Ivanti Unified Endpoint Management

The challenge

The Everywhere Workplace is here. To thrive in this new landscape (not just withstand it), organizations need to securely access and easily manage business data on any endpoint used by their employees, contractors, and frontline workers.

Today's modern digital workplace includes the use of diverse endpoints including Android, iOS, macOS and Windows 10. For some organizations, this scope could also include other immersive and rugged devices like HoloLens, Oculus, Zebra and more.

The needs are clear: manage privacy and compliance while minimizing risk and protecting the user experience. That means separating and protecting corporate apps from the personal apps of users' endpoint devices. It's possible to accomplish all this simply and securely with a unified endpoint management (UEM) solution.

Secure your everywhere workplace with the industry's first end-to-end, zero trust security platform

Ivanti UEM is powered by the first end-to-end, zero trust security platform to securely access and protect data across the Everywhere Workplace.

This platform validates each device to ensure that only authorized users, devices, apps and services can access business resources. This seamless process delivers security while preserving the user experience across any endpoint.

Organizations growing stronger in the Everywhere Workplace are doing so with enterprise mobile security at the core. That's a big shift, but Ivanti UEM makes it easy. And as your needs change, our UEM adapts with you. Build on it with enabling technologies to eliminate passwords (zero sign-on (ZSO)), to ensure user authentication (multi-factor authentication (MFA)) and to detect and mitigate endpoint security threats (mobile threat defense (MTD)).

Comprehensive security

Secure, manage, and monitor any corporate or personally-owned mobile device or desktop that accesses business-critical data. UEM has the visibility and IT controls to make it simple.

Whether you're embracing BYO devices, issuing company-owned devices or both, UEM enables security across a wide range of endpoints while managing the entire lifecycle of the endpoint including:

- Automated onboarding.
- Policy configuration and enforcement.
- Application distribution and management.
- Management and security monitoring.
- Decommissioning and retirement.

UEM is enabled on a proven, secure, scalable, enterprise-ready architecture with flexible deployment options that prioritize user experience while also maintaining the highest quality security standards.

Sentry acts as an email and content in-line gateway that manages, encrypts, and secures traffic between the mobile device and back-end enterprise systems. Tunnel is a multi-OS app VPN solution that allows organizations to authorize specific mobile apps to access corporate resources behind the firewall without requiring any user interaction.

Manage and grow your business confidently and securely with mobile and cloud

Organizational and user control. With UEM, organizations implement individualized mobility and security strategies to meet business needs at their own pace. User data stays private and corporate data stays protected, giving users and administrators alike control over their information.

Freedom of choice. Ivanti UEM is OS- and device-agnostic. Administrators can choose cloud or on-premises deployment based on their budget, and employees can use their favorite endpoints for work.

Experience-driven adoption. Ease of use equals higher adoption. Higher adoption means accelerated productivity and growth. UEM helps IT drive adoption by supporting a native user experience across productivity apps at work. This simplifies compliance while mitigating security threats and shadow IT.

Business resilience. Super secure. Super unobtrusive. Invisible and automated security ensures compliance while allowing your business to forge ahead.

Key use cases

- **Ensure privacy and compliance in organizations tasked with protecting sensitive data.** Secure business data on any endpoint while separating business and personal data.
- **Enable multi-device, multi-OS, multi-app management from a single console.** In a mixed-device environment with diverse operating systems and apps, unified management is top priority.
- **Empower frontline workers.** Support the field, fleet and mobile workers in healthcare, transportation, manufacturing and other industries relying on rugged devices or devices in kiosk mode.
- **Provide superior end user choice and seamless user experience.** To ensure productivity and user compliance, device choice and user experience are essential. Ivanti UEM provides streamlined onboarding and a superior on-device experience.

Security standards and certifications

- Common Criteria Certification
- CSA STAR
- CSfC
- DISA STIG
- EU-US Privacy Shield
- FedRAMP Authority to Operate
- FIPS 140-2 Affirmation
- SOC 2 Type II
- CCN (Spain)

Ivanti unified endpoint management

Device management and security	**Secure UEM**	**Secure UEM Premium**
Security and management. Secure and manage endpoints running iOS, macOS, iPadOS, Android and Windows 10 operating systems. Available on-premises and as a cloud service.	✓	✓
Mobile application management (MAM). Secure business apps with AppStation on contractor and employee devices without requiring device management.	✓	✓
Easy onboarding. Leverage services such as Apple Business Manager (ABM), Google Enrollment and Windows AutoPilot to provide users with automated device enrollment.	✓	✓
Secure email gateway. Sentry is an in-line gateway that manages, encrypts, and secures traffic between the mobile endpoint and back-end enterprise systems.	✓	✓
App distribution and configuration. Apps@Work is an enterprise app storefront that combined with Apple Volume Purchase Program (VPP), facilitates the secure distribution of mobile apps. In addition, capabilities such as iOS Managed Apps and Android Enterprise allow for easy configuration of app-level settings and security policies.	✓	✓
Secure connectivity	**Secure UEM**	**Secure UEM Premium**
Per-app VPN. Tunnel is a multi-OS VPN solution that allows organizations to authorize specific mobile apps to access corporate resources behind the firewall without requiring any user interaction.		✓
Conditional access	**Secure UEM**	**Secure UEM Premium**
Trust Engine. Combine various signals such as user, device, app, network, geographic region and more to provide adaptive access control.		✓
Passwordless user authentication. Passwordless multi-factor authentication uses device-as-identity for a single cloud or on-premises application.		✓

Ivanti unified endpoint management (continued)

Scale IT operations	Secure UEM	Secure UEM Premium
Helpdesk tools. Help@Work lets IT remotely view and control a user's screen, with the user's permission, to help troubleshoot and solve issues efficiently.	✓	✓
Reporting. Gain in-depth visibility and control across all managed devices via custom reports and automated remediation actions.	✓	✓
Secure productivity	**Secure UEM**	**Secure UEM Premium**
Secure email and personal information management (PIM) app. Email+ is a cross-platform, secure PIM application for iOS and Android. Security controls include government-grade encryption, certificate-based authentication, S/MIME, application-level encryption and passcode enforcement.		✓
Secure web browsing. Web@Work enables secure web browsing by protecting both data-in-motion and data-at-rest. Custom bookmarks and secure tunneling ensure that users have quick and safe access to business information.		✓
Secure content collaboration. Docs@Work allows users to access, create, edit, markup and share content securely from repositories such as SharePoint, Box, Google Drive and more.		✓
Mobile app containerization. Deploy the AppConnect SDK or app wrapper to provide an additional layer of security for your in-house mobile apps, or choose from our ecosystem of AppConnect integrated apps.		✓
Derived Credentials. Support two-factor authentication using common access cards (CAC) and personal identity verification (PIV).		✓

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company’s industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 78 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information,visit ivanti.com

ivanti

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