
Processor	<ul style="list-style-type: none">• Intel Xeon or similar CPU. Multi-core CPU, Dual core.
Memory	<ul style="list-style-type: none">• 16GB RAM – 32GB or more per server
HD	<ul style="list-style-type: none">• 600GB HD storage in an enterprise RAID configuration
OTHER	<ul style="list-style-type: none">• Gbit Ethernet NIC. Windows Server 2019 (Version 10.0.17763.1397) including updates to 09-2020. Docker version 19.03.11 or higher.



Click [here](#) to learn more about Bravura Security Fabric.

Bravura Security, Inc.

Corporate Headquarters
1401 - 1st Street S.E., Suite 500
Calgary, Alberta, Canada T2G 2J3
bravurasecurity.com

Contact Information
1.403.233.0740
Sales Toll Free: 1.877.386.0372 / 1.877.495.0459
sales@BravuraSecurity.com

© 2022 Bravura Security, Inc. All rights reserved.

All other marks, symbols and trademarks are the property of their respective owners.