ClearPath MSP
ClearWatch

SOLUTION BRIEF

from ClearPath MSP

CLEARWATCH SOLUTION BRIEF · MICROSOFT DEFENDER FOR ENDPOINT

Microsoft Defender, on every device.

How ClearWatch reads a client's Defender for Endpoint after one approval at Microsoft, matches each machine to its device and names the workstations Defender is missing.

PUBLISHED NOVEMBER 2026 LENGTH 6 PAGES APPLIES TO MICROSOFT DEFENDER FOR ENDPOINT

EXECUTIVE SUMMARY

Defender knows machines. You need clients.

The Microsoft Defender portal answers one tenant at a time, about the machines Defender already knows. An MSP needs more: is every workstation at this client onboarded, is the sensor still reporting, and is the machine with a high alert the one our monitoring watches? A workstation never onboarded is not in Defender at all.

ClearWatch connects to a client's tenant after its own administrator approves a read-only app at Microsoft, so no password is ever handed over. It reads every 10 minutes, matches each Defender machine to its ClearWatch device, puts Defender's health, risk and open alerts on the device page and runs built-in checks that alert like any other.

KEY TAKEAWAYS

- **No password, ever:** the tenant's administrator approves at Microsoft, and nothing of theirs is stored.
- **Read only:** two read permissions; ClearWatch never isolates, scans or changes anything in Defender.
- **Machines become devices:** matched by Entra device ID, then by computer name.
- **Gaps both ways:** workstations Defender does not list, and Defender machines ClearWatch does not know.

IN THIS BRIEF

01 **The challenge** — What one tenant at a time leaves to you — 2
02 **How ClearWatch connects** — One approval at Microsoft, read only — 2
03 **One tenant, one client** — Matching, and what is missing — 4
04 **Defender on the device** — States, alerts and the device card — 5
05 **Checks and alerts** — Onboarded, reporting, alerts — 6
06 **Good to know** — Requirements and limits — 6

WHO THIS IS FOR

MSPs whose clients run Microsoft Defender for Endpoint or Defender for Business, and IT teams with their own tenant, who want Defender's view of each machine beside the rest of their monitoring.

AT A GLANCE

CONNECTION	REFRESHED	PLACEMENT	ACCESS
Admin consent	**Every 10 minutes**	**Per client**	**Read only**
Approved at Microsoft by the tenant's administrator.	Machines, antivirus details and open alerts.	One tenant, one client; matching never looks outside it.	Nothing is ever written to Defender.

01 THE CHALLENGE

Defender answers by tenant, not by client

Defender for Endpoint watches each onboarded machine closely, and its portal lists them by tenant with Defender's own names. That suits running Defender. But a client wants to know every machine they own is protected, and an engineer wants that answer beside the machine's disks, patches and alerts, not in a second console opened one tenant at a time.

THE QUESTION	DEFENDER PORTAL ALONE	CLEARWATCH
Which client is this machine?	Switch to that client's tenant	Each tenant **connected to one client**
Is it the machine we monitor?	Compare names across two consoles	**Matched to its device** by Entra device ID or name
Which workstations is Defender missing?	A machine never onboarded is not listed	Every agent workstation **Defender does not list**
Has the sensor gone quiet?	Read each machine's last seen time	**Not reporting** after 3 days, and a check
Who is told about a high alert?	Another console to watch	Built-in checks, routed by **your notification policies**

A machine Defender never saw raises no alert

Defender can only report on the machines it knows. A workstation where onboarding never ran, or where the sensor was removed, is simply absent from the portal. ClearWatch already knows every machine its agent runs on, so it can name each Windows and Mac workstation Defender does not list, and fail a check on it.

02 HOW CLEARWATCH CONNECTS

One approval at Microsoft, then cloud to cloud

Defender for Endpoint reports to Microsoft's cloud, so ClearWatch reads it there: its own servers call the Defender API every 10 minutes, as a read-only app the client's administrator approved. Nothing is installed for it, and no ClearBridge is involved.

EACH MACHINE
Defender for Endpoint
The sensor reports to Microsoft exactly as it does today.

→

MICROSOFT CLOUD
The Defender API
Answers ClearWatch's questions about machines, antivirus and open alerts.

→

CLEARWATCH'S SERVERS
Device pages and checks
Matches machines to devices, runs the checks and raises the alerts.

ClearWatch only reads: every call to Defender is a read. The client's administrator can withdraw the approval in Microsoft Entra at any time.

YOU PROVIDE	WHAT IT IS
The tenant's domain or ID	The client's Microsoft domain, or its tenant ID, typed into **Add tenant**. ClearWatch looks the tenant up from the domain.
An administrator's approval	A Global Administrator or Privileged Role Administrator of the tenant presses Accept at Microsoft, once. Their password never reaches ClearWatch.
Not reporting after	How long Defender may go without seeing a machine before it reads as not reporting. 3 days by default, set per tenant.

02 HOW CLEARWATCH CONNECTS, CONTINUED

A domain, a link and an administrator's Accept

Under Manage, Integrations, Microsoft Defender, **Add tenant** opens a window. The tenant is connected to the organization chosen in the console's picker 1 : that client is where its machines are looked for.

Type the tenant's domain or tenant ID and press **Make link**. **Enable Defender** 2 takes an administrator of the tenant to Microsoft, where they sign in under their own MFA and press Accept. That creates the ClearWatch Defender Enterprise App in their tenant, and ClearWatch reads Defender as that app.

Approving needs a Global Administrator or a Privileged Role Administrator. If that is somebody else, copy the link for them 3 . It works for seven days and finishes only in your own ClearWatch session.

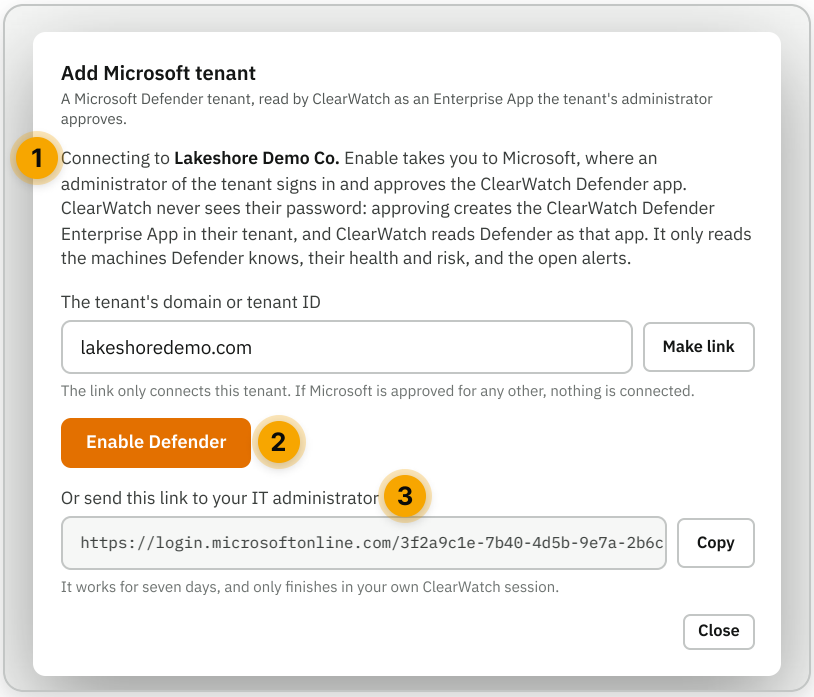


FIGURE 1 Add Microsoft tenant, rebuilt from the ClearWatch console with demo data.

What the approval grants

The ClearWatch Defender app asks for two application permissions on the Defender API, both reads. If a later version needs another, the connection reads **Needs approval again**, names the permission and offers the link, and nothing that needs it is read until the administrator approves.

PERMISSION	WHY CLEARWATCH NEEDS IT
Machine.Read.All	Every machine: health, onboarding, risk, exposure and antivirus details
Alert.Read.All	The alerts that are open now

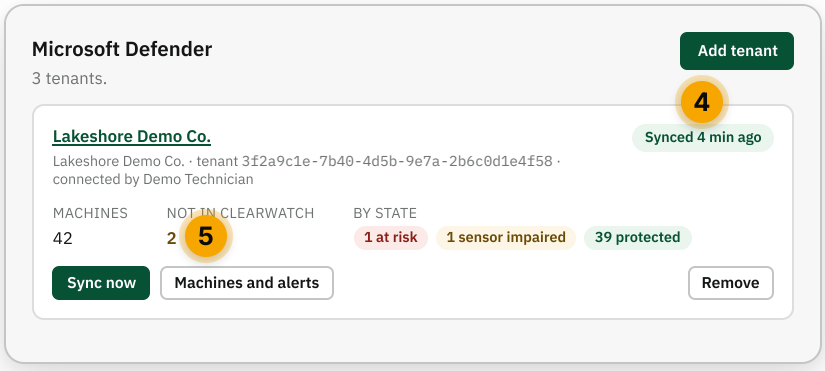


FIGURE 2 A connected tenant on the Microsoft Defender page.

Every tenant on one page

Each connected tenant is a card: when it was last read 4 , how many machines Defender lists, how many no ClearWatch device matched 5 , and its machines by state. **Sync now** reads it at once.

A tenant without Defender for Endpoint or Defender for Business cannot approve, and the window says so in a sentence.

03 ONE TENANT, ONE CLIENT

Every Defender machine matched to its device

A Microsoft tenant belongs to one client, so a connection does too, and a machine is only ever matched to a device at that client. A machine in one client's tenant can never be linked to another client's device.

Defender's Entra device ID is matched first, against the ID the ClearWatch agent reports. Failing that, the computer name. Two devices with the same name link nothing, and a link set by hand is never overwritten.

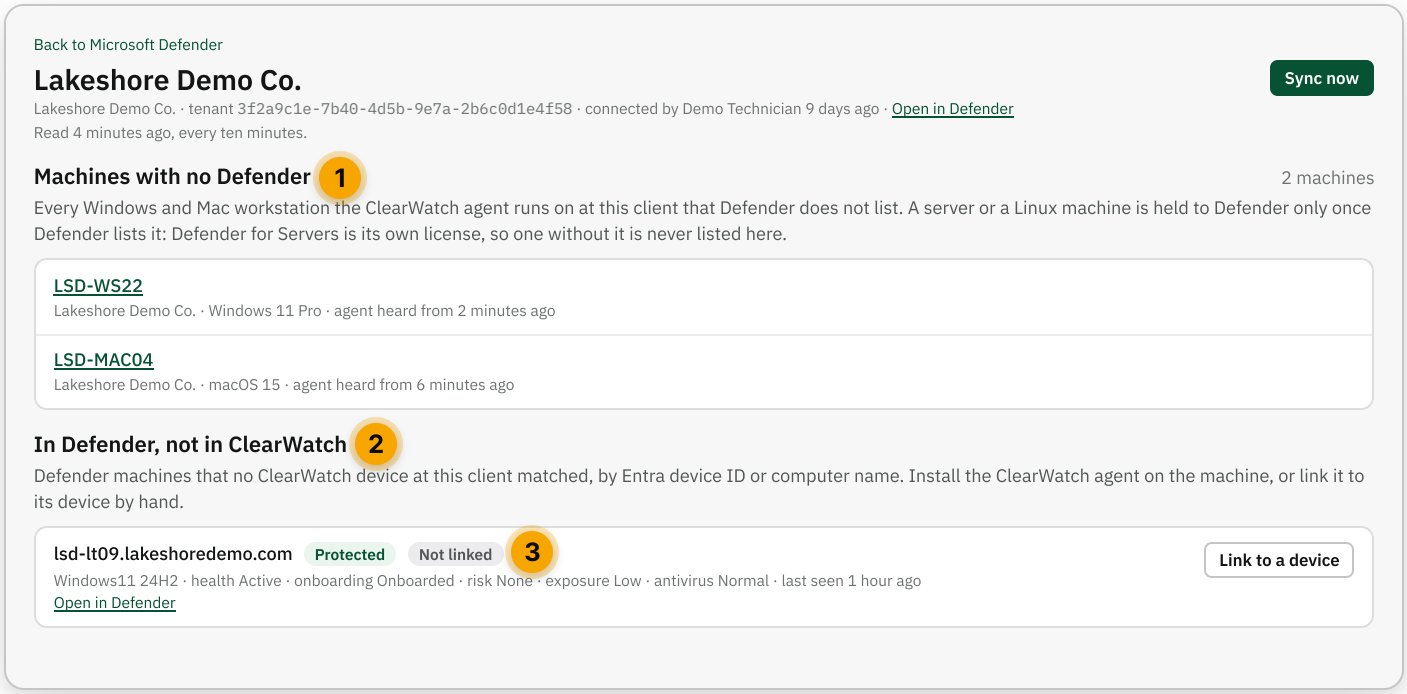


FIGURE 3 A tenant's page: the gaps in both directions come first (cropped: every machine and the open alerts follow).

Missing, in both directions

The tenant's page opens with what does not line up. **Machines with no Defender** 1 are the workstations ClearWatch watches and Defender does not list. **In Defender, not in ClearWatch** 2 are machines Defender protects that no device matched 3 : install the agent, or link one by hand. Which machines Defender should know depends on what they are:

MACHINE	HELD TO DEFENDER
Windows or Mac workstation running the ClearWatch agent	**Expected:** missing from Defender fails its check
Windows or Mac server, any Linux machine	**Once Defender lists it:** watched, never reported missing
Hypervisors, ClearBridge appliances, other systems	**Never**

04 DEFENDER ON THE DEVICE

Defender's view of each machine, in one word

Every machine gets one state, decided the same way on the tenant's page, the device page and in the checks. The worst that applies wins, and a word from Defender that ClearWatch does not recognize is shown as Unknown, never as Protected.

STATE	WHEN
At risk	Defender rates the machine's risk High or Medium, or a High or Medium alert is open on it
Sensor impaired	Defender reports impaired communication or no sensor data
Not reporting	Defender calls it inactive, or has not seen it within the tenant's window (3 days by default)
Unknown	No health or last seen time, or a health word ClearWatch does not know
Protected	Active, and none of the above

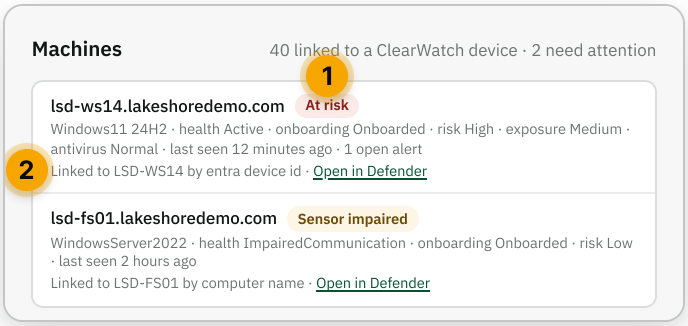


FIGURE 4 Machines on the tenant's page, worst first.

On the device's own page

Every machine says why it is not green (1) and how it was linked (2). Because it is matched to its device, the **Microsoft Defender** card sits in the device page's Security section beside everything else ClearWatch knows about it (3): health, onboarding, risk, exposure, the antivirus mode and how current its signatures and engine are.

The open alerts are listed on the card, each linking to the alert in Defender (4), and **Open in Defender** goes to the machine in the client's tenant.

The device's title row carries a **Defender** line with the same state. A workstation Defender should know and does not reads **Not onboarded** there instead.

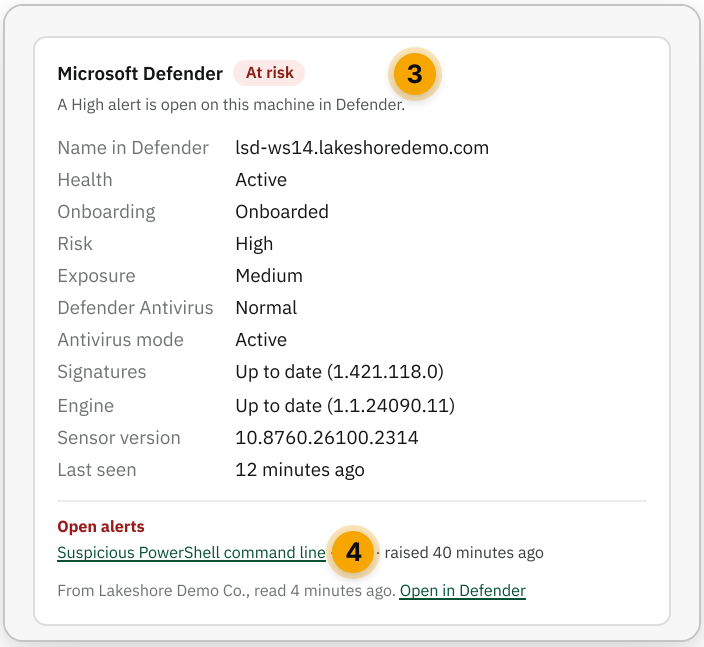


FIGURE 5 The Microsoft Defender card on a device page.

05 CHECKS AND ALERTS

Three checks, on from the start

The built-in monitor **Endpoint detection (Microsoft Defender)** ships in the **Microsoft Defender** template, switched on for every client and applied to Windows and Mac devices. Its checks answer nothing at a client with no connected tenant, so they measure exactly the clients that use Defender. A Warning goes to Needs attention, a Failed is an Alert, and every level is a default you can change, for everyone or for one device.

CHECK	WARNING	FAILED
Defender for Endpoint onboarded	None	A machine held to Defender has no Defender machine linked, or it is not Onboarded
Days since Defender for Endpoint saw it	3 days	7 days
Defender for Endpoint alerts	A Medium alert is open	A High alert is open

A missing machine is worded "Defender for Endpoint missing on" its host, so the alert says what is wrong. Low and informational alerts pass. Alerts follow your notification policies like any other check.

06 GOOD TO KNOW

Requirements

- Microsoft Defender for Endpoint or Microsoft Defender for Business in the client's tenant.
- A Global Administrator or Privileged Role Administrator of the tenant, to approve ClearWatch once.
- The ClearWatch agent on the workstations, for matching and for the list of machines with no Defender.
- Nothing on site: no ClearBridge, and nothing else installed.

Limits

- Read only: ClearWatch does not isolate, scan or run live response; that stays in Defender.
- Servers count only once Defender lists them, because Defender for Servers is its own license.
- Vulnerabilities (CVEs per machine) are not read.
- The Not reporting window is one per tenant, not per machine.

See Defender on every device, client by client.

Start a free trial, or ask us to connect your Microsoft tenant with you.

clearwatch.com

ClearWatch™ is a trademark of ClearPath MSP. Microsoft, Microsoft Defender, Microsoft Entra and Windows are trademarks of the Microsoft group of companies.
Screens show demo data.