DYOGUARD

PROTECT YOUR WEAKEST LINK

ENSURING SECURITY IN A WORLD FULL OF DEVICES

The way we work has changed both radically and rapidly over the last few years, and the way organizations approach cybersecurity and data compliance has to change, too.

The pandemic accelerated an already-present trend towards remote and hybrid working. Today's employees work from home more than ever before. They access company networks and critical data assets from laptops, tablets, and smartphones.

From a security standpoint, this has led to a whole host of new concerns. The thought of even one employee accessing sensitive data from a personal smartphone on an airport WiFi network is enough to send a CSO or compliance officer into palpitations. And it's happening again and again, every day.

Organizations need to rethink security. Cybersecurity today needs to involve multiple programs and strategies working together, bolstered by cloud management, to protect data across a range of scattered endpoint devices.

One of the best tools to achieve this is Microsoft Intune, a policy manager that incorporates policies and protects endpoint devices. Here at DYOPATH, we've found Intune to be an invaluable tool.

In this white paper, we'll explore the current risks and challenges facing organizations, how Intune helps solve some of these problems, and how you can use this technology to build a safer, more mature, and more modern organization.

Distributed Devices: A Big Challenge for Modern Organizations

Many companies operate — willingly or not — on the basis that any data can be accessed at any time on any device.

This approach comes with major risks:

- Research by IBM found that the average data breach cost increased by over $1 million whenever remote work was a factor.
- A report by Gitnux found that 60% of remote workers use unsecured personal devices to access their employer's network.
- The same report found that 63% of businesses have experienced a data breach due to employees working remotely.

With more people working remotely than ever before, these findings are alarming. These incidents can lead to major financial losses, downtime, reputational damage, and issues with data compliance. To keep your assets and organization secure, you need to protect your devices by both simplifying and securing endpoint management. Here are some of the areas to focus on:

- **Inventory** — you need to know where your devices are, where your assets are stored, who is accessing your data, where they're accessing it from, the types of systems being used, and more. This is all especially important when considering remote endpoints.
- **Patching** — you need to make sure all relevant devices are properly patched and updated to avoid any vulnerabilities that attackers could take advantage of. This applies to any devices your team members use to access your networks.
- **Deployment of agents** — if security agents or remote management agents need to access your devices, how will they do this? They need easy — ideally remote — access to your endpoints.
- **Deployment of software** — users should not be installing their own software if possible. Instead, you should have systems in place to install and deploy software across all relevant devices with the help of your IT service desk.
- **Wiping or encrypting devices** — in the event a device is lost or stolen, you'll want the option to quickly wipe it clean or encrypt critical data. This must be done as easily as possible from a remote location if you want to prevent key assets from potentially falling into the wrong hands.

Taking care of all these disparate areas requires the right approach, driven by the right technology. Only with the best tools can you confidently handle all the necessary areas without overloading your teams.

Microsoft Intune for Security & Data Compliance

Dealing with a large number of endpoint devices in many different places requires a unique approach. That's where Microsoft Intune comes in.

Let's explore some of the key benefits Intune offers:

- Simpler app and device management. Intune allows the management of a wide range of applications and devices across multiple locations in a much more streamlined way by providing tools to deploy, configure, and manage devices. Less employee burnout, as automation can handle large volumes of repetitive tasks that would otherwise put a huge strain on human staff
- Support for a wide range of different devices. This includes mobile devices, desktop computers, and virtual endpoints running Windows, Linux, iOS, Mac OS, or Android.

- Security. Intune allows access controls and protects data across all devices and accounts, both organization-owned and personal.
- Compliance and reporting features. These make it easy to quickly communicate issues to relevant people in the organization.
- Easy deployment of security agents and remote management agents to devices wherever they are.
- Easy deployment of software to your devices wherever they are.
- Easily wipe devices from afar. If devices are lost or stolen, Intune allows you to wipe them clean or encrypt key data to avoid sensitive information getting accessed by the wrong people.
- Ability to patch and update devices from one central point, without having to worry about being physically close to each individual device.

It's important to remember that Intune is just one piece of the puzzle — an extremely powerful piece, but best when supported by other solutions.

Using Intune to Modernize Your Workforce

Now that we've covered some of the key benefits Intune offers, let's take a look at some of the concrete steps involved in setting up Intune to help you collaborate from anywhere and securely access resources remotely.

Device Management

This is the stage where your devices are configured and enrolled. This requires each user to be in Azure Active Directory (Azure AD) and each device to be enrolled in Intune. The process can happen in two different ways:

- **User-based** — each end user installs a company portal on their own personal devices.
- **Administrative-based** — a corporate device is added via Azure AD and enrolled into Intune automatically. Administrators can join via group policies.

Once devices are enrolled, policies can be applied. Each device has a configuration profile that controls, for example, administrative rules and security settings.

Application Management

During this stage, app development is addressed and application configuration policies are set. These are the critical security controls and other policies that you don't want end users to be changing without expert oversight.

Applications can be deployed and assigned to specific users or groups, allowing users to install them or push the apps to devices. This is followed by device deployment, where Windows Autopilot provisioning is used to set up devices from scratch and pre-configure them.

Access Control

Access control involves setting up conditional access policies, role-based access control, and privileged identity management in Intune to restrict and control access to devices and applications. This can be based on factors such as location, compliance, or risk.

It's possible — and encouraged — to set up these policies in line with your organization's compliance policies and app configuration policies.

Device Security

Device security in Intune is a combination of features including device compliance policies, app protection policies, an always-on VPN, and Microsoft Defender for Endpoint.

Within Intune, you can define the compliance policies to make sure your users stay on the right side of all relevant regulations. For example, users might need to have antivirus software or all relevant updates installed, and without these, they won't be able to connect to company resources.

Using Windows Autopilot With Intune

Another powerful solution when it comes to device management is Windows Autopilot. If your organization uses Windows machines, Autopilot can be enormously helpful when it comes to managing and setting up your devices in line with your policies and demands.

Here's how it works: your end user will get a new computer that has been pre-provisioned to your Azure and Intune tenant. The device looks and feels like it's brand new, but when your user logs in with their corporate credentials, they'll be granted access to Intune and all the right policies and software will then be put into place as part of the setup process. It's a very simple and straightforward way to get new devices up to speed and working in line with Intune.

Why Work With DYOPATH?

Using Microsoft Intune to manage your endpoints can be done alone, but there are significant benefits to working with a Managed Services Provider like DYOPATH.

Here are some of the key reasons to choose us as a partner:

- We take a **business-first approach**. We understand how our clients' security needs tie into their wider business goals, and we can help you get the needle moving and make concrete progress in the directions you want.
- We have **extensive experience** spanning 35 years in a wide range of industries, including commercial, government, energy, education, and more. We have a presence around the world, with service desk operations centers in the US, UK, and Mexico.
- We have worked with the **federal government**, helping build the NERC CIP framework.

Most importantly of all, we generate **impressive results** for our clients, including 82% first-call resolution, 20%+ efficiency gains, and 98% user satisfaction.

Using Intune Within the IT Maturity Model

One of our main guiding principles at DYOPATH is that of IT maturity. Every organization out there is at a different stage of IT maturity, ranging from companies with a chaotic, reactive approach to IT all the way to fully mature organizations, where IT is tightly aligned with all business functions and goals.

When you start using Intune, you should have this concept in mind. Intune is an excellent tool to help you achieve IT maturity faster by helping you manage your devices and endpoint security in a way that recognizes and ties into your overarching business goals. Technology should always be focused on growing your business while minimizing cost and risk.

DYOPATH can help you identify where you are in terms of your current maturity and how to improve.

Using Intune to Elevate Your Team

Another principle that differentiates DYOPATH is our focus on client engagement. Our goal is to perform IT operations for your business in a way that elevates your teams and allows you to be more strategic.

When it comes to Microsoft Intune and Autopilot, we can help you identify how to improve delivery, deployment, and support for end users in a way that's both more secure and more capable. Safe in the knowledge that we're handling your infrastructure and support, you can elevate your work and start focusing more on the tasks and services that drive your business forward.

How We Do It

DYOPATH's approach to taking care of your IT services and infrastructure involves the combination of several end-to-end IT services, which can be broken down into a few key areas.

Managed Support for End Users

Our managed support extends from on-site users to remote users, wherever they are. This service also includes support for depot services, which Intune and Autopilot are both key parts of. Our depot works with you as you roll out Intune and Autopilot, helping with various tasks like registering users, identifying machine IDs, and more.

Managed Support for Infrastructure

We also offer support with infrastructure — your servers, storage, and networks. We handle the intricacies of your cloud management whether it's on-cloud, on-premise, or hybrid. This includes device and endpoint management and solutions like Intune and Autopilot to deploy and manage your various devices.

Managed Security Services

Security has always been an area of priority for DYOPATH. Our managed security services are designed to help you identify threats, prevent intrusions, and quickly respond to any issues to protect your infrastructure and avoid any downtime or breaches.

Security, as always, ties into your overall business goals. It's our job to keep your organization safe while ensuring your security is optimized for the resources, money, and time you have available, taking into account your unique infrastructure and the specific risks you face.

Microsoft Intune and Autopilot are two incredibly valuable tools for organizations that manage multiple devices across wide networks. **We help you harness this technology to make sure your devices are properly managed and protected, so you can support a productive remote workforce and ensure data compliance without significant risk. To learn more, schedule a call with us.**

If you want to learn more . . .

Visit our Website

Call us at (866) 609 - PATH

Email us at solutions@dyopath.com