ClearPath MSP
ClearWatch

SOLUTION BRIEF

from ClearPath MSP

CLEARWATCH SOLUTION BRIEF · DEFENSX

DefensX monitoring, client by client.

How ClearWatch reads a DefensX partner account and finds the workstations DefensX should protect and does not.

PUBLISHED NOVEMBER 2026 LENGTH 6 PAGES APPLIES TO DEFENSX PARTNER ACCOUNTS

EXECUTIVE SUMMARY

A machine without DefensX is not in DefensX

DefensX protects each machine's browsing and lists its agents under each DefensX customer in the partner dashboard. That shows the machines DefensX knows about. It cannot show the client's workstation that never got the agent, because that machine is not in DefensX to be missed.

ClearWatch reads the DefensX Partner API from its own servers with a Read Only key. Each DefensX customer is mapped to a client, each agent is matched to its ClearWatch device by computer name, and three built-in checks alert when a workstation has no DefensX agent, when DefensX stops hearing from one, or when its services stop on the machine.

KEY TAKEAWAYS

- **Nothing on site:** ClearWatch's servers read DefensX's cloud. No ClearBridge, nothing new installed.
- **Read only:** a Read Only key, and every call is a read. No DefensX policy is ever changed.
- **Both halves of missing:** workstations with no DefensX agent, and DefensX agents ClearWatch does not know.
- **Quiet where unused:** a client with no DefensX customer mapped gets no DefensX check at all.

IN THIS BRIEF

01 **The challenge** — What the partner dashboard leaves to you — 2
02 **How ClearWatch connects** — Cloud to cloud, with a Read Only key — 2
03 **Customers and agents** — Customers to clients, agents to devices — 4
04 **On every device** — The title row, the card, what is missing — 5
05 **Checks and alerts** — Three built-in checks and their defaults — 6
06 **Good to know** — Requirements and limits — 6

WHO THIS IS FOR

MSPs that deliver DefensX to their clients through a DefensX partner account, and want each machine's DefensX status beside the rest of their monitoring.

AT A GLANCE

CONNECTION
Cloud to cloud
One Read Only Partner API key per MSP.

REFRESHED
Every 10 minutes
Agents every pass; customer activity hourly.

HELD TO DEFENSX
Windows and Mac
Workstations always; a server once DefensX is found on it.

NOT REPORTING
After 3 days
The window, set per connection.

01 THE CHALLENGE

DefensX answers by DefensX customer, not by client

An MSP's DefensX partner dashboard lists customers and, under each, the agents DefensX has. That is the right view for running DefensX. The question a client is paying for is different: does every one of our workstations have DefensX, is it still reporting, and is it actually running? Answering it means setting DefensX's list beside the list of machines you manage, and comparing them by eye.

THE QUESTION	PARTNER DASHBOARD ALONE	CLEARWATCH
Which client is this customer?	DefensX's customer name	Each DefensX customer **mapped to a client**, once
Which workstations have no agent?	Not in DefensX to be missed	Every managed workstation compared, **missing ones listed and alerted**
Is the agent still reporting?	Read each agent's last seen	**Not reporting** past the connection's window
Is it running on the machine?	Look at the machine	DefensX's **services read from the machine** at each check-in
Who is told, and how?	Another console to watch	Three checks, routed by **your notification policies**

Workstations are expected; servers are an exception

A Windows or Mac workstation at a client that uses DefensX is expected to run it, so a missing agent is a finding. A server is watched only once DefensX is found on it, and is never reported missing. Linux machines, hypervisors and ClearBridge appliances are never held to DefensX.

02 HOW CLEARWATCH CONNECTS

Cloud to cloud, from ClearWatch's servers

DefensX's Partner API is a cloud service at one fixed address, so ClearWatch's own servers read it every 10 minutes. Nothing is installed at a client's site for it, and no ClearBridge is involved.

EACH WINDOWS AND MAC MACHINE
DefensX agent
Protects browsing and reports to DefensX, exactly as it does today.

→

DEFENSX CLOUD
Partner API
Answers with your customers, their agents and users, and each customer's recent activity.

→

CLEARWATCH'S SERVERS
Devices and checks
Maps customers, matches agents to devices, runs the checks and raises the alerts.

ClearWatch only reads: every call it makes to DefensX is a read. The key is stored sealed and used only by ClearWatch's servers, never sent to a machine.

YOU PROVIDE	WHAT IT IS
API key	A key created on the DefensX partner dashboard's **API Keys** page with **Read Only** access. If the key is limited to IP addresses, allow ClearWatch's servers. ClearWatch asks DefensX whether the key works before saving it.
Name	What the connection is called in ClearWatch.
Not reporting after	Minutes DefensX may go without hearing from an agent before the machine reads as Not reporting. Three days by default, from an hour up to 90 days.

02 HOW CLEARWATCH CONNECTS, CONTINUED

One key, at your MSP account

DefensX's Partner API is built for MSPs, so the integration is switched on and connected at the MSP's own account, under Manage, Integrations, DefensX. **Add connection** opens a window, and the connection belongs to the account chosen in the console's picker 1 . That says who owns it, not whose machines it finds.

The key is pasted once, or picked from keys already stored, and DefensX is asked whether it works before anything is saved. The window asks for **Read Only** access 2 , and **Not reporting after** sets how long an agent may be silent 3 .

Each MSP brings its own key, and a key's customers can only be placed under that MSP's own clients.

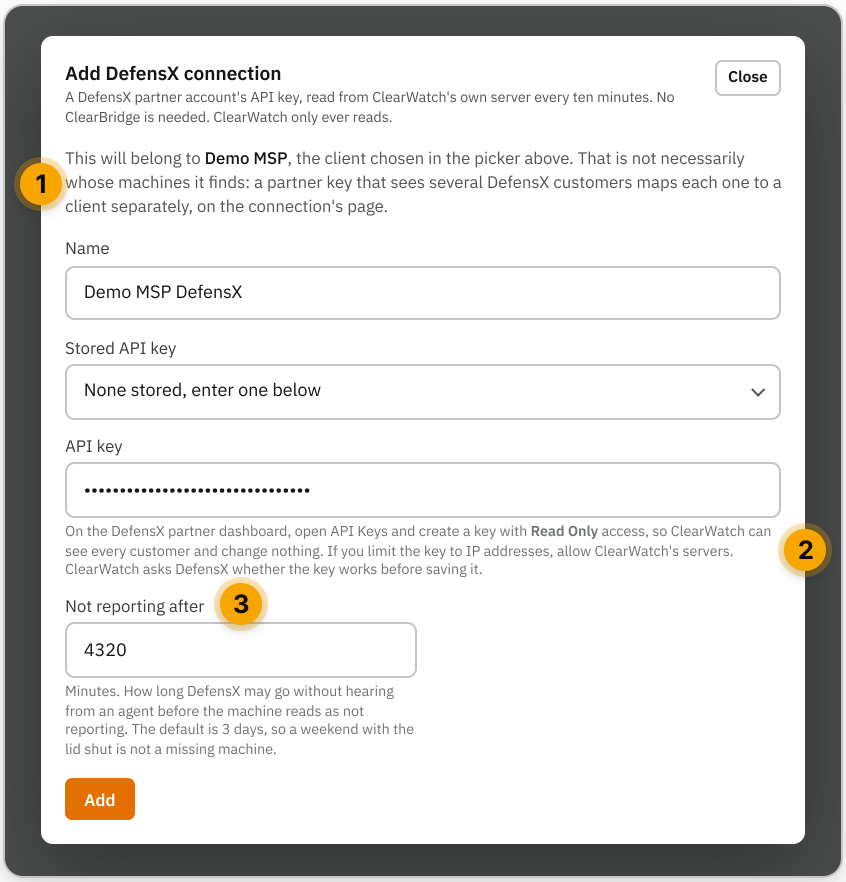


FIGURE 1 Add DefensX connection, rebuilt from the ClearWatch console with demo data.

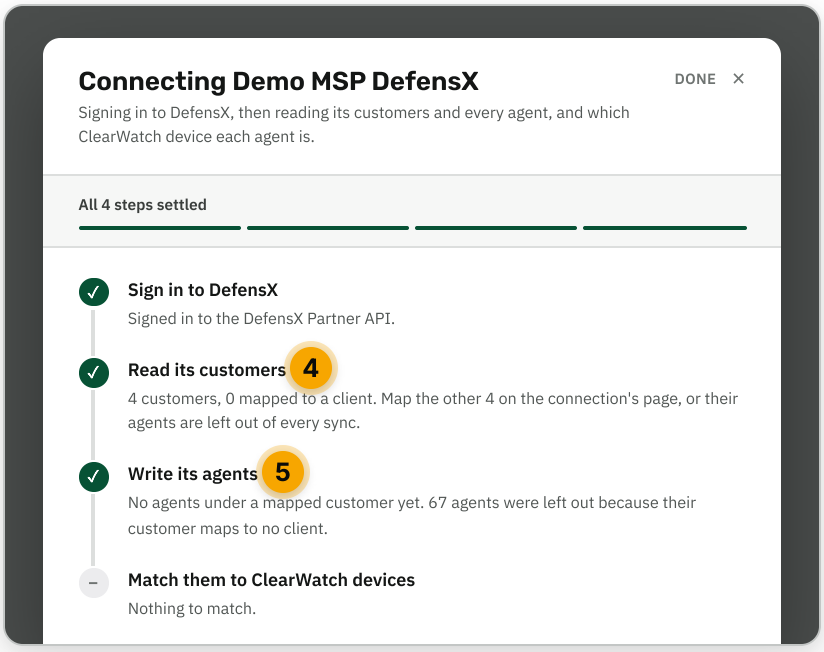


FIGURE 2 The first read of a new connection, step by step (cropped).

The first read, live

Pressing Add starts the first read at once and shows it step by step: sign in, read the customers, write the agents, match them to devices.

A key that sees a single customer maps it to the MSP on its own. With several, every customer waits for a person 4 , so their agents are counted and left out 5 rather than filed under a guess. Closing the window does not stop the read.

03 CUSTOMERS AND AGENTS

Each DefensX customer, placed under a client

Customers come first: an agent reaches a client only once its customer is mapped.

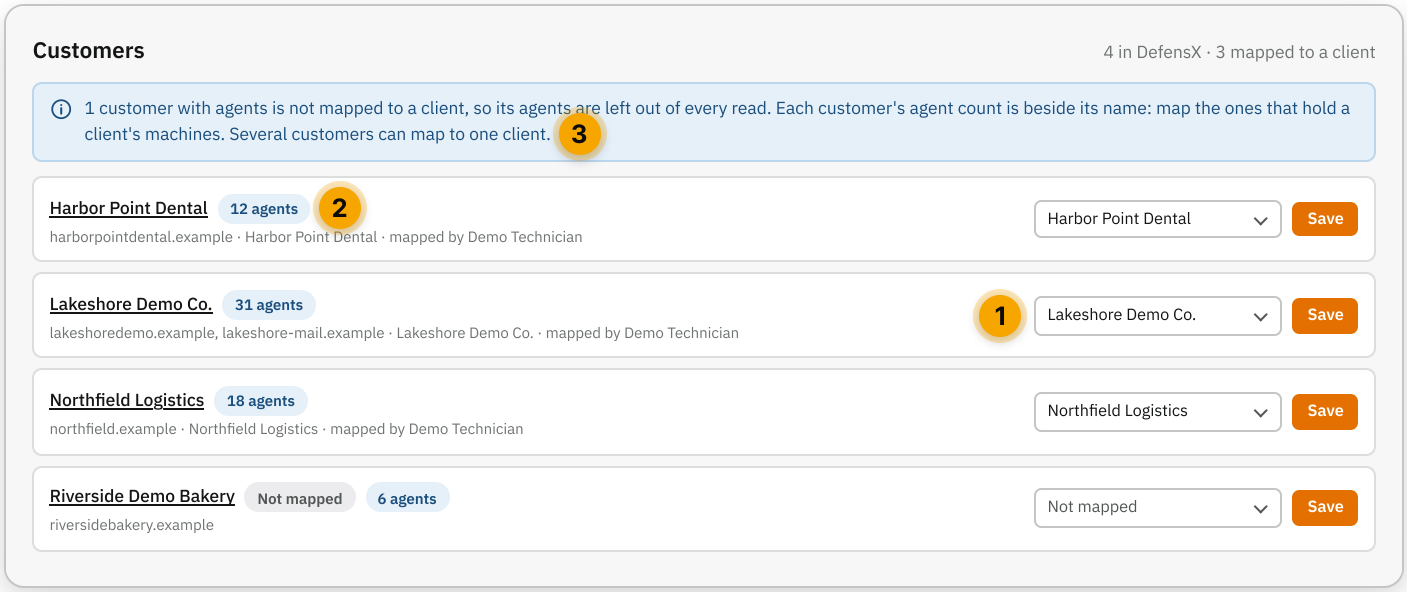


FIGURE 3 Customers on a DefensX connection's page. Each name opens that customer in DefensX.

Mapped by a person

Each customer is placed under a client with the client picker 1 , which offers only the MSP's own clients. Several customers can map to one client.

Counted, so it is seen

Each customer shows how many agents DefensX holds for it 2 , so an empty customer and the one holding every machine never look alike.

Never guessed

No name or domain matching: an unmapped customer's agents are counted and left out 3 until somebody maps it.

Every agent matched to its device

A DefensX agent carries a computer name and nothing else that identifies the machine, so the name is the evidence. It is compared past its DNS suffix and its punctuation, so **MacBook-Air.local** and **MacBook Air** are one machine 4 .

Two devices with the same name link nothing, and the page asks a person to enter the right one 5 . A link set by hand is never overwritten. Each row says why it is linked and opens the agent in DefensX.

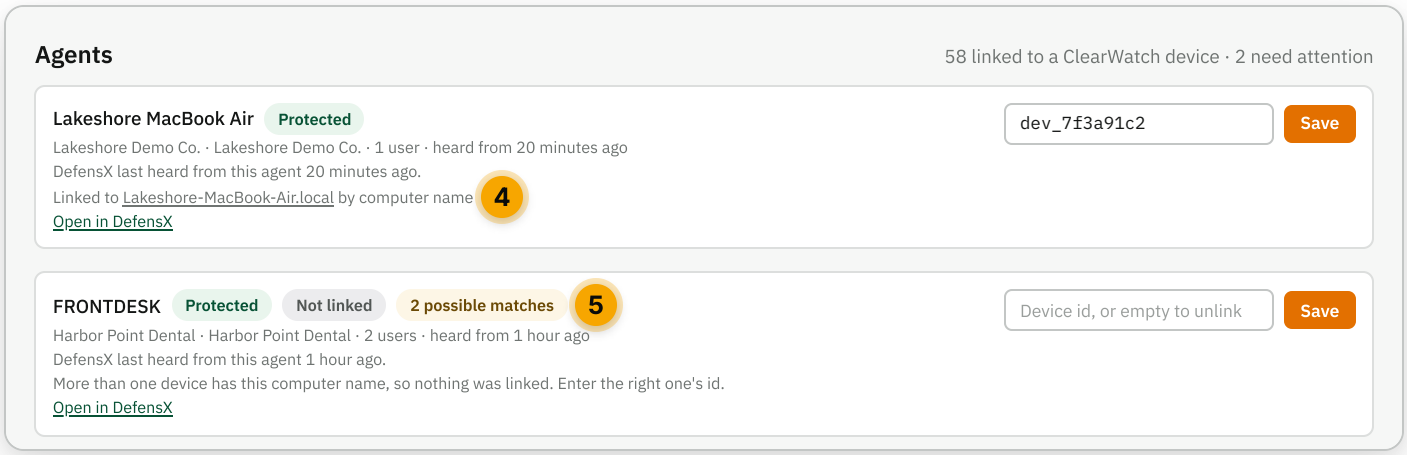


FIGURE 4 Agents on the same page, each with how it was linked.

04 ON EVERY DEVICE

What DefensX says, on the machine's own page

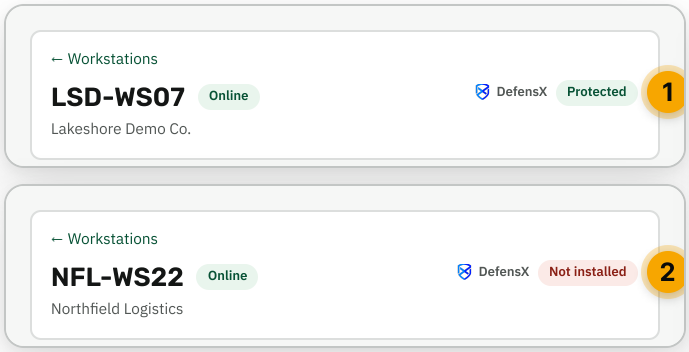


FIGURE 5 The DefensX line on two device pages' title rows (cropped; the row's buttons are left out).

Every Windows and Mac device page carries a **DefensX** line in its title row, below SentinelOne's where both are used. A linked agent shows its state, Protected, Not reporting, Uninstalled or Unknown, and the chip opens the agent in DefensX 1 . A workstation at a client that uses DefensX with no agent and no DefensX service running reads **Not installed** 2 ; one whose services are stopped reads **Not running**.

A machine at a client without DefensX, or a server where it was never found, shows no line at all.

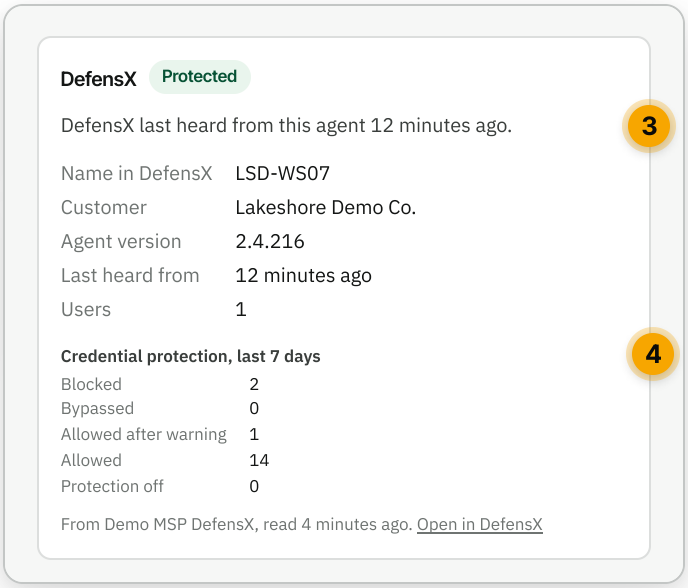


FIGURE 6 The DefensX card, in the Security section of the device's Software tab.

Beside the machine's own security posture, the DefensX card gives the state and why 3 , the agent's version, its users, and when DefensX last heard from it. Below, the last seven days of credential protection events by action 4 . If a customer has switched partner logs access off in DefensX, the card says **Not read** and why, never zero.

Missing, in both directions

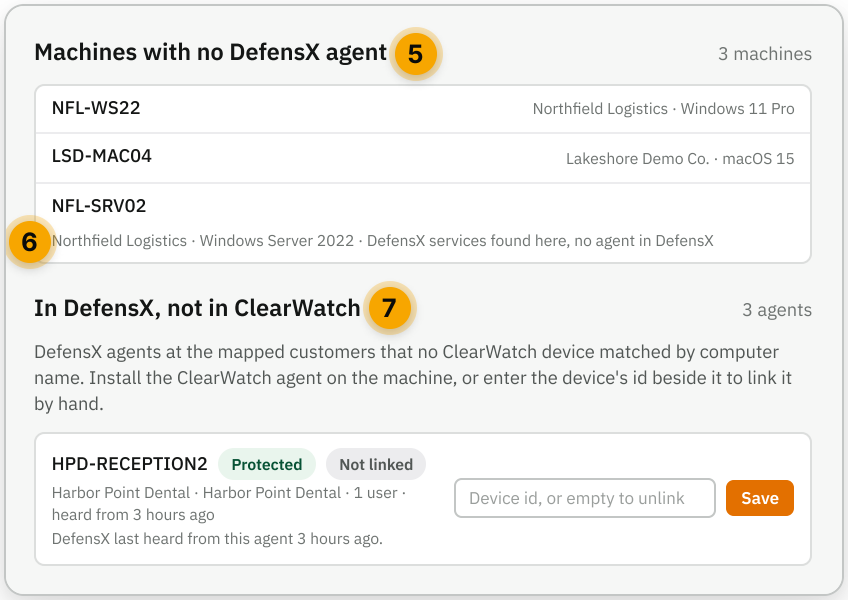


FIGURE 7 Both lists on the connection's page.

Machines with no DefensX agent 5 lists every Windows and Mac workstation the ClearWatch agent runs on, at a mapped client, that no DefensX agent reports. A server appears only when DefensX's services run on it and DefensX lists no agent 6 . The list and the alert use one rule, so they name the same machines.

In DefensX, not in ClearWatch 7 is the other half: agents nothing matched, each with a field to link it by hand.

The device list also offers a **DefensX** column, and filters can target *Protected by DefensX*, *DefensX state* and *Days since DefensX heard from it*.

05 CHECKS AND ALERTS

Three checks, on by default, silent where DefensX is not used

The built-in monitor **Web protection (DefensX)** carries three checks in the Endpoint protection group. The built-in template **DefensX** applies it to every client, over the filter **Windows and Mac devices DefensX protects**, and ships switched on. Every level is a default you can change, for everyone or for one device.

CHECK	WARNING	FAILED
DefensX agent present	None: it passes or fails	The client uses DefensX and DefensX lists no agent for this machine, or says its agent was uninstalled. The alert reads **DefensX agent missing on** the machine.
Days since DefensX heard from it	Above 3 days	Above 7 days
DefensX services running	None: it passes or fails	A DefensX service on the machine is not running, or none is installed on a workstation at a client that uses DefensX

Two views of one machine

The first two checks are DefensX's view, evaluated at the end of each read of DefensX. The services check is the machine's own view, read from the service list the ClearWatch agent already reports at check-in: the **DefensX Agent** service on Windows, **DefensXAgent** on a Mac, and the helpers beside them.

Why on by default is safe

Every check answers nothing for a client with no DefensX customer mapped, and for a machine not held to DefensX. So the template measures exactly the clients that use DefensX, including the workstations that have no agent to attach anything to. DefensX is web protection, so it never counts as a machine's antivirus.

06 GOOD TO KNOW

Requirements

- A DefensX partner account, and a Read Only API key from its API Keys page.
- If the key is limited to IP addresses, ClearWatch's servers allowed.
- The integration switched on, and the connection added, at your MSP account.
- The ClearWatch agent on the Windows and Mac machines you want compared.

Limits

- ClearWatch reads only: it changes no DefensX policy, agent or customer setting.
- An agent is matched by computer name alone; machines sharing a name are linked by hand.
- An agent with no ClearWatch device is listed on the connection's page, not added as a device.
- Blocked sites are each customer's hourly summary, not a per-machine history.

See every DefensX workstation, client by client.

Start a free trial, or ask us to connect your DefensX partner account with you.

clearwatch.com

ClearWatch™ is a trademark of ClearPath MSP. DefensX is a trademark of its owner. Screens show demo data.