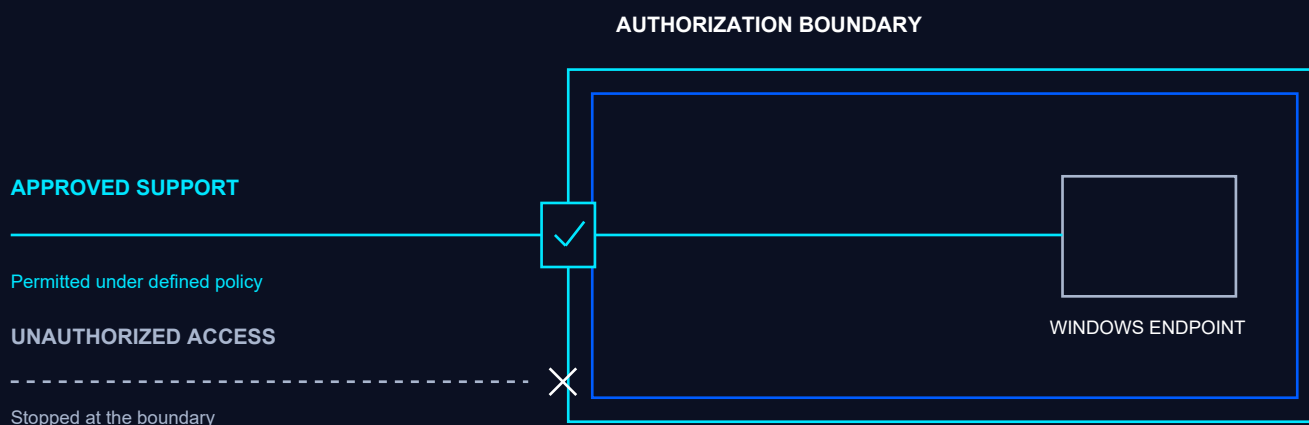


WINDOWS ENDPOINT PROTECTION

Executive & Technical Overview

Your endpoints. Your rules.



Illustrative protection model. Not a live product interface.

The Controlled Perimeter

Sentinel CS protects Windows endpoints through explicit authorization, context-aware detection, local policy enforcement, controlled response, and structured evidence.

This overview explains what the platform protects, how it acts, what it controls, and how organizations operate it. The focus is unauthorized remote access and the related execution, persistence, and security-control changes that affect endpoint trust.

PRODUCT ARCHITECTURE / POLICY / RESPONSE / OPERATIONS

01 / EXECUTIVE OVERVIEW

Protection with an explicit boundary.

Active control for Windows environments managed by businesses, IT teams, and service providers.

For business leaders

Sentinel CS makes authorization enforceable. It helps preserve approved support workflows while restricting unauthorized remote-access capability and relevant suspicious endpoint activity.

For technical teams

The protected Windows service owns local security state and policy enforcement. The console and Customer Portal expose status and authorized workflows without replacing the protection engine.

Guide to this document

- 03 EDR and the Sentinel CS scope
- 04 Identity and remote-access authorization
- 05 Architecture and evidence flow
- 06 Coordinated protection components
- 07 Response, containment, and verification
- 08 Portal, administration, and connectivity
- 09 Reporting and operational evidence
- 10 Maintenance, recovery, and updates
- 11 Operational scenarios
- 12 Scope, privacy, and deployment
- 13 Service model and subscription
- 14 Glossary and next steps



02 / ENDPOINT DETECTION & RESPONSE

From evidence to effective action.

EDR connects endpoint visibility, detection, investigation, and response.

Observe relevant activity

Collect process, service, execution, persistence, and selected security-setting signals so an investigation begins with evidence.

Detect with context

Evaluate identity, behavior, parent-child process relationships, and surrounding changes. Identify suspicious activity and policy violations.

Correlate events

Connect observations to an execution chain and associated capability. Separate ordinary administration from activity that violates authorization.

Respond under policy

Block prohibited execution, stop identified processes or services, and control associated persistence. Support containment and recovery within the defined product scope.

Verify the result

Check the resulting state and retain the observed outcome. A command being issued does not prove that the capability has been removed.

A focused security role

Sentinel CS complements antivirus and broader endpoint security operations. Its focus is authorization, remote-access abuse, suspicious Windows execution, persistence, and security tampering. EDR is a product category, not an independent certification.

03 / IDENTITY AND AUTHORIZATION

Remote access is a permission. Not an assumption.

Software identity and authorization answer different questions.

A valid Authenticode signature helps establish publisher identity and signed-code integrity. It does not establish that a tool is authorized on a particular workstation. Sentinel CS combines executable metadata, publisher information, provider artifacts, location, and deployment context with endpoint policy.

Approved support

TeamViewer, AnyDesk, or other approved tools are permitted only when identity, deployment, and use match explicit policy. Authorization is scoped; it is not a universal exemption.

Prohibited remote-management capability

ScreenConnect / ConnectWise Control and RMM families such as NetSupport Manager, Atera, N-able, SimpleHelp, DWAgent / DWSERVICE, MeshAgent, and Level RMM are evaluated against the applicable deny rules.

Windows-native remote access

Microsoft Quick Assist and Remote Desktop / RDP are governed through their configuration, use, and context. Legitimate administrative tools are not automatically classified as malware.

Confidence is not risk

Identity confidence describes the strength of software identification. Incident risk describes the significance of the observed use. The Policy Engine considers both, plus endpoint profile, maintenance state, and permitted response. Weak identity alone does not authorize destructive cleanup.



04 / ARCHITECTURE

Local enforcement. Explainable decisions.

A detector supplies evidence. Policy determines which response is authorized.

01 / Telemetry

Observe relevant endpoint activity and system state.

02 / Evidence

Normalize identity, time, execution context, and related observations.

03 / Detection

Identify suspicious behavior or a policy-relevant capability.

04 / Policy

Resolve authorization, profile, confidence, risk, and maintenance state.

05 / Response

Execute the permitted action against the identified capability.

06 / Verification

Check the intended effect on processes, services, artifacts, or configuration.

07 / Event Store

Preserve evidence, policy basis, action results, verification, and resulting state.

The protected service governs local protection. Closing the console does not stop or define its protection state. Module health and service health are reported separately so a running process is not mistaken for complete coverage.

05 / PROTECTION COMPONENTS

Five coordinated control points.

Website labels describe the protection layers; existing component names retain technical meaning.

Remote Access Guard

Identifies provider families through metadata, publishers, location, deployment artifacts, and context. Evaluates newly installed tools and existing remote-access capability.

Execution Control / Execution Guard

Examines browser or email activity leading to shells, scripts, downloads, and executables. Evaluates legitimate Windows utilities in context rather than globally prohibiting them.

Persistence Protection / Persistence Guard

Monitors services, scheduled tasks, autoruns, remote-access settings, and related account changes. Cleanup is tied to an identified, policy-prohibited capability.

Tamper Protection / Security Tamper Guard

Detects relevant changes affecting Sentinel CS, Defender, firewall, and remote-access controls. Self-protection restricts unauthorized interference with the agent.

Detection & Response / Policy and Response Engine

Combines findings with authorization and endpoint state. Selects a bounded action, checks its effect, and retains evidence of the outcome.

Startup and on-demand integrity checks add context on existing software and persistence. Correlation connects observations without treating every administrative event as a threat.



06 / RESPONSE AND VERIFICATION

Block the activity. Address its persistence.

Response is tied to identified software, sufficient evidence, and administrator authorization.

Execution attempt and policy evaluation

Identify the executable or provider and evaluate behavior, deployment, authorization, and maintenance state.

Block and stop

Prevent prohibited execution or stop an identified process or service within the configured response scope.

Quarantine and persistence control

Quarantine supported artifacts when justified. Remove associated persistence or restore affected configuration only when the evidence and authorization support that action.

Post-response verification

Check process, service, artifact, and configuration state. Record whether the intended effect was observed, incomplete, or unsuccessful.

Security event and investigation

Retain the evidence, policy decision, authorized action, response result, verification status, and endpoint state for technician review.

Containment has a defined scope

Containment means the supported action against the identified capability. It does not imply total network isolation, recovery of every resource, or unconditional threat removal. Uncertainty does not authorize deletion of unrelated software.

07 / PORTAL AND ADMINISTRATION

Enforced at the endpoint. Visible across the fleet.

Local protection and centralized administration have distinct responsibilities.

Windows agent

Use local evidence and applicable policy for critical protection decisions. Authenticated outbound communication supports status reporting, selected event delivery, and authorized service workflows.

Customer Portal

Review enrolled stations, connection status, selected security alerts, and organization-scoped administration. Manage per-endpoint licenses, subscriptions, and authorized workflows through a central account.

Identity and organization boundaries

Authenticated services validate agent identity and organization membership. Data and administrative operations remain scoped to their applicable organization context. Credentials and sensitive recovery material are not customer-facing content.

Connectivity is not enforcement

A heartbeat reports identity, version, health, protection state, and connectivity. Connection health, event delivery, module health, and response outcome are separate signals; a connected endpoint is not proof that every action succeeded.

When connectivity is unavailable

Locally available policy and protection logic continue to govern the endpoint. Fresh synchronization, online licensing operations, portal visibility, and cloud workflows depend on connectivity and configured service behavior.



08 / REPORTING AND EVIDENCE

A dated record. An accountable scope.

Station Activation & Monitoring Report

Document identity and reporting context

Provider-issued report number, issuer, issue time, evidence cutoff, template version, authenticity reference, and document status at issuance establish the record being reviewed.

Subscription and station inventory

The report summarizes licensed seats, allocation, registered stations, and recent recorded evidence. Station rows include identifiers, recorded versions, stored heartbeat timestamps, and status or limitations. Inventory is registered data, not an independent reconciliation of every business device.

Freshness and evidence exceptions

Read the report-specific freshness window alongside the evidence cutoff. Released historical rows are retained but excluded from current monitoring counts. Inconsistent stored timestamps can be flagged for review and excluded from applicable evidence.

Authenticity and retention

Original document bytes and their SHA-256 hash are retained in the authenticated Customer Portal. The authenticity reference supports traceability; it is neither a cryptographic digital signature nor a public document URL.

What this record establishes

It documents the registered inventory and stored evidence available at issuance. A subscription, registration, timestamp, or signed installer does not prove live health, continuous protection, active enforcement, or successful remediation. Missing cloud evidence does not prove local monitoring is disabled.

This provider statement is not an independent audit, insurance certificate, or HIPAA / NIST certification. It does not guarantee insurer acceptance or incident prevention.



09 / MAINTENANCE AND RECOVERY

Authorized work. A defined return to protection.

Serviceability preserves the authorization boundary.

Full Maintenance

Authorize a specific workstation for a time-limited maintenance window. Temporarily suspend only the protection actions covered by that authorization while retaining supervision, status, and an operational record. Protection reactivates when the authorized window ends.

Cryptographic Offline Recovery

Use device-context authorization for approved recovery when portal communication is unavailable. Offline operation is not permission to bypass protection, and recovery does not rely on a vendor-wide master password or a permanent bypass.

Signed updates and governed software rollback

Check software authenticity and integrity before installation or update. A governed rollback path supports return to an eligible previous software state. This is agent software recovery; it is not a promise of ransomware file restoration or universal system recovery.

Confirm the returned state

After authorized service operations, assess the service, configuration, module health, and applicable protection state. Restart, maintenance, offline recovery, and software rollback are different operations and are recorded distinctly.

Keep maintenance authorization and recovery material outside public documentation, ordinary diagnostics, and frontend content. Use the authorized workflow for the workstation.

10 / OPERATIONAL SCENARIOS

Policy meets real endpoint activity.

Illustrative scenarios show decision logic, not measured results or guarantees.

An unauthorized remote installer

A link or email leads to a remote-access installer. Identify provider artifacts and deployment context, evaluate authorization, block prohibited execution, and address associated persistence.

A renamed executable

A filename changes while publisher metadata or provider artifacts remain. Assess identity and context rather than trusting the filename.

A socially engineered script

Browser activity leads to a shell, download, or executable. Correlate the chain and apply the endpoint policy to the observed activity.

Persistent unauthorized access

A service, task, or autorun keeps prohibited capability active. Associate the mechanism with the identified software before authorized cleanup.

Unexpected security or RDP changes

Security exclusions, firewall rules, RDP configuration, or account activity change. Relate these signals to surrounding evidence and authorization.

Approved technical support

Support software matches explicit authorization. Permit the approved workflow under defined conditions; retain accountability when maintenance is authorized.

Applicable environments include professional offices, healthcare practices, small and midsize businesses, and managed IT providers. These examples do not establish industry-specific compliance.



11 / SCOPE, PRIVACY, AND DEPLOYMENT

Clear boundaries. Defined responsibilities.

A mature protection platform belongs within a broader security program.

Supported environment

Deploy the Windows agent on supported workstation configurations. Sentinel CS supports Windows 10 and Windows 11 environments. Confirm version, edition, compatibility, and operational requirements before rollout.

Selected security telemetry

Process metadata supports identity, execution context, persistence, security changes, policy decisions, and response outcomes. Records may contain identifying information such as device names or paths and are treated as operational data.

Privacy boundaries

Sentinel CS does not provide keylogging, screen capture, inspection of user document contents, or an arbitrary remote shell. Selective security telemetry is distinct from indefinite recording of all system activity.

Layered security responsibilities

Complement antivirus and Microsoft Defender. Maintain organization-wide identity controls, backups, patching, response procedures, and access governance. Sentinel CS does not claim inspection of all traffic, invulnerability, or prevention of every attack.

Licensing and administration

One station equals one licensed Windows computer. Station quantity determines the published monthly rate. Review deployment requirements, subscription administration, and authorized support with the team.

Endpoint protection alone does not establish HIPAA, SOC 2, PCI DSS, or other regulatory compliance. Organization processes and approved controls remain necessary.



12 / 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.

13 / GLOSSARY AND NEXT STEPS

A common language for controlled protection.

Key terms for business and technical teams.

Endpoint / station - A supported Windows system running the agent.

EDR - Endpoint Detection and Response: evidence-led visibility, detection, investigation, and response.

RMM - Remote Monitoring and Management software for administration and support.

Identity confidence - The strength of evidence identifying software or a capability.

Policy - Rules defining authorization, restrictions, and permitted response.

Persistence - Mechanisms that retain capability across sessions or restarts.

Tamper protection - Controls restricting or detecting unauthorized interference.

Heartbeat - An authenticated report of agent identity, health, version, and connectivity.

Event Store - Structured evidence, decisions, action results, verification, and state.

Full Maintenance - Authorized, time-limited service operation with return to protection.

Offline Recovery - Cryptographically authorized recovery without portal connectivity.

Software rollback - Governed return to an eligible previous agent software state.

Put your policies into action.

Contact Sales to discuss your Windows environment, access rules, and deployment requirements.

www.sentinelcsapp.com

portal.sentinelcsapp.com

admin@sentinelcsapp.com