ZONES™
Connecting Business & Technology

Embrace mobility to advance your enterprise

Enterprises have seen a dramatic increase in the use of mobile devices within their organizations in the last few years. New technologies and applications are helping to lower costs and provide an improved user experience. Employees are using mobile devices to access databases, process transactions and expedite requests.

Zones provides a suite of viable solutions that embrace mobility while meeting strict industry regulations. Mobile device management (MDM) enables enterprises to track mobile assets, secure access to sensitive data, distribute applications and content, and ensure devices are compliant with an organization's policies and industry standards.

Mobile Device Management (MDM)

Privacy and protecting sensitive data are the main concerns when exploring mobility initiatives. This requires an advanced solution that provides: strong user authentication using AD/LDAP, certificate-based access to email, Wi-Fi and VPN networks, and secure distribution of applications and documents.

Policy Enforcement

Often in the workplace, workers are using the same device, or alternate on a shared device, when performing tasks. This situation frequently occurs in enterprises adopting a CYOD (Choose Your Own Device) program. An MDM solution should ensure that data on those devices is protected from user to user with check in/check out capabilities. Before accessing the data on the device, each user must be authenticated before viewing configured data, apps and content set for them specifically by an MDM administrator.

Architecture

Architecture options enable IT administrators to manage all devices across the enterprise – staff, departments, federations and road warriors – from a single console. The entire device fleet can then be managed at a global level while empowering different groups or divisions to maintain visibility and control of devices.

Non-Corporate Devices

In many enterprises, employees are using their personal devices to access information – BYOD (Bring Your Own Device). These MDM solutions must have strong security capabilities that extend to all devices, so you can rest assured sensitive data is protected, whether on a corporate or employee-owned device. And when an employee leaves the corporation, the ability to remotely wipe all corporate information and intellectual property from the device is essential.

MOBILITY TRENDS:

Bring Your Own Device (BYOD)

- Any device owned by the user, used anywhere
- Users purchase, own and maintain the device
- Challenges: security, policy and integration, support expense

Choose Your Own Device (CYOD)

- Pre-approved device, owned by the company, used anywhere
- Company purchases, owns and maintains the device
- Challenges: security, scalability

Whether you choose BYOD, CYOD or a combination of both, Zones helps you confidently embrace mobility while maintaining IT policy control and purchasing standards. You can lock down options with preconfigured mobile bundles or give mobile device users the flexibility to choose from a select group of devices. A custom ZonesConnect eprocurement site enhances automation and control by enabling users to choose their mobile devices, routes purchases through your current approval process, and provides visibility through web reporting.

Applications

Applications and content are rapidly changing the IT landscape. Enterprises need a way to securely deploy these applications and more to an entire fleet of mobile devices. The MDM solution needs to be enabled to provide a dedicated application catalog as well as tools to help develop custom business applications, standardize user authentication, enforce security policies and manage application updates. Some MDM solutions have even developed applications that provide secure access to corporate documents and shared drives from a mobile device.

Zones solution architects help you put an MDM solution in place that enforces policies and procedures but enable innovation and growth. We'll ensure you have the technology in place to maintain a secure IT environment with control and visibility of the information being accessed on mobile devices.

Key Considerations

- **Architecture**
- **Device Control Levels**
- **Application Control**
- **Content Encryption**
- **Cross Platform Controls**
- **Interdependencies**
- **Scalability**
- **Business Case**

Definition of Terms

- **BYOD**: Bring Your Own Device
- **CYOD**: Choose Your Own Device
- **MAM**: Mobile Application Management
- **MCM**: Mobile Content Management
- **MDM**: Mobile Device Management
- **OTA**: Over the Air
- **MEAP**: Mobile Enterprise Application Platform