Portcullis

Datasheet
November 2026

Removable storage control for Windows

Closed by default. Open on purpose. On the record.

Portcullis blocks USB storage on every Microsoft Windows endpoint you manage, opens it for one device, one person and a set time, and records every decision in an audit trail the endpoints cannot write to. It runs on a Linux server you provide and validates its licence offline.

6
profiles ready on the first day, from record only to nothing removable

1,430
endpoints on one appliance of 4 vCPU and 8 GB, in our tests

Under 1 s
from a revoke in the console to the endpoint, in our tests

0
licence call-home: your licence is validated on the appliance, offline

01 Closed by default

- USB sticks and drives, memory cards, external disks and phones blocked by a blocking profile; a new appliance starts by recording only. Keyboards, mice, printers, webcams and readers left alone; Windows' own disks never touched.
- Six shipped profiles, from Baseline (record only) to Restricted (nothing removable).
- For everyone, a group, a department, one machine or a group that fills itself by rule; on a schedule; on or off the network.
- Encrypted media only: an unencrypted stick is read-only and Windows offers BitLocker To Go.

02 Open on purpose

- Users ask from their own desktop, with a reason. An approver opens the one drive asked for, from an hour to 30 days, ending on its own.
- Offline codes from the service desk open one device with no network, report on reconnect, and cannot be re-encoded to open more.
- A revoke lands on the endpoint in under a second.
- Lockdown closes one endpoint's removable storage within seconds and overrides console grants.

03 On the record

- Every device connection recorded, controlled or not.
- A hash-chained operator audit trail that endpoints cannot write to.
- Alert rules to email, your SIEM or Microsoft Sentinel; the agent reports its own stop.
- Eight reports, on demand or emailed on a schedule.
- Subject access export and erasure; pseudonyms one switch away.

04 Yours to run

- One bundle, nothing downloaded: under a minute to install, and updates from the console in about a minute, in our tests.
- Backup and restore built in, and drilled.
- Agent and MSI are code-signed; agents install only updates carrying the same trusted signature.
- Licensed offline. A late renewal never leaves an endpoint unprotected or a user stuck.

Try it for 30 days on up to 25 endpoints with no licence. Ask the partner who looks after your IT.

Technical specification overleaf

Supplied by GW Consult. Contact us at gwconsult.co.uk/contact

Technical specification

Appliance	
Form	One container under Docker on a physical or virtual Linux server you provide, holding the database, policy, audit trail and console.
Operating system	Ubuntu 22.04 LTS or 24.04 LTS, recommended and tested; the installer can install Docker on these. Other 64-bit Linux with Docker Engine 24 or later and Compose v2.
Server	x86_64 only. Tested on 4 virtual processors and 8 GB of memory, with 10 GB of free disk.
Network	Inbound TCP 443, or a port you choose. Outbound only to the update service and any email or SIEM you set up; none at an isolated site. Device data stays on the appliance.
Install and update	One bundle of about 280 MB, nothing downloaded; installs in under a minute in our tests. Signed updates through the console in about a minute, backed up first. A changed bundle or a downgrade is refused.
Resilience	Built-in backup and restore, drilled. Your own certificate and chain can replace the appliance's without cutting off agents.
Endpoints and agent	
Endpoints	Microsoft Windows, virtual desktops included; a desktop notifier for requests and offline codes. Controlled: sticks and drives, memory cards, phones, and disks on Thunderbolt, USB4, eSATA or FireWire; CD and DVD drives and serial adapters by a switch. Never the disks Windows runs from.
Deployment	A code-signed MSI, for Configuration Manager or another deployment tool. A fleet enrolment token rolls it out across an estate; the console writes a one-line command for a single machine.
Updates	Delivered to the appliance from a hosted update service, or from a bundle at an isolated site, and released to pilot endpoints first, then everyone. Agents install only updates carrying the trusted signature, with revocation checked.
Trust	Agents pin the appliance's key; no setting turns certificate checking off. Agent credentials are readable only by SYSTEM and Administrators, and agent tokens rotate daily.
Records, alerts and integration	
Audit trail	Operator actions hash chained; endpoint events stamped with the appliance's time and the endpoint's own name.
Alerts	Rules, each with its own switch, severity and thresholds, to email and SIEM.
SIEM	UDP, TCP, TLS or HTTPS, as RFC 5424 syslog, CEF, LEEF or JSON, with real event names and severities. Microsoft Sentinel through the Logs Ingestion API, with the setup script written for you.
Email	Alerts, a digest and each access request's progress, by SMTP or Microsoft 365; request emails a service desk can file.
Reports	Eight, from executive summary to audit trail, as PDF or CSV, on demand or emailed on a schedule.
Operators and privacy	
Operators	Microsoft Entra ID sign-in with groups mapped to roles, or a password and a second factor for every local operator. Groups and departments synced from Entra ID or Active Directory.
Privacy	Subject access export and erasure for one person; pseudonyms for what leaves the appliance (off by default); retention purging on by default.
Licensing	
Basis	Per managed endpoint, up to the number licensed, warned at 90%. One to three years.
Evaluation	30 days on up to 25 endpoints, with no licence.
How it is checked	On the appliance, offline. A licence is bound to one appliance by its install code and survives upgrades and restores.
If it lapses	After 30 days' grace the appliance steps down in stages, refusing new endpoints first. Endpoints keep enforcing policy, and offline codes, revokes and access decisions always work.

Microsoft, Windows, BitLocker, Entra and Sentinel are trademarks of the Microsoft group of companies. Ubuntu is a trademark of Canonical Ltd. Docker is a trademark of Docker, Inc.; Thunderbolt of Intel Corporation; USB4 of USB Implementers Forum; FireWire of Apple Inc. All other trademarks are the property of their respective owners. Facts as of appliance 0.9.37 and agent 0.6.93, November 2026.