

Mobile Device Management 101 for MSPs

Key considerations to know
before choosing an MDM

Introduction

The proliferation of mobile devices as work tools has changed how people work and businesses operate. This is both a good and a bad thing. While mobile devices can improve productivity, they can also introduce risk in the form of network complexity, gaps in device management, and mismanaged applications and data.

Fortunately, the solution to managing mobile devices and reducing risk is not out of reach. To ensure your clients' endpoints are secure, use a comprehensive mobile device management (MDM) solution that is part of an overall unified endpoint management strategy — even better if it's part of an all-in-one solution that enables you to manage, support, and secure all endpoints within a single console to minimize complexity and cost.

This eBook describes MDM and shows you what to look for in a solution that will not only allow you to add value for your clients but also have a positive impact on your bottom line.

What is MDM?

MDM is an endpoint management tool specifically designed to help you provision, monitor, manage, and secure mobile devices on your network at scale. As an MSP you can deliver predictable, positive access to and management of all your clients' mobile devices because MDM helps you:

- ▶ **Standardize mobile device management**
- ▶ **Deploy and manage mobile apps**
- ▶ **Create and enforce mobile device policies at scale**
- ▶ **Improve your overall security posture**
- ▶ **Provide a better end-user experience**

According to a 2023 Verizon Enterprise [report](#), personal and company-owned mobile devices are among the top three most common targets for cyber attacks, and due to their portability, they are more likely to be lost or stolen. An MDM solution can help you support your clients' employees who are accessing company data on-the-go, while at the same time ensuring the clients' endpoints are protected.

While offering MDM is a value-added service for your clients, managing mobile devices can lead to increased complexity and greater security risks. In addition, you may need to invest in more tools to manage, patch, secure, and provision them, which of course cuts into your new revenue stream. So, as an MSP, you need an MDM solution that can help you expand your business while increasing efficiency for your team and maintaining profitability.

Why MSPs need MDM

Whether you're a small MSP managing 50 or 1,000 endpoints or a large MSP managing 10,000 or 100,000 endpoints, the challenges you face are similar. You need to provide high-quality service to your client base while continuing your marketing efforts, and meeting or, better yet, exceeding revenue goals. When mobile devices are included in the client endpoints you're now managing, an MDM solution can help you more effectively manage them.

With an MDM solution as part of your endpoint management offering, you can

- ▶ **Increase monthly billings**

By adding mobile devices to the endpoints you manage for current clients you can incrementally increase your monthly billings. [Fortune](#) projects the use of mobile devices to grow by more than 27% by 2032, making MDM a steadily increasing revenue stream for MSPs.

- ▶ **Win more business**

With MDM in your endpoint management portfolio, you can offer prospective clients a more comprehensive service that puts you a step ahead of the competition.

- ▶ **Harden endpoint security**

By managing your clients' mobile devices, you'll reduce the risk of cyber attacks, which benefits the client and protects your reputation.

- ▶ **Improve IT efficiency and quality of service**

An MDM solution can help your team better manage client endpoints and improve responsiveness to other issues.

The benefits of MDM for MSPs



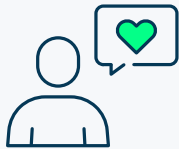
More efficient mobile device management



Faster onboarding



Better security for mobile devices



Improved client experience



Increased monthly billings



More comprehensive offering

What to look for in an MDM solution

► **Centralized management**

No matter where your clients' mobile devices are located, your team needs to monitor, manage, and secure them remotely. A platform with a centralized dashboard allows you and your team to more efficiently manage clients' mobile devices alongside servers, workstations, laptops, virtual machines, and networking devices – all within a single console.



▶ **Strong security features**

Security for mobile devices is more important than ever. MDM hardens your endpoint security by allowing your team to create comprehensive security policies and deploy them at scale to all mobile devices. This includes preventing installation of apps known to pose security risks, enforcing the requirement for strong passwords, the use of encryption, and more.

▶ **Support for multiple operating systems**

Your MDM solution should be flexible enough to support Android and/or Apple (iOS or iPadOS) mobile devices so that the clients' users can continue to use the devices they prefer. This also allows you to control costs and complexity by investing in a single solution to seamlessly manage and support them all.

▶ **Support for multi-tenancy**

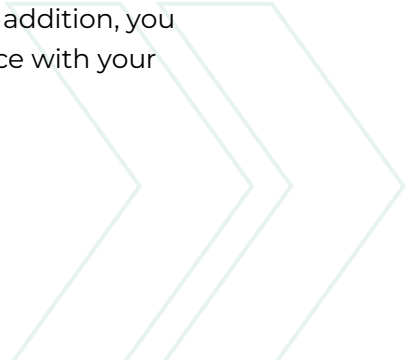
As an MSP supporting multiple clients, multi-tenancy is a must-have feature of the MDM solution you choose. Multi-tenancy gives you the ability to manage multiple client organizations separately through a single tool. And if a single client has multiple offices, including satellite or new offices, you can manage all of these through the MDM solution's multi-tenancy functionality because it allows you to configure multiple APNs certificates, ADE profiles, content tokens, and Android Enterprise connections.

▶ **Consolidate your tech stack**

An MDM tool that integrates into your existing endpoint management solution reduces complexity, improves workflows, and lowers licensing costs by enabling you to use fewer tools and fewer vendors.

▶ **Easy to learn, easy to use**

Given the varying levels of expertise on your team, you want an MDM solution that doesn't require special training to learn and is easy to deploy, manage, and master. Ideally, the solution should offer familiar workflows for both Android and Apple devices, so your technicians don't have to specialize in one or the other platform. In addition, you want to be up and running quickly so you can keep pace with your workload and maintain maximum efficiency.



Other functionality you need

▶ **Inventory and tracking**

Maintain accurate mobile device inventory and strengthen loss prevention actions by implementing automated actions on devices that move outside of a defined geofence.

▶ **Application management**

Install, remove, or block applications on mobile devices.

▶ **Provisioning and configuration management**

Provision and secure mobile devices, to ensure essential applications are installed to support specific user workflows and the device is properly configured to meet compliance regulations.

▶ **Remote troubleshooting**

Access and view mobile device screens to diagnose and resolve issues quickly and eliminate the need for site visits – saving time and minimizing disruptions to user productivity and workflow.

Why NinjaOne MDM for MSPs

Single platform for centralized management

No matter where your clients' mobile devices are located, your team needs to be able to onboard, monitor, manage, and secure them remotely. NinjaOne MDM streamlines device onboarding with its intuitive dashboard. Once all the mobile devices are provisioned, it's easy to enforce mobile device policies and provide ongoing support at scale through the dashboard.

Support for multi-tenancy

NinjaOne MDM multi-tenancy is perfect for MSPs managing multiple clients because it allows you to manage the mobile devices of different client organizations separately within the same easy-to-use platform you've come to know and trust.

Support for multiple operating systems

NinjaOne MDM is an extension of the NinjaOne RMM solution. From the RMM dashboard you can support [Windows](#), [macOS](#), and [Linux](#) operating systems as well as VMs and networking devices. And with the MDM tool you can add support for [Android](#), [iOS](#), and [iPadOS](#). There's no need for a separate instance for each device type or operating system. Not only does this simplify client device management, but it reduces the number of tools needed to manage all endpoints, resulting in significant cost savings to you and your clients.

Robust security features

NinjaOne benefits both the client organization and the device user by protecting and managing personal devices and any data related to the organization or its projects, while respecting the device owner's privacy and personal information. If NinjaOne detects a device has fallen out of compliance based upon defined conditions, automated corrective actions can be taken. If automated remediation is not configured, your admins can be promptly alerted as to the issue and take immediate corrective action, limiting the threat risk and potential device downtime.

Easy to learn, easy to use

Cloud-native NinjaOne MDM, is built to have a short learning curve so it's easy to deploy, easy to learn, and easy to use. You won't need specialists or additional staff or training for your team to be able to deploy and manage the NinjaOne solution. If your team has a mix of experience and subject matter expertise, you can still quickly deploy NinjaOne MDM and start managing and monitoring your clients' mobile devices in no time.

No.1 Rated MDM on G2

NinjaOne customers rated our MDM solution [#1 on G2 Crowd](#)

That's a testament to our dedication to innovations that serve the needs of our customers.

NinjaOne MDM also offers

Inventory and tracking

Complete visibility into all managed Android, iOS, and iPadOS devices, ensuring accurate and updated inventory for better risk management

Application management

Effortlessly install, update, and remove apps, ensuring focused usage and streamlined app lifecycle management

Provisioning and configuration management

Efficiently provision and secure mobile devices to ensure essential applications are configured for a robust, compliant posture, and seamless integration into the client's IT environment

Remote troubleshooting

Remotely access and view users' mobile device screens to diagnose and resolve issues quickly, minimizing disruptions to user productivity and workflow

Learn more about [NinjaOne MDM](#)

About NinjaOne

NinjaOne automates the hardest parts of IT to deliver visibility, security, and control over all endpoints. The NinjaOne automated endpoint management platform simplifies work for tens of thousands of customers and is proven to increase productivity, reduce security risk, and lower IT costs. NinjaOne is obsessed with customer success and provides free and unlimited onboarding, training, and support. NinjaOne is #1 on G2 in endpoint management, patch management, remote monitoring and management, and mobile device management.

Try NinjaOne for free at

<https://www.ninjaone.com/freetrialform/>