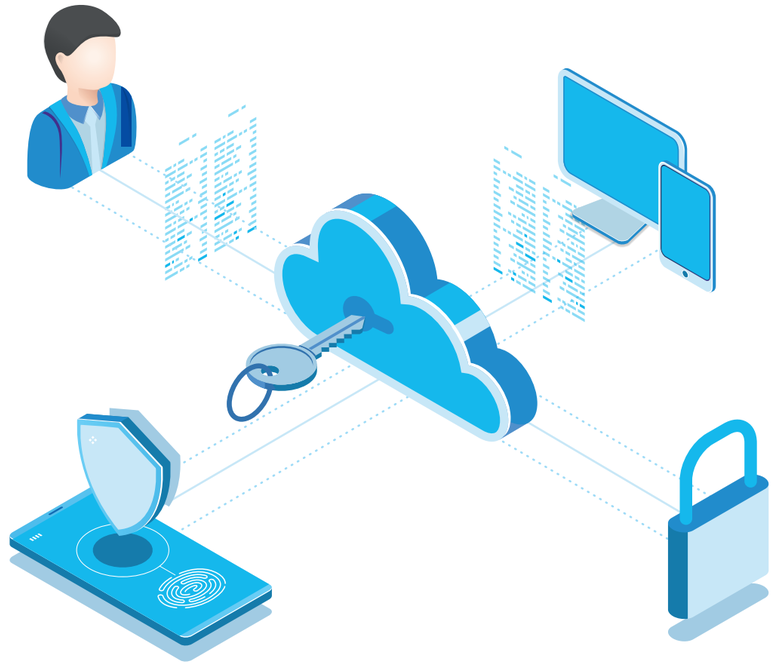


MODERN MANAGEMENT

Whitepaper: The Six Pillars of **Modern Management**

Disrupting legacy IT operations with six transformations

mobile mentor

Introduction

Legacy IT operations are no longer fit for purpose

IT operations have been following the same operating model for the past 30 years: the domain model. This model was designed for desktop computers and local data centers. Setup your private network, put in a proxy and a firewall, keep everything good inside and everything bad out.

Technology has evolved and capabilities have been expanded but underlying it all is the same IT operations paradigm developed more than three decades ago.

Meanwhile, the way work gets done has changed

Employees use laptops on the go. They email with personal smartphones. Data is constantly outside the protection of the domain, and remote work is the new normal. The domain model is no longer fit for purpose.

The good news is Microsoft has been developing new capabilities and technologies designed from the ground up as a cloud-first operating model. Given the domain model was designed to address the needs of companies large and small 30 years ago, these new features have been termed as "Modern" Management.

Modern Management achieves more with less

Modern Management is fundamentally designed for companies who want to be able to work anywhere, anytime, anyhow. It drops the concept of a domain and accepts that keeping your data behind a firewall and throttled by a VPN is no longer right.

Modern Management addresses security in a fundamentally different manner through zero-trust. It removes the need to manage operating system updates with over-the-air (OTA) updates. It leverages cloud security and introduces new protections.

Laptops can be sent directly to employees and auto-configure on sign in. Passwords are replaced with biometrics. Employee support can happen remotely, from anywhere.

The **So What** of Modern Management

In 2020, digital transformation was forced upon the world. Remote work became a requirement rather than a luxury and many businesses were left scrambling to support employees.

Modern Management arms your business with the tools and capabilities to survive regardless of the environment. Employees can work anywhere, anytime, and you can protect and secure your data outside of your network.

Modern Management isn't just about convenience. It's about business continuity. It's about ensuring your employees can focus on value creation. With Modern Management work becomes an activity, not a place.

Passwordless Authentication

Zero Touch Provisioning

Remote Support

LET'S TAKE A CLOSER LOOK AT THE 6 PILLARS OF MODERN MANAGEMENT

Zero Trust Network

Over the Air Updates

Cloud Data

Zero-Trust Network

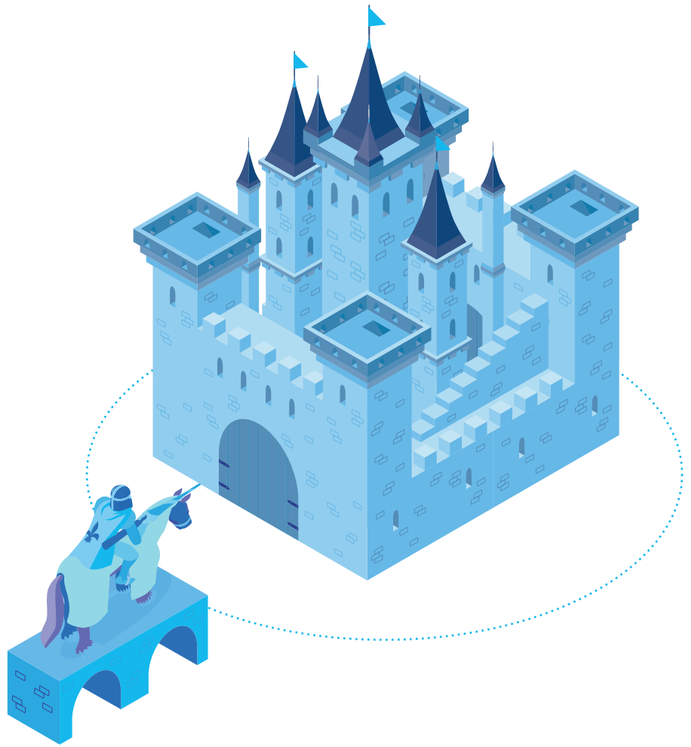
Cloud-first security to lower risk and ease access for employees

Working remotely traditionally meant using a VPN to access company resources.

Resources and files were kept within the company's domain and security measures were placed on the boundary between the public internet and the company. Firewalls, VPNs, and virtual machines are just a few of the pieces of infrastructure commonly used to support this model.

Once past the firewall or with a VPN connection, the computer accessing the resources was assumed to be trusted and secure and therefore allowed to access company resources.

Some companies deploy countermeasures to reduce risk, but the management of all these components is both costly and time-consuming. If a single link is mis-configured, company information can be exposed.



LEGACY

Zero-Trust Network

Cloud-first security to lower risk and ease access for employees

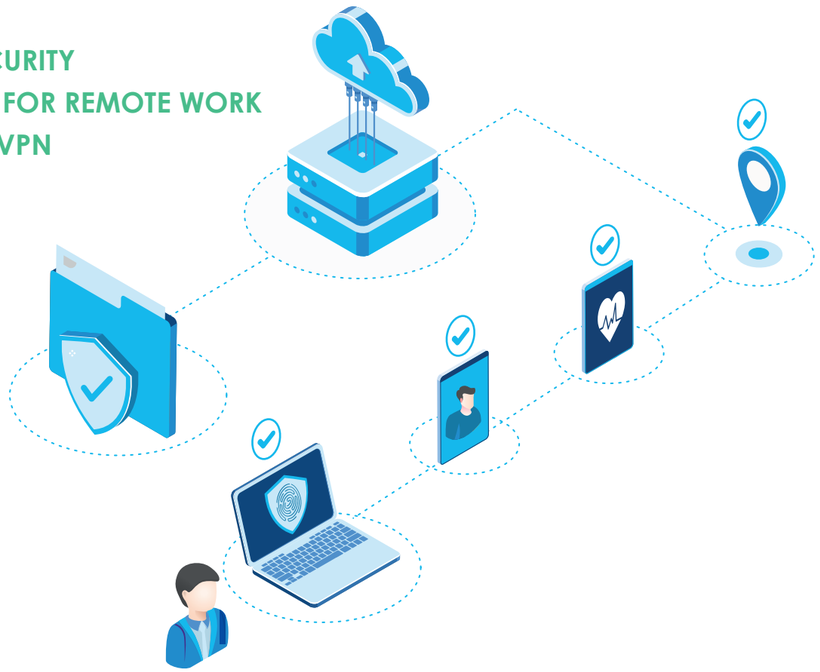
Zero-trust assumes all devices are untrusted and cannot access company resources until proven otherwise. Guilty until proven innocent. This is typically achieved through device attestation, conditional access policies, and multi-factor authentication. All these capabilities come native with Modern Management.

With zero-trust, access is granted or denied upon every access request and additional security is applied dynamically based on risk. Data access requirements are strengthened conditionally based on the security posture of the machine, the location of the employee, the sensitivity of the data, and more.

IT Administrators can adjust the rules to permit, block or present multi-factor authentication (MFA) challenges to specific device categories and modify security for specific resources. Geo-fencing – restricting access based on the location of the employee or only allowing access from a specific network – can be enabled and configured.

Zero-trust reduces costs by reducing the need for a VPN, firewall, and virtual machines. It increases security by dynamically applying rules. Employees love being able to access their data on the go, without the need for cumbersome and throttling VPNs and virtual machines.

- **BETTER SECURITY**
- **DESIGNED FOR REMOTE WORK**
- **DROP THE VPN**



Zero-Trust

1. Is a cloud-first security model that abandons the domain.
2. Zero-trust verifies the device, the person and their location.
3. Zero-trust uses MFA, conditional access, and geo-fencing.

SOLUTION

Over-the-Air Updates

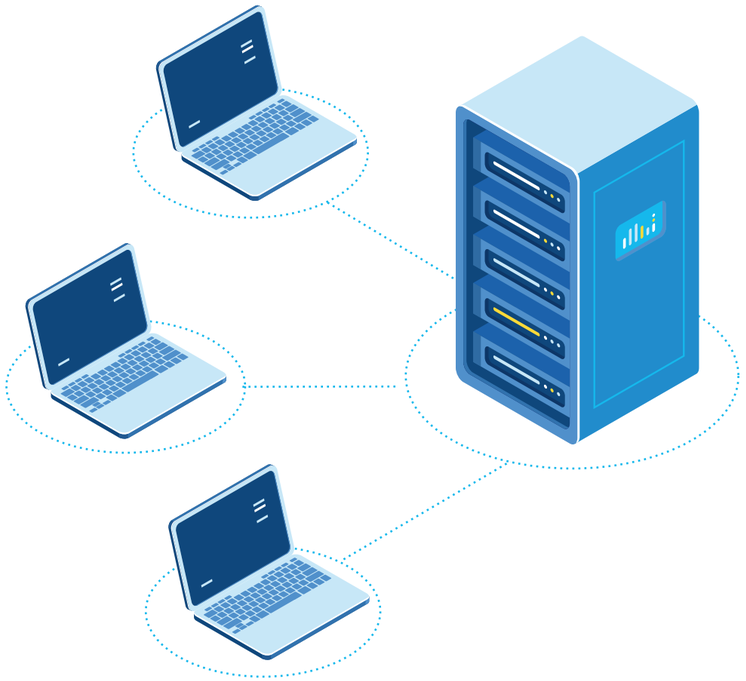
Operating System updates without the complex infrastructure

Updates to the Windows operating system used to be a big program of work for every company, typically requiring months or years of planning, change management, and tons of work.

Windows updates used to rely on Group Policy, SCCM integrated with WSUS, and required IT Admins to install and configure servers to perform updates.

Traditional updating requires the device to be domain joined and can cripple VPN traffic during large updates.

In 2016 Microsoft introduced the concept of Windows as a Service. Instead of a big release every 3 years, they developed Windows 10 with semi-annual updates, like the regular over-the-air updates for iOS and Android on mobile devices.



LEGACY

Over-the-Air Updates

Operating System updates without the complex infrastructure

Windows Updates for Business can now be handled like iOS and Android updates – silently, over-the-air, with minimal impact.

Windows update management using Microsoft Intune is based on deployment rings. Set the maximum deferral period for semi-annual feature updates and monthly quality updates with security updates.

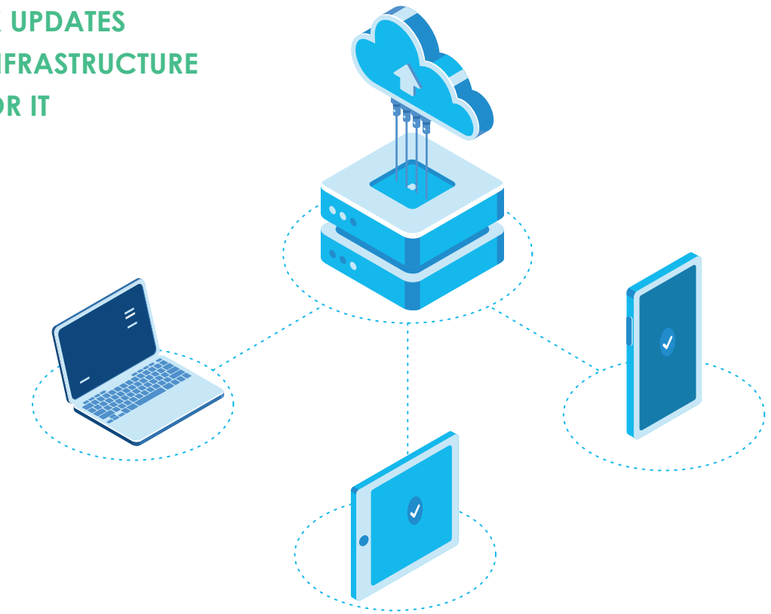
Now with regular updates delivered over-the-air, employees are prompted to restart their device and the updates are automatically installed in a couple of minutes.

Network latency and bandwidth concerns are eliminated as employees will update from their own internet connections. Domain joining is no longer required.

Admins can check compliance in Windows Azure by enrolling devices in Windows Analytics.

OTA updates save time and money by eliminating the infrastructure and all the effort that was required for testing, deployment and change management.

- OFF NETWORK UPDATES
- NO UPDATE INFRASTRUCTURE
- LESS WORK FOR IT



SOLUTION

Over-the-Air Updating

1. Removes the need for update infrastructure for Windows.
2. Allows updates from anywhere, even outside the domain.
3. OS updates managed through Windows Update Rings.

Cloud Data

Access files from anywhere while improving security

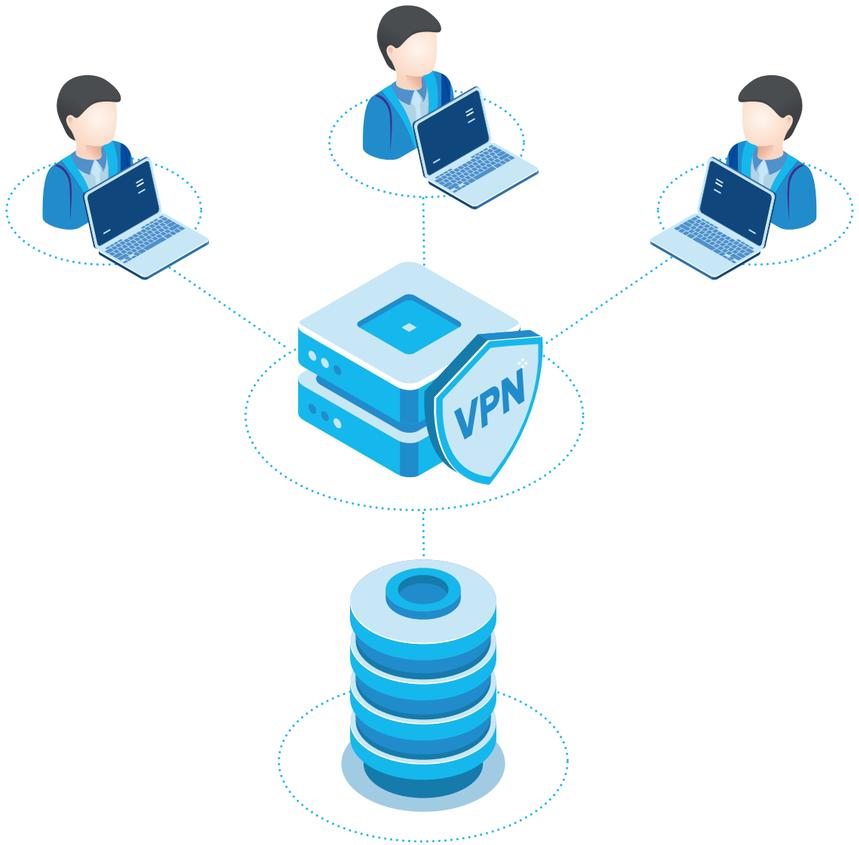
Private data centers and on-premise servers are still considered to be more secure than cloud storage in some industries. Other industries are going all in with cloud.

Some of the reluctance is because data breaches in public cloud services must be notified to regulators, whereas breaches to private storage are rarely disclosed.

The average time to identify a data breach worldwide is 197 days[1].

Managing a combination of cloud, on-premise storage and private data centers is inefficient and expensive. On-prem / data center storage must be supported by a local team who potentially have limited knowledge and stretched resources.

Once upon a time companies generated their own electricity. As they shifted to public generation infrastructure, they appointed a VP of Electricity to oversee that function. Data storage is likely to become a utility service like electricity, delivered more cost effectively and securely by large scale providers.



LEGACY

[1] IBM-Ponemon Institute

Cloud Data

Access files from anywhere while improving security

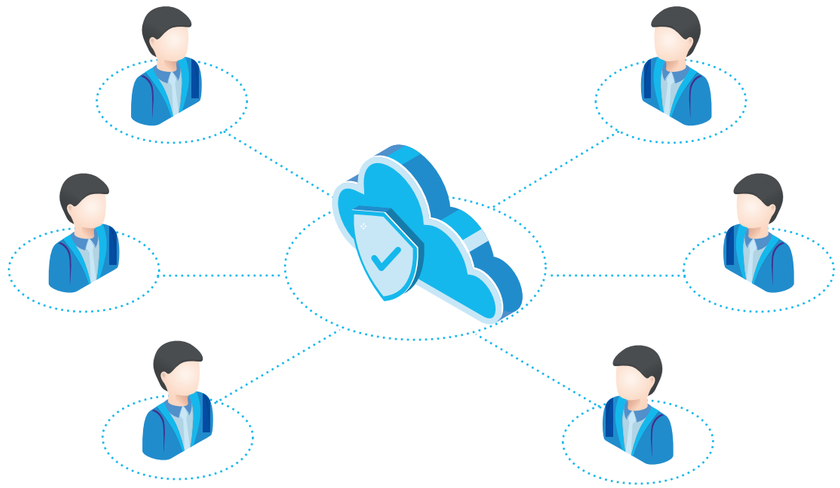
The investment in public cloud infrastructure is measured in trillions of dollars. This includes analytics, threat detection, threat hunting, monitoring and risk mitigation.

Large cloud vendors like Microsoft receive trillions of security signals each day and use artificial intelligence and machine learning to detect anomalies in traffic patterns.

These cloud vendors can afford to hire the brightest minds to protect cloud data and build ever-increasing levels of security to stay ahead of the bad actors and malware.

With the collective intelligence of the security community and the economics of the public cloud, local storage is simply no longer as secure or viable.

- **LIVE DOCUMENT COLLABORATION**
- **NO VPN**
- **AUTOMATIC BACKUP**



Cloud Data

1. Eliminates the need to manage storage infrastructure.
2. Security controls for encryption, file backup and versioning.
3. Live collaboration on all Microsoft Office files without a VPN.

SOLUTION

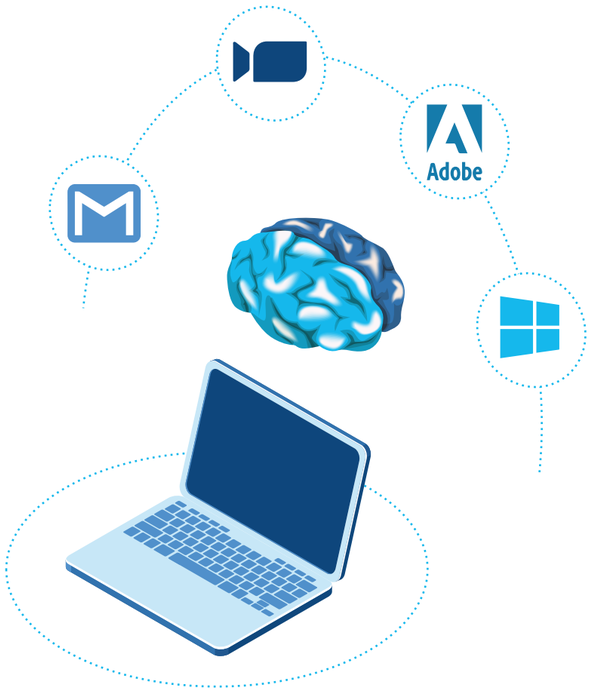
Passwordless Authentication

Sign in with biometrics for faster access and better security

The combination of a username and password was a great innovation at MIT in 1961 and unlocked an explosion in the use of applications and services.

However, passwords have become a major inconvenience for knowledge workers who have an average of 90 different passwords between home and work.[1] Some employees use the same passwords for personal and company accounts, and most will use the same password for multiple accounts.

Phishing attacks – where an employee is tricked into giving away their username and password – are among the most successful attacks against businesses today. Users are notoriously bad at detecting phishing emails, especially on smartphones. Security breaches resulting from phishing are increasing in cost and severity.



LEGACY

[1] Digital Guardian

Passwordless Authentication

Sign in with biometrics for faster access and better security

Windows 10 joins iOS and Android with excellent biometric authentication. Now employees can authenticate into their machines and apps with their face or fingerprint.

Further, Microsoft offers an app called Microsoft Authenticator to provide MFA capabilities more securely than text messaging.

Passwordless authentication is a beautiful experience for employees. Millions of people enjoy Touch ID and Face ID on iOS devices. Passwordless authentication is faster, less prone to error, and employees cannot be tricked into giving away their biometrics.

Passwordless authentication is enabled through the combination of cloud identity (Azure Active Directory), biometrics (Windows Hello), and SSO (Single Sign On) integration to applications.

Almost all modern cloud / SaaS vendors offer some form of SSO capability and many businesses will only select cloud vendors that support SSO. It's also possible to enable some on-premise applications with SSO capability.

Passwordless authentication is far more secure and greatly simplifies the employee's life. Employees love it.

- NO PASSWORD RESET
- BETTER SECURITY
- USERS LOVE IT

Passwordless Authentication

1. Saves time for everyone and improves security for the business.
2. Uses biometrics to authenticate into Windows and Office 365.
3. SSO can be extended to on-premise and cloud applications.

SOLUTION

Zero-Touch Provisioning

Remote Device setup and configuration without IT intervention

For over 20 years IT administrators have manually provisioned new Windows machines with an image and a package of applications and drivers.

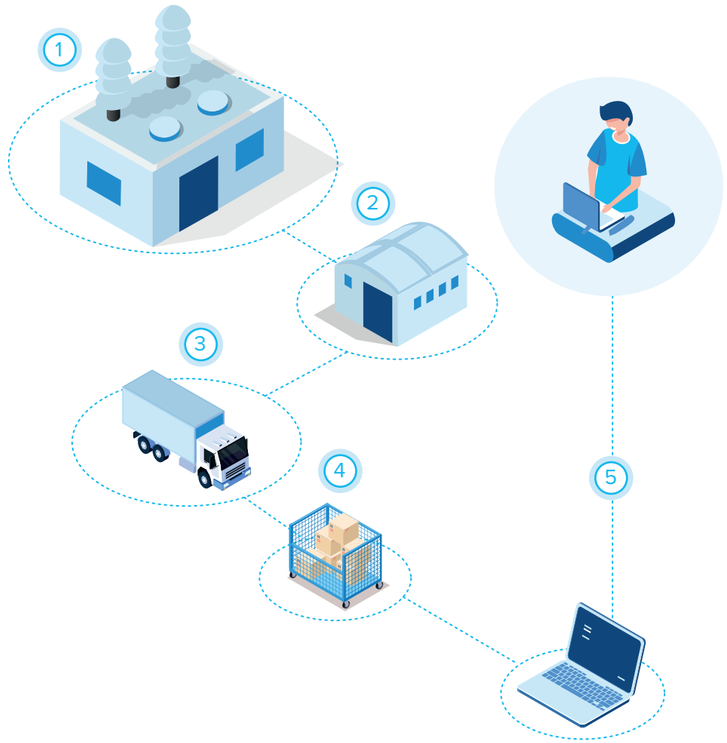
Typically, this takes a couple of hours per machine and requires a significant effort for skilled IT people to maintain at scale. This imposes a delay in the procurement process and in some companies it literally takes weeks to get a new laptop ready.

Apple introduced their device enrollment program (DEP), which enabled companies to order iOS and macOS devices that automatically enroll in a mobile device management system.

This was extremely successfully and saved about 20 minutes per device as each new iPhone was automatically enrolled in mobile device management (MDM).

Samsung followed with Knox Mobile Enrollment which led to Android Zero-Touch as part of Android Enterprise. These programs saved millions of hours per month for corporate device employees.

However, it was Microsoft that had the greatest impact on IT resources by launching Windows Autopilot to automate the set-up and enrollment of a Windows machine in Intune.



2 weeks to get a laptop ready for a new employee

LEGACY

Zero-Touch Provisioning

Remote Device setup and configuration without IT intervention

By combining all the programs above, IT Admins can achieve Zero-Touch Provisioning for Windows, Macs, iPhones, iPads, and Android devices.

Order and ship devices directly to employees anywhere in the world, even directly to their home.

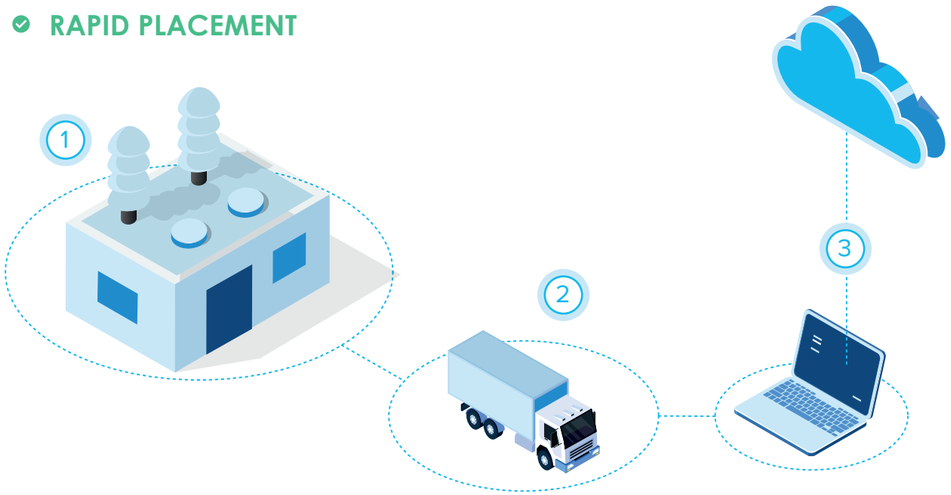
Users log in with their company credentials and the device self-configures with security, applications and content. Under most conditions a device will complete setup in 30 minutes, including encryption.

The IT department is no longer the bottleneck between procurement and employees receiving their device. IT no longer needs to take delivery and work on the device first.

Zero-Touch Provisioning saves precious time for IT and enables new employees to be onboarded faster.

Lost and broken devices can be replaced rapidly from buffer stock or can be shipped overnight with no need for IT to perform device setup.

- TIME SAVING FOR IT
- DIRECT SHIPMENT TO USERS
- RAPID PLACEMENT



Approximately 2 days to get a new laptop

Zero-Touch Provisioning

1. Remote setup and configuration of all your devices.
2. Eliminates images and packages for Windows.
3. Supports rapid device replacement.

SOLUTION

Remote Support

Work from anywhere meets support from anywhere

Most companies have relied on their local IT resources, or a local IT service provider to address hardware and software related issues.

In addition to the great migration to the cloud, device ownership models are changing worldwide. BYO is more prevalent for all device categories and device-as-a-service (DaaS) is a growing industry.

At the same time, the use of printers, faxes, on-premise servers, and local storage is in rapid decline and accelerating as more people work remotely.

Clearly the need for local, onsite IT support is declining in a world where there is less reliance on local hardware and a greater need to support a remote workforce.

LEGACY

Remote Support

Work from anywhere meets support from anywhere

The modern workplace empowers employees to be more self-sufficient with self-service resources for many tasks. Fortunately, remote support tools have matured enormously in recent years with the improvement in mobile apps, portals, and remote diagnostic tools.

However, self-service tools are far from perfect and the gap between these tools and the human experience is where support is needed.

Modern Management aligns support to remote work by increasing support options – email, phone, support app, chat and self-service options.

Modern Management delivers a support team that fully understands the needs of remote workers and is highly responsive to their needs.

This reduces traditional costs of on-site support and empowers a generation of remote workers.

- MORE SUPPORT OPTIONS
- SELF SERVICE
- TIGHTER SLA'S

Remote Support

1. Enables remote workers to support themselves.
2. Allows workers to get support when and where they need it.
3. Aligns support to the needs of remote workers.

SOLUTION

Conclusion

Modern Management brings six disruptive changes to IT operations

Zero-Trust Network enables you to secure your information anywhere, on any device, not just within your domain.

Over-the-Air Updates reduces update infrastructure and ensure devices remain compliant when off network.

Cloud Data gives employees access to documents without a VPN and live collaboration is enabled by default.

Zero-Touch Provisioning enables you to order and ship devices directly to employees without manual imaging.

Passwordless Authentication delights your employees and protects your business from phishing attempts.

Remote Support provides your employees with 24x7 support that is purposefully designed for modern workers.

mobile-mentor.com

USA +1 877 707 3848

NZ +64 9 888 0512

AUS +61 2 9575 4827

Are you ready for Modern Management?