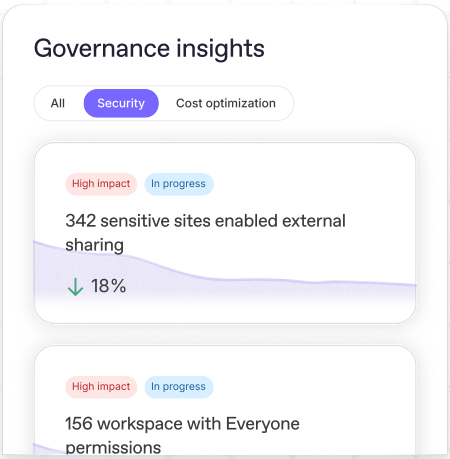
ShareGate Protect

Protect at a technical glance

ShareGate Protect is an operational governance layer that gives IT professionals a clear view of access, highlights where exposure is building, and supports practical day-to-day governance across Microsoft 365.

It brings together Microsoft-reported signals into a single operational experience and provides guided actions that keep remediation safe, intentional, and predictable.

Protect focuses on visibility, context, operational governance, and safe cleanup.



Data sources and coverage

THE CHALLENGE

Microsoft 365 spreads identity, sharing, and workspace signals across multiple admin centers. IT professionals often lack one dependable place to understand how access works and where exposure is forming. Protect brings these signals together in one place.

SIGNALS PROTECT USES

- Microsoft Graph and Microsoft 365 reporting APIs
- SharePoint, OneDrive, and Microsoft Teams admin workloads
- Sharing link configuration and usage
- Entra ID users, security groups, dynamic groups, and guest accounts
- Ownership and basic activity signals surfaced through Governance Risk Assessment

COVERAGE INCLUDES

- SharePoint sites and document libraries
- OneDrive accounts and sharing links
- Internal, external, and guest exposure pathways
- Microsoft Teams and their underlying SharePoint sites and Microsoft 365 Groups
- Microsoft 365 Groups and relevant Entra ID groups tied to collaboration
- Tenant-wide inventory of sites, teams, groups, and OneDrives for governance visibility

Protect complements Microsoft Purview, SharePoint Advanced Management, and Microsoft 365 admin centers. It does not replace classification, DLP, or regulatory compliance tooling. Instead, it helps IT professionals see and address access conditions that affect how well those controls work.

Protect operates within standard Microsoft 365 admin permission models and does not require elevated or nonstandard privileges.

Visibility, risk, and context model

THE CHALLENGE

IT professionals often know issues exist but lack a single, reliable way to understand where they originate, how broad they are, or which access pathways contribute to them.

Protect provides a clear and consolidated view of Microsoft-reported access and exposure conditions.

VISIBILITY INTO ACCESS AND EXPOSURE

- Workspace-level inventory paired with identity-level access signals
- How access is granted through links, group membership, inheritance, and external identities
- Oversharing indicators based on sharing scope, audience, and exposure pathways
- Exposure created through inherited access patterns surfaced across multiple admin views but not unified
- Inactivity and usage drift that contribute to sprawl and unmanaged risk
- Governance Risk Assessment signals surfaced at scale

CONTEXT THAT REDUCES INVESTIGATION STEPS

- Ownership gaps and orphaned workspaces surfaced early
- Direct mapping of identity and access factors shaping each condition
- Severity reflecting breadth and depth of exposure
- Custom reporting to demonstrate governance coverage and track progress

GROUNDED AND RELIABLE TRENDLINES

- Trend views based on real Microsoft-reported signals
- No predictive scoring or content inspection
- Focus on access, identity, and workspace conditions
- Support for informed, confident operational governance decisions

Action and safety model

THE CHALLENGE

Fixing access issues across multiple admin centers can be slow, inconsistent, and difficult to track. IT professionals often lack a safe, predictable way to clean up exposure across workspaces.

Protect provides guided remediation IT operators can trust.

SUPPORTED ACCESS AND GOVERNANCE ACTIONS

- Tightening or adjusting sharing links
- Updating workspace access
- Assigning or confirming owners
- Reviewing and removing inactive or unnecessary workspaces using Microsoft-supported deletion operations
- Reviewing and adjusting external or guest access
- Lifecycle hygiene based on inactivity or ownership gaps, not workspace restructuring or migration planning

All actions use Microsoft-approved Graph and admin APIs. Protect supports bulk remediation, but nothing is executed automatically or without operator review and confirmation.

Protect focuses on workspace- and access-level changes for governance hygiene and does not modify tenant-wide configuration settings.

Every change is fully logged so IT professionals can see what changed, who approved it, and when, supporting clear accountability and audit needs.

How Protect works day to day

Protect is designed for the operational side of governance. It helps IT professionals keep collaboration clean and safe without adding complexity.

- One place to review access, exposure, identity signals, and workspace conditions
- Clear explanations of why conditions exist and which factors contribute
- Support for recurring governance and access hygiene cycles
- Faster investigation with fewer steps to trace how access is forming
- Guided remediation that keeps every action safe, auditable, and operator-led

Fit within the Microsoft ecosystem

Protect works with your existing setup.

- Microsoft Purview manages classification, labeling, and compliance posture
- Microsoft 365 admin centers expose workload-specific settings and configuration
- SharePoint Advanced Management provides advanced site and lifecycle controls

Protect brings these signals together, surfaces access and lifecycle issues, and guides safe remediation in one place.

Protect also supports AI readiness by improving access hygiene so content is not broadly accessible before tools such as Copilot expand visibility. AI readiness is the outcome of good access hygiene, not a dependency for using Protect.

How Protect performs in technical evaluation

Protect is built to answer the core questions IT professionals raise during evaluation:

- Visibility you can trust through consolidated Microsoft-reported signals
- Clear explanation of issues with context that reduces investigation time
- Practical oversharing reduction without operational overhead
- Safe, traceable remediation aligned with Microsoft-approved patterns
- Predictable capability boundaries with no hidden enforcement
- Less manual investigation by reducing tool switching

Protect supports technical evaluation by showing what is happening in the environment and providing a safe, structured way to act.

Protect centralizes visibility, explains access and identity conditions, and helps IT professionals fix issues safely without switching across multiple admin centers or writing custom scripts.

It complements Microsoft-native governance capabilities and supports the everyday work of keeping Microsoft 365 clean, safe, and predictable.

See how Protect gives IT professionals operational clarity that Microsoft 365 alone does not surface today.

Talk to our team to experience Protect in action and get a clear view of access, exposure, and day-to-day governance across your Microsoft 365 environment.