Microsoft NETAS

Endpoint Management & Windows Deployment Implementation Services

What is an endpoint?

Mobile devices running iOS and Android are obviously an enormous presence in business today, but their capabilities and vulnerabilities are still a fraction of those of desktop and laptop computers. The management and security of mobile devices generally is handled separately from desktops and laptops, but there is clearly a movement toward consolidation.

Windows administration is typically done using Microsoft Endpoint Configuration Manager (MECM) or a similar third-party system running on-premises. But new products, including Microsoft Intune, adopt the Mobile Device Management (MDM) model of moving this function into the cloud.

While it's essential to enable employees with the flexible, work-from-anywhere capabilities and devices they need, the benefits of a strong endpoint management and security strategy are clear, which we'll dive into **Netas Endpoint Management & Windows Deployment Implementation Services**

Empower employees with modern technologies

The modern workplace is increasingly hybrid and remote, which means employees need to be able to stay connected to the enterprise from anywhere. Without the right tools—and secure support for those laptops, mobile devices, and other endpoints—projects stack up, deliverables get pushed back, and critical opportunities get missed.

These setbacks can also affect team morale. When technology gets in their way, employees can become frustrated, unproductive, and restless. On the other hand, when empowered with tools that are optimized for modern workloads, their experience, wellbeing, and productivity improve.

Whether in the office or on the front lines, remote or on-site, your employees show up to do a job. They're expecting a modern workplace approach that encompasses a range of work styles and provides the tools they need to get the job done: laptops, mobile devices, productivity tools, collaboration apps, and more. A workplace that's optimized for what employees need to do every day, wherever they're working and however they need to work, is quickly becoming a competitive differentiator in attracting and retaining top talent as well.

5X Increase in remote job postings on LinkedIn since the pandemic

73% Of workers want flexible remote work options to continue

43% Of the global workforce is likely to consider leaving their current employer within the next year

2021 Work Trend Index, Microsoft.com

Simplify device management and security

Today's IT department is faced with managing an ever-increasing mix of corporate-owned and personal devices. Meanwhile, seasonal fluctuations, project updates or sudden shifts in the business lead to heavy workloads for the IT department.

During the pandemic, organizations scrambled to equip their employees to work remotely whether they were ready for it or not. Some employees were using company and personal devices, dated hardware, and logging in on unsecured networks.

This highlighted the need for the IT department to quickly image hundreds or even thousands of personal devices with a company's proprietary applications and collaboration tools, and to ensure that critical security features were installed.

In order to onboard, manage, and secure every one of those devices—no matter what network they're connecting on—you need a modern endpoint strategy that lets you:

Easily manage who has access to what by controlling devices from a single tool

Automatically push updates to apps, so that everyone is getting the best, most secure experience

Take advantage of analytics to continuously improve user experience

With the right endpoint modernization strategy, employees get a secure experience on every mobile device, tablet, or laptop they're using. All while eliminating major IT administration headaches such as managing dated hardware, software and device deployment, as well as reducing costs for support, setup, and training.

Secure your hybrid work environment

$8.94M

Average cost of a successful attack against endpoints due to loss of IT and end-user productivity and theft of information assets.

2020, Third Annual Study on the State of Endpoint Security Risk, Ponemon Institute

Your employees want to connect to the enterprise from anywhere: their work computer in the office, their personal mobile on a public network, or even their roommate's laptop. This modern workplace reality of working anytime, anywhere—on personal devices, company computers, applications, virtual desktops, and more—can expose your company to significant security risk. And the rapid pace of business has often meant sacrificing security for productivity.

In the past, when the enterprise was more-or-less constrained to a physical location, it was simpler for IT to manage and deploy devices and how they connect to corporate resources. Now, securing the organization means additional layers to verify users, limiting access based on specific business scenarios, and proactively assuming a breach could happen. These security principles—known as Zero Trust—are nearly impossible without modern endpoints.

With modern endpoints, you can feel more confident about the security of personal and company-issued devices, no matter where and how they're connecting. You can control who has access to what, apply security settings to devices that are dispersed across the country or the world, and remove sensitive data when an employee leaves the company. Having centralized control and visibility also means your IT team can take system-wide action within minutes if there's a breach.

Your path to a connected, secure workplace

Empowering your teams and streamlining your IT oversight through modern endpoints does not have to be a complicated journey. The key is to understand your current security exposure and the steps you're taking to close those gaps, optimize those security workflows to meet the demands of hybrid work, and push them out to every endpoint.

With modern endpoints, you enable a dynamic enterprise that can react quickly to challenges and opportunities while attracting the most skilled talent. Every employee should be able to connect virtually with other team members, customers, and partners, as well as to the data and tools they need to do their jobs whether they're remote, hybrid, or simply accessing applications on the go. All while reducing burdensome and time-consuming IT oversight—such as onboarding, management, and updates—while enabling you to implement Zero Trust practices across your entire organization.

Modernized endpoints within reach

As you modernize endpoints in your enterprise, you should look for a solution that is:

Built-in, not bolted on

Microsoft offers best-in-class solutions within the ecosystem of apps, devices, and software you're already using. Using an integrated solution lets you benefit from trillions of signals that allow the platform to adapt to protect every customer better, then push that protection down to the last mile of devices.

Secure

Microsoft supports Zero Trust security architecture on every endpoint within your enterprise. Cloud-based authentication secures devices based on factors you control, granular access privileges secure both data and productivity, and real-time analytics and threat protection give you the visibility.

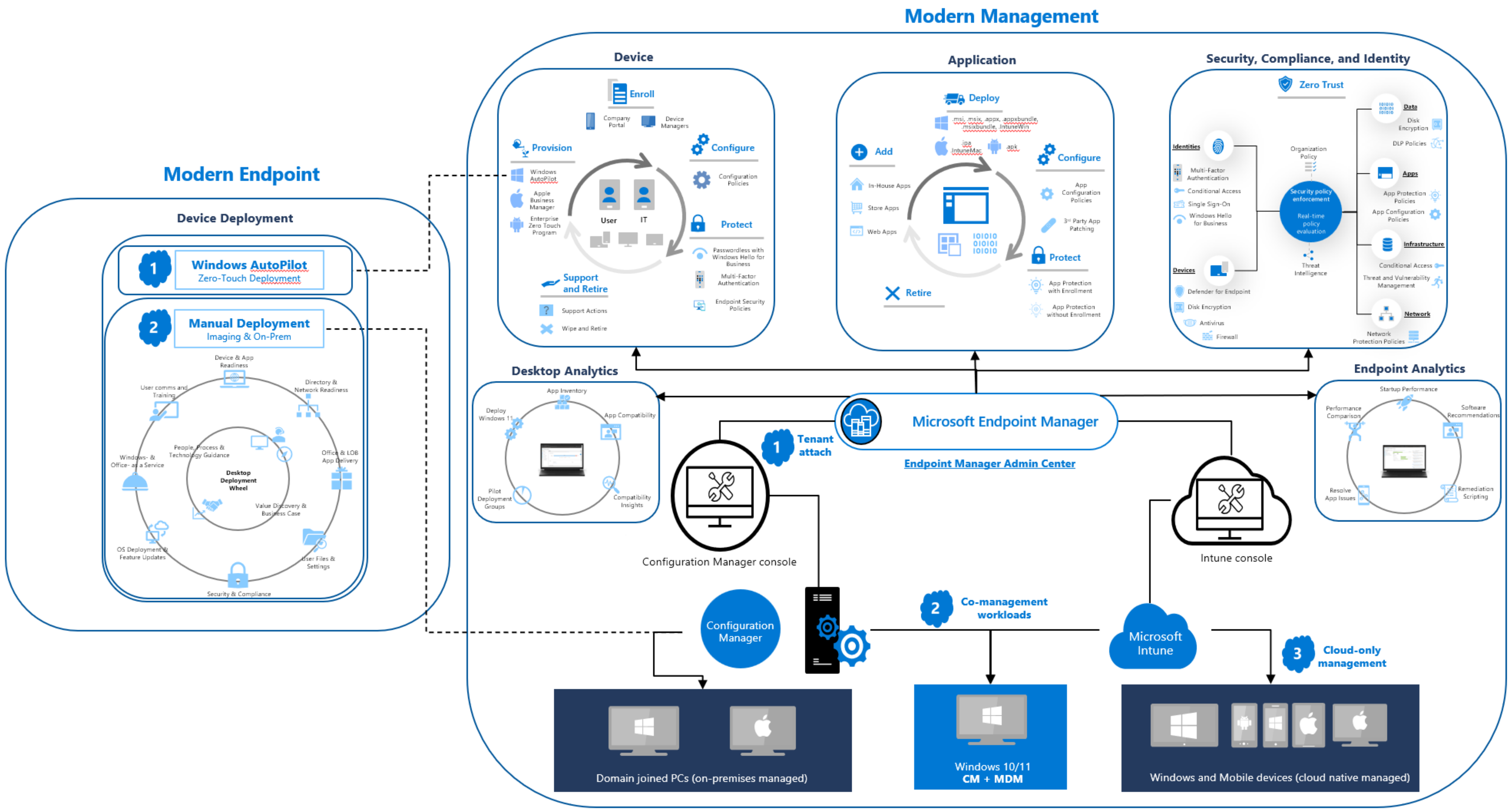
Interconnected

Workers can do their best work when they're plugged into a coherent ecosystem of applications, file sharing, and communication tools—regardless of what device they're using. Microsoft gives users a first-rate experience anywhere and everywhere they connect to your business. and speed you need to address threats immediately.

How NETAS can help

*Netas can help you implement **Modernize Endpoint Reference Architecture** step-by-step like below.*

- **Mobile Device Management Implementation :** including Windows, iOS/iPadOS/MacOS, Android/Android Enterprise platforms. Netas supports Management of MDM Lifecycle by provisioning, enrolling, configuring, protecting, supporting and retiring devices.
- **Mobile Application Management Implementation :** by deploying, configuring, protecting and retiring applications with or without enrollment.
- **Zero-Trust Framework Implementation :** by protecting identity, devices, data and application layers.
- **Endpoint Analytics Implementation :** by ensuring performance comparison, start-up performance, resolve application issues, software recommendations and remediation scripting.
- **Device Deployment Implementation :**
  - Windows AutoPilot (Zero Touch Deployment Experience)
  - Manuel Deployment (Desktop Deployment Wheel Methodology with Microsoft Endpoint Configuration Manager)



Ready to get started?

Connect with us today to see how NETAS can help you experience endpoint modernization in your own environment:

www.netas.com.tr

mscozum@netas.com.tr

Microsoft NETAS