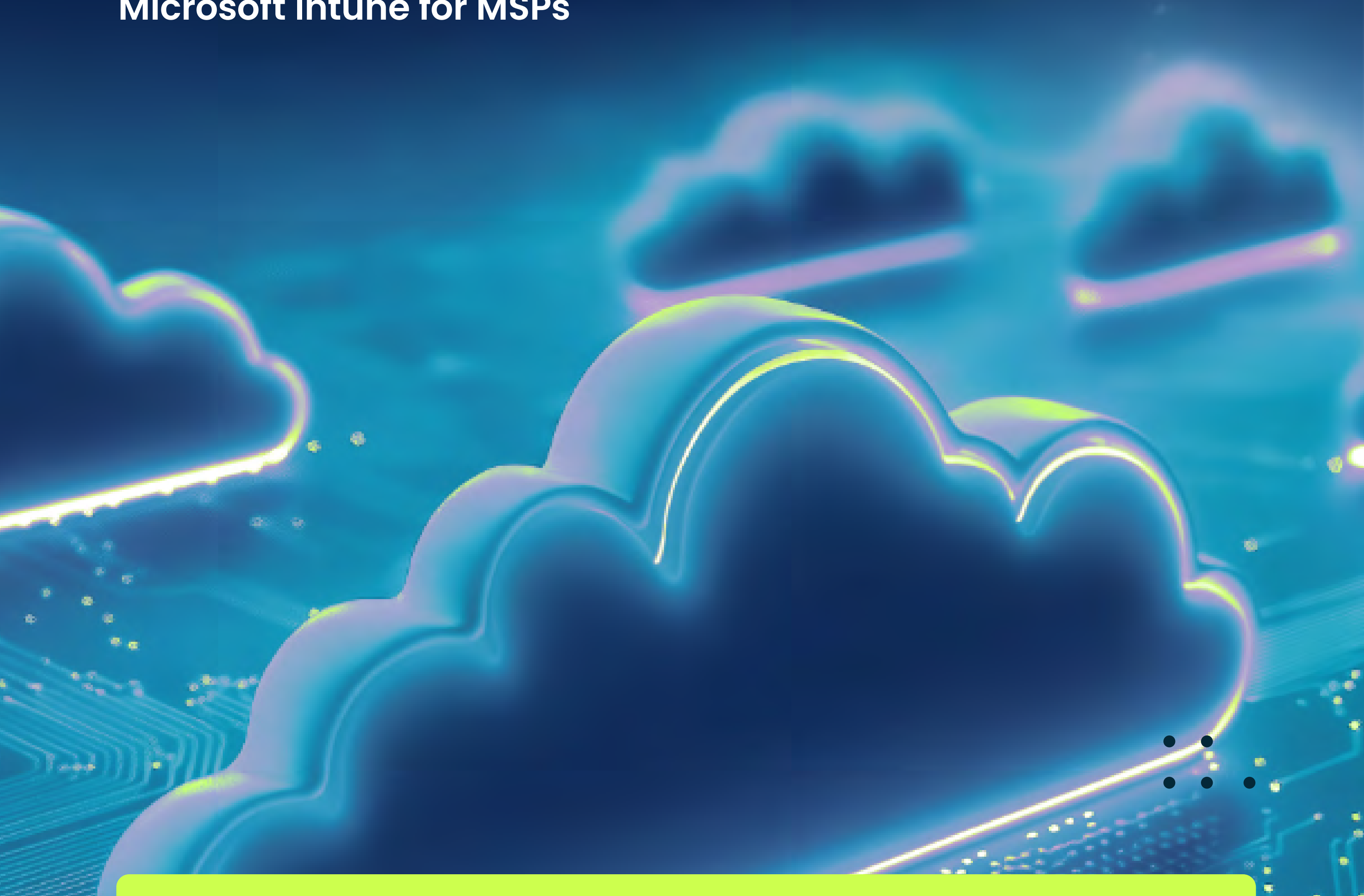
nerdio

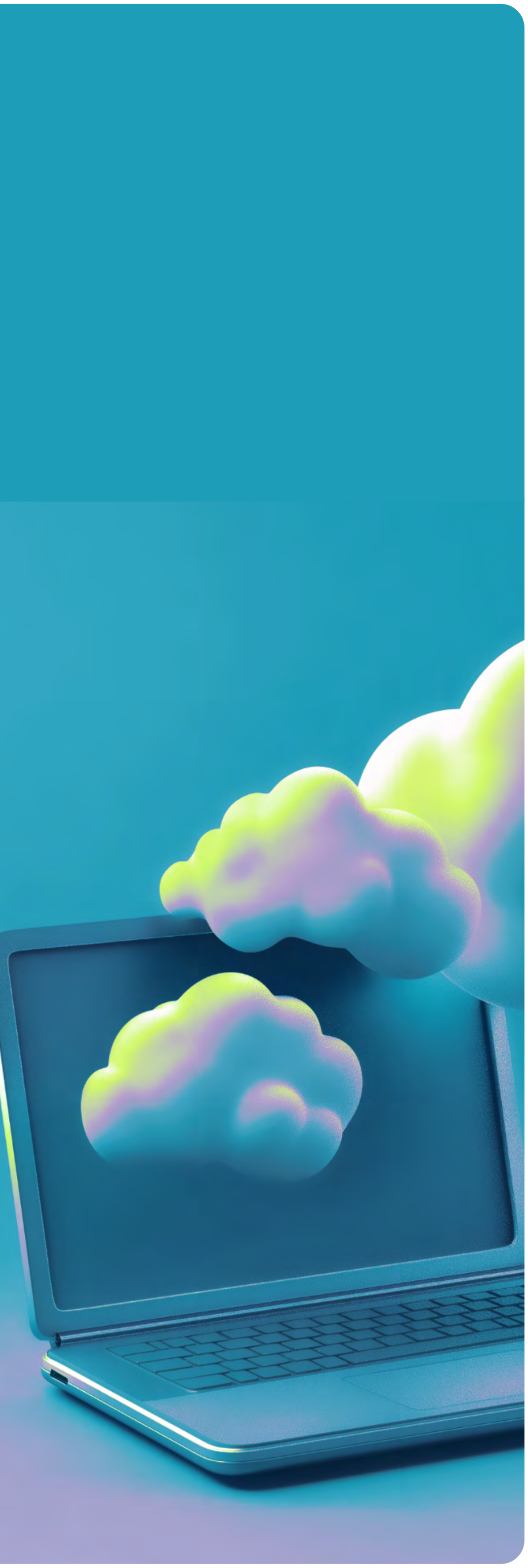
WHITE PAPER

NERDIO MANAGER FOR MSP

Endpoint management made easy

The ultimate guide to
Microsoft Intune for MSPs





Effective endpoint management is paramount for organizations seeking to maintain security, compliance, and productivity across their IT infrastructure.

Managed services providers (MSPs) play a crucial role in delivering comprehensive endpoint management solutions that meet the diverse needs of their clients.

This guide explores how Microsoft Intune revolutionizes endpoint management by offering unparalleled efficiency, scalability, and security. From user onboarding to threat detection and from compliance enforcement to software deployment, Intune empowers MSPs to streamline their operations, optimize service delivery, and exceed client expectations.

MSPs will gain valuable insights into how they can leverage Intune to enhance their endpoint management practices, differentiate their service offerings, and capitalize on the opportunities presented by the Microsoft Cloud ecosystem.

Whether you're a seasoned MSP looking to modernize your operations or a newcomer seeking to establish a competitive edge, this guide will provide you with the knowledge and strategies you need to succeed in today's dynamic marketplace.

History of endpoint management

Endpoint management as it is known today traces its roots back to the advent of broadband in 2005. This marked a significant turning point for MSPs as they gained the ability to resolve issues remotely for the first time. This newfound capability revolutionized the way IT support was delivered, empowering MSPs to efficiently manage and maintain their clients' endpoints without the need for physical presence.

The endpoint management field is defined by a dichotomy between legacy players and newcomers. Established names such as Kaseya, ConnectWise (CW), and N-able dominate the scene, leveraging their experience and market presence to provide endpoint management solutions. However, they face increasing competition from emerging players like SuperOps, NinjaRMM, and SyncroMSP. These newcomers bring fresh perspectives and innovative approaches to endpoint management, challenging the status quo and driving industry-wide evolution.

As the market matures, consolidation has become a prevailing trend. Major players seek to expand their offerings and solidify their positions through strategic acquisitions and mergers. This has resulted in a shifting landscape, with companies like SolarWinds being absorbed by N-able and Datto acquiring AutoTask to create DattoRMM. Then, Kaseya bought Datto, which included DattoRMM in its portfolio. These consolidations aim to enhance product portfolios, streamline operations, and better serve the evolving needs of MSPs and their clients. However, they also allow these legacy players to increase pricing by bundling tools together, ultimately giving MSPs fewer choices and requiring more long-term contracts to get better pricing.

Rumors and speculations have further fueled the dynamic nature of the industry, with talks swirling around potential mergers of larger organizations. Such discussions underscore competitive pressures and constant flux within the endpoint management sector, driving companies to adapt, innovate, and collaborate to stay ahead.

The evolution of endpoint management continues to shape the way MSPs deliver value to their clients, laying the groundwork for a future defined by efficiency, scalability, and innovation.

Traditional endpoint management

Traditional endpoint management solutions have long been the cornerstone of IT support strategies, relying on agent-based solutions to monitor, manage, and maintain endpoint devices.

These methods typically involve the deployment of software agents on individual devices, enabling centralized control and administration by MSPs.

Self-hosted vs. hosted solutions

One key consideration within traditional endpoint management is the choice between self-hosted and hosted solutions:

- **Self-hosted solutions** involve the installation and maintenance of endpoint management infrastructure within the MSP's own data center or on-premises environment. This approach provides greater control and customization options but requires significant upfront investment in hardware and ongoing maintenance costs. However, they still tend to be lower cost compared to hosted counterparts.

- **Hosted solutions** are provided as a service by RMM vendors, offering scalability, flexibility, and reduced administrative overhead. However, they may come with subscription-based pricing models that can impact long-term cost considerations and lock MSPs into multi-year or auto-renew contracts to get lower prices with few exit options.

Security risks

Security risks are inherent in traditional endpoint management methods, particularly with agent-based solutions. Vulnerabilities in popular platforms like Kaseya VSA, ConnectWise ScreenConnect, and SolarWinds have been exploited by threat actors, leading to data breaches and system compromises. Without strong security protocols and tools, MSPs risk losing customers if issues occur. MSPs must prioritize security measures, such as regular patching, network segmentation, and multi-factor authentication to mitigate these risks and protect client endpoints.

Compatibility issues

Another challenge with traditional methods is the lack of modern awareness and compatibility with emerging technologies. For instance, some solutions may misclassify devices, such as mistaking Intune-joined devices as workgroup machines or incorrectly identifying Microsoft AVD (Azure Virtual Desktop) instances as servers. This lack of awareness can lead to mismanagement, security vulnerabilities, and operational inefficiencies, highlighting the need for continuous adaptation and updates in endpoint management practices.

When considering traditional endpoint management solutions, MSPs must carefully evaluate their options, accounting for factors such as cost, security, and compatibility with modern technologies. By staying informed and proactive, MSPs can effectively weigh the advantages and disadvantages of traditional methods while exploring other innovative solutions to meet the evolving needs of their clients.

Introduction of Microsoft endpoint management (Intune)

Microsoft's endpoint management solution, Intune, made its debut in 2010 primarily as a mobile device management (MDM) solution. While initially facing competition from other players, such as MaaS 360, MobileIron, and Airwatch, Intune quickly demonstrated its potential for growth and improvement.

In its early stages, Intune underwent a transformative journey, evolving into a more robust and comprehensive solution. By approximately 2016, significant enhancements had propelled Intune into the spotlight, garnering increased attention and consideration from organizations seeking effective endpoint management solutions.

The maturity of Intune during this period marked a significant milestone in its development. With refinements in functionality, user experience, and security features, Intune emerged as a compelling choice for organizations looking to streamline device management across various platforms.

The shift in perception towards Intune around 2016 represented a pivotal moment in the endpoint management landscape. Organizations began recognizing Intune as a credible alternative to traditional MDM solutions, appreciating its integration with the broader Microsoft ecosystem and its ability to address evolving needs in an increasingly mobile-oriented environment.

As Intune continued to evolve, it expanded its capabilities beyond MDM, embracing the concept of **unified endpoint management (UEM)**. This strategic evolution reinforced Intune's position as a versatile solution capable of effectively managing and securing endpoints across different device types and operating systems.

Since its inception, Intune has remained committed to innovation and adaptation, continually refining its features to meet the evolving demands of modern IT environments. Today, Intune stands as a leading endpoint management solution, empowering organizations to achieve greater efficiency, security, and flexibility in their IT operations compared to traditional solutions.

Core components of endpoint management

Endpoint management encompasses various components essential for effectively managing and securing endpoint devices within an organization. Let's break down some key aspects, such as agent installation, automatic enrollment, zero trust, monitoring, and security posture, comparing traditional endpoint management solutions with Microsoft Intune.

Agent install vs. automatic enrollment

Agent installation in traditional solutions

Traditional endpoint management solutions often require manual installation of agents on each endpoint device. This process can be time-consuming and prone to errors, especially in large-scale deployments. Additionally, agents may need to be updated regularly, adding to administrative overhead.

Automatic enrollment with Microsoft Intune

In contrast, Microsoft Intune offers automatic enrollment capabilities, streamlining the onboarding process for endpoint devices. Through integration with **Entra ID** (formerly Azure Active Directory), devices can be automatically enrolled and configured with policies, ensuring consistency and efficiency across the organization. This approach reduces deployment time and simplifies management tasks for IT administrators.

Zero Trust

Zero Trust in traditional solutions

Some traditional endpoint management solutions do not contain robust Zero Trust capabilities, relying on perimeter-based security measures that may not adequately protect against modern threats. This approach can leave organizations vulnerable to advanced cyberattacks and insider threats.

Zero Trust with Microsoft Intune

Microsoft Intune embraces a **Zero Trust security model**, ensuring that access to resources is continuously evaluated based on multiple factors, such as device health, user identity, and behavior. Using features like **Conditional Access** and **Endpoint Security**, Intune enables organizations to enforce granular access controls and dynamically adapt security policies to effectively mitigate risks.

Monitoring

Monitoring in traditional solutions

Traditional endpoint management solutions offer robust monitoring capabilities, often providing visibility into device status and performance metrics. These vendors have sophisticated live monitoring capabilities, and their solutions were purpose-built for MSPs to add specific information crucial to the help desk engineering team troubleshooting each device.

Monitoring with Microsoft Intune

Microsoft Intune delivers comprehensive monitoring capabilities, leveraging **Microsoft Defender for Endpoint** to provide real-time visibility into device security posture and threat detection. By integrating with **Microsoft 365 Defender**, Intune enables centralized monitoring and response across endpoints, identities, and applications, empowering organizations to detect and remediate threats rapidly.

Security posture

Security posture in traditional solutions

Some traditional endpoint management solutions lack built-in tools for assessing and improving security posture. Organizations may struggle to quantify their security posture and identify areas for improvement effectively.

Security posture with Microsoft Intune

Microsoft Intune includes **Secure Score**, a built-in tool that evaluates an organization's security posture based on recommended best practices and compliance standards. By providing actionable insights and prioritized recommendations, **Secure Score** helps organizations strengthen their security defenses and enhance overall resilience against cyber threats.

Supported devices in Microsoft Intune

Microsoft Intune provides comprehensive support for a wide range of devices, enabling organizations to manage and secure their endpoint devices seamlessly across diverse platforms.

Intune offers support for the following device types:

- **Windows:** Intune provides robust management capabilities for Windows devices, including PCs, laptops, and tablets. IT administrators can enforce security policies, deploy software updates, and manage device configurations to ensure compliance and bolster security.

- **Apple:** Intune offers efficient management of Apple devices, including Mac computers and iOS devices such as iPhones and iPads. With Intune, organizations can enforce security settings, deploy applications, and remotely wipe devices to protect corporate data on Apple devices.

- **Android:** Intune extends its management capabilities to Android devices, enabling organizations to manage security settings, enforce compliance policies, and distribute applications through the Google Play Store or Intune Company Portal.

- **Linux (Ubuntu):** Intune also supports the management of Linux devices running Ubuntu, allowing organizations to enforce security policies, deploy applications, and manage device configurations for Linux-based endpoints.

Device enrollment

Enrolling devices into Intune is a straightforward process designed to ensure ease of use for both IT administrators and end-users. Here's a brief overview of the enrollment process:

- **Windows:** For Windows devices, IT administrators can use the Intune Enrollment Guide to enroll devices through Entra ID join. This process involves configuring device settings in the Azure portal and guiding end-users through the enrollment process.

- **Apple:** Intune supports the Apple Device Enrollment Program via Apple Business Manager. IT administrators can use these programs to automatically enroll Apple devices into Intune during the initial setup process, simplifying device deployment and management.

- **iOS and Android:** Intune offers mobile device management (MDM) capabilities for iOS and Android devices, allowing organizations to enroll devices over the air (OTA) through the Intune Company Portal app or by using enrollment profiles. End-users can follow simple on-screen instructions to enroll their devices and gain access to corporate resources.

- **Linux (Ubuntu):** Intune supports enrollment of Linux devices running Ubuntu through the Intune agent for Linux. IT administrators can deploy the Intune agent to Ubuntu devices and enroll them into Intune for centralized management and policy enforcement.

By following the Intune Enrollment Guide tailored to each device type, organizations can ensure a smooth and secure enrollment process, enabling them to easily manage and secure their endpoint devices across Windows, Apple, iOS, Android, and Linux platforms.

Endpoint management remote control options

Microsoft Intune offers remote control capabilities to empower IT administrators with efficient and secure access to endpoint devices for troubleshooting and support. Let's explore Intune's remote control capabilities and how they compare to traditional remote access tools.

RemoteHelp

Intune RemoteHelp is a built-in remote control solution that allows IT administrators to remotely troubleshoot and assist users with technical issues on their managed devices. With RemoteHelp, administrators can initiate remote sessions directly from the Intune console, enabling them to view the device screen, interact with applications, and troubleshoot issues in real time.

Traditional remote access tools

While Intune RemoteHelp provides native remote control capabilities, organizations may also consider traditional remote access tools for managing endpoint devices:

- **ScreenConnect:** Now part of ConnectWise Control, ScreenConnect is a feature-rich remote support solution that offers remote access and troubleshooting capabilities for endpoint devices. While ScreenConnect provides extensive functionality, organizations may find Intune RemoteHelp more convenient due to its seamless integration with the Intune management console and centralized management of device access.

- **VSA (Virtual System Administrator):** Part of the Kaseya VSA platform, VSA provides comprehensive remote management capabilities for IT environments. However, Intune RemoteHelp offers a more streamlined and integrated approach to remote control, enabling organizations to leverage their existing Intune infrastructure for device management and support tasks.

- **TeamViewer:** A popular remote access solution that offers cross-platform support for remote troubleshooting and assistance. While TeamViewer provides robust functionality, organizations may prefer Intune RemoteHelp for its tighter integration with Microsoft's ecosystem and centralized management capabilities within the Intune console. Prior to the release of RemoteHelp, TeamViewer was the only integrated remote control solution within Intune.

In summary, **Intune RemoteHelp** provides organizations with a native remote control solution that easily integrates with the Intune management console. While traditional remote access tools like ScreenConnect, VSA, and TeamViewer offer extensive functionality, Intune RemoteHelp offers a more integrated and straightforward approach to remote troubleshooting and support tasks within the Microsoft ecosystem.

Intune updates (OS and App)

Microsoft Intune offers robust capabilities for managing updates to both operating systems and applications, providing organizations with structured and efficient methods for keeping their endpoint devices secure and up to date. Let's delve into Intune's update management features and compare them to legacy remote monitoring and management (RMM) solutions.

Legacy RMM patch management

Legacy RMM solutions typically offer patch management functionality for operating system updates, allowing IT administrators to deploy security patches and updates to endpoint devices. However, these solutions may lack integrations found in Microsoft Intune.

Legacy RMM script-based third-party app management

Similarly, legacy RMM solutions may offer script-based management for third-party application updates, enabling IT administrators to deploy software patches and updates using custom scripts or automation tools. While effective, this approach may require manual intervention and lack the centralized management and reporting capabilities provided by Intune.

Windows updates

Intune simplifies the management of Windows updates, features, and drivers through granular control over update rings. IT administrators can define deployment rings based on device groups or user roles, allowing for a phased rollout of updates to minimize disruption and ensure compatibility with organizational workflows.

IT administrators can create policies on how and when patches roll out. Then, they can assign those policies to device groups so Intune can tell Windows Updates on the local machine to patch according to policy. This closely ties into Compliance status, which affects security and access to corporate documents and resources via Conditional Access.

Nerdio Manager Unified Application Management (UAM)

Nerdio Manager for MSP's Unified Application Management feature enhances Intune's update capabilities by providing a centralized platform for managing and deploying applications across endpoint devices. This integration streamlines the application lifecycle management process, from deployment to updates and retirement, ensuring consistency and efficiency in software management.

Microsoft WinGet

Windows Package Manager (WinGet) is a command-line tool introduced by Microsoft to simplify the installation and management of applications on Windows devices. With a rich history of development and community contributions, WinGet has evolved into a powerful package manager that complements Intune's application deployment capabilities.

WinGet works by using manifest files that define the metadata and installation parameters for applications. IT administrators can use WinGet commands to search for, install, update, and uninstall applications from public repositories or private repositories hosted internally within their organization.

Public and private repositories

WinGet leverages public repositories such as the Microsoft Store and GitHub to source application manifests and binaries. These repositories provide a vast catalog of applications curated by Microsoft and the community, ensuring a diverse selection of software for organizations to deploy via Intune.

In addition to public repositories, organizations can set up private repositories to host custom or proprietary applications for deployment via Intune. Private repositories offer greater control over software distribution and ensure compliance with organizational policies and security requirements.

Intune update management capabilities

Intune's update management capabilities, coupled with integrations like Nerdio Manager's Unified Application Management and support for WinGet, provide organizations with a modern and efficient solution for keeping their endpoint devices secure and up to date. Compared to legacy RMM solutions, Intune offers greater automation, centralized management, and flexibility in managing operating system and application updates, empowering organizations to maintain a strong security posture and improve productivity across their IT infrastructure.

Intune security

Microsoft Intune offers a comprehensive suite of security features designed to protect endpoint devices, safeguard organizational data, and mitigate security risks effectively. Let's explore some key aspects of Intune's security capabilities.

Defender for Business

Intune integrates seamlessly with Microsoft Defender for Business, providing advanced threat protection capabilities to defend against malware, ransomware, and other cyber threats. Defender for Business employs next-generation antivirus (NGAV) and endpoint detection and response (EDR) technologies to detect and respond to sophisticated attacks in real time, enhancing the overall security posture of endpoint devices.

Configuration profiles

Configuration profiles in Intune serve as the modern equivalent of group policy objects (GPOs), allowing IT administrators to enforce security settings, device configurations, and compliance policies across endpoint devices. With configuration profiles, organizations can achieve consistent security posture and configuration management across their entire device fleet, regardless of device type or location.

Defender policies and exclusions

Intune enables organizations to define and enforce Microsoft Defender antivirus policies to protect endpoint devices from malware and other security threats. These policies allow IT administrators to configure antivirus settings, define scan schedules, and specify threat detection and remediation actions. Additionally, administrators can create exclusions to exclude specific files, folders, or processes from antivirus scans, reducing false positives and optimizing system performance.

Security baselines

Intune provides predefined security baselines based on industry best practices and regulatory standards, such as the Microsoft Security Baseline and CIS Benchmarks. These baselines offer a set of recommended security configurations and settings that organizations can apply to their endpoint devices to enhance security posture and ensure compliance with security standards.

CIS Benchmarks

Intune (via Nerdio) supports CIS Benchmarks, which are industry-standard configuration guidelines for securing systems and applications. By applying CIS Benchmark recommendations through Intune configuration policies, organizations can align their security configurations with recognized best practices and reduce the risk of security vulnerabilities and compliance violations. CIS recently announced Critical Security Controls v8, which maps to NIST’s Cybersecurity Framework.

Hardened images for servers and AVDs

Intune (via Nerdio) enables organizations to deploy hardened images for servers and AVDs, ensuring that virtual desktop environments are secure and compliant with organizational security policies. By creating and deploying custom images with preconfigured security settings and software configurations, organizations can streamline the provisioning process and mitigate security risks associated with virtual desktop infrastructure (VDI) deployments.

TIP For those wanting to perform similar actions with a Windows 365 Cloud PC or with physical endpoints, Nerdio Manager’s Intune integration into GitHub can provide that option.

Threat and vulnerability management

Intune paired with Microsoft Defender provides built-in threat and vulnerability management capabilities, allowing organizations to identify, assess, and remediate security threats and vulnerabilities across their endpoint devices. By using threat intelligence from Microsoft Defender

Antivirus and Microsoft 365 Defender, Intune enables organizations to proactively detect and respond to security incidents, minimizing the impact of cyber threats on their IT infrastructure.

Intune offers a robust set of security features and capabilities to protect endpoint devices and organizational data from evolving cyber threats. From advanced threat protection with Defender for Business to security configuration management with configuration profiles and security baselines, Intune empowers organizations to strengthen their security posture and maintain compliance with regulatory standards and industry best practices.

Intune scripting

Microsoft Intune empowers MSPs with powerful scripting capabilities, enabling them to automate tasks, deploy configurations, and manage endpoint devices efficiently.

Windows Scripts (PowerShell)

Intune allows MSPs to leverage Windows PowerShell scripts to perform a wide range of tasks on endpoint devices, including configuration changes, software installations, and system maintenance. PowerShell scripts offer extensive functionality and flexibility, allowing MSPs to customize and automate routine tasks to meet the specific needs of their clients.

By utilizing PowerShell scripts in Intune, MSPs can streamline management workflows, reduce manual intervention, and increase operational efficiency across their client environments.

With Intune, MSPs can create PowerShell scripts to:

- Configure device settings and policies
- Install or uninstall software applications
- Modify registry settings
- Retrieve system information and logs
- Execute custom actions and commands

Scripting variables

Using the concept of variables is important for MSPs managing multiple customers. Often, MSPs will want to reuse scripts for multiple customers, but this can be tricky without a tool like Nerdio Manager. With Nerdio’s Scripted Actions and handling of Intune policies, specific areas within a PowerShell script or a JSON file (Intune Policy) can be replaced with a variable instead of its absolute value.

For example, if an MSP wants to run a script to install a piece of software from a website, the URL might be unique to that download of that software per customer. Instead of making a separate script for each customer, a singular script can be used. In place of that absolute URL, a variable can be used to define that value, and that value can be stored securely in an Azure KeyVault and called when the script gets executed.

With Nerdio, a single script or Intune policy can be used for all customers, but for each script that is executed or Intune policy that is copied down to the customer tenant, it will behave and act differently. This saves a tremendous amount of time and effort for any organization managing multiple customers. Once a new policy is created or updated, within the hour, it can be replicated across all customers' tenants and applied immediately.

TIP With Nerdio Manager, Intune scripting capabilities empower MSPs to automate and organize management tasks, enhance operational efficiency, and deliver exceptional service to their clients.

Intune reporting and compliance

Intune equips MSPs with robust reporting and compliance capabilities, enabling proactive management of endpoint devices and ensuring adherence to security standards and regulatory requirements. Let's explore how Intune supports proactive management and compliance, plus some legacy best practices in proactive management.

Proactive management in Intune

MSPs using Intune can take a proactive approach to managing endpoint devices, allowing them to anticipate and address issues before they impact productivity or security. By leveraging Intune's reporting and monitoring features paired with Microsoft Security, MSPs can identify potential issues, enforce compliance policies, and implement remediation actions to maintain the health and security of client environments.

Legacy proactive management best practices

Intune builds upon legacy proactive management best practices, offering modernized approaches to monitor and maintain endpoint devices. Some examples of legacy proactive management best practices include:

- **Reporting online/offline status:** Intune provides insights into the online/offline status of endpoint devices, allowing MSPs to track device connectivity and address network-related issues promptly.
- **Low disk space monitoring:** Intune enables MSPs to monitor disk space usage on endpoint devices and proactively identify devices at risk of running out of storage capacity. This allows MSPs to take preventive action, such as disk cleanup or expansion, to avoid performance degradation or data loss.

- **Querying service status:** Intune allows MSPs to query the status of critical services and processes on endpoint devices, helping them identify and troubleshoot potential issues related to service failures or performance degradation.

Threat, vulnerability, and compliance management with Defender

Intune goes beyond legacy proactive management practices by offering integrated threat, vulnerability, and compliance management capabilities. MSPs can utilize Intune to:

- Identify and remediate security threats and vulnerabilities on endpoint devices.
- Enforce compliance with regulatory standards and organizational security policies.
- Generate reports and audit logs to demonstrate compliance and adherence to security best practices.

TIP By combining proactive management with advanced threat detection and compliance management features, Intune empowers MSPs to maintain a secure and compliant IT environment for their clients.

Intune device onboarding and offboarding

Efficient device onboarding and offboarding processes are essential for MSPs to ensure smooth transitions and maintain security when managing endpoint devices. Microsoft Intune offers various methods and tools to optimize these processes, from manual methods to automated enrollment options. Let’s explore how Intune facilitates device onboarding and offboarding.

Intune OOBE, Autopilot, Windows Configuration Designer

Intune offers several automated enrollment options to streamline user onboarding:

- **Out of Box Experience (OOBE):** Intune integrates with Windows OOBE, allowing MSPs to configure device settings and policies during the initial setup process. This ensures that devices are provisioned with the necessary configurations before users activate them.
- **Autopilot:** Autopilot simplifies device provisioning by allowing MSPs to pre-configure devices and enroll them in Intune automatically. Users can then complete the setup process with minimal intervention, reducing deployment time and complexity.
- **Windows Configuration Designer:** Windows Configuration Designer enables MSPs to create custom provisioning packages that automate device setup and enrollment in Intune. This tool offers flexibility for configuring device settings and deploying applications based on organizational requirements. This is an excellent option for mass deployment taking place at an MSP bench.

Manual enrollment and retirement

In cases where automated enrollment is not feasible, Intune supports manual enrollment and retirement of devices:

- **Manual enrollment:** MSPs can manually enroll devices in Intune by installing the Company Portal app or configuring device settings manually. This method provides flexibility for onboarding devices that do not support automated enrollment options.

- **Retire:** When offboarding devices or decommissioning devices, Intune allows MSPs to retire devices from management. This process removes device configurations and policies applied through Intune, ensuring that decommissioned devices no longer pose security risks.

Rewst integration

Rewst, a comprehensive user and device management platform, integrates with Intune to streamline user onboarding and offboarding processes. Leveraging Rewst integration, MSPs can automate user provisioning, enforce security policies, and manage device lifecycles seamlessly within their existing workflows.

Intune offers a range of methods and tools to facilitate user onboarding and offboarding, from manual methods to automated enrollment options. By capitalizing on Intune's capabilities and integrating with platforms like Rewst, MSPs can optimize these processes, enhance security, and improve operational efficiency when managing endpoint devices for their clients.

The case for continuing with traditional endpoint management solutions

While Microsoft Intune offers compelling features and advantages, some organizations may hesitate to transition from traditional endpoint management tools. Let's explore the reasons why some might choose to continue with their current solutions while acknowledging potential drawbacks.

Patch management

Traditional endpoint management tools often provide robust patch management capabilities, allowing organizations to efficiently deploy updates and patches across their device fleet. These tools offer granular control over patching schedules and configurations, ensuring timely remediation of vulnerabilities and compliance with security policies.

Live monitoring

Live monitoring tools, such as ConnectWise Backstage, offer real-time insights into endpoint performance and security events. These platforms enable IT teams to proactively identify and address issues as they arise, minimizing downtime and enhancing overall system reliability. Additionally, features like remote troubleshooting and diagnostic tools streamline support workflows, empowering IT administrators to swiftly resolve issues.

PSA integration

Many traditional endpoint management tools integrate well with professional services automation (PSA) platforms, facilitating efficient workflows and improved collaboration between IT teams. Integration with PSA systems enables automated ticket creation, asset tracking, and centralized management of service requests, enhancing operational efficiency and customer satisfaction.

Ecosystem integration

Many traditional endpoint management tools boast extensive ecosystem integration capabilities, allowing organizations to leverage complementary solutions for enhanced functionality and interoperability. Integration with third-party security tools, network monitoring platforms, and productivity suites enables organizations to build comprehensive IT ecosystems tailored to their specific needs and requirements.

While traditional endpoint management tools offer several advantages, it's essential to recognize potential limitations and drawbacks compared to modern solutions like Microsoft Intune. These may include:

- **Complexity and scalability:** Traditional solutions may struggle to scale and adapt to the evolving needs of modern IT environments, particularly in highly dynamic or distributed settings.
- **Security risks:** Legacy systems may lack the robust security features and threat detection capabilities found in newer solutions like Intune, leaving organizations vulnerable to emerging cyber threats and compliance issues.
- **Maintenance overhead:** Some endpoint management tools often require significant manual intervention and upkeep, leading to increased administrative overhead and operational complexity. Additionally, many require long-term contracts that lock MSPs in with specific vendors, even if they become dissatisfied.

While traditional endpoint management tools have served organizations well in the past, they fall short in addressing the evolving challenges of today's IT industry. By carefully evaluating the limitations and drawbacks of legacy solutions, organizations can make informed decisions about transitioning to more modern and comprehensive alternatives.

The case for Microsoft Intune

Microsoft Intune presents a compelling case for organizations seeking a modern, comprehensive endpoint management solution. Let's delve into key advantages that make Intune the superior choice for managing and securing endpoint devices.

Agentless management

One of the standout features of Microsoft Intune is its agentless management approach, which eliminates the need for cumbersome software agents on endpoint devices. This streamlined approach reduces deployment complexity and minimizes performance overhead, resulting in a more efficient and user-friendly management experience for IT administrators and end-users alike.

Fewer vulnerabilities

Intune's architecture prioritizes security, resulting in fewer vulnerabilities and common vulnerabilities and exposures (CVEs) compared to traditional endpoint management solutions. By utilizing Microsoft's robust security expertise and continuous threat intelligence updates, Intune provides organizations with a proactive defense against emerging threats, reducing the risk of security breaches and data compromises.

Latest integrations and innovations

Intune stands at the forefront of innovation, offering integration with the latest advancements in endpoint management and security. Through seamless integration with Microsoft 365 and Azure services, Intune enables organizations to leverage cutting-edge technologies such as AI-driven threat detection, cloud-native management capabilities, and predictive analytics to stay ahead of evolving threats and operational challenges.

Integration with Microsoft Security

Intune's integration with the broader Microsoft Security ecosystem enhances its effectiveness and extends its capabilities beyond traditional endpoint management. By combining forces with solutions like Microsoft Defender for Endpoint and Entra ID, Intune creates a unified security platform that provides end-to-end visibility, threat detection, and response across endpoints, identities, and cloud services. This holistic approach heightens organizations' security posture and enables proactive threat mitigation across their entire IT infrastructure.

Threat analytics and vulnerability management

Intune empowers organizations with advanced threat analytics and vulnerability management capabilities, enabling proactive identification and remediation of security risks. By leveraging insights from Microsoft Threat Intelligence and Security Graph, Intune helps organizations prioritize vulnerabilities and security incidents based on risk severity, guiding informed decision-making and resource allocation to mitigate potential threats effectively.

Overall, Microsoft Intune offers a compelling value proposition as the premier endpoint management solution for organizations of all sizes. With its agentless management approach, robust security posture, simplified integration with Microsoft's ecosystem, and advanced analytics capabilities, Intune empowers organizations to enhance productivity, strengthen security, and adapt to the growing IT industry demands.

The opportunity for a Microsoft Cloud-based MSP practice with Nerdio

While native Microsoft Intune offers powerful endpoint management capabilities, deploying and managing it efficiently can be a daunting task for organizations, consuming valuable time and resources. However, by integrating Nerdio Manager for MSP into their workflows, managed service providers can transform their Intune deployment and management processes, ensuring seamless operations and superior service delivery to their clients.

Simplifying deployment and management

Nerdio simplifies the deployment and management of Microsoft Intune for MSPs through a suite of automated workflows, centralized management features, and template-based configurations. Using Nerdio's platform, MSPs can streamline deployment tasks such as device enrollment and policy configuration, reducing manual effort and maintaining consistency across client environments.

Centralized management console

The centralized management console provided by Nerdio integrates Intune with other Microsoft Cloud services, offering MSPs a single interface to administer Intune settings alongside Entra ID and Microsoft 365. This integration improves operational efficiency and simplifies administration, enabling MSPs to deliver exceptional service while minimizing complexity.

Advanced features for MSPs

Moreover, Nerdio offers robust features such as role-based access control, automated monitoring, and reporting for Intune, empowering MSPs to customize permissions, track device compliance, and proactively identify issues. With integration with Nerdio Manager for MSPs, management tasks become even more efficient, consolidating billing, provisioning, monitoring, and support efforts within a unified platform.

Unlocking new opportunities

By harnessing the power of Nerdio's integrated solutions, MSPs can optimize their Intune deployment processes, elevate service delivery, and ensure a superior experience for their clients. With Nerdio Manager, the journey to perfecting Intune deployment becomes not only achievable but also a testament to the efficiency and effectiveness of MSPs in delivering cutting-edge solutions to their clients.

Furthermore, embracing a Microsoft Cloud-based MSP practice presents an immense opportunity for MSPs to capitalize on the growing demand for cloud services and digital transformation initiatives. By leveraging Microsoft's comprehensive suite of cloud solutions, including Intune, Azure, and Microsoft 365, MSPs can position themselves as trusted advisors in guiding organizations through their cloud journey. With Nerdio Manager as their partner, MSPs can seize this opportunity to expand their service offerings, drive revenue growth, and establish long-term partnerships with their clients.

Interested in learning more about how Nerdio simplifies Intune deployment and management?

Schedule a demo today and unlock the full potential of the Microsoft Cloud ecosystem and your MSP cloud practice.

About Nerdio

Nerdio is a leading provider of powerful, simplified cloud management solutions for businesses of all sizes. Trusted by managed service providers (MSPs) and enterprise IT departments alike, Nerdio equips organizations with seamless, cost-effective management tools for Azure Virtual Desktop (AVD), Windows 365, and comprehensive Modern Work solutions.

With thousands of customers worldwide, Nerdio accelerates cloud adoption, enabling companies to thrive in an era of hybrid work by providing modern, future-proof technology that adapts to evolving workplace needs.

For more information, please visit **www.getnerdio.com**.

nerdio

WEB www.getnerdio.com
EMAIL hello@getnerdio.com