ClearPath MSP
ClearWatch

COMPARISON GUIDE

from ClearPath MSP

CLEARWATCH COMPARISON GUIDE · ACTION1

Patching that works, and proves it.

Action1 promises patching that just works, with no on-site infrastructure. ClearWatch proves each run, keeps one copy of each update per site, and is a full RMM around it.

PUBLISHED NOVEMBER 2026 LENGTH 5 PAGES COMPARES CLEARWATCH AND ACTION1

EXECUTIVE SUMMARY

Patching, carried all the way

Action1 is a patching tool with a generous free tier: Windows, macOS and Linux, a curated third-party catalog, update rings, vulnerability deadlines and, since October, signed high-risk commands. It stays close to the endpoint: no network monitoring, no backup integrations, and peer sharing that covers its own third-party packages only.

ClearWatch proves each patch run worked, caches Windows Update and apt updates on an on-site ClearBridge with a mode that takes nothing from the internet, and adds what a patch tool leaves out: monitoring with a diagnosis, the network, backups, and every command signed by a separate authority.

KEY TAKEAWAYS

- **Patching with proof:** install rounds, the lockdown read back, every restart owed.
- **One copy per site:** Windows Update and apt updates cached on a ClearBridge.
- **More than patching:** monitoring, the network, backups and remote control.
- **Every command signed:** every command, enforced from install, keyed in hardware.

IN THIS GUIDE

01 **Just works** — And shows its work — 2
02 **Site cache** — One copy per site — 3
03 **Every command signed** — Only in ClearWatch — 4
04 **Side by side** — And how we compared — 5

WHO THIS IS FOR

IT teams and MSPs running Action1 today, or choosing between the two.

AT A GLANCE

ACTION1'S CLAIMS	SITE CACHE	EVERY COMMAND SIGNED	BEYOND PATCHING
Answered	**ClearBridge**	**From install**	**Included**
Just works, no infrastructure, signed commands.	Windows Update and apt, with a cache-only mode.	Every command, not only high-risk ones.	Monitoring, network, backup, remote control.

01 JUST WORKS

ACTION1 SAYS

“Patching That Just Works”

ACTION1.COM, HOME PAGE, NOVEMBER 2026

Windows, macOS (not major upgrades) and Linux on x64, with update rings gated on success and a 99% success rate Action1 does not explain.

Just works, and shows its work

ClearWatch patches Windows, third-party apps and Linux across the Debian, Red Hat and SUSE families by policy, then checks its own work. An update that needs a second pass gets one in the same window, up to five rounds 3 .

The Windows Update lockdown is read back from each machine rather than assumed 2 , and every restart a machine owes is recorded with the update that needs it and when it happened 1 .

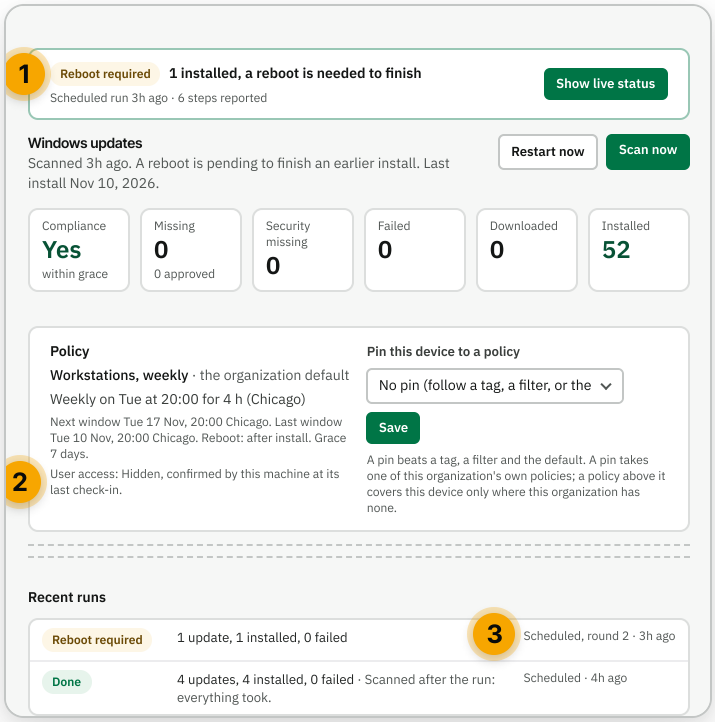


FIGURE 1 A workstation's Patches tab: the restart it still owes, the lockdown it reports back, and each install round. The update list is left out to fit.

Patching, side by side

CAPABILITY	CLEARWATCH	ACTION1
Windows and third-party apps Windows Update and third-party apps, patched by policy.	✓ **Windows Update plus winget**	✓ Own catalog, no winget
Linux patching Approved Linux updates installed by policy, each result recorded.	✓ **Debian, Red Hat, SUSE**	✓ DEB and RPM, x64
Several install rounds per window Updates that need a second pass get one in the same window.	✓ **Up to five passes**	⊖ Retries offline only
Update lockdown verified The Windows Update lockdown is read back from each machine.	✓ **Read back per machine**	◑ Set, not verified
Owed-restart ledger Each restart owed, which update needs it, and when it happened.	✓ **Owed, why, and done**	◑ Required reboots report

02 SITE CACHE

ACTION1 SAYS

“without VPNs or on-prem infrastructure”

ACTION1.COM, NOVEMBER 2026

Action1's peer sharing passes its own third-party packages between agents on a subnet. Windows updates come from Microsoft through Delivery Optimization, Linux updates from each distribution, and there is no cache-only mode.

One copy per site, and nothing from the internet if you say so

A ClearBridge holds updates for its site and fills Windows Update's and apt's own caches, so each machine installs from next door and the installer verifies what it gets.

A policy set to a ClearBridge at the site only 1 holds an update until the bridge has it, so a site on a metered or closed connection takes nothing from outside, and only a bridge at the device's own site serves it 2 .

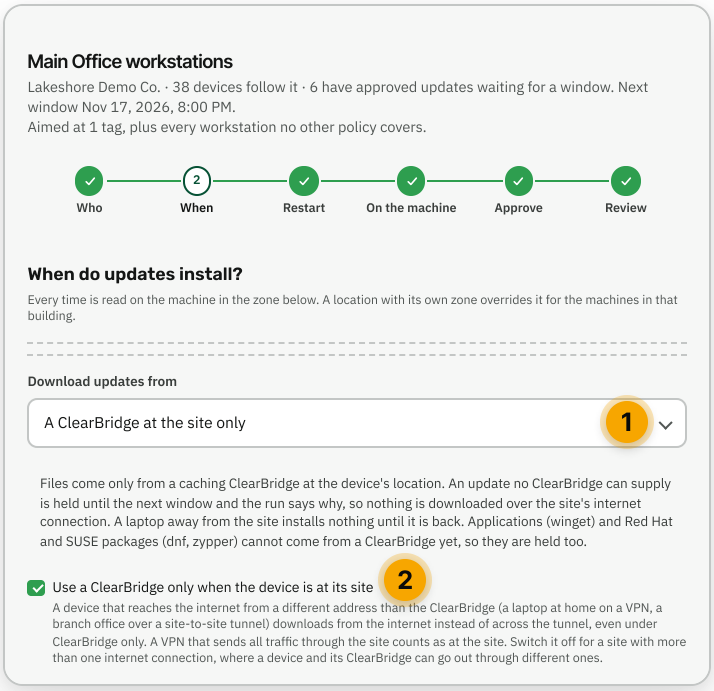


FIGURE 2 A patch policy's When step: updates come only from the site's ClearBridge, and only while the device is at that site. The install windows are left out to fit.

What else a ClearBridge does

CAPABILITY	CLEARWATCH	ACTION1
Agentless with failover On-site collectors pool together and cover for each other.	✓ **Collector pools, auto failover**	⊖ Agent endpoints only
Built-in IPAM Subnets, address conflicts and DHCP scopes, inside the RMM.	✓ **Subnets, conflicts, DHCP**	⊖ Not documented
Cabling topology map Drawn from LLDP and CDP, cables sized by measured bandwidth.	✓ **LLDP, CDP, bandwidth**	⊖ Not documented
Controllers and cameras Omada, UniFi and Meraki controllers, and IP cameras.	✓ **Omada, UniFi, Meraki, cameras**	⊖ Not documented

03 EVERY COMMAND SIGNED

> ACTION1 SAYS
> **"no high-risk command can run on your endpoints without your cryptographic authorization."**
> ACTION1 PRESS RELEASE, OCTOBER 27, 2026

A machine acts only on a signed command

An RMM can run anything on every machine it manages, which makes it the most valuable thing an attacker can reach. ClearWatch takes the power to command machines away from the console itself.

CLEARWATCH CONSOLE
A person asks
Run a script, open a session, install updates, uninstall an agent.

→

COMMAND AUTHORITY
Checked, then signed
A separate service checks that person's own approved permission, then signs with a key held in a hardware security module.

→

THE MACHINE
Verified, or refused
The agent checks the signature against keys built into it, and refuses anything unsigned.

WHAT IT COVERS

- **Everything that changes a machine:** scripts, remote control, the terminal, patch installs, uninstalls and protection settings.
- **A key that never leaves its hardware:** held in a hardware security module, apart from the console's servers.
- **Refused when unsigned:** new agents enforce from the first day.
- **Permissions checked twice:** a raise counts only once another administrator signs it off. Nobody raises themselves.
- **Automation under approved rules:** schedules, self-healing and patch windows run only within rules a person approved.
- **Sessions signed too:** each remote control window and terminal signs its own input.

What Action1 documents

Action1 introduced Endpoint Takeover Prevention in October 2026: high-risk commands need a signature from a key the customer creates in the browser. It is rolling out by region, existing customers can postpone it, and losing every admin key means reinstalling every agent. ClearWatch signs every command that changes a machine, with a key in a hardware security module, enforced from the first install.

Every action accounted for

CAPABILITY	CLEARWATCH	ACTION1
Every command signed A separate authority signs each action; the agent refuses anything unsigned.	✓ **Separate authority, HSM key**	◑ High-risk only, rolling out
Audited before it runs An action that cannot be logged first is refused.	✓ **Refused if not logged**	⊖ Not documented
Installers verify the signer Every install script checks the agent's signature first.	✓ **Every install script**	⊖ Not documented
Agent tamper protection No uninstall without a code from the console, set per client.	✓ **Uninstall code, per client**	◑ Agent control ops signed
Client-controlled access A client can refuse or withdraw a provider's access.	✓ **Client can refuse**	⊖ Not documented

04 SIDE BY SIDE

Action1 and ClearWatch: all 40 capabilities

Included · Partial · Add-on · Not offered or not documented

CAPABILITY	CW	ACTION1
Quiet onboarding baseline	✓	Not documented
Diagnosis before the page	✓	Not documented
Knows when data stops	✓	Offline alerts only
Checks only where they apply	✓	Not documented
Outage-first routing	✓	Not documented
End-user experience score	✓	Not documented
Agentless with failover	✓	Agent endpoints only
Switch config history	✓	Not documented
Browser SSH to devices	✓	Not documented
Cabling topology map	✓	Not documented
Switch front and back views	✓	Not documented
Storage drive-bay view	✓	Not documented
Built-in IPAM	✓	Not documented
Controllers and cameras	✓	Not documented
Windows and third-party apps	✓	Own catalog, no winget
Linux patching	✓	DEB and RPM, x64
Several install rounds per window	✓	Retries offline only
Owed-restart ledger	✓	Required reboots report
Self-healing	✓	Not documented
Inherited custom fields	✓	Not documented

CAPABILITY	CW	ACTION1
Every command signed	✓	High-risk only, rolling out
Audited before it runs	✓	Not documented
Update lockdown verified	✓	Set, not verified
Installers verify the signer	✓	Not documented
Agent tamper protection	✓	Agent control ops signed
Remote control	✓	Built-in remote desktop
Recording by client policy	✓	Not documented
Support without an agent	✓	Not documented
Searchable terminal recordings	✓	Not documented
Multi-vendor backup view	✓	No backup integrations
Backup status per device	✓	No backup integrations
SentinelOne	✓	Not documented
Microsoft Intune	✓	Not documented
Password vault	✓	Not documented
Client-controlled access	✓	Not documented
AI assistants (MCP)	✓	Third-party MCP only
API and webhooks	✓	REST API
Incident paging	✓	Not documented
Co-managed IT	✓	Not documented
Help on every page	✓	Separate docs site

How we compared. Each vendor's own public documentation, release notes, product and pricing pages, checked October and November 2026; quotes are from Action1's own pages as of November 2026. Included means it does what ClearWatch does, in the RMM itself, at no extra license; Partial covers part of it; Add-on needs a separately licensed product or tier; Not documented means we found no public documentation, not that the vendor cannot do it. Every cell is backed by a source, available on request. Screens are rebuilt from the ClearWatch console with demo data.

Running Action1 today?

Start a free trial, or ask us to walk you through ClearWatch on your own devices.

clearwatch.com

ClearWatch™ is a trademark of ClearPath MSP. Action1 is a trademark of Action1 Corporation. All other names are trademarks of their respective owners.