DATASHEET

Ivanti UEM for iOS and iPadOS devices

The demand for iOS-based devices such as iPhones and iPads among enterprise users has exploded. Employees want to use their iOS devices for accessing both corporate resources as well as personal data and are putting more pressure on IT to support them. By combining the Ivanti mobile-centric security platform with Apple's expanding ecosystem of endpoints and apps, IT admins can now securely deliver the full value of iOS mobility to end users. Ivanti provides a seamless and native enduser experience during device enrollment, and the unified console enables organizations to reduce the complexity and costs of managing a fleet of iOS devices.

The largest companies in the world trust Ivanti as their endpoint management solution. Available as a highly scalable cloud or onpremises solution, Ivanti Unified Endpoint Management (UEM) was purpose-built to secure and manage corporate apps and data across any device. Ivanti was the pioneer of iOS in the enterprise, delivering the platform's first private app storefront, BYOD privacy controls, and certificate-based identity management.

Comprehensive App Management

Ivanti UEM was designed for IOS app management and distribution that includes in-house apps, App Store apps, and web apps: By using a single console for app and OS distribution and updates, UEM improves user productivity.

- Secure, identity-based delivery of in-house and App Store apps through the Apps@Work private enterprise
- Improve productivity by using secure user apps such as Ivanti Email+ for containerized corporate email, calendar, contacts; Docs@ Work for secure document storage; Web@Work for secure browsing into your intranet.
- Enable DLP through selective wipe of business apps and apps data on the IOS and iPadOS devices
- Blacklist/whitelist of apps to protect against inappropriate access
- Containerization and dynamic policy to protect data-at-rest and enable compelling app-based user experiences through AppConnect

Challenge

- Enable iOS app distribution and management
- Support BYOD initiatives
- Protect corporate data and user privacy
- Preserve native iOS experience
- Unified console for management of IOS and iPadOS fleet deployments

Solution

- Ivanti Neurons for UEM

Benefits

- Complete app management – secure delivery, data containerization, tunneling
- App download without network latency
- Data loss prevention (DLP) for iOS email
- Privacy protection and data separation
- Identity-based security through certificates
- Multi-user configuration for shared devices
- Secure productivity apps on the go
- Enterprise integration thru extensible APIs
- Scales to fit your device growth needs
- Multi-tier management for delegation
- Flexible deployment options: cloud and on-premises

Enhanced Security

Mobile IT is responsible for the protection of corporate data. Ivanti provides security across the data lifecycle while preserving end-user privacy:

- Separate business and personal data using AppConnect to maintain compliance with corporate and regulatory requirements
- The ability to prevent flow of sensitive enterprise data from managed to unmanaged apps and services via Shortcuts
- Automatic provisioning and enforcement of security and configuration settings for Exchange, FaceTime, iCloud, iMessage, SCEP, screen capture, Siri, VPN, Wi-Fi, Office365, Outlook, Slack and SFDC
- Set password policies and deploy certificates to secure the device
- Seamlessly activate eSIM (virtual SIM) through a provider using automated device enrollment
- Protect data at rest by encrypting business data using FIPS 140-2 cryptographic modules
- Enable granular app-level access control using a secure access gateway
- Protect data in motion using a per-app VPN that provides a secure tunnel to backend resources
- Set up automated policy violation responses to free IT from daily administrative tasks.
- Supports tiered compliance - providing IT capability to launch responses automatically over a period of time
- Combine various signals such as user, device, app, network, geographic region, and more to provide conditional access to devices to various on-prem sources and SaaS applications

Ivanti establishes the data loss prevention (DLP), privacy, and access control protections Mobile IT needs to be able to adopt iOS and IPadOS across the organization.

Key Use Cases

- Ensure privacy and compliance in organizations primarily concerned about protecting sensitive data: Secure business data on any endpoint and separate business and personal data on various endpoints including Apple devices
- Enable multi-device, multi-OS, multi-app management from a single console: The organization has a mixed device environment with iPhones, iPads, Macs, Android based devices, Win 10 laptops and PCs, Zebra, Oculus, etc. Unified management of these devices with different OSs and apps is top priority.
- Empower Apple frontline workers Support the field and mobile workers in Healthcare, Transportation, Manufacturing, and other industries who use Rugged Devices or devices in Kiosk mode.
- Provide a superior end user choice and delightful user experience: When user choice and end user experience matters, Ivanti UEM provides the simplest Apple onboarding and superior on device experience which improves user productivity
- Industry security certifications for UEM: Gain industrystandard security certifications such as FIPS 140-2 Validated Container, Common Criteria MDM PP V3.0, DISA STIG, FedRAMP, and National Cryptologic Center – Assurance High
- Provide security automation for device compliance: Automated compliance: deletes all business data on compromised device without any manual IT actions
- Multi-app, multi-cloud, support: Connect securely to hybrid resources. Connect to SaaS based solutions with Ivanti Access and connect to on-premises resources with Ivanti Tunnel.
- Flexible deployment models (On-premises/Cloud) basedon your needs.

Complete Endpoint Lifecycle Management

Ivanti UEM provides complete device lifecycle management from onboarding and provisioning to retirement.

- Provides a unified console to onboard and manage your iPhone, iPad, macOS, Apple TV and Apple Watch endpoints
- Supports provisioning of corporate-owned, BYOD, kiosk or single App mode, and shared device use cases across your organization
- Supports a new way to roll-out BYO using Managed Apple IDs for maximum user privacy - called User Enrollment
- Leverages Apple Business Manager (ABM) and Apple School Manager (ASM) for out-of-the-box configurations
- Wipe corporate data off a device at the end of the device lifecycle, employee termination, or loss of equipment. Ivanti tightly integrates iOS into Microsoft environments with Office 365, Azure Active Directory, SharePoint, Exchange, Certificate Authority and SCCM.

Customer Perspective

"From day one, Ivanti has helped us with clinical care decision making. This includes decision making that saves lives. Now that we've deployed 3,000 iPads and established a way to secure and manage them through Ivanti, the sky's the limit for our mobile strategy," says Walker. "There's almost no limit to the ways we can deliver apps that boost clinician effectiveness and enable better patient outcomes. This is exactly what we hoped our mobile initiative would be."

- Mark Walker,

Head of IT, Oxford Health NHS Foundation Trust

"The iPad secured by Ivanti is an excellent tool for ad hoc meetings because we can access secure business files immediately, in any location. This allows us to have productive, in-person meetings with customers or colleagues anywhere. It's especially important while traveling because it supports all of our daily business needs."

- René Degros,

European Sales Director at Canon Medical Systems Europe.

Continued on next page...

About Ivanti

Ivanti is the mobile-centric security platform for the Everywhere Enterprise, enabling a secure workforce through a zero trust approach. Ivanti's platform combines award-winning UEM capabilities with passwordless MFA (zero sign-on) and mobile threat defense (MTD) to validate the device, establish user context, verify the network, and detect and remediate threats to ensure that only authorized users, devices, apps, and services can access business resources in a "work from everywhere" world.

Ivanti establishes the data loss prevention (DLP), privacy, and access control protections Mobile IT needs to be able to adopt iOS and IPadOS across the organization.

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