

Checklist: lock down remote support tools

Based on CISA advisory AA23-025A and the CISA Guide to Securing Remote Access Software. From xcelcor.com/insights/block-unauthorized-rmm-tools.

1. Decide what's allowed

- ☐ Approved RMM tool (help desk): _____ Owner: _____
- ☐ Approved RMM tool (MSP, if different): _____ Owner: _____
- ☐ Publisher (code-signing certificate) recorded for each
- ☐ Our own server or tenant address recorded for each
- ☐ List of machines that should have each tool

2. Block everything else from running

- ☐ App Control for Business policy in audit mode, logs reviewed
- ☐ Publisher rules allow only the approved tools
- ☐ Publishers of other RMM products denied, including portable copies
- ☐ Rules cover installers (MSI) and scripts, not only executables
- ☐ Policy moved from audit to enforced

3. Control where tools connect

- ☐ Approved tool limited to our own server or tenant where possible
- ☐ Approved tool reachable only from inside the network, VPN or VDI
- ☐ Common RMM ports and protocols blocked at the perimeter
- ☐ Other vendors' cloud and relay domains blocked at DNS filter or web gateway
- ☐ Network detection alerts on traffic to RMM servers

4. Alert when one starts anyway

- ☐ Alert: RMM process starting from Downloads or Temp
- ☐ Alert: new remote access service on a machine
- ☐ Alert: App Control or AppLocker events naming a remote tool
- ☐ Alerts go to on-call, not a weekly report

5. Tell staff

- ☐ Written rule: IT never emails a link or calls asking you to install remote software
- ☐ One place to report, with no blame

If you find one

1. Isolate the machine.
2. End the session, stop the tool, record path, server and times.
3. Ask the user what they did during the session.
4. Reset passwords from a clean device, revoke sessions and tokens.
5. Look for other remote tools and new accounts.
6. Report: report@cisa.gov, (888) 282-0870, and ic3.gov.

From Xcelcor Guardian · xcelcor.com/insights/block-unauthorized-rmm-tools