Ivanti Unified Endpoint Management Product Portfolio

Ivanti provides the platform to manage and secure the Everywhere Workplace. Using the Ivanti platform, Everywhere Workplace can enable employees to work from anywhere, while ensuring that corporate data is secure on any device, application, or network. In addition, advanced capabilities such as passwordless multi-factor authentication (MFA) and mobile threat defense (MTD) and phishing protection ensure that organizations are continuously protected against identity theft and targeted mobile attacks.

Ivanti products are available in the following packages, designed to help you on your journey to becoming an Everywhere Workplace.

Ivanti Unified Endpoint Management (UEM)

The product for modern device security and management. UEM is available in the following bundles:

1. **Secure UEM** – Streamline security and management capabilities for iOS, macOS, Android, and Windows based devices.

   Capabilities:
   - Separate personal and business data to maintain user privacy and security.
   - End-to-end device lifecycle management.
   - Over-the-air provisioning of BYO and corporate-owned iOS, macOS, Android, and Windows based devices.
   - Remote app deployment and configuration.
   - Helpdesk tools to make remote support more efficient.
2. **Secure UEM Premium** – Extend security and device management capabilities with secure productivity suite, secure connectivity, and advanced conditional access capabilities for cloud apps and on-premises services.

   Capabilities:
   - Secure connectivity with scalable multi-OS VPN solution.
   - Prevent unauthorized users, devices, and applications from connecting to business services.
   - Secure email, browsing, and content management apps to enable remote productivity.

Ivanti incapptic Connect

Reduce app development costs and accelerate deployments with a simpler and more efficient workflows for secure app development, publishing, and updates.

Capabilities:

- Simplify the app development and distribution process with automatic validation, distribution, and updates via a self-service portal.
- Minimize app errors and defects that can add costly cycles to the development process.
- Eliminate unnecessary development delays so business innovation can keep moving forward.

Ivanti Zero Sign-on (ZSO)

For organizations who want to eliminate passwords to reduce the risk of data breaches.

Capabilities:

- Passwordless MFA for both cloud and on-premises applications.
- MFA application with support for push notifications, one time PIN, and QRcode scans.
- Integration with UEM for conditional access.

Ivanti Threat Defense (MTD)

We've embedded mobile threat detection and remediation capabilities into our UEM apps to make deployment, detection, and remediation easier and more effective. MTD is available in two bundles.

- MTD – Protect and remediate against known and zero-day threats and phishing attacks on mobile devices, while also leveraging basic app analytics.

Capabilities:

- Threat detection and automated on-device remediation for Android and iOS devices.
- Protect against phishing attacks, device vulnerabilities, malicious apps, and network exploits such as man-in-the-middle attacks.
- Gain visibility into risky app usage and leverage basic app policies to whitelist or blacklist apps.

Ivanti Unified Endpoint Management

Device management and security	Secure UEM	Secure UEM Premium
Security and management – Secure and manage endpoints running Apple's iOS, macOS, iPadOS, Google's Android, and Microsoft's Windows operating systems. Available on-premises and as a cloud service.	✓	✓
Mobile application management (MAM) – Secure business apps with Ivanti AppStation on contractor and employee devices without requiring device management.	✓	✓
Easy on-boarding – Leverage services such as Apple Business Manager (ABM), Google Zero-Touch Enrollment and Windows AutoPilot to provide users with automated device enrollment.	✓	✓
Secure email gateway – Ivanti Sentry, 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, an enterprise app storefront, 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.	✓	✓
Scale IT operations	**Secure UEM**	**Secure UEM Premium**
Helpdesk tools – Help@Work lets IT remotely view and control a users' 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 connectivity	**Secure UEM**	**Secure UEM Premium**
HPer app VPN – Ivanti 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.		✓

Ivanti Unified Endpoint Management (continued)

Secure productivity	Secure UEM	Secure UEM Premium
Secure email and personal information management (PIM) app –Ivanti 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.		✓
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.		✓
Partner Device Compliance – send device information – including compliance – to Microsoft Endpoint Manager for Azure AD Conditional Access		✓
Passwordless user authentication for one service – Passwordless multi-factor authentication using device-as-identity for a single cloud or on-premises application.		✓

Ivanti incapptic Connect

Publish your custom apps in record time	Secure UEM Premium
Self-service portal for custom app deployment – Automate signing, resigning, provisioning profile updates, and deployment of new Android and iOS app features with just a click.	✓
App store compatibility – Compatible with Ivanti UEM, VMware Workspace ONE, Microsoft Intune, Apple App Store and Google Play Store.	✓
IP and asset protection – Roles based separation of access, secured data in motion & data at rest, incl. protection of your credentials, distribution certificates, and provisioning profiles.	✓

Ivanti Mobile Threat Defense (MTD)

Product Portfolio	MTD	MTD Premium
Threat detection – Protect against known and zero-day threats and active attacks with sophisticated machine learning and behavior-based detection on the mobile endpoint.	✓	✓
Threat remediation – Limit time of exposure for possible exploitation and stop zero-day attacks with policy-based compliance actions that provide alerts of risky behaviors, proactively shuts down attacks on the endpoint with or without network connectivity.	✓	✓
Advanced app analytics - Continually evaluate mobile apps risks to identify privacy and security risks.		✓

NOTE: *This is an add-on and requires Secure UEM or Secure UEM Premium SKUs*

Ivanti Zero Sign-on

Adaptive security and conditional access for any cloud service or in-house apps	ZSO
Passwordless user authentication – Passwordless multi-factor authentication using device-as-identity to protect against credential theft. Supports authentication from iOS, Android, macOS, and Windows based devices.	✓
Stroger authentication factors – Replace passwords with stronger authentication factors including biometrics, authenticator apps, push notifications, one-time PINs (OTP), and QRcodes.	✓
Conditional access – Integration with Secure UEM Premium allows for conditional access based on signals such as user, device, app, network, and location.	✓
Intuitive user experience – Customizable access and remediation workflows to enable users to self-remediate without requiring assistance from the IT helpdesk.	✓

NOTE: *This is an add-on and requires Secure UEM Premium SKUs*

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