



EXECUTIVE BRIEFING 01 / SEPTEMBER 2026

Secure work. Clear responsibility.

A managed working environment for people,
applications and data.

DESKBRIDGE WORKSPACE · AT A GLANCE

- 01 Named access with roles and clear ownership
- 02 Repeatable onboarding, support and offboarding
- 03 Connected Sovereign applications, with scope agreed

Secure workspaces. Managed access. Audit ready.
deskbridge.uk/briefings/workspace/

The operating model

Most organisations do not need more software. They need more control over how work is done, who can gain or grant access, and how accountability is maintained.

That is the idea behind DeskBridge Workspace: a managed operating environment for people, business applications and data. It gives staff, contractors and suppliers a controlled place to work, with identity, support, security and evidence connected to the same service boundary.

This is not simply a remote desktop, a file-sharing portal or another Microsoft 365 alternative. It is the operating layer around the working environment: who can enter, what they can use, how access changes, what happens when someone leaves, how suspicious material is handled, and what evidence remains.

What DeskBridge Workspace does

Workspace provides approved access routes into hosted working environments, with named users, role-based scope and structured onboarding and offboarding. The local laptop, desktop or browser becomes an access route rather than the place where the organisation must trust every file, application and session.

Depending on package and scope, the service brings together:

Hosted workspace access and approved applications

Identity, MFA and FIDO2/WebAuthn-ready controls where supported

DeskBridge Authenticator for sign-in, approvals and recovery workflows

Managed mail and identity administration

Helpdesk-backed support and change records

Structured joiner, mover and leaver handling

Monitoring foundations, backup expectations and continuity planning

Contractor and supplier access with expiry and review dates

Client-safe dashboards, reports and evidence packs

DeskBridge Sovereign applications included inside the Workspace model

Two office suites, one governed workspace

DeskBridge Workspace can offer a choice of two open-source office environments, allowing the client to select the experience that best matches its documents, users and working style.

LibreOffice

LibreOffice is a mature, widely adopted open-source suite covering word processing, spreadsheets, presentations, drawing and databases. It is a strong fit for organisations that value broad desktop compatibility, a familiar traditional office model, long-established file-format support and freedom from per-user office licensing. It is especially useful where users work mainly with local or shared documents and need a capable general-purpose suite.

ONLYOFFICE

ONLYOFFICE offers a modern interface and strong compatibility with Microsoft Office formats, including DOCX, XLSX and PPTX. It is a good fit for teams that exchange documents with external clients, prefer a Microsoft-like editing experience, or want collaborative document work to feel closer to browser-based office platforms. It can reduce friction when documents move between DeskBridge, clients and suppliers.

The choice is practical, not ideological. DeskBridge can help a client choose the suite that best matches its document estate and user expectations, while keeping both inside the same access controls, support model and evidence boundary. That means the office application can vary without the organisation having to rebuild its security and governance around it.

Security that is part of the working day

DeskBridge security is built around controlled operation. Access is named and scoped. Support actions are recorded. Contractors can receive time-bound access. Offboarding is a service event rather than a hurried checklist. Sensitive files can be staged, inspected and governed before release where the agreed scope supports it.

DBAV, DeskBridge's anti-malware and content-analysis layer, is designed to do more than place a green tick beside a file. It combines signature scanning with bounded, metadata-only analysis for suspicious scripts, macros, Office and PDF structures, web shells, downloaders, credential-theft indicators and other risky patterns. It can also correlate bounded file-integrity signals relevant to ransomware, such as mass change, entropy bursts, extension churn, ransom notes and controlled canary changes.

DBAV does not expose or retain raw file content in its decision records. It produces stable verdicts, rule identifiers, digests and evidence references. Unsafe or excessive structures fail closed. A suspicious result blocks automated release pending governed review. This makes security auditable without turning the scanning system into another uncontrolled copy of the client's data.

Guardian is the control and response layer around those signals. When DBAV identifies a serious event, Guardian can validate the exact tenant, company, device, folder or endpoint target, preserve evidence, freeze an approved storage path or snapshot, and route the matter for authorised containment and recovery. DBAV recommends; Guardian independently revalidates. Neither component silently performs a destructive action or bypasses approval, rollback and kill-switch controls.

That separation is powerful. It means a detection is not confused with an incident response action, and a response action is not trusted merely because a scanner suggested it. The result is a security service that can explain what it saw, why it classified it, who approved the response, what was preserved, and how recovery was controlled.

Where Workspace can reduce cost

The saving is not only a licence comparison. It comes from removing the hidden cost of fragmented IT: multiple suppliers, duplicated administration, unmanaged endpoints, password and recovery work, emergency offboarding, support conversations with no record, migration surprises and audit evidence assembled under pressure.

A smaller business can obtain a disciplined operating model without hiring a full internal team for identity, workspace administration, mail, security, onboarding and evidence. A larger or contractor-heavy organisation can reduce the number of uncontrolled trust paths and the time spent proving what happened.

DeskBridge Workspace is therefore an investment in lower operational friction and lower exposure. It gives people a usable environment, leaders visibility, and the organisation a record it can use with clients, insurers, auditors and its own board.

The practical outcome

Staff work. Contractors work. Documents move. Support happens. People leave. Security events are investigated. The difference is that these activities happen inside a service designed to keep control and evidence attached to the work.

DeskBridge Workspace is for organisations that want secure work to be ordinary, supportable and accountable.

DeskBridge: secure workspaces. Managed access. Audit ready.

Start with the outcome your organisation needs.

Tell us your team size, the systems you use today and the access, workflow or evidence problem you most want to solve.

01 • Workspace

The controlled working environment.

02 • Sovereign

The connected business applications.

03 • Pilot

A scoped, supported evaluation.

Request a pilot scope review

deskbridge.uk/briefings/pilot/

£12 per user per month for the first three months. Sign up by 30 October 2026. Acceptance, application readiness and agreed service scope apply.

Read the companion briefings

[DeskBridge Sovereign](#) — Explore the connected application family for records, people, documents, business activity, communication and operational insight.

[DeskBridge Pilot Programme](#) — Review the £12 per user per month paid pilot, first-three-month offer, migration and hosting benefits, scope and application process.

Contact DeskBridge

deskbridge.uk/contact/
contact@deskbridge.uk

Capabilities depend on the agreed package, deployment and readiness. This briefing describes the service model; your written proposal defines the delivery scope. Pilot migration charges, hosting requirements, tax treatment and post-pilot pricing are confirmed in the quote.

DeskBridge Ltd • Company number 17123038 • Wales, United Kingdom
Edition 1.0 • 7 September 2026