5 WAYS TO ENHANCE DATA PROTECTION WITH HEXNODE

Hexnode UEM is an industryleading endpoint management solution offering a rich set of features to secure, manage, and remotely monitor the devices used within your enterprise.

Why do you need data protection?

- Prevent accidental data leaks
- Significantly reduce the possibility for a data breach
- Compliance requirement
- Enabling the safe use of personal device in workplace (BYOD)

HEXNODE'S WALLS OF DEFENSE

1 Safe and secure

Hexnode's Data Encryption and VPN Settings

Configure VPN settings to establish secure connections

Set up device encryption programs like BitLocker and FileVault

Deploy certificates for access authorization

The Scenario

With security and data breaches growing more rampant, organizations want to manage their devices securely within their network.

By setting up **VPN** configurations and **DATA ENCRYPTION**, the device can be secured within the enterprise network.

2 Securing Your Perimeter

Hexnode's Dynamic Groups and Geofence Policy

Apply conditional policies with dynamic groups and geofences

Automate access allocation based on device location or preset conditions

The Scenario

It is more secure to grant role specific access to employees but manually managing the access rights of devices can be difficult.

Automate the device configuration process with **DYNAMIC GROUPS** and create a **GEOFENCE** to restrict the device within a geographic boundary.

3 Keeping It Contained

Hexnode's Profile Owner

Prevents mixing of personal and corporate data

Decreases the odds of experiencing a data leak

Work container removal on device non-compliance

The Scenario

The increase in personal devices brought to the workplace has also increased the need to manage them without compromising employee privacy.

Enabling a **WORK PROFILE** on the employee's device will create a container for hosting the work data, separating it from personal data.

4 Anytime Anywhere

Hexnode's Location Tracking and Remote Wipe

Device tracking with GPS location

Counter unauthorized access attempts by enabling LOST MODE

Executing device wipe action as a last resort

The Scenario

A stolen or misplaced company device becomes a vulnerability. Hence, retrieving or erasing the data in it becomes a priority.

With real-time **LOCATION TRACKING**, the device can be recovered. A device wipe will erase all data from the corporate device securing a potential liability.

5 Keeping Them In Check

Hexnode's Periodic Scan and Reports

Periodic scans to spot noncompliant devices

Detailed Reports with devicespecific information

Schedule reports to be sent to your email periodically

The Scenario

It isn't easy to keep track of every device used within the enterprise. The need to identify and get information on non compliant devices greatly increases

Identifying non-compliant devices by performing **COMPLIANCE CHECKS**. From perusing the **REPORTS**, we can obtain more detailed information.

hexnode

mdm-support@hexnode.com
partners@hexnode.com

For more information visit : www.hexnode.com

US: +1-833-439-6633 | Int.: +1-415-636-7555