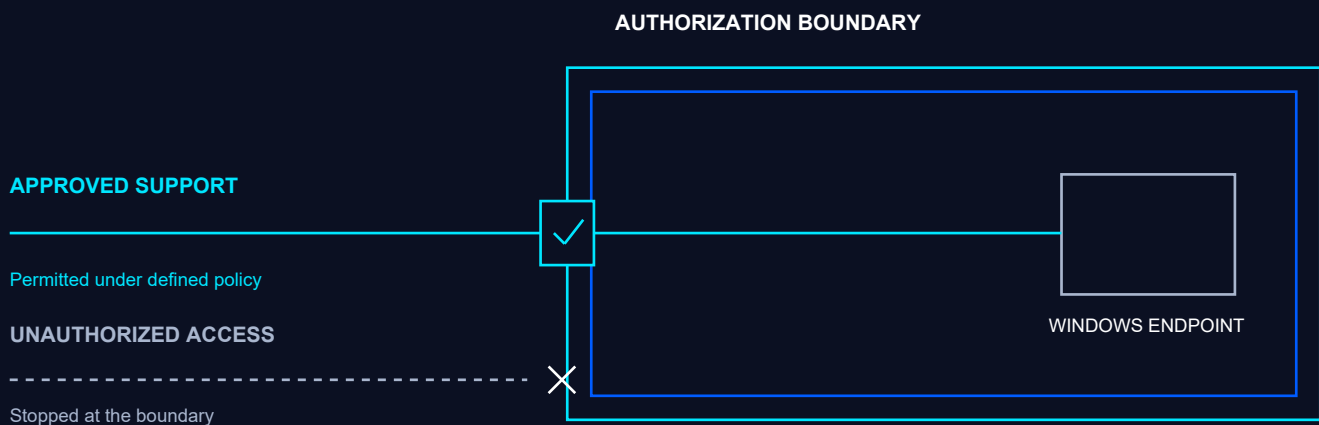


WINDOWS ENDPOINT PROTECTION

Your endpoints. Your rules.

Active endpoint protection that detects suspicious activity, blocks unauthorized remote access, and responds where threats begin.



Illustrative protection model. Not a live product interface.

Trust has a boundary.

Sentinel CS establishes a policy-controlled perimeter around Windows endpoints. It identifies software and relevant activity, evaluates authorization, and applies protection actions at the station.

Remote access is a permission.

Legitimate remote-support tools can create unauthorized access when used outside approved workflows. Sentinel CS permits approved support under defined rules and blocks prohibited activity according to policy.

For organizations that need control over their Windows environment, administered by an appointed IT professional.



COORDINATED PROTECTION

Detect. Decide. Block. Respond.

Five control points reinforce the endpoint boundary.

01 / Remote Access Guard

Identify remote-access tools and evaluate provider, publisher, location, and deployment context. Apply explicit authorization before permitting access.

02 / Execution Control

Detect suspicious execution chains and stop prohibited processes or services. Turn policy into action where software runs.

03 / Persistence Protection

Control associated services, scheduled tasks, and startup mechanisms that allow unauthorized activity to return.

04 / Tamper Protection

Restrict unauthorized interference with the agent and detect relevant changes to Windows security controls.

05 / Detection & Response

Connect identity, behavior, and context to a bounded response. Retain evidence of the decision, action, and verified result.

A controlled response sequence

Execution attempt > policy evaluation > block and stop > remove unauthorized persistence > record and verify the security event.

ScreenConnect / ConnectWise Control and other RMM tools are evaluated against policy. TeamViewer and AnyDesk are permitted only when their identity and use match authorization. A valid signature is evidence of identity, not permission to run.

OPERATION AND ADMINISTRATION

Local action. Central visibility.

Protection that fits authorized IT operations.

Enforced on the station.

The local service evaluates evidence and applies endpoint protection policy. Critical decisions use local rules and context; cloud services support administration and visibility.

Managed across the fleet.

Use the Customer Portal to review enrolled stations, connectivity, security alerts, licenses, and subscriptions. Connectivity and protection state remain distinct operational facts.

Maintenance with a defined end.

Authorize workstation-specific, time-limited maintenance. Retain supervision and a record of the operation. Protection reactivates when the authorized window ends.

Recovery under authorization.

Cryptographic Offline Recovery supports approved service operations when portal communication is unavailable. Disconnecting a station does not grant permission to modify its protection.



REPORTING AND OPERATIONAL EVIDENCE

Inventory. Evidence.

Station Activation & Monitoring Report

A provider-issued record

A dated report brings together the subscription snapshot, licensed-seat allocation, registered stations, recorded agent versions, and stored heartbeat evidence.

Evidence with a defined cutoff

Issue time, evidence cutoff, and the stated freshness window establish the reporting context. Station rows identify the recorded evidence and its limitations; historical released records are distinguished from current inventory.

Traceability through the Customer Portal

The report carries an authenticity reference and document status at issuance. Original document bytes and their SHA-256 hash are retained in the authenticated Customer Portal. The reference is not a cryptographic digital signature or a public document URL.

A snapshot with clear boundaries

Registered inventory and recent cloud evidence do not attest live endpoint health, continuous protection, or successful response. Missing or stale evidence does not establish that local monitoring is disabled. The report is a provider statement, not an independent audit or a compliance certificate.



SERVICE MODEL AND SUBSCRIPTION

An IT-led service.

Organizational use only. Individual and personal-use subscriptions are not offered.

IT administration and clinical continuity

Your appointed IT professional owns deployment, organization-specific rules, approved support workflows, and Maintenance Mode. Validate clinical, billing, laboratory, and support tools before rollout. If a legitimate tool is restricted, IT reviews the event, adjusts the rule or authorizes maintenance, then checks the workflow and returned protection state.

Healthcare engagement and BAA

Sentinel CS and healthcare customers will sign a Business Associate Agreement (BAA) as part of the service engagement. The signed agreement defines responsibilities for handling and safeguarding protected health information within the agreed scope.

Included with the monthly subscription

Active subscriptions include ongoing updates to new Sentinel CS versions and unlimited technical support for the appointed IT resource. Support contact information and chat are provided exclusively to active customer accounts.

Local diagnostic logs and export

Logs are generated locally for diagnostics. When IT initiates an export in the software, it is delivered to the registered customer email and made available in the Customer Portal account. Logs can also be shared with support. Export delivery is distinct from routine heartbeats and selected security events.

Customer documentation

After account activation, customers receive documentation covering subscription administration and cancellation procedures. Contact Sales with service questions before subscribing.

www.sentinelcsapp.com

portal.sentinelcsapp.com

admin@sentinelcsapp.com