ClearPath MSP
ClearWatch

SOLUTION BRIEF

from ClearPath MSP

CLEARWATCH SOLUTION BRIEF · SENTINELONE SINGULARITY ENDPOINT

SentinelOne monitoring, on every machine.

How ClearWatch reads your SentinelOne console, maps its sites to clients, finds the machines with no agent and alerts on threats.

PUBLISHED NOVEMBER 2026 LENGTH 6 PAGES APPLIES TO SENTINELONE SINGULARITY ENDPOINT

EXECUTIVE SUMMARY

SentinelOne protects. Is it everywhere?

SentinelOne's console lists the machines it has an agent on. It cannot list the ones it has never heard of: a new laptop nobody enrolled, a server rebuilt without the agent, a service that was stopped. And in an MSP's console each client is a site, so "is this client fully protected?" means comparing two lists by eye.

ClearWatch does not replace SentinelOne. It reads the console every 10 minutes with a Viewer service user's token, maps each site to a client and matches each agent to the device ClearWatch already watches. Then it checks both directions, alerts on threats and protection that is off, and lets a running SentinelOne pass the antivirus checks.

KEY TAKEAWAYS

- **Read only:** a Viewer service user. ClearWatch never isolates, scans or acts on a threat.
- **Sites become clients:** each site mapped once by a person; an unmapped one is counted, never guessed.
- **Missing, both ways:** a machine with no agent is listed and alerted; an agent ClearWatch does not know is added to Discovered.
- **One verdict:** where SentinelOne runs, the antivirus checks pass instead of failing on Defender.

IN THIS BRIEF

01 **The challenge** — What SentinelOne's own console leaves to you — 2
02 **How ClearWatch connects** — From ClearWatch's servers, with a Viewer token — 2
03 **Sites to clients** — One console, many clients — 4
04 **Agents and machines** — Matching, missing agents, the device page — 4
05 **Checks and alerts** — Five checks, on by default — 6
06 **Good to know** — Requirements and limits — 6

WHO THIS IS FOR

MSPs that protect their clients with SentinelOne, and IT teams with their own SentinelOne console, who want proof the agent is on every machine, beside the rest of their monitoring.

AT A GLANCE

CONNECTION	REFRESHED	ACCESS	NOT REPORTING
Cloud to cloud	**Every 10 minutes**	**Viewer role**	**After 3 days**
Nothing installed on site, and no ClearBridge.	Sites, agents and open threats in one read.	A service user's token. ClearWatch only reads.	The window, set per connection.

01 THE CHALLENGE

SentinelOne sees its agents, not the machines without one

SentinelOne's console is built to run SentinelOne: sites, agents, threats and policies. It is very good at what its agents report. What it cannot show is the machine that has no agent, and an engineer wants protection answered beside the machine's disks, patches and alerts, not in a second console.

THE QUESTION	SENTINELONE CONSOLE ALONE	CLEARWATCH
Which client is this agent?	A site name, inside SentinelOne	Each site **mapped to a client**, once
Which machines have no agent?	Not listed anywhere	**Listed and alerted**, client by client
Is it the machine we monitor?	Compare names across two consoles	**Matched to its device** by serial, MAC or name
Is the agent still reporting?	Read each agent's last active date	Past the window, **Not reporting**
Why does Defender say antivirus off?	A false alarm somebody learns to ignore	**SentinelOne running passes** the antivirus checks

Two halves of one question

The console says whether SentinelOne lists a machine. The machine's own service list says whether SentinelOne is running on it. An agent whose service was stopped can stay listed for days before the console notices, so ClearWatch asks both: the console at every sync, and the machine at its next inventory.

02 HOW CLEARWATCH CONNECTS

From ClearWatch's servers, read only

SentinelOne's console is a cloud service, so ClearWatch reads it the same way: its own servers call the console's API every 10 minutes. Nothing is installed at a client's site, and no ClearBridge is involved.

EACH MACHINE
SentinelOne agent
Protects the machine and reports to its console, exactly as it does today.

→

SENTINELONE CLOUD
Your console
Answers ClearWatch's questions about sites, agents and open threats.

→

CLEARWATCH'S SERVERS
SentinelOne integration
Maps sites, matches agents to devices, runs the checks and raises the alerts.

The token stays on ClearWatch's servers. Only an address on sentinelone.net is accepted, and a redirect is never followed, so the token cannot be carried to another host.

YOU PROVIDE	WHAT IT IS
Console address	Pasted from the browser's address bar, for example **https://usea1-demo.sentinelone.net**. Only the host is kept.
API token	A service user's token, made in SentinelOne under Settings, Users, Service Users, with the **Viewer** role at the account or site to be read.
Not reporting after	Minutes without word from an agent before its machine reads as not reporting. 3 days by default, from an hour up to 90 days.

02 HOW CLEARWATCH CONNECTS, CONTINUED

A console address and a Viewer token

Under Manage, Integrations, SentinelOne, **Add connection** opens a window. The connection belongs to the client chosen in the console's picker 1 , which for an MSP is usually its own organization: that says who owns the connection, not whose machines it finds.

The console address is pasted as it is 2 . The token belongs to a service user with the **Viewer** role 3 , so ClearWatch can see everything and change nothing. A token already stored, or one held in Keeper, can be picked instead of pasted.

Not reporting after 4 is how long an agent may stay silent before its machine counts as missing. Three days by default, so a weekend with the lid shut is not a missing laptop.

Pressing Add starts the first read at once and shows it step by step: sign in, read the sites, write the agents, match them to devices. Closing the window does not stop it.

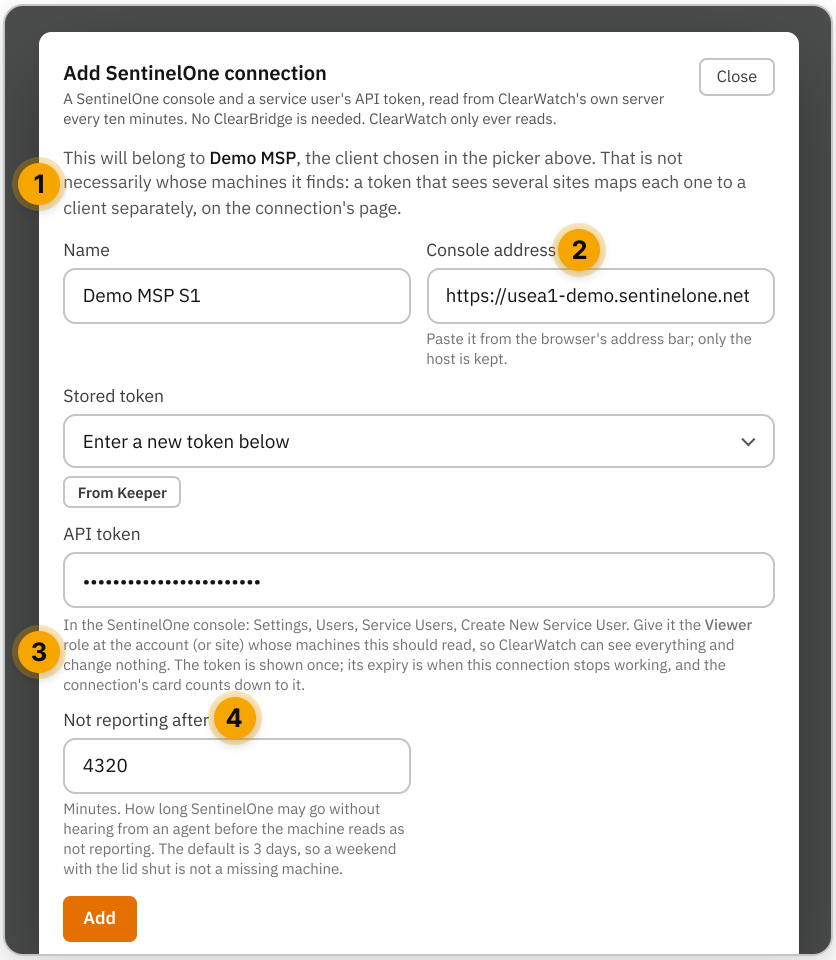


FIGURE 1 Add SentinelOne connection, rebuilt from the ClearWatch console with demo data.

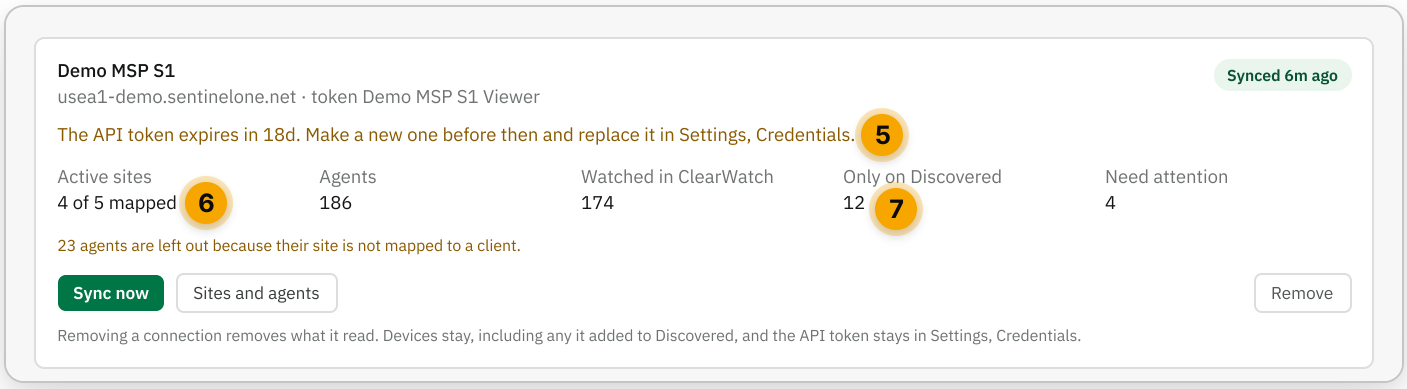


FIGURE 2 A connection's card on the SentinelOne integration page.

A service user's token expires on a date chosen when it was made, and the day it lapses every machine goes quiet at once. ClearWatch reads the expiry at each sync and the card says it in amber a month ahead 5 .

The card counts what matters: sites still to map 6 , agents watched in ClearWatch, and agents ClearWatch only knows from Discovered 7 , kept apart so neither hides in the other.

03 SITES TO CLIENTS

One console, many clients

An MSP's console usually holds a site per client. On the connection's page, each site is mapped to one of your clients by a person.

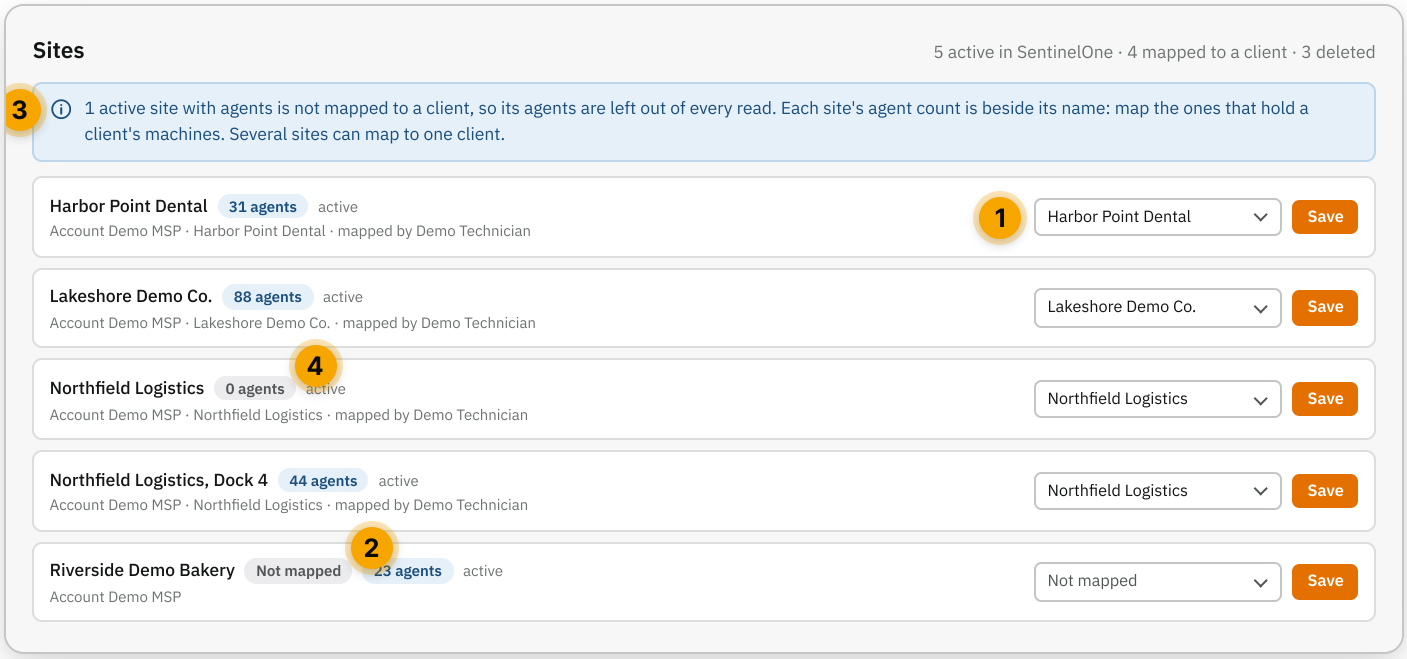


FIGURE 3 The Sites list on a SentinelOne connection's page.

Mapped by a person

Each site is placed under a client with the client picker 1 , and several sites can map to one client. A mapping stays through every later read.

Unmapped is never guessed

No name matching, no fallback: an unmapped site's agents 2 are counted and left out 3 , so a client never inherits another's machines.

Counts show the real site

Every site shows how many agents it holds, so an empty parent 4 is not mistaken for the site holding the machines. Deleted sites are folded away.

04 AGENTS AND MACHINES

Every agent matched to the machine it runs on

A SentinelOne agent reports the same hardware the ClearWatch agent does, so the hardware is tried first and the names after it. The first rule that finds exactly one device links it.

Two devices that match equally link nothing: the page says so and a person enters the right device. A link set by hand is never overwritten, and an automatic link whose evidence goes away (a new board, a rename) is dropped at the next read.

RULE, IN ORDER	COMPARES
Serial number	The agent's serial against the device's, when it is a real one
Network card address	Any physical MAC against the device's adapters
Computer name	The name, past its domain suffix, against the device's
Hypervisor guest name	The same name against what the hypervisor calls the guest

04 AGENTS AND MACHINES, CONTINUED

Every agent, worst first, with SentinelOne's own reason

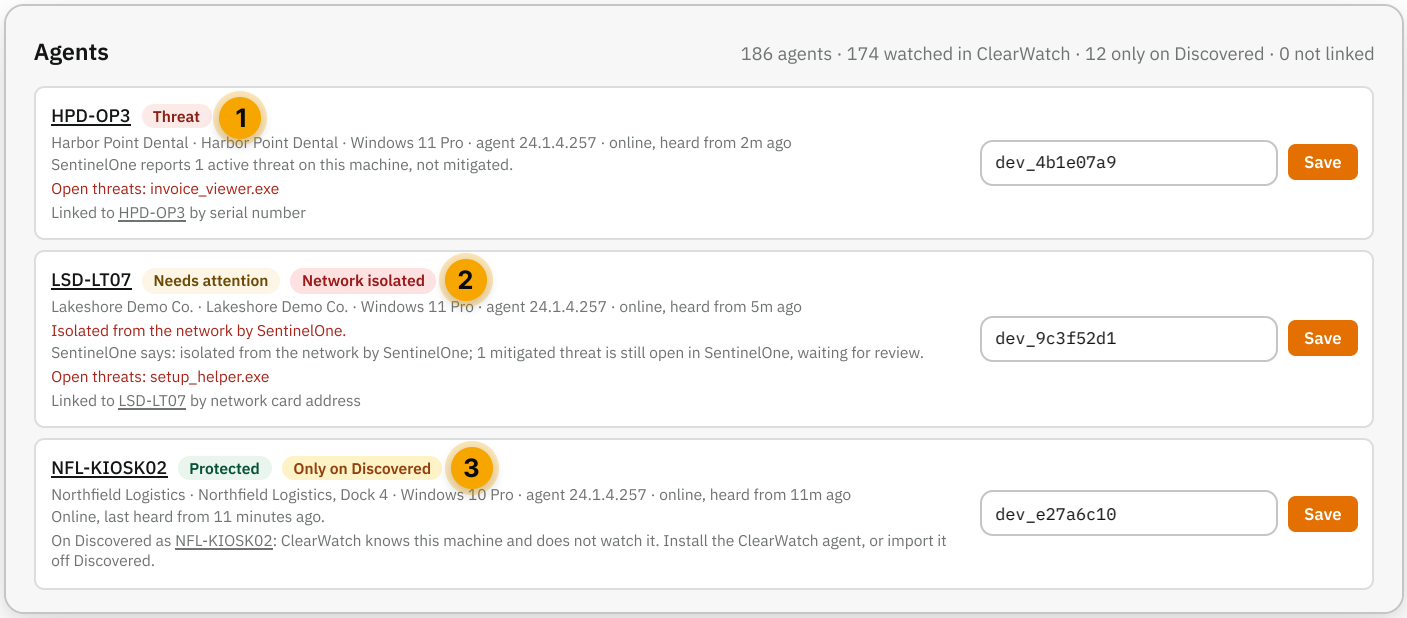


FIGURE 4 Agents on the same page (cropped: the protected machines follow below).

Each agent has one state, decided in one place: a threat SentinelOne has not mitigated (1) outranks silence, and silence outranks a warning. A machine SentinelOne has isolated from the network (2) is said in plain words. An agent offline for an hour stays Protected: SentinelOne keeps protecting a laptop with its lid shut.

A mitigated threat still waiting for an analyst is not hidden behind a green chip: it warns, by name. An agent on a machine ClearWatch has never seen is added to Discovered (3), unlicensed and free until somebody imports it. Each name opens that machine in SentinelOne's console.

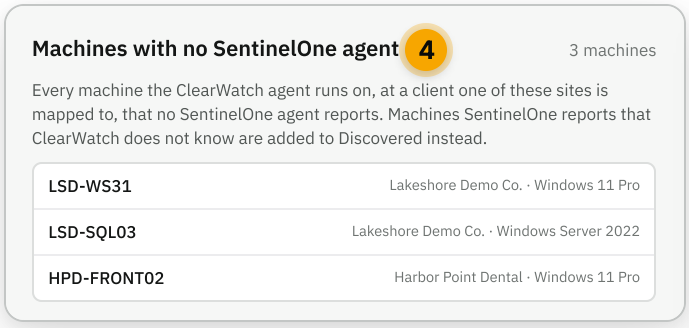


FIGURE 5 The missing half, on the connection's page.

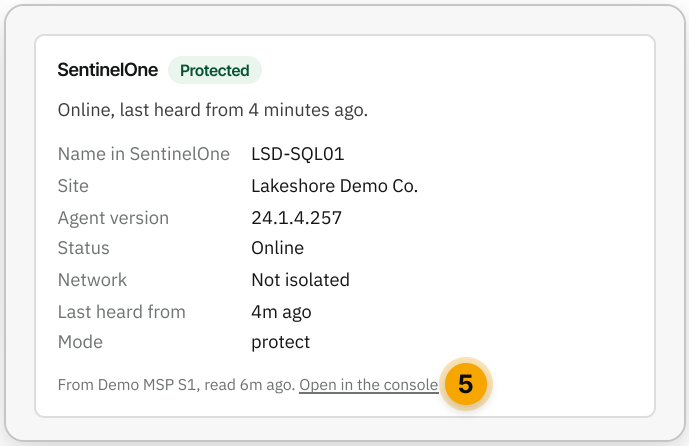


FIGURE 6 The SentinelOne card on a device's page.

The other half: every machine ClearWatch watches at a client that uses SentinelOne, with no agent reporting it (4). Hypervisor hosts and ClearBridge appliances are left out. The same rule drives the presence check, so the list and the alert name the same machines.

On the device's own page, the card says what SentinelOne says, and when it was read. **Open in the console** (5) goes to that machine's own page in SentinelOne, and the title row shows **SentinelOne Protected**, or **Not installed** where the agent is missing.

05 CHECKS AND ALERTS

Five checks, on from the first sync

The built-in **Endpoint protection (SentinelOne)** monitor is applied by the built-in SentinelOne template to every machine the ClearWatch agent runs on, except Proxmox hosts and ClearBridge appliances. Every check answers nothing for a client with no site mapped, so only the clients that use SentinelOne are measured. Warning is Needs attention, Failed is an alert, and every level is a default you can change.

CHECK	WARNING	FAILED
SentinelOne threats	A mitigated threat still open for review, named	An active threat SentinelOne has not mitigated, named
SentinelOne agent present	None	No SentinelOne agent reports the machine: "SentinelOne agent missing"
SentinelOne agent health	Out of date, a reboot, a missing permission, detect only, or isolated	Protection switched off
Days since SentinelOne heard from it	3 days or more	7 days or more
SentinelOne services running	None	A SentinelOne service is stopped, or none is installed, read from the machine's own service list

The antivirus checks agree

Where SentinelOne runs, Defender steps aside, and a plain antivirus check would fail the machine. At a client with a site mapped, a running SentinelAgent service answers the antivirus checks instead: **Protected by SentinelOne (Defender stepped aside)**, and the definitions age reads **Not checked: protected by SentinelOne**.

Filters for everything else

Three filter fields, **Protected by SentinelOne**, **SentinelOne state** and **Days since SentinelOne heard from it**, target templates, patch policies, schedules and alert routing like any other. "Protected by SentinelOne is no" finds the machines without it.

06 GOOD TO KNOW

Requirements

- A SentinelOne console on sentinelone.net, and a service user with the Viewer role at the account or site to be read.
- That service user's API token, stored for the organization that owns the connection.
- Nothing on site: no ClearBridge, and nothing new on the machines.

Limits

- The token expires on the date SentinelOne set for it; replace it before then, or every machine reads as not reporting.
- ClearWatch reads only: isolating, scanning and acting on threats stay in SentinelOne's console.
- The not reporting window is one per connection, not per machine.

Prove SentinelOne is on every machine.

Start a free trial, or ask us to connect your SentinelOne console with you.

clearwatch.com

ClearWatch™ is a trademark of ClearPath MSP. SentinelOne and Singularity are trademarks of SentinelOne, Inc. Screens show demo data.