Data Visibility & Protection

Sensitive data is spread across endpoints, cloud platforms, email, file shares, applications, and business systems. Protecting that data requires visibility into where it resides, who can access it, how it moves, and whether it is adequately protected. Brite helps customers improve data protection through discovery, classification, DLP support, access control, encryption guidance, backup strategy, and monitoring.

By combining data visibility with managed security and policy enforcement, Brite helps reduce the risk of unauthorized access, accidental exposure, and data loss.

Why Data Visibility & Protection?

Identify Sensitive Data
Understand where critical and regulated data resides across cloud, endpoint, email, and infrastructure environments.

Control Access & Movement
Apply access policies, monitoring, and DLP controls to reduce unauthorized sharing or exfiltration.

Support Compliance & Resilience
Protect sensitive information while supporting regulatory obligations, incident response, and business continuity.

Data Discovery Support
Help identify sensitive data locations across cloud repositories, endpoints, email systems, file shares, and business platforms.

Classification & Policy Alignment
Support classification efforts that align data sensitivity with appropriate access, retention, and protection policies.

Data Loss Prevention
Implement or manage DLP controls to reduce unauthorized transmission of sensitive information through email, cloud, or endpoints.

Access Monitoring
Monitor suspicious access patterns, unusual file activity, and potential insider or compromised-account behavior.

Backup & Recovery Alignment
Support resilient backup and recovery strategies to protect critical data from ransomware, deletion, or operational disruption.

Brite

Brite.com
1.800.333.0498
SalesInfo@Brite.com