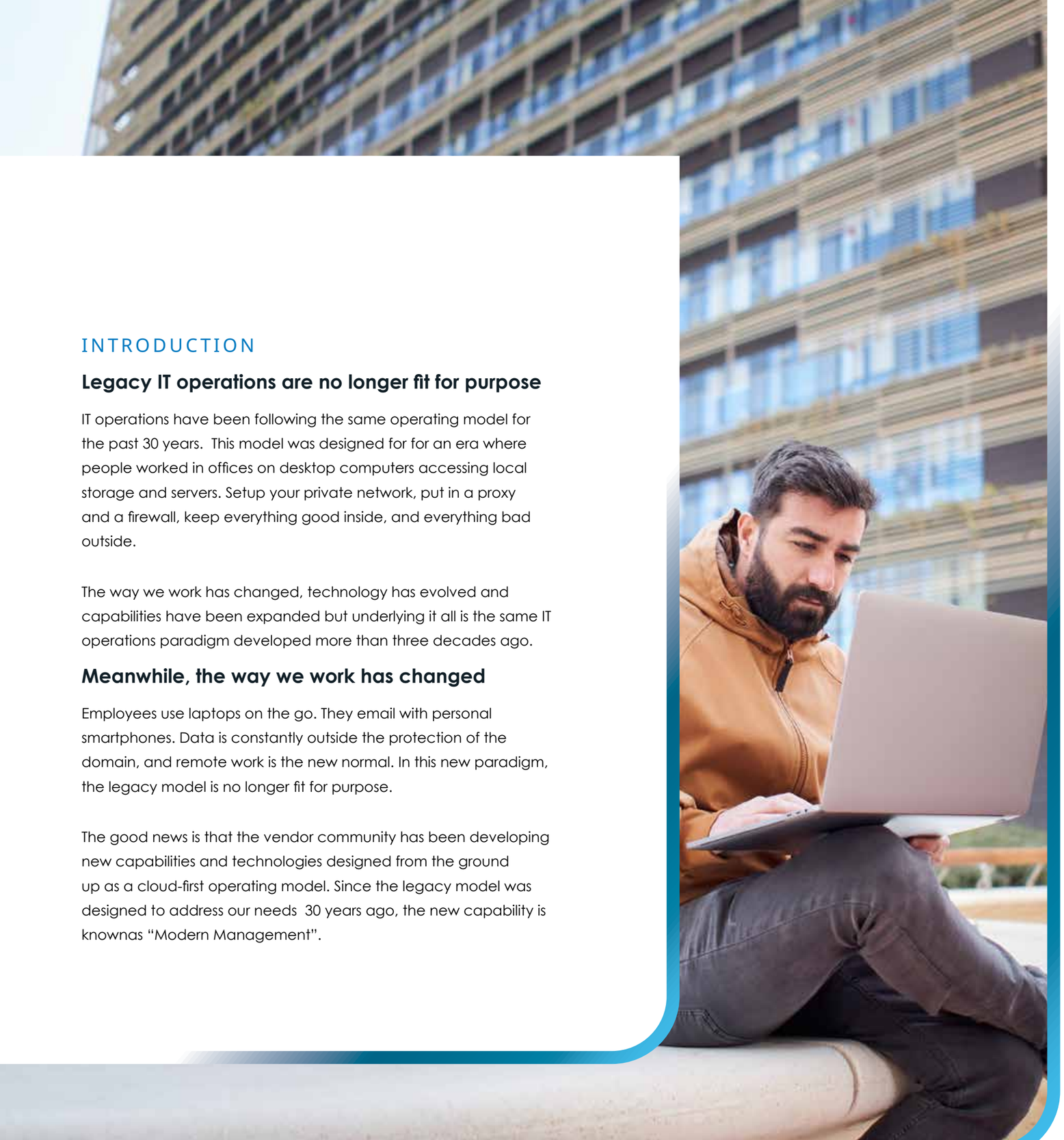
mobile mentor

The Six Pillars of Modern Management

DISRUPTING LEGACY IT OPERATIONS WITH SIX TRANSFORMATIONS



INTRODUCTION

Legacy IT operations are no longer fit for purpose

IT operations have been following the same operating model for the past 30 years. This model was designed for for an era where people worked in offices on desktop computers accessing local storage and servers. Setup your private network, put in a proxy and a firewall, keep everything good inside, and everything bad outside.

The way we work has changed, 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 we work 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. In this new paradigm, the legacy model is no longer fit for purpose.

The good news is that the vendor community has been developing new capabilities and technologies designed from the ground up as a cloud-first operating model. Since the legacy model was designed to address our needs 30 years ago, the new capability is knownas “Modern Management”.

START YOUR MODERN JOURNEY

Content

MODERN MANAGED SERVICES

Achieve More With Less

Modern Management is 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, with the same security applied to all users, regardless of where they work.

It removes the need to manually update operating system updates by leveraging silent over-the-air (OTA) updates. It leverages cloud security and introduces new protections.

Modern management removes the need for double-handling every new devices and now devices can be sent directly to employees and auto-configured upon sign in.

Passwords are replaced with biometrics, Single Sign-On and MFA.

Employee support can happen remotely, from anywhere.

Work is an activity, not a place.

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 and thrive. Employees can work anywhere, anytime, and you can protect and secure your data outside of your network.

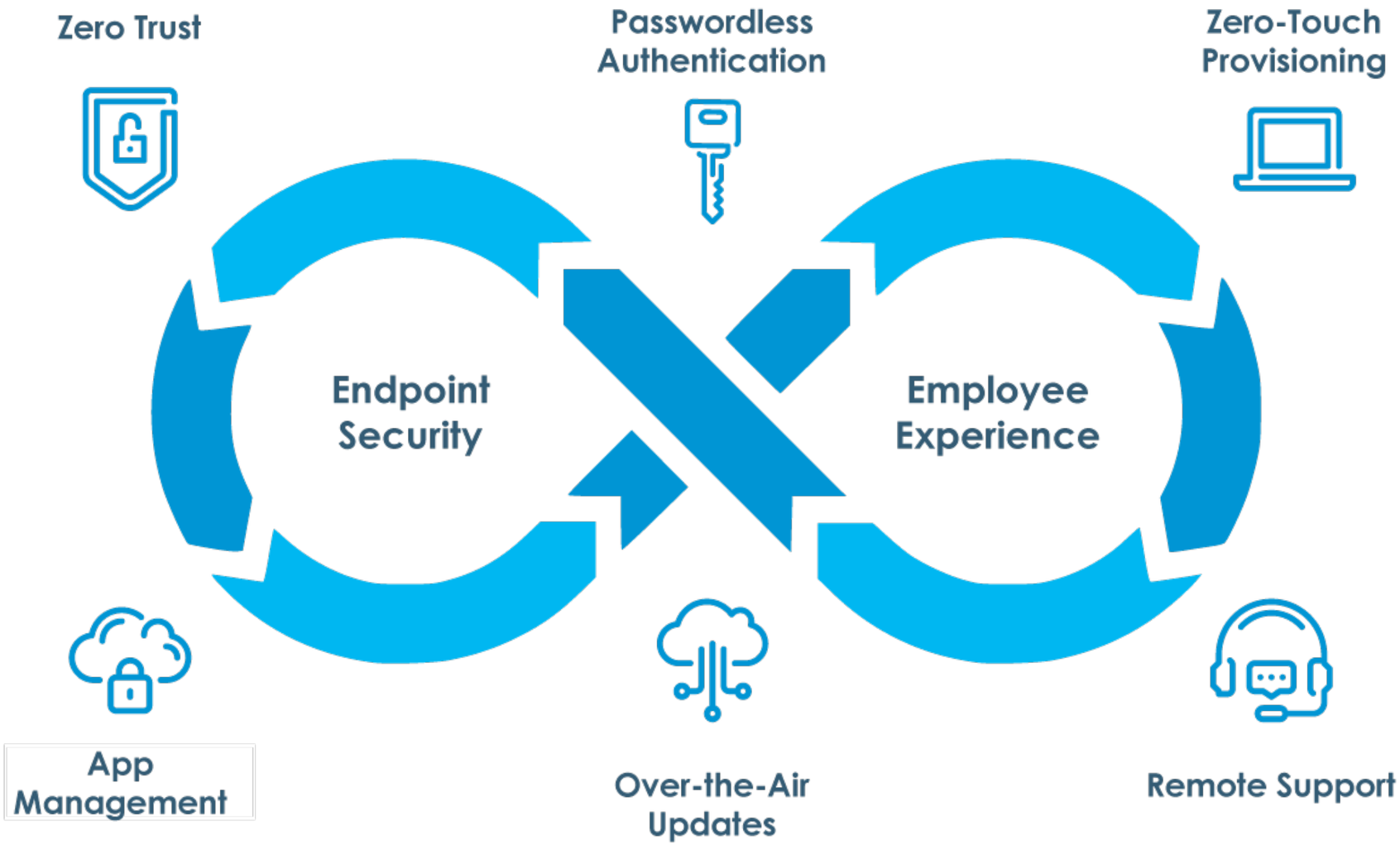
Modern Management isn't just about convenience. It's about business continuity. It's about ensuring your employees can focus on value creation. With Modern Management work becomes an activity, not a place.

Are You Still Asking These Questions?

1. **Why** do we need a VPN to access company resources?
2. **Why** are we still dealing with passwords for devices and apps?
3. **Why** do we manually provision every Windows device?
4. **Why** is it so hard to keep company devices up to date?
5. **Why** can't we patch vulnerable applications faster?
6. **Why** are we still providing local, on-site, IT support resources?

A CLOSER LOOK

The Six Pillars of Modern Managment



LEGACY

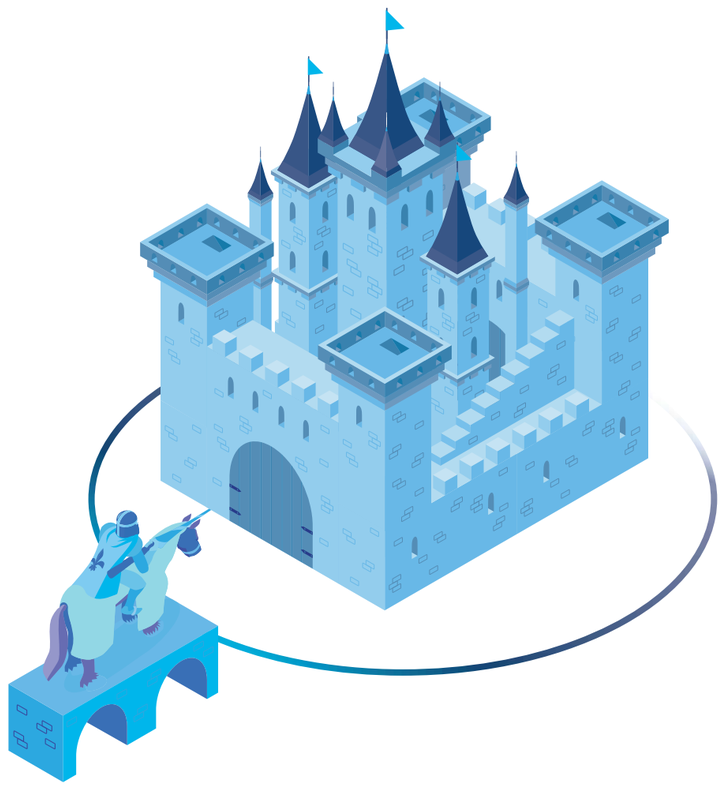
Castle-and-Moat

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 were developed in the last century to support this model.

Once past the firewall or with a VPN connection, the computer accessing the resources is 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 misconfigured, company information can be exposed.



SOLUTION

Zero Trust Architecture

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 dynamically 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 and virtual machines.

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.

LEGACY

Passwords

The combination of a username and password was a great innovation in 1961 and unlocked an explosion in the use of applications and services. However, passwords have become a major liability for knowledge workers who have an average of 90 different passwords between home and work.

We know from the 2022 Endpoint Ecosystem study that only 31% of knowledge workers use a password management tool and 69% save their passwords in a personal journal, in an app on their phones or in a spreadsheet. What could possibly go wrong?

Also, 67% admit they choose passwords that are easy to remember, often using their pet's name and date of birth and many people re-use the same passwords for personal and work 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.

SOLUTION

Passwordless Authentication

Operating System updates without the complex infrastructure

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

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

Further, the Microsoft Authenticatorapp now includes number matching and GPS location to improve MFA and avoid "accidental approvals".

Passwordless authentication is enabled through the combination of cloud identity (Azure Active Directory), biometrics (Windows Hello), Single Sign-On, MFA and Conditional Access policies.

Almost all modern cloud / SaaS vendors offer some form of SSO capability and many businesses will only select cloud apps that SAML compliant. It is also possible to connect some on-premise applications with SSO capability.

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

Passwordless Authentication

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

LEGACY

Manual Provisioning

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.

In 2014 Apple introduced their device enrollment program (DEP), which enabled companies to order iOS and macOS devices that automatically enroll in their mobile device management system.

This was extremely successful 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 automates the set-up and enrollment of a Windows machine in Intune.

SOLUTION

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.

Zero-Touch Provisioning

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

LEGACY

App Management

IT departments have been managing applications for decades. Legacy apps get deployed to machines via Config Manager, scripting, or are placed directly onto the image itself.

Updating applications required extensive testing to ensure continuity – both when the application version changed and when a new operating system came out. Users needing an application contacted IT and a support staff member installed the app – usually after a convoluted approval process that takes time and wastes money.

In the past decade, there's been an explosion of SaaS applications, web applications, and mobile applications, which don't follow the traditional model. The biggest challenge is the rate of change e.g. applications like Google Chrome may be updated on a weekly basis.

Outline the challenges with MSI, EXE etc

Failing to update apps leaves users exposed, but resources are limited and IT often cannot keep all apps current. Further, web apps and mobile apps may expose company data outside the perimeter.

SOLUTION

Modern App Management

Operating System updates without the complex infrastructure

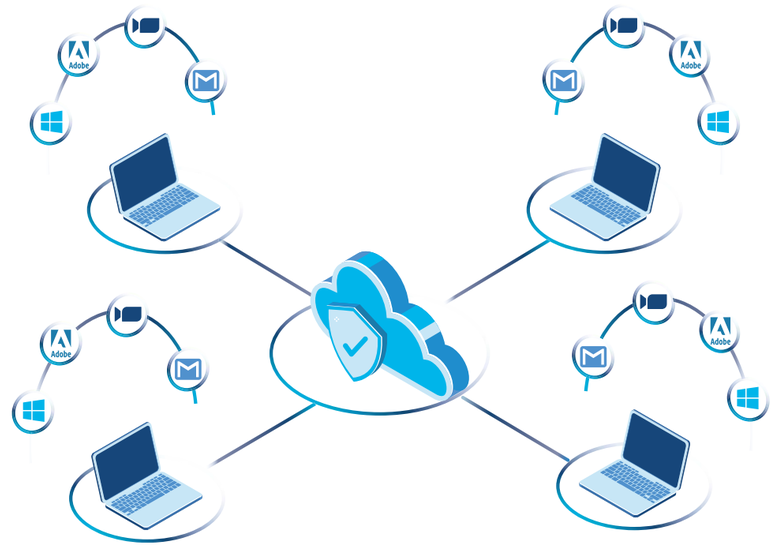
With Modern Management, applications are deployed by Microsoft Intune based on group membership, separating security controls from app deployment.

Third party tools can be used to automate app packing so companies can keep all applications current without the manual effort. We need to talk about MSI, EXE and other app formats….

IT departments can dictate which apps are pushed and which apps are available in the company's app store. Users who want additional apps can self-serve – reducing downtime and workload for IT .

Further, Intune App Protection Policies can be used to protect data within Microsoft Office apps on company and BYO smartphones, reducing the threat landspace.

With modern app management, users are empowered, the company is safer, and data is protected.



Application Management

1. Reduces Zero Day Exposure via policy.
2. Protects company data with work apps on mobiles.
3. Streamlines deployment and reduces helpdesk calls.

LEGACY

Manual Updates

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 CMG and required IT Admins to install and configure servers to perform updates.

Traditional updating requires the device to be domain joined, or rely on a VPN for remote workers.

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.

SOLUTION

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. You can define 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, or using a VPN 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.

Over-the-Air Updates

1. Removes the need for update infrastructure for Windows.
2. Allows updates from anywhere, without a domain or VPN
3. OS updated managed through Windows update rings.

LEGACY

Traditional Support

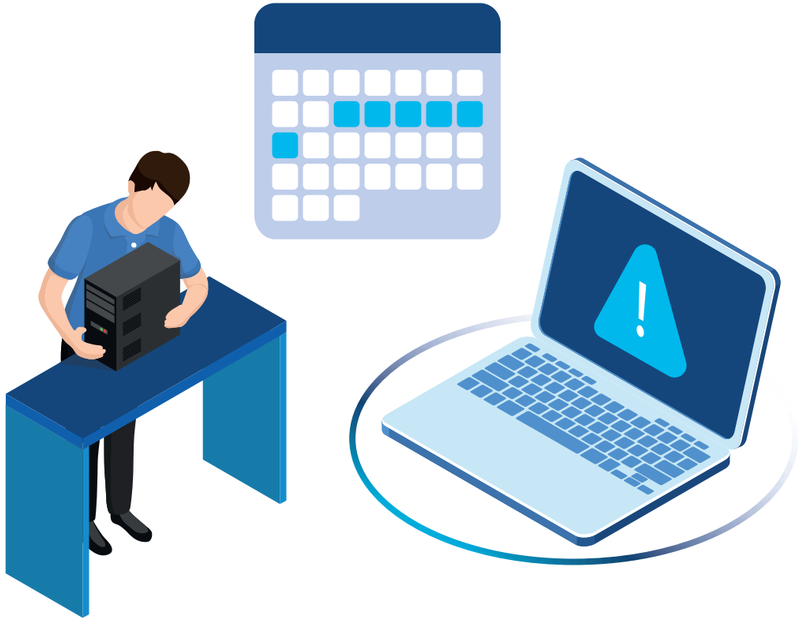
Most companies have relied on their local IT resources or a local IT service provider to address hardware and software related issues.

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 support is declining in a world where there is less reliance on local hardware and a greater need to support a remote workforce.

RESOLUTION IN DAYS



SOLUTION

Remote Support

Work from anywhere meets support from anywhere

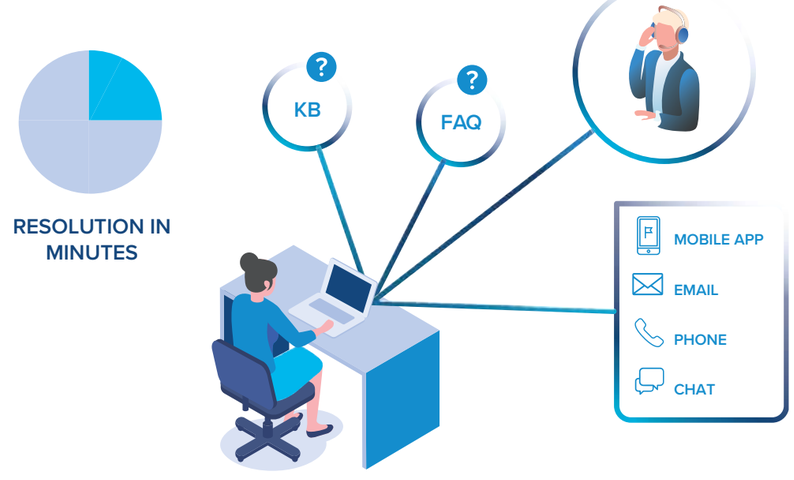
The modern workplace empowers employees to be more self-sufficient with self-service resources for many tasks. Fortunately, remote support tools have matured enormously in recent years with the improvement in mobile apps, portals, and remote diagnostic tools.

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 the traditional cost of onsite support and empowers a generation of remote workers.



Remote Support

1. Enables remote workers to support themselves.
2. Allows workers to get support when and where its needed.
3. Aligns support to the needs of remote workers.

CONCLUSION

Are you ready?

Modern Management brings disruptive change to IT operations capabilities.

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 the traditional cost of onsite support and empowers a generation of remote workers.

mobile mentor

USA +1 877 707 3848

New Zealand +64 9 888 0512

Australia +61 2 9575 4827

mobile-mentor.com