uncountable

DATA LOSS PREVENTION

Data Loss Prevention, Built In

Uncountable controls not only how data is stored, but how it moves: how much can be exported, what protection travels with an exported file, and what is checked coming in.

Deployed by 175+ global enterprises

Dow · DuPont · SunChemical a member of the DIC group · repsol · Sika · Clariant · Mondelēz International · Beiersdorf

Three Layers of Defense

Independent layers, so no single control has to catch everything

3	Groups	100%	Live
Layers of Defense	**Enforcement**	**Files Scanned**	**Admin Alerts**
Export limits, labels, scanning	Not one-size-fits-all	No exceptions by type	Notified as it happens

How Each Layer Works

Two-Tier Enforcement
A warning threshold allows the export but notifies admins; an error threshold blocks it outright.

Group-Level Configuration
Quota period and thresholds are set per user group, so limits flex by role.

Usage Visibility
Admins track notebooks exported and files viewed per user, to catch unusual activity early.

Labels Travel With the File
Purview classification is enforced wherever the file goes next, governed by your own policies.

External-Open Restrictions
A properly configured label can block an exported file from being opened outside the organization.

Scanned on the Way In
Every uploaded file is checked for malware before it's accepted, regardless of type.

The Broader Security Picture

These export- and file-level controls sit alongside the credentials and safeguards Uncountable already has in place.

SETUP

Admin Sets the Rules

Quota period, warning threshold, and error threshold are configured per user group.

MONITORING

Usage Is Tracked in Real Time

Every export counts against that group's limit for the current quota period.

OUTCOME

Enforcement Is Automatic

Warning: the export proceeds and admins are notified. Error: the export is blocked and admins are notified.

- A single compromised or careless account can't quietly export the full formulation history.
- Exported files carry your classification rules with them, even after they leave the platform.
- The platform itself is not a vector for introducing malicious files into your environment.
- None of this requires new agents or software on the user's device.
- Enforcement doesn't depend on someone noticing after the fact.

Certifications and Infrastructure Safeguards

SOC 2 Type II & ISO 27001
Independently audited certifications, current and unqualified.

Encryption Everywhere
AES-256 at rest, TLS in transit, schema-level tenant isolation between customers.

99.9% Uptime SLA
A 10-minute RTO/RPO target with documented disaster recovery.

SSO & SCIM
Single sign-on with automatic user provisioning and deprovisioning.

48-Hour Breach Notification
A committed notification window if an incident occurs.

Network Monitoring
AWS GuardDuty (IDS) and Datadog (SIEM) monitor the environment continuously.

Security by architecture, not by exception.

Talk to Our Security Team
This overview covers export controls and file protection. Additional documentation, including our SOC 2 report and penetration-test summary, is best covered in a live working session.

uncountable®