
ivanti
Unified Endpoint Management
for the Everywhere Workplace
ivanti.com

Table of Contents

Introduction

Mobility and IT consumerization have become a way of life in the enterprise. In simpler terms: today's users expect to get their work done from anywhere at any time using a variety of devices, from desktop and laptop PCs to tablets and smart phones. This has become even more relevant in the Everywhere Workplace. At one time, the most "serious" work was done on laptop and desktop PCs with mobile devices used only for email and other limited purposes on the road or at home. Today, users expect to access the same information, run many of the same applications and services, and get much of the same work done on any device, whether it's company-owned or BYOD. Trends in PC development are blurring the lines between what is a PC and what is a mobile device.

This mobile device equality has created a significant challenge to the enterprise, but there's also a clear opportunity. First, the challenge: IT must implement policies to manage and secure sensitive applications and information accessed by and stored on each device without compromising the user's productivity, preferred mobile work style, and personal use of the device. In spite of best intentions and efforts, in many enterprises today, endpoint management and security have not kept up with device equality.

The risk of taking no action? IT organizations open themselves up for threats and data breaches. Without context (employee, their devices and location, zero trust and personalized employee experiences), IT is forced to create a lockdown state to avoid risk that impacts employee productivity.

IT needs a solution that can adjust security policy per employee automatically, proactively monitor the network and alert the IT team immediately.

Managing devices in an age of data breaches

The approach in most enterprises: one management system or set of management systems for desktops and laptops, and an entirely separate management system, vendor and strategy for mobile devices such as smartphones and tablets. In many cases, there are two different IT positions focused on mobile devices and traditional endpoint systems when different management tools are being used.

This approach has serious drawbacks, particularly in the age of increasingly frequent and damaging data breaches. Mobile devices are prone to loss and theft, which exposes them and their enterprise applications and data to compromise. Mobile malware is a rising potential entry point into the corporate network. Aside from loss, theft and malware, there are other serious challenges and implications to deploying two different management systems for different devices.

Common end user experience

Separate management applications and strategies make it difficult to provide the common user experience across devices that users expect. Onboarding, provisioning and supporting multiple devices can become unnecessarily complex and time-consuming. This is where we get into the opportunity.

Secure the Everywhere Workplace with a solution that lets you discover and manage all your employees' devices from cloud to edge; implement secure zero trust access with contextual automation; and deliver personalized experiences for every employee wherever they work. The impact: improved productivity with better operational speed, cost, and quality of service.

Common user policies

Protecting sensitive enterprise information and network access requires crafting a strict set of user access and security policies. As mobile device use becomes more prevalent and sophisticated, IT is challenged to craft and deploy a common set of identity and access policies and policy framework across all endpoint systems used by each employee. Deploying a common set of policies is more complex when using two completely separate management systems. A simpler approach: use a single unified endpoint management (UEM) solution. This also helps mitigate the complexity of having multiple teams involved.

Many companies once had their IT staff in charge of desktop and laptop devices, while smartphones were handled by telecommunications staff. This meant the two teams had different skills, priorities and perspectives.

This type of arrangement included unseen gaps in policy creation and deployment that left the door open to hackers and data breaches. In addition, relying on two different management platforms with seemingly identical policies means they can be deployed differently at times, leading to hidden gaps.

A unified UEM system creates a single set of user access and security policies and deploys them consistently and fluidly across all user devices.

Management costs and resources

Working with two separate management platforms with different vendors, support contracts and interfaces requires more time, training and resources than using a single platform. Not only are onboarding, support costs and resource requirements greater, but any changes to the user's status or access rights requires policy changes in two separate systems, which is resource-intensive and more prone to error than using a single management system.

More time and resources spent on device management also means less time and resources devoted to technology strategies that enhance the business. With the pace of technology change and the increasingly vital role this change plays in business competitiveness, IT departments are better off if they can spend as little time as possible on day-to-day management tasks.

The myth of integration

As enterprise mobility management (EMM) platforms have become more prominent in the enterprise, their vendors have begun touting integration with existing desktop and laptop endpoint management platforms. This is an encouraging trend, but the supposed integration among very different systems doesn't yield the same savings and ease of use as a single UEM system, interface and vendor relationship. The focus of UEM is now about deploying a consistent set of policies and support resources for each user across all their devices, rather than an artificial separation between mobile and traditional systems and devices. Such a system should deliver the following capabilities across all devices:

Endpoint management of all user devices, which includes device discovery and inventory, provisioning of the device (OS deployment / device enrollment), software/mobile app distribution), support and remote control.

Security enforcement that enables stronger operational security with patch management, endpoint security, software distribution, updating and identity and access policy enforcement. In the case of mobile devices, remote lock and wipe after suspected loss or theft are important capabilities.

Asset management that helps track software licenses, contracts, warranties and leasing arrangements.

Provisioning, including user onboarding and offboarding of new devices and device images. User self-provisioning is a capability provided by many MDM solutions and should be offered in a comprehensive endpoint management solution as well.

Ideally, all these application and data security capabilities should be tightly integrated with the same UEM system so that managing user laptops, PCs, mobile devices, applications and information are all achieved with a single screen and a single consistent set of enterprise policies that open the door for a single staff to be able to manage everything.

The Ivanti solution

The Ivanti solution for managing user devices eliminates the artificial separation between traditional desktop and laptop systems and their mobile device counterparts. Ivanti focuses on unified endpoint management, delivering a single enterprise IT management solution and set of policies for managing the entire lifecycle of all the devices run by each enterprise user. With UEM, the user – not the device – is the focus. With this user-centered approach, Ivanti offers the only comprehensive management solution that delivers the same seamless experience users expect across all their devices. Capabilities of Ivanti's industry-leading Endpoint Manager include:

Discovery and inventory.
Ivanti automatically discovers and inventories all managed and unmanaged PCs, laptops, smartphones, tablets and other mobile devices connected to the network, regardless of operating system. With the Ivanti Cloud Services Appliance, IT can even discover and inventory devices in remote locations and manage them across low-bandwidth connections, with no VPN required.

Operating system deployment and distribution.
Ivanti simplifies and automates installation and immigration of Windows and macOS operating systems across all your relevant user systems, retaining user, applications, settings and files in order to restore them to a new or existing machine.

Software distribution.
Ivanti automates software distribution across all devices from Windows to Mac to iOS- and Android-enabled mobile devices. Patented enterprise-distribution technologies can distribute large software packages across thousands of devices in minutes with minimal bandwidth consumption.

Simple, user-based administration.
Allows IT to implement a single user configuration and security policy across all the devices a user carries. With this capability, a single policy deployment can connect and provision a new-employee device in minutes.

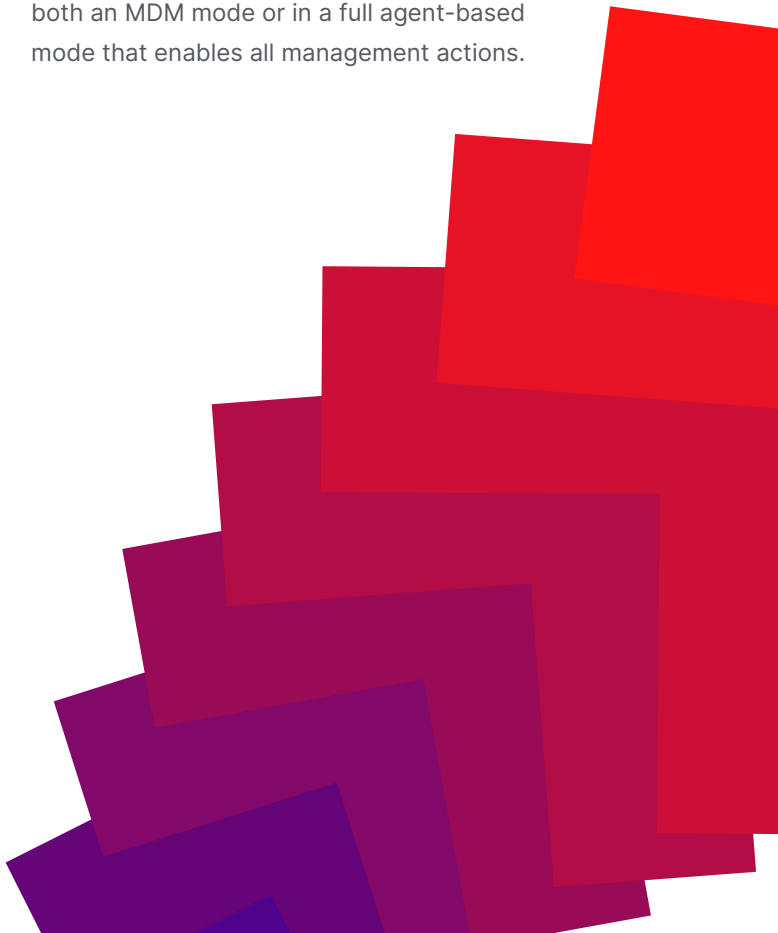
Software license management.
These tools offer automated software license audit and monitoring to help organizations purchase only what they actually need, and provide detailed information to help renegotiate vendor licensing agreements to control costs. Intelligent use of software license management can save enterprises thousands or even hundreds of thousands of dollars.

Systems dashboards and reporting
to gain visibility into how all systems - including PCs, Macs, smart phones and tablets - are operating. Xtraction can provide CIOs, department heads and IT directors with timely visual graphs and charts for business presentations that demonstrate the value of IT and decision-making. It even provides tools for ROI-benefit reports. Ivanti also includes comprehensive threshold monitoring and alert tools so IT can address problems before they affect the business.

Ivanti remote control and problem resolution.
IT can take control of devices to remedy support issues or transfer files among systems when possible.

Power management.
Create and deploy power management policies across the network.

Comprehensive enterprise mobility management.
This includes mobile application management, mobile device management and mobile security management capabilities like remote device locate, lock and wipe. This capability can also manage desktops, laptops and hybrid devices in both an MDM mode or in a full agent-based mode that enables all management actions.



ivanti

Role-based workspaces.
Users can access all the IT services, including the service desk and security updates they depend on and are entitled to across all their devices.

Optional modules integrate tightly with Endpoint Manager to provide asset management; software and hardware lifecycle management; and service management; with processes to maintain user productivity and organizational efficiency.

Ivanti UEM helps support all the devices people use, and improves both user and IT productivity. With the unified Ivanti approach to device and application management, enterprise IT gains a solution that reduces endpoint management costs and resource requirements, fills in gaps in endpoint security, and delivers a seamless user experience.

Time to leverage user-centered IT

There was a time when PCs and laptops lived in different worlds and had different capabilities than their mobile device counterparts. At that time, there was some logic to developing and deploying separate management systems for each. In today's Everywhere Workplace, users depend on all their devices to get their work done. In this environment, having two separate management systems creates an unnecessary burden for both users and IT.

Unified endpoint management from Ivanti eliminates this burden by focusing security and management on the user, delivering not only unified management but a single, unified user experience on any device, anywhere, at any time.

ivanti.com
1 800 982 2130
sales@ivanti.com