MOBILE DEVICE MANAGEMENT

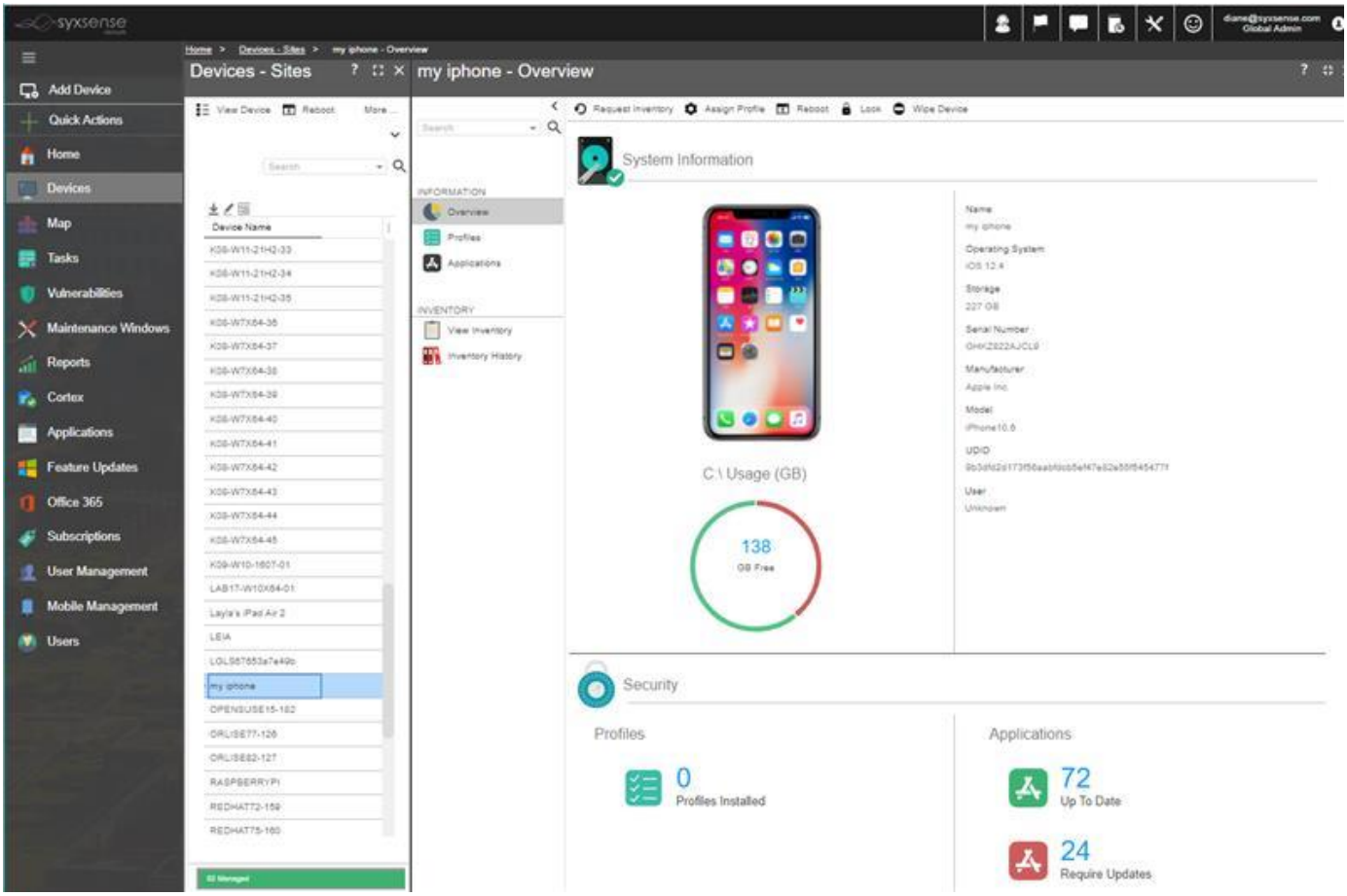
Manage, control, and secure mobile devices.

Mobile devices are increasingly integral to the efficiency and productivity of organizations but are often missing from IT endpoint management strategies. The more devices with access to a network means more potential vulnerabilities for attackers to exploit. Mobile devices present additional challenges to IT administrators as they look to protect company data on phones and tablets at the same level of security as traditional desktops and servers.

With Syxsense mobile device management (MDM), you can manage, configure, and secure iOS, iPadOS, and Android devices from your Syxsense console alongside your current inventory of Windows, Mac, and Linux devices. The cloud-based solution provides IT teams control over mobile endpoints no matter their ownership or location.

Enrolled devices are added to your Syxsense console and visible in your inventory list with their hardware and software details. This includes operating system (OS), available and free storage space, serial number, and manufacturer details, applications and any required updates, and the profiles assigned to the device.

You can apply configuration changes, compliance requirements, or application deployments and rollbacks across all mobile devices.



DEVICE SECURITY

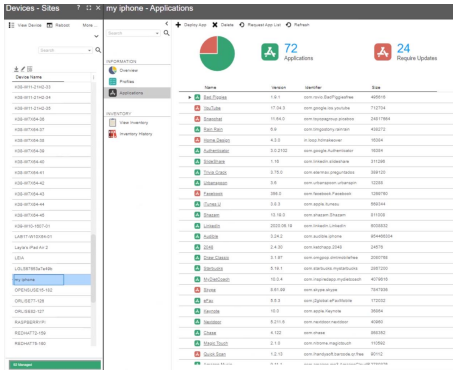
Security for mobile devices begins at the lock screen. It's the first line of defense for ensuring the safety of company data and ultimately your entire network. Cybersecurity measures alone can't keep devices from falling into the wrong hands, but they can be an effective barrier to entry if it happens.

With Syxsense, you can set requirements for the type and complexity of security challenges, such as PINs and passwords, that users need to meet. If a passcode doesn't meet these conditions, Syxsense can restrict the device from accessing work data or applications that communicate with your network. This allows you to enforce compliance with security policies on every endpoint in your organization, for company-issued devices and bring-your-own-device (BYOD).

As phones and tablets are more mobile than traditional endpoints, protecting access to resources such as email accounts and VPN servers requires additional device control. From the Syxsense console, you can remotely lock and wipe devices no matter their location. It keeps your network secure even in the event a mobile device is lost or stolen and can make offboarding employees leaving your organization easier and more efficient.

To ensure mobile devices remain up-to-date with new releases, Syxsense can monitor and enforce OS updates through scheduled deployments or automatic updates. The updates are configurable for individual devices or groups of devices.

APPLICATIONS



Application management for mobile devices in Syxsense gives you extensive control over installations, remote deployments and rollbacks, updates, and download restrictions in company-issued devices. For BYOD, the same controls are available for assigned profiles that contain and isolate work data and applications on devices and require additional security challenges for access.

From the Syxsense console, you can silently install applications and version updates to enrolled devices in your network without user intervention. The silent deployment prevents disruption to productivity for end users, and silent autoupdate policies prevent any delay in applications updates that could leave your devices vulnerable.

Applications can be whitelisted, blacklisted, or removed from devices remotely from your console and you can set download restrictions that limit the application installations available to users. Any application that supports managed configurations can be remotely and silently configured from Syxsense.

DATA CONTAINERIZATION

You can isolate corporate data on company-issued mobile devices or BYOD in Syxsense with distinct Security Profiles. The Security Profile segregates access to and usage of applications within a protected area of the device. In addition to any required PIN or password restrictions, you can set additional levels of authorization to access corporate data or applications within the assigned profile.

The Security Profile is treated like a high security, cordoned off zone of a mobile device.

Applications and company resources that connect to your network are only visible andaccessible with secure credentials. Containing your organization's data within profiles enables you to monitor, manage, and enforce security measures beyond the lock screen. If an employee works on a BYOD tablet or checks company email on their cell phone, you can disallow any overlap with personal data or applications. If an employee clicks a suspicious link or downloads a corrupt application, your company resources are inaccessible and blocked from attack within the Security Profile.

Data containers also provide a balance between corporate security and user privacy concerns on personal devices that employees use for work. IT teams retain control over the management and security of applications and data that communicate with the company network without an employee's private information becoming visible to administrators.

If your organization issues company-owned mobile devices, containerization with Security Profiles adds an extra layer of protection. While IT teams have more control over company devices, it's still impossible to totally control everything an employee does on a device. The Security Profile isolates corporate data and applications from the rest of the device to ensure your network stays secure and protected from threats.

ESSENTIAL QUESTIONS

Do I allow employees to use personal devices for work? Can employees access email or other types of work data from personal cell phones or tablets?

Can I enforce password protection on mobile devices that employees use for work?

Can I remotely lock or wipe data from a mobile device in the event its lost or stolen?

Can I install/uninstall applications or configure settings remotely OTA without disrupting end users?

Can I set policies to autoupdate applications with new releases?

Can I restrict mobile devices that aren't in security compliance from accessing my network and corporate data?

Are corporate data and applications isolated from personal data on BYOD?

syxsense

www.syxsense.com

info@syxsense.com

(949) 270-1903