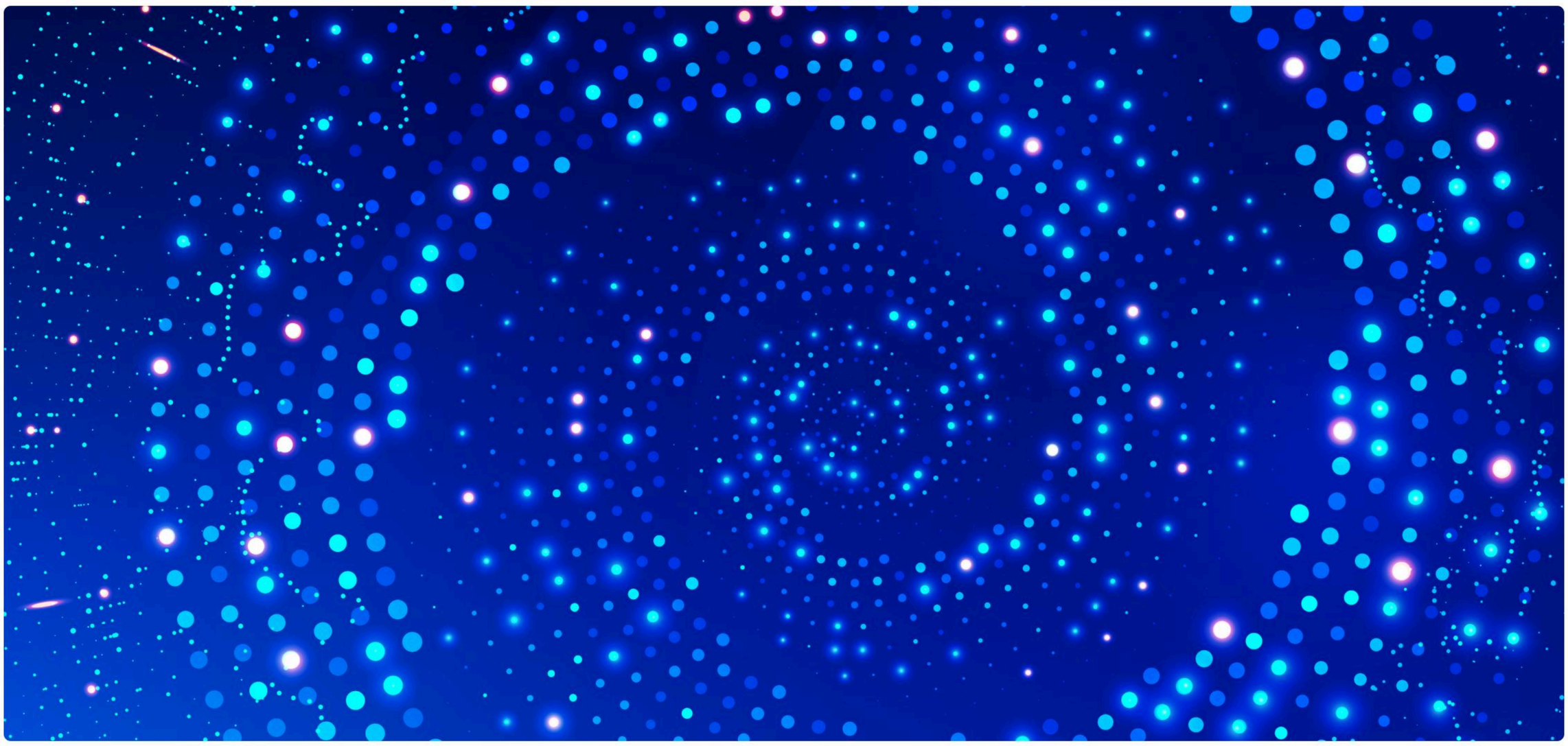
Use Case

Rethink External Sharing: From Guest Chaos to Trusted Collaboration

eSHARE



The Rise of Guest Accounts in the M365 Era

As digital collaboration becomes central to business operations, organizations increasingly rely on external sharing to stay connected with partners, clients, and vendors. Microsoft has attempted to make this easier by enabling guest access across tools like SharePoint, Teams, and OneDrive. At first glance, it seems like a practical solution.

But with convenience comes compromise.

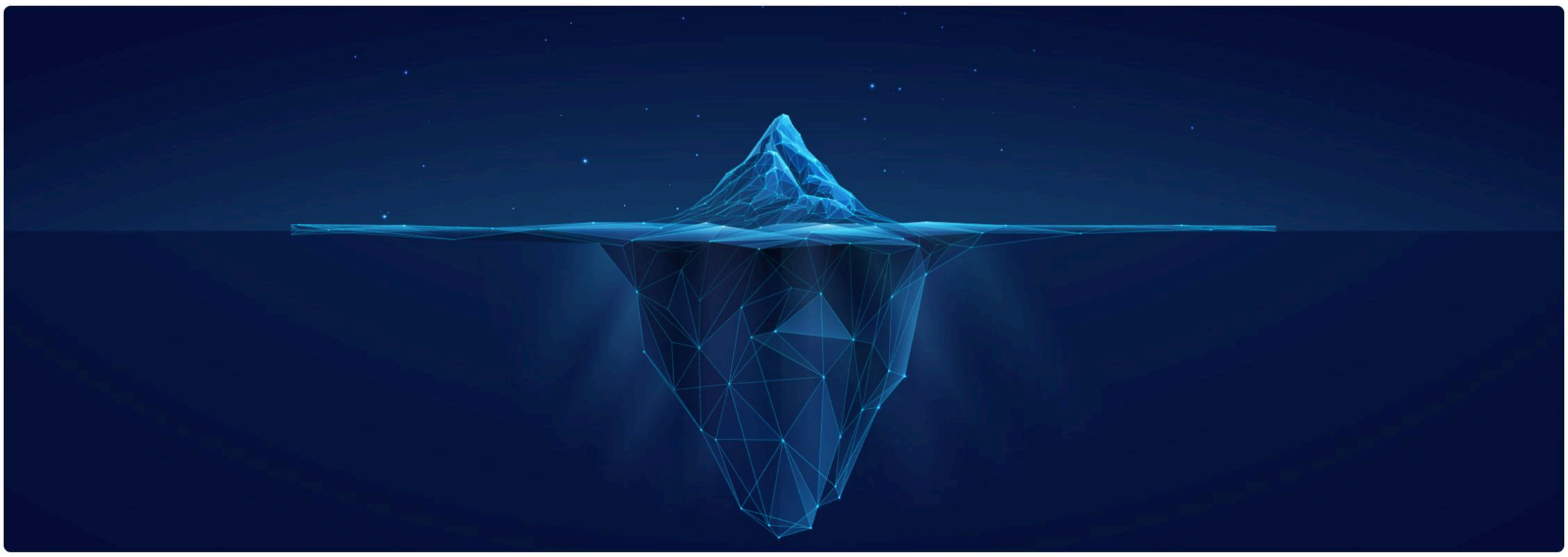
Guest accounts, originally designed for lightweight access, have become the default method for external collaboration. As their numbers grow, so do the administrative burdens and security risks. Many enterprises now find themselves managing thousands—or even tens of thousands—of guest identities, with little visibility into who has access to what.

Gartner's research (Assessing External-Sharing Options in Microsoft 365 by Max Goss) confirms this trend, noting that many organizations adopt guest access without fully considering the implications on governance, security, and cost.

It’s a model that’s become too open, too complex, and too costly.

The Hidden Costs of Guest Access

What begins as a quick fix for external collaboration often becomes a hidden drain on business resources.



Business Costs

Guest accounts might appear “free,” but the overhead they create is far from it. Each guest identity must be managed, supported, and governed. IT teams spend valuable time maintaining access, resolving login issues, and troubleshooting user permissions. In large organizations, this adds up—fast.

Even more pressing is the licensing complexity. While guests may not always require full licenses, their activity still impacts infrastructure, storage, and support operations. The result? A growing administrative burden with unclear ROI.

Security Costs

Every guest account is a potential entry point. Without clear ownership and lifecycle management, these accounts often remain active far longer than needed. Stale access, orphaned identities, and over-permissioned users expand the attack surface—and increase the risk of data exposure.

One global enterprise, for example, struggled to manage thousands of external identities in its open Microsoft 365 environment. The lack of clear controls and visibility led to mounting security concerns and added complexity in governance.

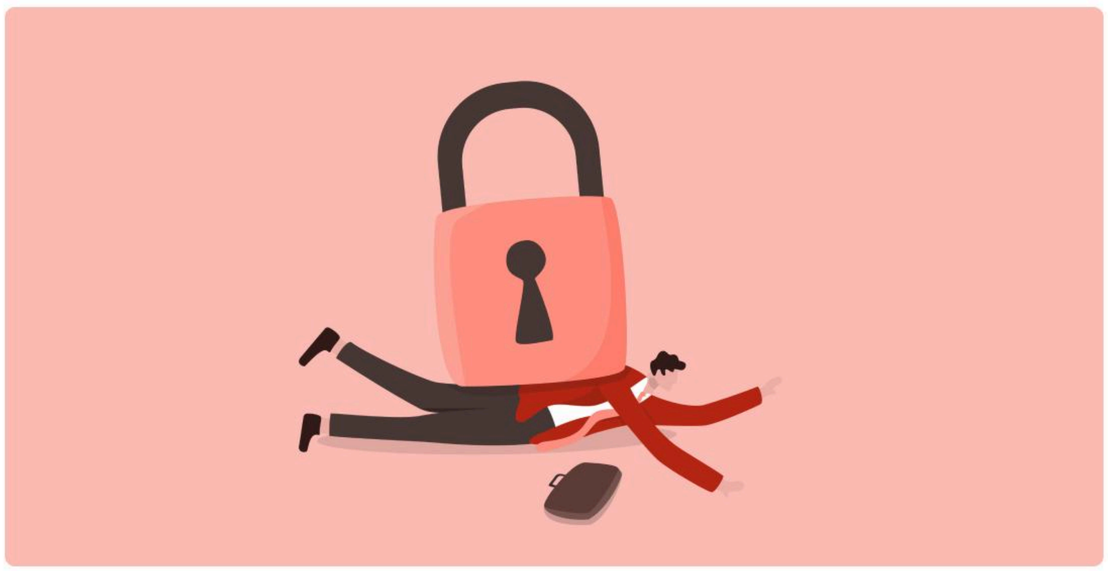
As external sharing grows, so does the chance of shadow IT, non-compliant behavior, and unintended data leaks. Guest access becomes not just a tool—but a liability.

Why Open Sharing Fails

Open sharing environments may seem efficient on the surface—but they often fail where it matters most: speed, control, and security.

Slow and Inefficient

When users rely on guest accounts for every external interaction, the process slows down. Inviting users, waiting for acceptance, dealing with login issues—all these steps introduce friction. And when deadlines are tight, this friction becomes a blocker that leads to shadow sharing.



Lack of Control

Open tenants create governance blind spots. External identities are often created ad hoc, with limited oversight. IT and compliance teams struggle to track who has access, to what, and for how long. There's no built-in lifecycle, no consistent deprovisioning process, and no scalable way to maintain alignment with policy.

Insecure by Design

When anyone can be invited into your tenant, risk increases. Users often have more access than needed, and temporary collaboration becomes permanent exposure. This open model goes against the principle of least privilege, creating a sprawl of unmanaged identities.

For organizations that need to move fast without compromising security, open sharing simply doesn't hold up. It creates too many questions, too many risks—and not enough accountability.

The eSHARE Alternative: Trusted Collaboration

eSHARE offers a smarter, more secure approach to external collaboration - one that doesn't rely on guest accounts at all.

Integrated with Microsoft 365

eSHARE works seamlessly with Microsoft 365, enhancing—not replacing—your current tools. Content stays where it is (SharePoint, OneDrive), while external users engage through eSHARE's Trusted Collaboration fabric. There's no need to re-train users or overhaul existing systems.

Governance Built In

Every interaction through eSHARE is governed by digital restrictions. Access is time-bound, role-specific, and fully auditable. External collaborators get the visibility they need, and nothing more. This approach drastically reduces over-permissioning, orphaned accounts, and long-term exposure.

No Guest Accounts. No Risk Sprawl

eSHARE enables organizations to collaborate across boundaries without granting external users access to the core tenant. Instead of provisioning identities, eSHARE provides secure, controlled access to specific content - enforced by policies, not passwords.

Built for Scale and Simplicity

Whether you're working with a few vendors or thousands of partners, eSHARE offers consistency. No more custom processes, one-off exceptions, or risky workarounds. Just a controlled, scalable way to collaborate—without sacrificing security or speed.

Use Case Highlights: Reducing Risk at Scale

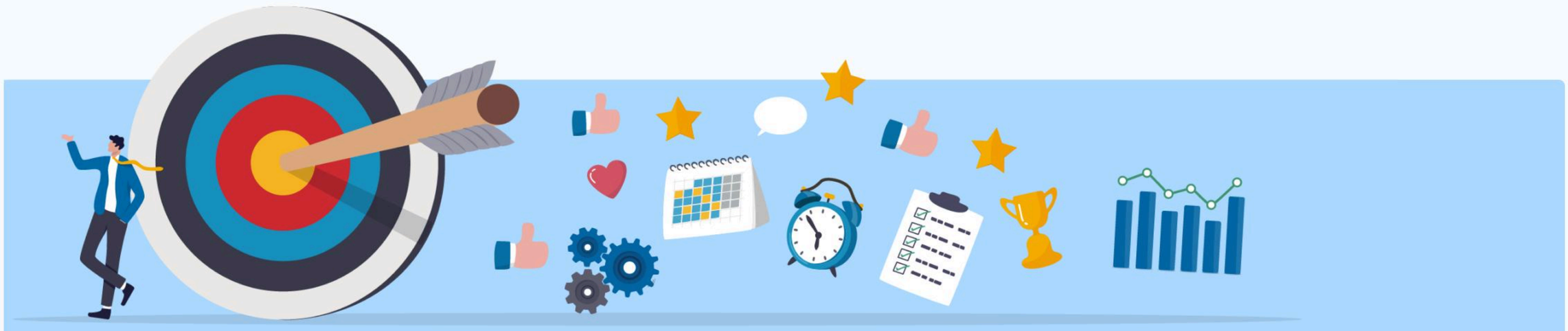
A global enterprise in the healthcare sector faced growing challenges managing external collaboration across its Microsoft 365 environment. With thousands of third-party partners and vendors requiring access, the organization had relied heavily on guest accounts—leading to complexity, risk, and inefficiencies.

The Problem

Over time, the number of guest users skyrocketed. External identities were scattered, difficult to track, and often left active long after projects ended. The IT team struggled to manage lifecycle processes, while the security team flagged concerns about increased exposure and lack of visibility.

The Shift

By implementing eSHARE, the organization introduced a digitally restricted layer on top of its existing Microsoft 365 infrastructure. Instead of issuing guest accounts, external collaborators were granted time-limited, policy-driven access to only the content they needed.



The Outcome

Thousands of guest accounts were decommissioned, reducing identity sprawl.

Security posture improved, with full audit trails for every shared file and interaction.

The IT team regained control over external access—without slowing down the business.

What once required complex identity management now runs with precision and simplicity. This shift not only cut down operational overhead, but also helped the organization meet compliance expectations with greater confidence.

Key Takeaways

Guest accounts were never designed for the scale or sensitivity of today’s external collaboration needs. As organizations grow and partnerships expand, relying on open sharing models creates unnecessary risk, operational drag, and governance headaches.

No guest accounts

no identity sprawl, no lifecycle chaos

Trusted Collaboration

built-in governance and auditability

Microsoft 365 integration

no disruption to existing workflows

Scalable and secure

whether you're collaborating with five partners or five thousand

Modern collaboration doesn’t have to mean giving up control. With eSHARE, organizations can move fast, stay secure, and reduce costs—all without compromising user experience.

Next Steps

If your organization is struggling with the cost, complexity, or security risks of guest access, it’s time to rethink your approach.

eSHARE gives you the tools to collaborate externally—without opening your environment.

Let’s talk.

Contact us to see how eSHARE can help you simplify external sharing or book a demo to experience it in action.

Linkedin
Contact Us
www.eshare.com

eSHARE