BRAVURA PASS · WHITE PAPER

Password Management for the Passwordless Era

Passwordless for Your People. Managed for Your Enterprise.

Across cloud, SaaS, on-premises, legacy, and mainframe systems, Bravura Pass turns credentials into a managed enterprise service. Your people get a passwordless experience while IT keeps verified control everywhere passwords still live.



Contents

Two parts. Part one sets out the problem: why passwords persist, what they cost, and where the passwordless path meets a hybrid estate. Part two shows how Bravura Pass solves it, and what the business case looks like.

Executive summary 03

PART ONE: THE PROBLEM PASSWORDS STILL CAUSE

Why passwords persist 05

Why credentials still overwhelm the enterprise 05

The threat and compliance landscape 06

The passwordless future and the hybrid present 07

From user effort to enterprise command 08

Technical challenges that still break password management 09

PART TWO: HOW BRAVURA PASS SOLVES IT

Inside Bravura Pass 11

The Bravura Security connector library 14

Architecture and resilience: passwords as a service 14

How Bravura Pass compares 15

The business case, and an upgrade path without disruption 16

Where this matters most, and rapid, provable recovery 17

Key takeaways and conclusion 18

About Bravura Security 19

Talk to us 20

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

EXECUTIVE SUMMARY

Federated single sign-on consolidated a great deal of access. It did not consolidate everything.

Much of your cloud and SaaS estate now authenticates through one identity provider. A stubborn tail of systems sits outside single sign-on: on-premises and legacy applications, non-SSO tools, mainframes, and the directories and privileged accounts underneath. Each one still depends on a credential you have to manage.

That tail costs you twice. It floods the help desk with reset tickets. It also leaves a door open: credential abuse remains one of the most common ways attackers get in. Federation raises the stakes further. When a single identity provider unlocks everything, the credentials behind it and beyond its reach matter more, not less.

The passwordless future is arriving fast. Yet most organizations live in a hybrid present. You need both served at once. Bravura Pass does that. It turns passwords into a managed enterprise service. Credentials are created, rotated, and synchronized automatically to each user's Bravura Safe, retrievable from anywhere. Your people get a passwordless experience. IT keeps verified, policy-driven control.

A secure, encrypted vault sits at the center of that service. Bravura Safe stores and delivers credentials under policy. Lifecycle automation and enterprise-wide resets hand users the right credential safely, with no manual handling.

39%
of breaches involve credential abuse somewhere in the attack chain

48%
of breaches now involve ransomware, up from 44% the previous year

Up to 85%
reduction in password-related help desk volume with Bravura Pass

Sources: Verizon 2026 Data Breach Investigations Report; Bravura Pass data sheet, bravurasecurity.com.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.



PART ONE

The problem passwords still cause

Why passwords persist, what they cost you, and where the passwordless path meets a hybrid estate.

Why passwords persist

The industry is moving to passwordless authentication. Passwords, however, will remain in service for years, for several practical reasons.

They cost far less to deploy and support than most alternatives. They back up stronger factors when a token is lost or a phone is left at home. And many legacy, on-premises, and non-SSO systems still expect a password and cannot accept anything else. Mainframes, where you run them, are no exception.

Expectations have changed on both sides of the login. Users want access without the friction of remembering and typing credentials. Security teams want passwords off the table as an attack surface. Both groups are right. The challenge is serving both while passwords still run parts of your business.

Bravura Pass resolves this. It removes the password from the user's experience without pretending the password has left your systems. Behind the scenes, credentials stay under enterprise control: created, synchronized, rotated, and recovered automatically.

Why credentials still overwhelm the enterprise

Password problems are not small inconveniences. They slow people down, bury support teams, and open real exposure points for attackers. Four pressures compound the problem.

The Help Desk Tax

Our customers describe the same pattern before deployment. DTCC fielded a high volume of password calls from 3,800 internal and 80,000 external users, and a large bank was handling tens of thousands of password reset calls a month, enough to break its help desk service levels (Bravura Security case studies, bravurasecurity.com/aboutus/casestudies). Each reset ticket is a productivity loss for the user and a cost for IT, repeated thousands of times a year.

The Breach Exposure

Credentials remain one of the attacker's favorite keys. When users juggle many passwords, they reuse them, write them down, and pick weak values. Each shortcut widens the opening. When a breach hits, slow or manual credential recovery turns a contained event into a prolonged one.

The Hybrid Sprawl

Each system outside single sign-on adds another credential to manage and another point of failure. Each one enforces its own rules for length, complexity, expiry, and reuse. Keeping them aligned by hand does not scale.

The Compliance Burden

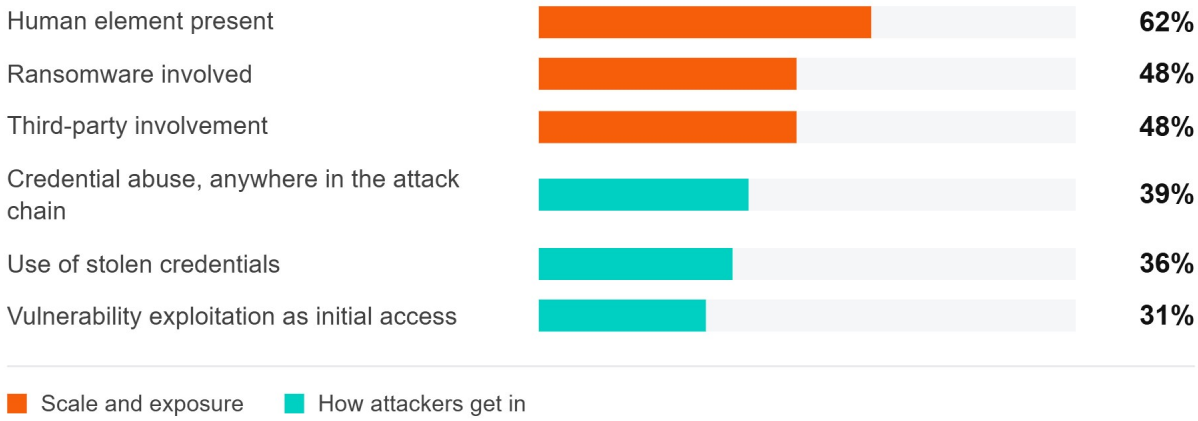
Regulators expect audit-ready evidence that credentials are controlled. You must prove who reset what, when, and under what authority, across the whole estate, not just the systems inside a single vendor's ecosystem. Fragmented tools make that proof expensive to assemble.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

Credential abuse is still the leading vector across the full attack chain

The numbers explain why identity security budgets keep growing, and why recovery speed now matters as much as prevention. Exploitation of vulnerabilities is now the most common initial access vector. Counted anywhere in the attack chain, credential abuse still leads. Among third parties, weak passwords and permission misconfigurations took almost eight months to reach 50% remediation.

Share of breaches, Verizon 2026 DBIR



The lesson

The lesson is not that credentials stopped mattering. Attack entry points are shifting, yet credential abuse is still the overall leading vector. And the credential weaknesses that linger, especially across third parties, take the longest to close.

Compliance pushes the same way

NIST SP 800-63B-4, PCI DSS v4.0.1, HIPAA, and ISO 27001 expect strong password policy, verified identity, and audit-ready records. Identity Threat Detection and Response is gaining ground for real-time anomaly detection, session termination, and automated containment. Identity security has become a board-level priority. Buyers increasingly want one platform that unifies self-service reset, strong authentication, breach response, and compliance, rather than a drawer full of point tools.

Source: Verizon 2026 Data Breach Investigations Report, pp. 10, 11, 12, 16, 20, 29 (verizon.com/dbir).

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

The Destination: Passwordless

Passwordless authentication is the right direction. When users authenticate with phishing-resistant factors instead of typing a secret, phishing loses most of its power. Login gets faster. The password stops being something a person has to remember, reuse, or leak.

Bravura Pass delivers that experience now. Users authenticate with strong factors and integrated multi-factor methods. They stop thinking about the password behind the scenes.

This also changes the help desk. Password resets are among its largest workloads: DTCC cut reset calls by over 25% and moved four of twelve support staff to other work (DTCC case study, bravurasecurity.com). Remove the password from the user's experience, and that queue shrinks sharply. The desk stops running on reset tickets and gets time back for real problems.

More important, the help desk stops being a target. Attackers social-engineer support staff into resetting a password or an MFA factor to hijack an account. The Verizon 2026 DBIR records attackers impersonating help desk agents, or users needing a password reset, and finds phone-centric social engineering 40% more successful than email (pp. 16, 50). When recovery runs on automated self-service and verified factors, that human-in-the-loop opening narrows.

Bravura Pass also lets support teams assist users without elevated privileges. Fewer people hold the power to reset a credential, so insider risk drops and the attack surface around the help desk keeps shrinking.

The Reality: A Hybrid, Password-Reliant Estate

Most organizations cannot flip a switch and retire every password. Critical systems still depend on them: legacy line-of-business applications, non-SSO tools, older directories, and, in some sectors, mainframes. A strategy that waits for the last password to disappear leaves those systems exposed for years.

Bravura Pass meets that reality head-on. It manages the full password lifecycle across every connected system, so the credentials you cannot yet remove stay strong, synchronized, and recoverable. You move toward passwordless at your own pace, without leaving the rest of the estate unmanaged.

This is the balance that matters. Lead with the passwordless experience for your people. Keep enterprise-grade control over the passwords that still exist. Bravura Pass gives you both from a single platform.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

FROM USER EFFORT TO ENTERPRISE COMMAND

Password ownership moves from the individual to the enterprise

Traditional self-service password reset addresses just the last step of the problem: the reset itself. It leaves creation, rotation, and recovery on the user's shoulders, and it assumes the directory is always available. Bravura Pass flips that model.

Before, with traditional SSPR	After, with Bravura Pass
Users are responsible for fixing their own password problems, often involving the help desk.	Enterprise automation manages the full credential lifecycle.
Users hold a separate password for each system outside single sign-on.	Users sign in without passwords. The enterprise holds the credentials.
Reset tickets consume a large share of help desk volume.	Ticket volume drops sharply through automation.
Assisted resets require help desk staff to hold elevated admin rights.	Delegated and assisted resets need no elevated privileges.
Policies are inconsistent from one system to the next.	Consistent policy spans SaaS, cloud, on-premises, and legacy systems.
Mass resets rely on brittle scripts during an incident.	Coordinated mass password reset strengthens breach response.

The result is a predictable, automated credential service rather than a recurring user burden. Self-service recovery keeps a place in that service, as the way back in when an edge case breaks, but it is no longer the model.

IN PRACTICE

Lead with the passwordless experience for your people. Keep enterprise-grade control over the passwords that still exist.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

TECHNICAL CHALLENGES

The hard problems live at the edges, not on the central server

Synchronizing and resetting passwords on a central server is straightforward. The hard problems live at the edges, where users get locked out, work offline, or depend on encryption and certificates. A serious solution must solve these hard problems, not just the easy, happy path.

Locked-Out Users

A user who forgets a network password or trips an intruder lockout cannot reach a normal browser or application to fix it. They need a path to recovery that does not depend on the login they just lost. Bravura Pass opens that path from the lock screen, a phone, or another device.

Cached Credentials on the Endpoint

Windows caches the password a user types at the login screen so they can work offline. After a reset, the cache and the directory can fall out of step, which locks the user out again. Bravura Pass keeps the endpoint and the directory aligned so a reset actually restores access.

Directory Replication Delays

In a distributed directory, a new password can take time to replicate to each controller. A user who resets in one location may still fail to log in against another. Bravura Pass accounts for replication so recovery holds across the environment, not just at one node.

Full-Disk Encryption

A user who forgets the password that unlocks an encrypted drive at boot time is stuck before the operating system even loads. Bravura Pass lets them recover through self-service, without waiting on a support analyst.

Mobile and Disconnected Users

Remote and traveling users hit password problems far from the corporate network, often on a laptop that authenticates against a cached credential. Bravura Pass supports recovery for these users through web, mobile, and phone-based workflows.

PKI and Certificate Passwords

Certificates and hardware tokens still rely on a PIN or password that users forget. Bravura Pass manages these authentication factors alongside directory passwords, so the whole set stays recoverable through one consistent process.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.



PART TWO

How Bravura Pass solves it

Lead with the passwordless experience for your people. Keep enterprise-grade control over the passwords that still exist.

INSIDE BRAVURA PASS

One platform for every authentication factor a user holds

Bravura Pass manages the full set of authentication factors a user holds, across every connected system, from one platform. These are the capabilities that make that possible.

A Passwordless User Experience

Nothing reduces friction like removing the password entirely. Users authenticate with verified factors while Bravura Pass creates, rotates, and resets the underlying passwords behind the scenes. People stay productive without thinking about credentials.

Password Synchronization Across Hybrid Systems

Bravura Pass synchronizes passwords across Active Directory, cloud, SaaS, and legacy systems. Automated lifecycle enforcement keeps each credential aligned with enterprise policy, so users have fewer passwords to manage and far fewer chances to get locked out.

Self-Service Password, PIN, and Account Recovery

Users reset passwords, unlock accounts, and recover access from desktop, mobile, or phone, without calling the help desk. Recovery works from full-screen browsers, mobile browsers, phone calls, and the PC login screen, so help is available wherever the problem happens.

Modern Enterprise Mass Password Reset

Mass resets used to mean brittle scripts, desynced systems, and locked-out users. Bravura Pass performs coordinated, real-time, verified resets across directories, SaaS apps, legacy systems, and non-SSO applications at once. Everything updates together, and new credentials are delivered securely through the Bravura Safe vault. Users can reach them immediately, without brittle scripts or a cleanup phase.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

Secure Credential Delivery With Bravura Safe

Automating the password lifecycle and resetting credentials at scale depends on storing and handing over new secrets securely. That is the job of Bravura Safe, the encrypted enterprise vault built into the Bravura Security Fabric. Lifecycle automation and enterprise mass password reset both depend on it.

When Bravura Pass creates or rotates a credential, Bravura Safe holds it, ready for secure retrieval. During an enterprise-wide reset, this lets thousands of new credentials reach users at once, safely and automatically, with a full record of who received what.

Bravura Safe is also a full enterprise password manager in its own right. It securely stores, autofills, and manages the credentials and secrets your workforce uses daily from one central place. That turns secure credential delivery from a fragile manual step into a dependable, audited service.

Unified Authentication, MFA, and SSO

Bravura Pass supports passwordless login, multi-factor authentication, and single sign-on through strong factor verification. It works with your enterprise authentication tools and can also trust an external identity provider, so you enforce consistent policy across the estate.

Zero-knowledge by design

Bravura Safe holds each credential in a zero-knowledge encryption architecture. No spreadsheets, no email hand-offs, and no external tools in the loop.

Works with what you run

Microsoft Entra ID MFA, Okta, Duo Security, RSA SecurID, and HYPR, or an external identity provider you already trust.



WHY IT MATTERS

Secure delivery is what makes a mass reset finish. Without it, new credentials travel by spreadsheet and email, and the cleanup phase never ends.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

Policy Enforcement and Real-Time Strength Feedback

Bravura Pass enforces password policy across each connected system, in line with NIST SP 800-63B-4. It supports length-based policies rather than relying on composition rules alone, and when a user changes a password, it screens each candidate against known-compromised credentials. When a compromise comes to light, administrators can force a reset, for one user or many. Bravura Safe also alerts users to compromised passwords stored in their vault, so they can change them.

Where a legacy system still requires its own composition or expiry rules, Bravura Pass enforces those too, including on platforms that cannot enforce rules themselves. Real-time strength feedback guides users toward stronger passwords the moment they choose one.

Self-Service Encrypted Drive Unlock

Users recover encrypted drive keys through self-service workflows, which cuts IT involvement while preserving strong authentication and data protection.

Compliance-Ready Dashboards and Reporting

Audit trails and centralized dashboards support NIST, PCI DSS, ISO 27001, and internal compliance programs. You get full visibility into password, recovery, and authentication activity, plus the evidence auditors ask for.



Self-service recovery works wherever the problem happens: desktop, mobile, phone, or the PC login screen.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

The Bravura Security connector library

Each capability in this paper depends on one thing: reaching the systems where credentials actually live. The Bravura Security connector library is how Bravura Pass gets there. It connects the platform to your target systems and manages accounts, passwords, groups, and access requests across each one.

The library spans the full hybrid estate. Prebuilt connectors reach directories, cloud and SaaS applications, databases, operating systems, network devices, and mainframe platforms. This breadth lets Bravura Pass manage credentials far beyond the Microsoft ecosystem, including the legacy and non-SSO systems that carry much of your credential risk.

No two enterprises run the same systems. When a target is not already in the library, the connector framework supports custom connectors, built against a well-documented connector SDK. You bring niche, in-house, and legacy applications under the same managed lifecycle as everything else.

Connectors are built for real-world conditions. When a target system is unavailable during an update, Bravura Pass queues the change and retries it automatically on a configurable schedule. A transient outage does not leave credentials out of sync.

The connector library is the reach behind the rest of the platform. It makes consistent policy, synchronized passwords, coordinated mass reset, and audit-ready reporting work across the estate.

For the current list of supported connectors, visit **bravurasecurity.com/technology/platform**.

Architecture and resilience: passwords as a service

Bravura Pass treats credentials the way modern IT treats infrastructure: as a managed, automated service rather than a manual chore. Credentials are created, rotated, synchronized, and recovered automatically across every connected system.

Resilience is the point that sets this apart. Because credentials live in the Bravura Safe vault, retrieval keeps working through an outage. Users and responders still reach the credentials and secrets they need, even when a directory or authentication service is down. The vault stands apart from those systems, so an outage in one does not lock people out of everything. Automated rotation preserves credential health, and audit-ready tracking backs your compliance obligations.

The Bravura Safe vault is the backbone of that model. Because credentials are held and delivered from one encrypted store rather than scattered across systems, automation and recovery draw from a single trusted source.

Because the platform reaches far beyond a single vendor's ecosystem, it closes the gaps that tools limited to the Microsoft ecosystem leave open. Support teams can assist users without elevated privileges, which reduces insider risk and tightens your overall posture.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

HOW BRAVURA PASS COMPARES

Bravura Pass covers the credentials other tools do not reach

Versus Traditional SSPR

Legacy self-service password reset tools focus on help desk deflection and stop at the reset. They were not built to control creation, rotation, or synchronization across the estate. Bravura Pass manages the full lifecycle and adds coordinated breach response.

Versus Microsoft Entra ID SSPR

Microsoft Entra ID handles resets inside the Microsoft ecosystem. It does not reach the legacy and non-Microsoft systems where much of your credential risk actually lives. Bravura Pass complements Microsoft Entra ID by covering the credentials Microsoft does not touch, with real-time synchronization, policy-driven resets, and breach containment across the whole estate.

Capability	Traditional SSPR	Microsoft Entra ID SSPR	Bravura Pass
Self-service reset	Yes	Yes	**Yes**
Full lifecycle: create, rotate, sync	No	Partial	**Yes**
Legacy, non-Microsoft, and mainframe reach	Limited	No	**Yes**
Enterprise mass password reset	Scripts required	Scripts required	**Yes**
Credential retrieval during an outage	No	No	**Yes**
Passwordless user experience across Microsoft and hybrid-joined systems	No	Partial	**Yes**
Passwordless user experience across non-Microsoft and legacy systems	No	No	**Yes**
Audit-ready compliance reporting	Partial	Partial	**Yes**

WHERE TO START

If Microsoft Entra ID already handles your cloud resets, keep it. Bravura Pass adds the legacy, non-SSO, and mainframe reach, plus enterprise mass reset and recovery through an outage.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

THE BUSINESS CASE

The return shows up in three places: cost, risk, and resilience

Up to 85%
reduction in password-related help desk volume

Over 25%
fewer reset calls at DTCC after deployment

4 of 12
DTCC support staff moved to other work

Lower Operating Cost

Password resets rank among the highest-volume tickets IT handles. Bravura Pass reduces password-related help desk volume by up to 85%. Support teams then spend their time on higher-value work instead of resets.

Reduced Breach Risk

Stronger, synchronized, policy-enforced credentials shrink the attack surface. Coordinated mass reset lets you re-secure credentials across the estate in one action rather than a frantic scramble of scripts. That difference can decide how far a breach spreads.

Faster, Provable Recovery

When an incident forces an enterprise-wide credential reset, speed and proof both matter. Bravura Pass gives you a repeatable, verified recovery plan. It also generates the evidence you need for auditors, executives, and cyber-insurance requirements.

Sources: Bravura Pass data sheet, bravurasecurity.com/products/bravura-pass; DTCC case study, bravurasecurity.com/aboutus/casestudies.

An upgrade path without disruption

For existing customers, this is an evolution of the platform you already trust, not a migration. You upgrade in place. Existing integrations and configurations carry forward. There is no rip-and-replace and no retraining.

The current release adds a modern, accessible interface, a stronger reporting foundation, expanded APIs with fine-grained authorization, and enterprise-grade mass password reset. You unlock next-generation capability while everything that already works keeps working. That means faster time-to-value and a low-friction path to higher security, stronger governance, and a better user experience.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

WHERE THIS MATTERS MOST

Hybrid estates feel the credential problem. Regulated, high-scale industries feel it most.

Financial Services

Banks and insurers face strict mandates for password strength, multi-factor authentication, and audit evidence under frameworks such as PCI DSS. Bravura Pass enforces consistent policy and produces the records examiners expect, across legacy and modern systems alike.

Healthcare

Clinical staff cannot wait on the help desk when a login fails at the point of care. Self-service recovery from any device keeps caregivers working, while HIPAA-aligned audit trails document each action.

Higher Education

Campuses manage huge, seasonal, and diverse user populations across many systems. Flexible identity verification and self-service recovery cut reset volume without weakening security for students, faculty, and staff.

Energy, Utilities, and Manufacturing

Operational environments mix modern IT with long-lived legacy and control systems. Bravura Pass reaches those systems, keeps credentials synchronized, and supports coordinated recovery when an incident spans both worlds.

Built for rapid, provable recovery

A single compromised password can escalate into a major incident when recovery is slow or manual. Cyber-insurance terms and modern compliance expectations increasingly assume you can restore credentials across the enterprise quickly, and prove it.

Bravura Pass makes that plan repeatable. Coordinated mass password reset restores credentials across directories, SaaS, legacy, and non-SSO systems in one verified action. Secure delivery gets new credentials to users without manual handling. Audit-ready reporting proves the reset completed, giving executives, auditors, and insurers the evidence they ask for.

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

KEY TAKEAWAYS

Serve the passwordless future and the hybrid present at the same time

- [ ] **Passwordless is the destination. A hybrid, password-reliant estate is the present.**
  Bravura Pass serves both at once.

- [ ] **Credentials become a managed enterprise service.**
  Created, rotated, synchronized, and recovered automatically.

- [ ] **Bravura Safe stores and delivers each credential under policy.**
  It keeps recovery working through an outage.

- [ ] **Coordinated mass password reset secures credentials across the estate in one verified action.**
  With evidence for auditors.

- [ ] **Password-related help desk volume drops by up to 85%.**
  Bravura Pass data sheet, bravurasecurity.com.

Conclusion

Bravura Pass lets you serve the passwordless future and the hybrid present at the same time. Your people get a passwordless experience today. IT keeps verified control of credentials across the estate, including the legacy platforms other tools cannot reach. Password management becomes a managed, automated, resilient service.

See Bravura Pass in action

Request a demo against your own environment at bravurasecurity.com/request-demo.

Request a demo

Copyright © Bravura Security Inc. 2026. All Rights Reserved.

Bravura Security

One Platform.
Total Protection.

Bravura Security is an analyst-recognized leader with decades of experience. We built one platform from the ground up for Identity, Privileged Access, and Password management.

Bravura Identity

Lifecycle, access requests, and certification in one governed flow.

Bravura Privilege

Just-in-time privileged access with full session audit.

Bravura Pass

Self-service password and credential management at scale.

Bravura Safe

Enterprise vaulting for passwords, passphrases, and secrets.

See it against your own environment

To learn more, visit bravurasecurity.com, get in touch, or call 1.403.233.0740.

Request a demo

Bravura Security

Talk to us

SALES

sales@bravurasecurity.com
1.403.233.0740

SUPPORT

support@bravurasecurity.com
Portal: bravurasecurity.com

HEAD OFFICE

Bravura Security Inc.
PO Box 27008, RPO Tuscany
Calgary, Alberta T3L 2Y1

About this paper

Published by Bravura Security, 2026. Industry figures cited in this paper are drawn from the Verizon 2026 Data Breach Investigations Report. Customer outcomes are drawn from published Bravura Security case studies and data sheets.

Sources

1. Verizon, "2026 Data Breach Investigations Report," 2026. verizon.com/dbir
2. Bravura Security, DTCC case study and customer case studies. bravurasecurity.com/aboutus/casestudies
3. Bravura Security, Bravura Pass data sheet. bravurasecurity.com/products/bravura-pass
4. Bravura Security, supported connectors. bravurasecurity.com/technology/platform

Copyright © Bravura Security Inc. 2026. All Rights Reserved. Bravura Security, Bravura Security Fabric, Bravura Identity, Bravura Privilege, Bravura Pass, Bravura One, and Bravura Safe are trademarks of Bravura Security Inc. All other trademarks are the property of their respective owners.