Networks. Plus People. Plus Service.

HOW TO READ YOUR MONTHLY REPORTS

The Monthly Executive Report provides an array of information to include OS Patching, 3rd Party Patching, Endpoint Availability, and Advanced Endpoint Security.

Many of the fields in the interactive report contain “drill down” data that expands on effected endpoints or provides additional event data. Fields with drill down data will switch to a “pointer finger icon” to open the expanded data.

How drill-downs work

Drill Down Data is only available with the interactive report and may not be accessible from the PDF Version of the report.

Drill Down Data is displayed in an excel table style format and is limited to the first 250 entries, if more detailed information is required please let the NWP Team and we can generate it for the organization.

Click a score, summary number, chart bar, pie slice, or plotted point to open supporting data.

Details vary: a score may show a monthly site summary, while patch and security charts show device or event records. Counts can include multiple records per device.

Example Drill Down:

Results are limited to the first 250 rows of data.

SITE	SYSTEM NAME	FRIENDLY NAME	OPERATING SYSTEMS	ENDPOINT TYPE	KB / UPDATE	PATCH TITLE	PATCH RELEASE DATE	PATCH STATUS	NOC RECOMMENDATION	CLASSIFICATION
			Microsoft Windows 11 Pro	Desktop	5120708	2026-08 .NET Framework Security Update (KB5120708)	Aug 10, 2026 7:00 PM	Pending Reboot	APPROVED	Security Updates
			Microsoft Windows 11 Pro	Desktop	5120708	2026-08 .NET Framework Security Update (KB5120708)	Aug 10, 2026 7:00 PM	Pending Reboot	APPROVED	Security Updates
			Microsoft Windows 11 Pro	Desktop	5120708	2026-08 .NET Framework Security Update (KB5120708)	Aug 10, 2026 7:00 PM	Pending Reboot	APPROVED	Security Updates
			Microsoft Windows 11 Pro	Desktop	5120708	2026-08 .NET Framework Security Update (KB5120708)	Aug 10, 2026 7:00 PM	Pending Reboot	APPROVED	Security Updates
			Microsoft Windows 11 Pro	Desktop	5121003	2026-08 Security Update (KB5121003) (26200.9168)	Aug 10, 2026 7:00 PM	Pending Reboot	APPROVED	Security Updates
			Microsoft Windows 11 Pro	Desktop	5121003	2026-08 Security Update (KB5121003) (26200.9168)	Aug 10, 2026 7:00 PM	Pending Reboot	APPROVED	Security Updates
			Microsoft Windows 11 Pro	Desktop	5121003	2026-08 Security Update (KB5121003) (26200.9168)	Aug 10, 2026 7:00 PM	Pending Reboot	APPROVED	Security Updates
			Microsoft Windows 11 Pro	Desktop	5121003	2026-08 Security Update (KB5121003) (26200.9168)	Aug 10, 2026 7:00 PM	Pending Reboot	APPROVED	Security Updates

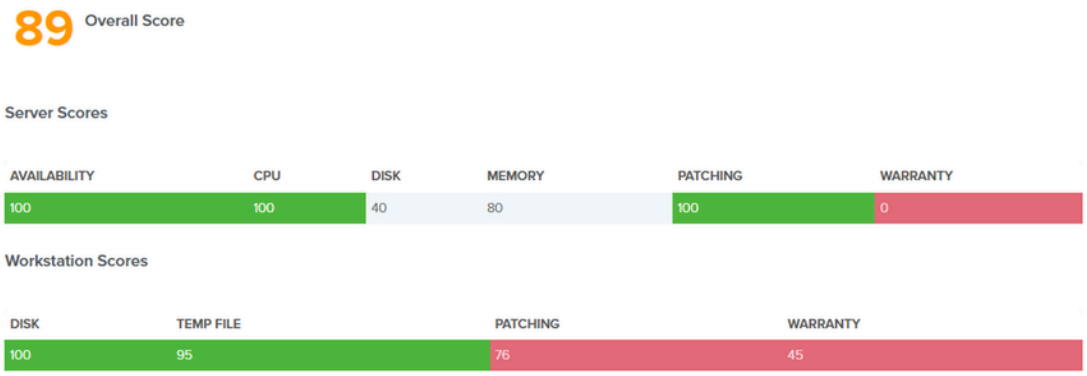
Networks. Plus People. Plus Service.

HOW TO READ YOUR MONTHLY REPORTS

Report Sections

Health scores

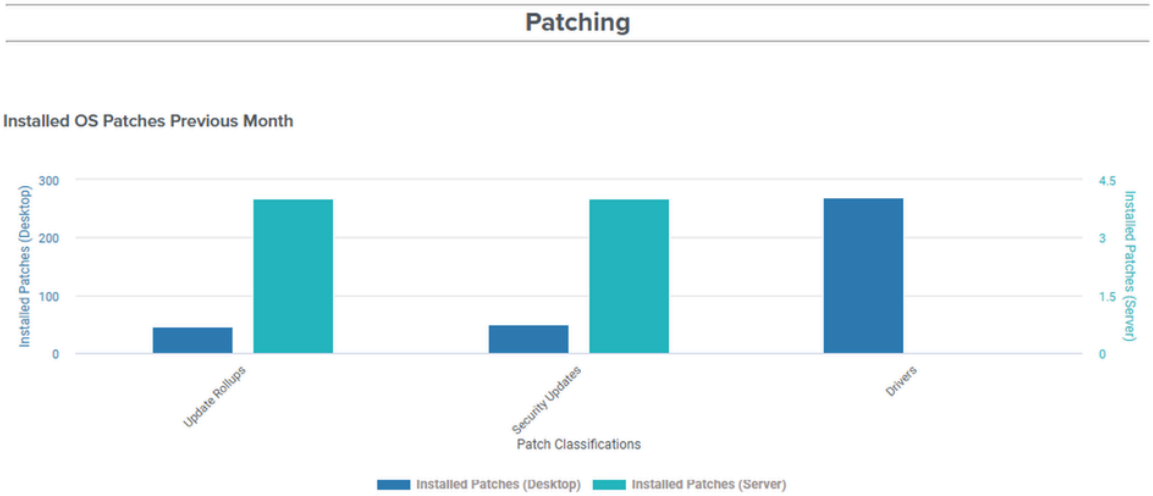
The Overall Score is weighted. Server and workstation scores highlight availability, performance, disk space, patching, temporary files, and warranty status. A score is not a utilization percentage.



Devices & Patches

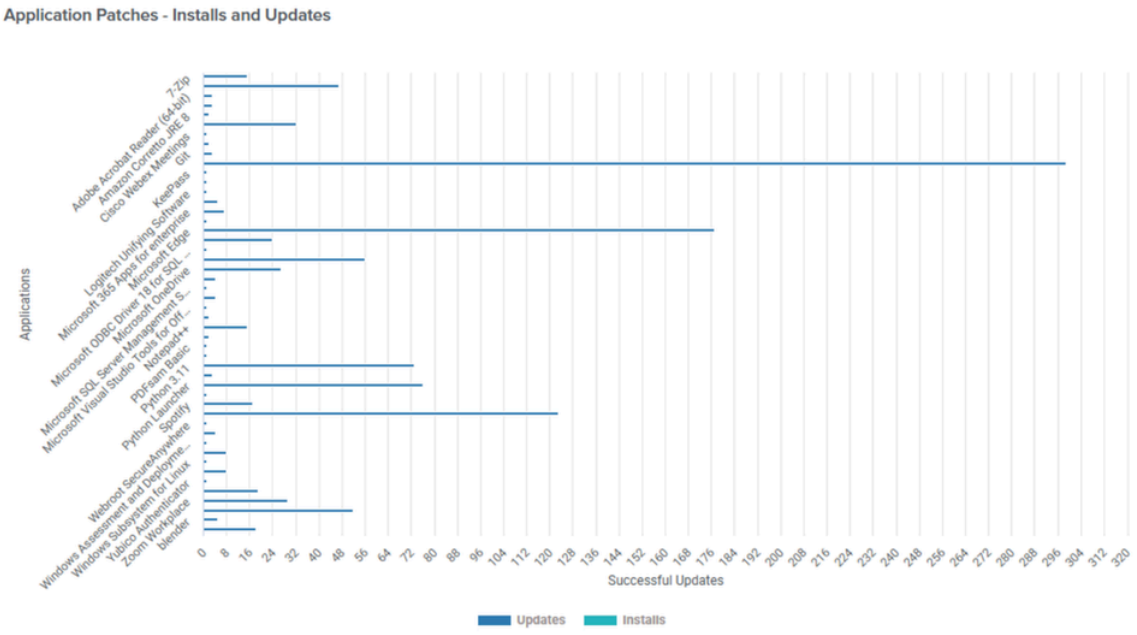
Server/workstation totals show the monitored inventory. This information is also available in the RMM Agent Status Report section.

OS and application charts show completed installations or updates for both OS Updates and 3rd Party Patching. Selecting the colored portion of the bar graphs will open additional drill down data.



Networks. Plus People. Plus Service.

HOW TO READ YOUR MONTHLY REPORTS



Patches Missing & Pending Reboot & Classification

Missing Patches breaks down into several categories:

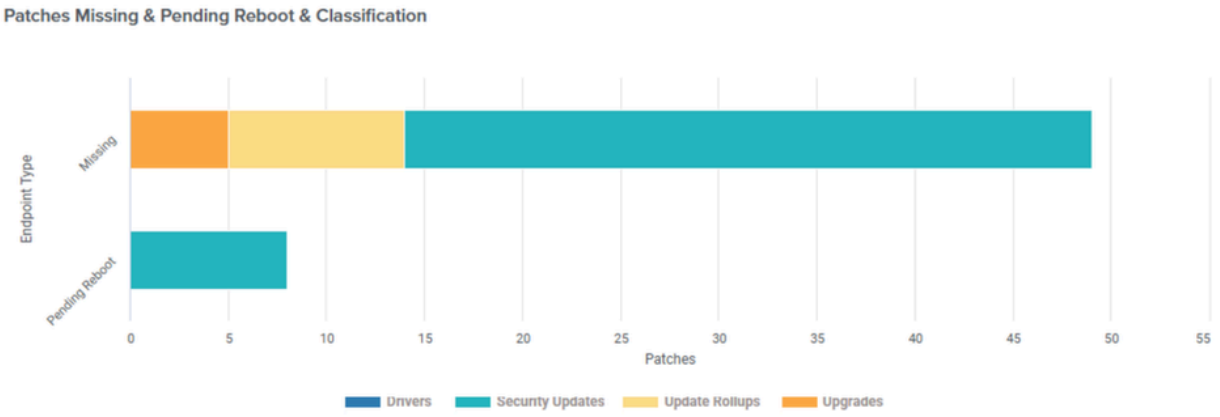
- Upgrades – OS Version Updates (Windows / MAC)
- Update Rollups – Combined Updates into one bulk update (Windows)
- Security Updates – Updates to Windows security features / definitions
- Drivers – Software updates for input / output devices (ex. Keyboards / printers / monitors)

Pending Reboots indicates systems that at report generation needed to be rebooted to complete a restart to finish installing updates. Normally these are handles by the system patching policy, or a forced reboot is executed if a system has not rebooted in over 30 days (Desktops only).

(Image on next page)

Networks. Plus People. Plus Service.

HOW TO READ YOUR MONTHLY REPORTS



Agent Status & Offline Devices

RMM Agent Status: Manifest of systems registered to the site

RMM Agent Status Report

SITE NAME	TOTAL WORKSTATIONS	WORKSTATIONS NO CONTACT >60 DAYS	TOTAL SERVERS	SERVERS NO CONTACT >60 DAYS	TOTAL DEVICES
[redacted]	84	4	9	0	93
Total	**84**	**4**	**9**	**0**	**93**

Endpoints Offline: Systems that have not checked into the RMM portal in over 30 days and may have been retired / decommissioned. Please notify the NWP Team if any of these systems should be removed.

Endpoints Offline > 30 Days

SITE NAME	SYSTEM NAME	LAST CHECKIN	LAST LOGGED ON USER
[redacted] Inc	[redacted]	Sep 8, 2025	[redacted]
Inc		Jun 8, 2026	
Inc		Aug 11, 2025	
Inc		Oct 7, 2025	

Networks. Plus People. Plus Service.

HOW TO READ YOUR MONTHLY REPORTS

Advanced Endpoint Security Summary

MDR (Managed Detection and Response) totals show resolved/unresolved threats, new devices, and total MDR Endpoint counts.

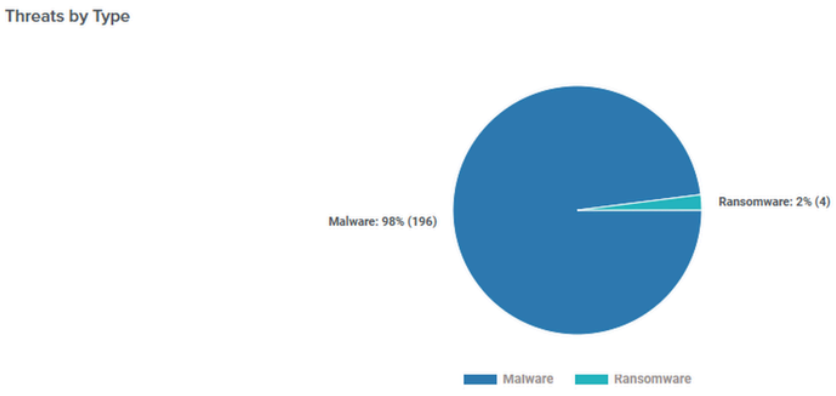
Advanced Endpoint Security - MDR

200 Threats Resolved - Prev Month	**0** Threats Unresolved Threats Unresolved
3 New Devices Last Calendar Month	**225** Threats Resolved - Prev 3 Months
89 Device Count Total Endpoints	

Threats Breakdown - Last Calendar Month

Analyst Verdict separates true and false positives. Read these together: a detection does not necessarily mean a successful attack.

Threat Breakdown - Last Calendar Month



networksplus.com
support@networksplus.com

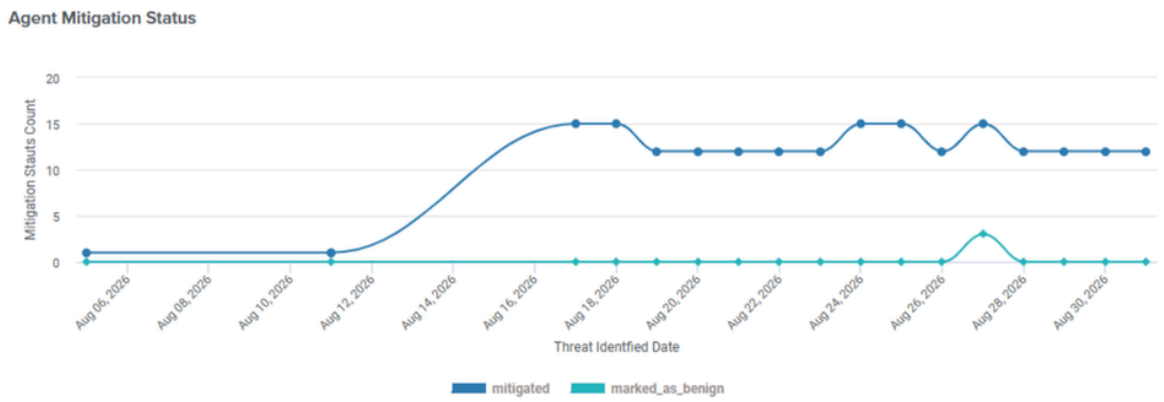
NETWORKS PLUS

Networks. Plus People. Plus Service.

HOW TO READ YOUR MONTHLY REPORTS

Agent Mitigation Status

This shows threat events and their status over the calendar month. Drill down data is available for each day an event occurred.



Agent Verdict

This graph has a consolidated view of threat events over the last month. Drill down data is available for each verdict type.