Flyer

opentext™

Unified Endpoint Management over the Internet

Manage, secure and protect your endpoints and data, anywhere

Unified Endpoint Management at a Glance:

OpenText's Unified Endpoint Management portfolio allows you to manage devices inside or outside your corporate firewall using standard web protocols enabling you to:

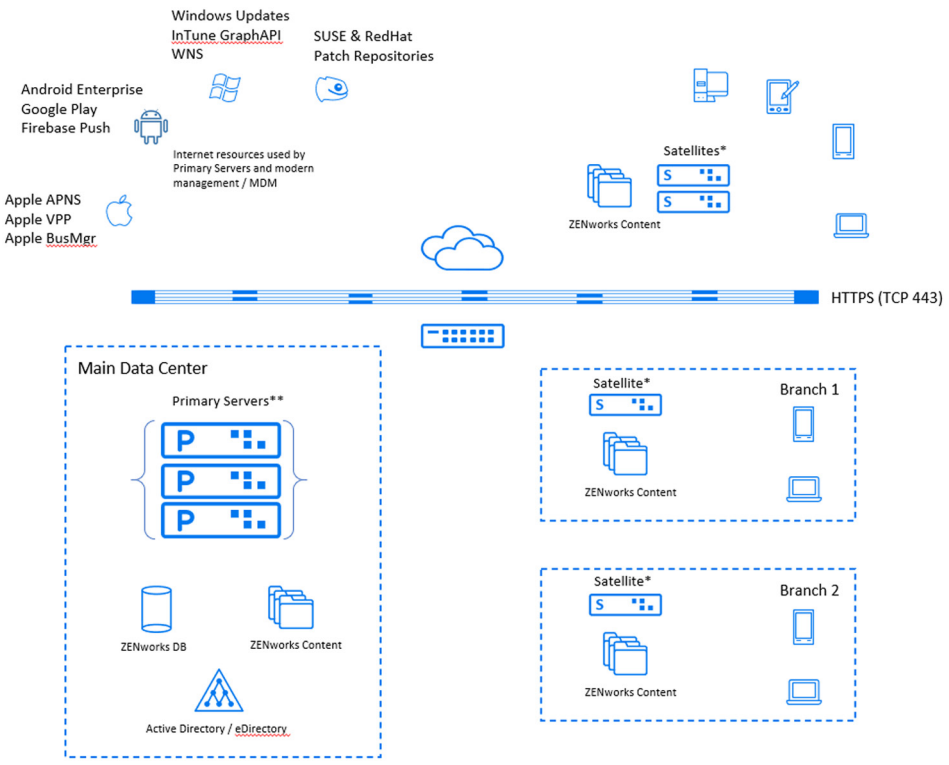
+ Manage mobile or desktop computing devices
+ Deliver configuration policies, changes and applications to your devices, anywhere
+ Inventory your devices wherever they go
+ Provide remote assistance to your end users
+ Adjust policies and application access based on location
+ Keep devices patched and secure
+ Protect data on your endpoints with corporate-defined data protection policies
+ Securely stream applications to users' corporate owned and BYO devices.
+ Provide self-service access to software and other corporate resources

OpenText™ Unified Endpoint Management

Do you have multiple management tools for different device types? OpenText™ ZENworks offers a full set of management capabilities allowing you to provision and maintain the lifecycle of your devices and the software on them, maintain a robust hardware and software inventory and deliver configuration and software updates. Quicktasks allow endpoint managers to take immediate action on devices even when they are outside the firewall, allowing you to push patches, initiate immediate inventory requests, lock/unlock devices and much more.

Internet Friendly Endpoint Management

Can you manage your devices wherever they go or does your solution require expensive VPN connections users are always forgetting to establish? ZENworks 2020 uses an internet-friendly architecture that has been built for managing your devices regardless of whether they are at home, in your office, at the Starbucks down the street and whether they are mobile, laptop or desktop endpoints. Because it uses industry standard protocols like HTTPS, you can easily manage any of your devices. This includes endpoint management for your iOS, Android, Windows 10, MacOS and



*Optional, if not present then devices connect to Primary
** All devices must be able to connect to at least 1 Primary Server via HTTPS for configuration and MDM data

Linux endpoints. With ZENworks 2020 you deploy one or more Primary Servers in your data center. Once your servers are deployed you can manage all your devices by simply ensuring that the HTTPS port is open between the devices you want to manage and your primary server. If your environment involves multiple locations, ZENworks easily extends its internet architecture by providing a satellite server to help manage the movement of large amounts of data to be closest to where the devices are located. In fact, we've even seen customers deploy satellites to the cloud to offload the download of large content from expensive network connections on-prem. The figure on the previous page shows a common multi-site environment that supports all device types both inside and outside the corporate firewall. Unlike other solutions, no VPN connection is required for administrators to see and manage the devices or end users to access their resources.

Secure Your Devices

Are you sure your endpoints aren't the low hanging fruit that hackers will use to access your network? Can you be sure they logged into the VPN last week to get the latest patches? ZENworks provides a wide range of capabilities to protect your devices from common security threats. OpenText™ ZENworks Patch Management provides the ability to automatically identify patch-based vulnerabilities, remediate the vulnerabilities by automatically applying company defined patch policies and provide monitoring of the process. This allows you to ensure your devices are patched to prevent many known attacks. With OpenText™ ZENworks Endpoint Security you can protect many additional threat vectors using capabilities such as removable storage access, application blacklisting, VPN enforcement, Wi-Fi security controls and more. Like all the capabilities presented, these can be managed and deployed anywhere the user has a connection to the internet.

Protect Your Data

How are you protecting the data that users are creating on their endpoints? If you depend on the user to store their data in a specific folder like their OneDrive or Dropbox, you risk the chance of important data being lost. With Connected MX you can easily define corporate-controlled data protection policies that will back up files based on location, file type and more. The continuous data protection nature of OpenText™ Connected MX not only helps protect you from events like device loss, theft and hardware failure, but also provides user self-service capabilities to recover from accidental deletions or file updates. With Connected MX your data is securely encrypted and stored in the cloud so users can recover their data no matter where they are or what type of device they are on.

ZENworks also helps protect your data by providing Folder, Full Disk, Mobile Device and Removable Drive encryption capabilities, protecting your endpoint data at rest. By providing a wide range of encryption capabilities, ZENworks helps you protect your end user devices whether they copy files to a USB stick, put information on a mobile device, or created content on a corporate laptop. With the ability to report on the devices that are encrypted in addition to the files that are being copied to removable media, you can also prove that your devices are encrypted if they are lost or stolen.

Stream Your Applications

How are you dealing with a significant portion of your workforce doing their job from somewhere other than the office? Your users need access to the applications that allow them to do their job, no matter where they are. OpenText™ Desktop Containers with Application Streaming enables you to package your enterprise Windows applications in a lightweight container and then stream them to any device your user has. This includes corporate owned or BYO devices running any of your favorite platforms including Windows, MacOS, iOS, Android and even Chrome OS. With Desktop Containers the application is run on the device when it makes sense and streamed from a Terminal Server when it needs to. With native profile management capabilities that ensure the user's application profile follows them from device to device, you can ensure they have the best possible experience no matter how they are accessing their apps. With native integration with corporate cloud storage solutions such as Google Drive, Dropbox and Microsoft OneDrive, your users will be able to securely access and store files without having to worry about data being left on the device they are using.

Connect with Us

OpenText CEO Mark Barrenechea's blog

And if you are an educational institution, the Desktop Containers solution now includes LTI Integration capabilities, allowing you to surface all the applications your students need right in your learning management system.

Learn more at

www.microfocus.com/en-us/products/zenworks-suite/overview

www.microfocus.com/en-us/products/endpoint-backup-protection/overview

www.microfocus.com/opentext

opentext™