Security

In our increasingly interconnected world, security is not just a luxury, it's a necessity. As your organization undertakes the device refresh and (re)Enrollment process, it's essential to prioritize device security at every stage. FileWave provides a variety of tools that can help you enforce security protocols and provide a secure operational environment for your users. Here's what you can do:

Prioritize Device Security

From the onset, it's crucial to enforce security protocols on all devices. This includes installing security updates, setting secure device settings, and ensuring the proper configuration of all software. FileWave's device management tools allow you to automate these tasks, ensuring that all devices adhere to your organization's security standards.

- You'll need to ensure that you are actively patching all of your systems to avoid painful situations.
- If you have local admin accounts think about solutions like Integrating EasyLAPS with FileWave for macOS that will rotate the password in a secure way. Remember that when someone leaves your organization they may know a password that is on every single device.

Train Users on Security Protocols

User behavior is a critical factor in device security. Conduct training sessions to inform users about your organization's security protocols, the importance of regular software updates, safe internet practices, and how to identify and report potential security threats. FileWave's tools can assist in disseminating this information, making users active participants in maintaining device security. You can easily script notifications via PowerShell on Windows or use tools like swiftDialog Deployment (macOS PKG) on macOS.

- Use even a generic annual security training program. There are many simple and short video based training courses.

Monitor Device Status

Regular monitoring of device status can help detect any security issues early on. Use FileWave's reporting and analytics tools to perform routine checks, track device performance, and detect any irregularities that may indicate a security threat. This proactive approach can prevent minor issues from escalating into major security breaches.

- Custom Fields can be very powerful in this regard.

Respond to Security Incidents

Despite your best efforts, security incidents can still occur. When they do, it's important to have a response plan in place. FileWave can assist in identifying affected devices, isolating them to prevent the spread of security threats, and restoring them to a secure state.

- Have procedures in place before an incident occurs so you know what you'll plan to do. Build out even a basic Playbook for the things you can think of that might happen.

Review and Improve Security Measures

Security is an ongoing process. Post (re)Enrollment, review your security practices and use the insights gained to improve them. FileWave's reporting tools can provide valuable data to assist in this review, helping you continually enhance device security.

By taking a comprehensive and proactive approach to security during the device refresh and (re)Enrollment process, you can provide a secure operational environment for your users and protect your organization's valuable data and resources.

Revision #11
★Created 13 July 2023 16:46:46 by Josh Levitsky
✎Updated 26 July 2023 14:29:04 by Tony Keller