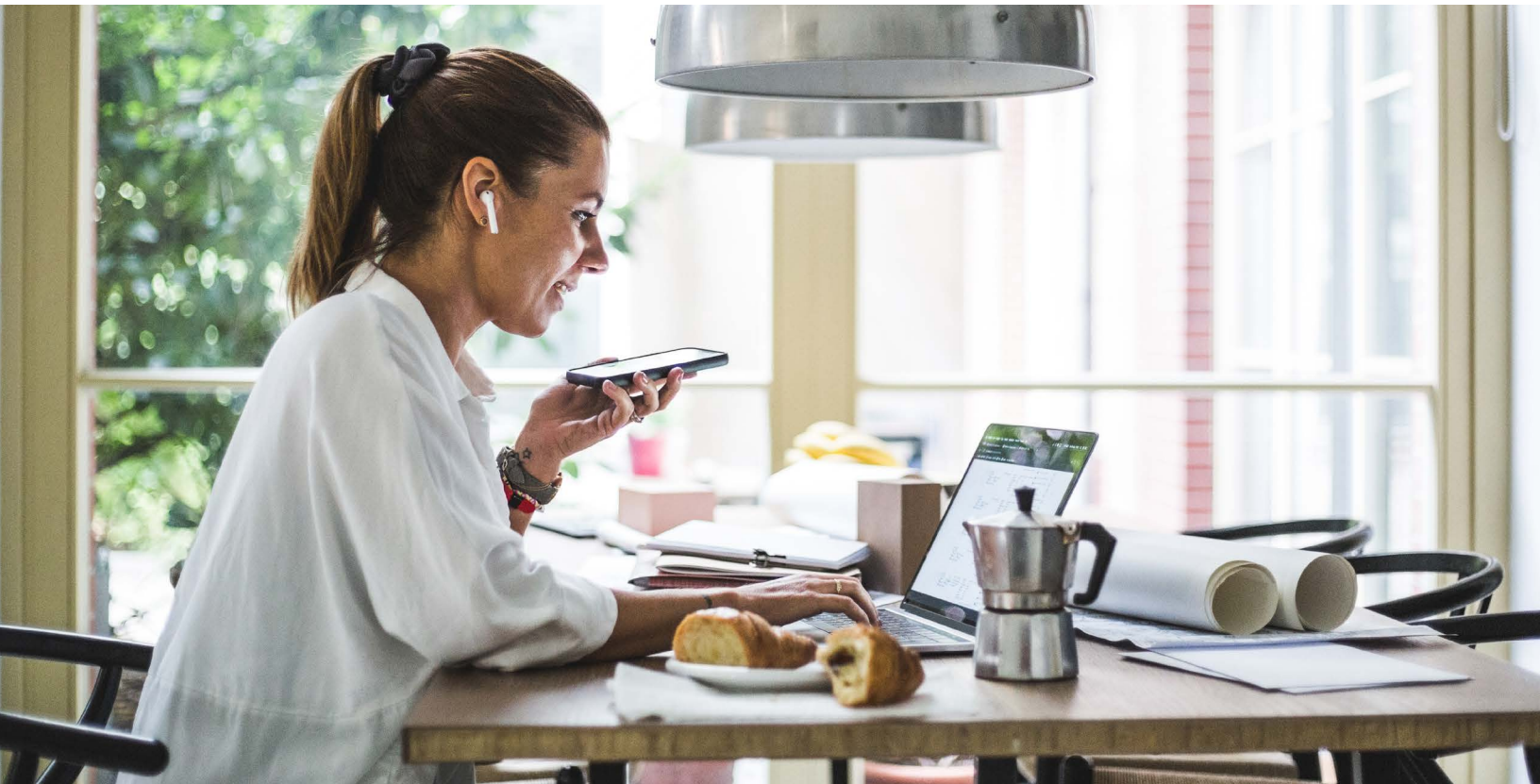
Data Sheet

Citrix Endpoint Management: Leveraging modern style management for all endpoints

Citrix Endpoint Management is a comprehensive solution which unifies client management and enterprise mobility management. Users have single-click access to all of their apps with the Citrix Workspace app, while IT can easily configure, secure and manage any device including desktops, laptops, smartphones, tablets and IoT devices. With Endpoint Management technology, IT gets a modern management style platform capable of managing endpoints providing users with better user productivity, security and business agility, for the freedom to experience work and life their way.



Features of Citrix Endpoint Management

Configure, secure, provision and support endpoints with Unified Endpoint Management	
Endpoint management	Manage and configure corporate and bring-your-own (BYO) devices throughout their lifecycle Support every major platform including iOS, Android, Windows 10, MacOS, Android for Work, Samsung Knox, Chrome, along with IoT devices: Workspace Hub and Alexa for Business
Workspace Environment Management	Manage configurations for commonly used GPOs and lock down Windows 7, 8.1, and 10 devices. WEM optimizes physical desktops for optimized performance. Resource optimization to get more out of their hardware and an improved experience
Real-time Active Directory integration	Integrate with LDAP in real-time to perform user authentication and to manage group policies Apply policy changes immediately based on LDAP changes
Policy configuration	Manage a comprehensive array of policies: passcodes, device ownership, apps and device resources, platform-specific policies, encryption, device status and location
Security and compliance	Ensure end-to-end security and compliance across device platforms, including rooting and jailbreak detection, pre-enrollment device checks, geo-fencing and tracking, context-aware policies, app blacklist/ whitelist and full or selective wipe of devices Initiate automated compliance actions when devices deviate from policy
Scalability and high availability	Ensure scalability through industry-standard HA with active clustering at all tiers
Ease of administration	Centralize administration through a console with customizable dashboard and role-based access and views Configure notifications, receive alerts and easily deploy mobile policies by mixing and matching parameters across groups and users
Provisioning and self-service enrollment	Provide rapid over-the-air provisioning and self-service enrollment with one-time passcodes and server auto-discovery Deploy apps through an enterprise app store as well as app push and removal
Enterprise integration	Seamlessly plug in to existing IT infrastructure including LDAP, Microsoft Exchange, PKI, NAC, VPN, WiFi and SIEM
Monitoring and support	Enable remote support and troubleshooting including VOIP and chat Create reports including unmanaged or rogue devices, compliance reporting, app and device inventory, blocked status and system alerts

App management with largest ecosystem of apps built for business including Multi-MAM support	
Device decommissioning	Automatically decommission devices if they are lost or based on user status in Active Directory Perform selective or full wipe of devices based on status
Self-service web portal	Allow mobile users to locate, lock or wipe lost/stolen devices without waiting for Help Desk support.
Mobile Application Management	Deliver any mobile app to devices with a native user experience
App security	Use mobile app container technology to separate mobile enterprise apps and data from personal apps 50+ MAM policies that do not require device enrollment Secure business apps and data with encryption and mobile DLP technologies
Control app interactions	Enable seamless communication between mobile productivity apps Enforce policies around activities such as cut-and-paste between apps
Multi MAM support	MAM flexibility so that you can apply the level of control your security policies require including 3rd party app store apps and Intune for O365 apps, as well as support for Samsung KNOX, SAFE and Android containers
App policies	Implement granular policy-based management and access controls over HTML5 and native mobile apps
MDX SDK	Enable any mobile app with MDX SDK Wrap any mobile or SaaS app to be imported into Endpoint Management with no additional development needed

Secure email and browser apps	
Secure Mail	Provide containerized, native mobile email, calendar and contacts app for iOS and Android devices that leverages unique security features including multiple layers of encryption and micro-VPN technology for application data isolation
Conference services integration	Enable users to automatically launch and join conference services such as GoToMeeting, Skype for Business, Webex and Lync directly from their Secure Mail calendars with Fast Dial and Fast Join
Business-class workflows for email attachments with Secure Mail	Easily access, sort and save email attachments with the Secure Mail attachment repository. Allow attachments from device photo gallery with simple to use “Attach Last Photo” option.
Advanced email capabilities	Support HTML emails, Office 365, Lotus Notes, Out-Of-Office (OOO) notifications, S/MIME encryption, and Free/Busy calendar integration
Information Rights Management (IRM) support	Enable Secure Mail to support exchange Information Rights Management (IRM) capabilities, which allows a sender to prevent recipients from forwarding, modifying, printing, faxing, saving, or cutting and pasting the message content
Secure Web	Provide a full-featured secure mobile browser that leverages MDX Technologies for additional security, including a micro-VPN for intranet sites and encryption for the browser cache, bookmarks, cookies and history Allow for security functionality including URL blacklisting, whitelisting, and bookmark/homepage push

Unified corporate app store	
Citrix Content Collaboration[1]	Provide full view, edit, and share capabilities to all Content Collaboration data, including file systems, network drives and SharePoint
Email attachment encryption	Encrypt email attachments in the native mobile email app of iOS devices
Enterprise app store	Enable users to self-select their apps from an administrator-provided list of approved applications
Deliver mobile apps	Deliver mobile apps from a unified app store to all devices
Deliver web/SaaS apps	Deliver web and SaaS apps from a unified app store to all devices
Deliver Windows apps[2]	Deliver Windows apps and virtualized apps from a unified app store to all devices

Multi-factor single sign-on	
Strong authentication	Provide strong authentication, including RSA tokens, certificates and smartcards, into the corporate workspace
Touch ID	Support for Touch ID offline authentication
Single sign-on to apps and data	Provide one-click access to users' applications and data with no additional passwords
PIN-based authentication	Set PIN-based authorization for Secure Hub for access to all apps and data
Kerberos authentication support	Enable Kerberos, client certificate authentication

End notes
1. Available for Workspace and Content Collaboration customers
2. Available for Workspace and Desktop and App Virtualization customers

citrix

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States