Platinum Teknology

Remote Monitoring & Maintenance Program (RMM)

RMM Powered by Ninja

THE ONLY COMPLETE, SCALABLE IT MANAGEMENT PLATFORM

THE SYSTEM PROVIDES RMM
(REMOTE MONITORING AND MANAGEMENT),
REMOTE ACCESS, SERVICE DESK, & PATCH MANAGEMENT
FOR ONE PLATFORM

PRODUCTS & SERVICES AVAILABLE

Remote Monitoring and Management:

Remote Monitoring and Management (RMM) is a remote monitoring software that allows Managed Service Providers (MSPs) to monitor as well as manage network endpoints, computers, mobile devices, and entire IT infrastructure remotely from a centralized console. RMM is also known as Remote IT Network Infrastructure Management.

An RMM program is deployed through an "agent" (a small software footprint), which is installed on client systems, workstations, servers, and mobile devices

It's these agents that send back to the MSPs information about client machines; the information includes machine status, machine health etc. Thus the MSPs, by deploying RMM tools, gather insight into client networks. They are thus able to monitor machines remotely, maintain them and keep them up-to-date and even get the machines to stay ahead of issues and resolve them remotely.

An alert (often referred to as a 'ticket') is created when one of the agents deployed on a machine/network detects a problem. This ticket is sent to the MSP. The MSP then takes the necessary action to get the issue resolved. Tickets are classified on the basis of the type of the issues and their severity; this kind of clarification helps MSPs identify issues as critical or non-critical.

Monitoring and Alerting

Get Monitoring Data In Real-Time, Before Your Users Come To You With Questions

Our monitoring and alerting capabilities include:

- Performance thresholds (i.e. CPU usage, hard disk usage, etc)
- Windows Services
- Low footprint agent
- Identify endpoints which contain vulnerabilities and need to be patched

Endpoint Managment

Manage Any Device, On Any Network, From Any Location

Our monitoring and alerting capabilities include:

- Remote command line /Powershell
- Script deployment
- Start and stop services, processes
- Install and uninstall software

Virtual Machine Management

Improve virtual machine and virtualized resource management

Ninja VMWare monitoring tools enable you to monitor and allocate client virtual resources:

- Create, delete, and monitor snapshots
- Optimize storage usage by pruning old or oversized snapshots
- Start, stop, suspend, reset, or delete virtual machines
- Reallocate resources for better capacity planning and management

Mobile App

Monitor and manage all IT assets on-the-go with your IOS or Android device

NinjaRMM's mobile app notifies you of critical issues while you're on the go:

- OS & 3rd party patch status
- Alerts in progress
- Threats detected
- Server status
- Reboots pending
- Node approvals
- Active tasks

IT Automation and Scripting

Automate daily tasks with on-demand, scheduled, or triggered scripts to keep endpoints up and running

IT Automation tools for Infrastructure and Process Monitoring:

- **Set all scripts and scheduled actions to run at a time convenient for you and your clients. And for compliance and auditing purposes, you can trust our tracking system to provide reliable records of every action**

- **Schedule patches, antivirus scans, scripts, and any other IT actions at a time of your choosing. The product lets you be an "IT Ninja," doing important work behind the scenes without interrupting client workflow**

Patch Management

Remotely deploy and patch OS and third party software to keep your endpoints protected

Simplify Patching with Ninja RMM:

- Automated patching across all supported versions of Windows
- Detailed patch reporting will help you identify non-compliant endpoints
- NinjaRMM's third-party patching engine will keep your endpoints up-to-date with support for software from over 120 vendors, without you having to worry about user interference. Keep devices current with the latest features, and also protect your endpoints from security breaches

Managed Antivirus

Monitor endpoint virus protection activities and keep them secure with a single view of threats

Manage Security From Inside Your RMM:

- Whatever security product you use, you can configure all of the options from within the NinjaRMM dashboard. Schedule on-demand or weekly scans, define exclusions or take remediation actions — all from inside the easy-to-navigate UI

- Reporting is a great way to audit your endpoints, as a way to monitor active infections or track definition statuses in order to identify unsecured devices. Reports are also a handy way to remind your clients of all the valuable service you provide, by detailing past infections or the current state of antivirus protection

Remote Access

Take control of Endpoints via built-in remote access tools

Device Inventory:

- Built from the ground up using 21st-century technology, the platform queries all of the devices in NinjaRMM instantaneously
- Securely and remotely access your devices from anywhere, in just one click, using either TeamViewer or Splashtop. You'll be able to create users, devices, groups, and permissions, and do it with confidence: all remote sessions are protected by TLS and 256-bit encryption

Asset Management

Track inventory, usage, and the health of your hardware, software, and subscriptions

Easily Discover, Monitor & Evaluate Your IT Assets:

- Quickly determine if any devices have an operating system (OS) approaching end of life (EOL) and deserving of an upgrade. The NinjaRMM asset summary report details Windows and Mac devices, including vendor and model, OS version, install date, uptime and more

- See the full mix of network management software (NMS) devices per location by type and vendor. NinjaRMM provides make, model, type and status details of the various networking devices at each of your customer's offices or facilities

Reporting

Keep track of your assets, employees, and tasks, and report on outcomes

Reporting Tools Help You Show Off All Of Your Hard Work:

- With the amount of data thrown off by every endpoint or network device, it can be easy for IT managers to get lost in the weeds. Rely on NinjaRMM to supply a cogent executive summary for a high-level overview of your organization's IT health
- NinjaRMM offers a host of in-depth reporting features. You can look at connection reports of TeamViewer and Splashtop activity, patch compliance reports across different device groups and organizations, or a report on which devices triggered the most alerts. An asset inventory sums up the details of your workstations, servers, and network devices

Endpoint Protection Software

What is Endpoint Protection?

Endpoint protection refers to the security solutions that are used to address issues pertaining to endpoint security. Thus, it can be defined as securing and protecting endpoints against all kinds of attacks, zero-day exploits and those inadvertent data leakages that happen due to human errors.

Endpoint protection is what helps prevent targeted attacks and APTs (advanced persistent threats), which can't be prevented using antivirus solutions alone. Endpoint protection solutions provide enterprises with a full spectrum of security solutions that can be managed centrally and which helps secure endpoints- servers, workstations etc connected to endpoints, plus the many endpoint devices.

Why Endpoint Protection Software?

Endpoint Protection or Endpoint Security fosters solution to protect and secure the endpoints from zero day exploits or unknown malwares or advanced persistent threats. Conventional Antivirus cannot be a standalone solution to drive out the adamant threats, with that in place, Endpoint protection took its form to deliver absolute security solutions ensuring complete data protection for enterprises. Endpoint Protection delivers centralised security solutions to secure workstations, servers and devices that are connected to access the enterprise networks.

NinjaRMM Endpoint Protection Integrated Vendors

WEBROOT
Bitdefender
Malwarebytes