PATCHING. HOW HARD CAN IT BE?
Harder than you think. Trust us. We know a thing or two about patch management, as we have been doing this for over ten years. And not just IT patch management. We understand the difference between patching your laptop vs. the intricacies of patching your relays, PLC’s and other OT equipment. You can’t just recklessly patch your OT equipment. It takes planning, validation and intent. We know that.

WHY IS IT NECESSARY?
Industrial control systems (ICS) in critical infrastructure are high-risk targets for attack and exploitation. Consistently monitored patches & updates can help resolve security vulnerabilities, functional issues and meet regulatory compliance requirements.

NERC CIP compliance regulations state that registered entities are required to have a patch management process for tracking, evaluating and installing cyber security patches for their identified cyber assets of applicable systems.

HOW DOES IT WORK?
Provide us with your list of assets and we’ll take it from there. We may need your help from time to time to help clarify what equipment you have. (Again, it’s critical that we get it right.) If you don’t have an asset list or need help to verify this list, we can have our team of experts help you. While we are analyzing your assets, we will provide monthly patch due diligence reports for your security and compliance programs.

WHAT YOU RECEIVE

IN-DEPTH ANALYSIS
A comprehensive investigation of your assets to determine supportability and audit-ready documentation of those items that are no longer supported by the vendor.

CUSTOM PATCH AVAILABILITY REPORTS
No less than every 35 days, FoxGuard will provide a custom report with patch due diligence on your specific assets. We give you a list of all of your items and tell you which ones have patches. Need to know if they are a security-related patch? Yeah. We got that too.
DO YOU COVER EVERYTHING?

FoxGuard remains committed to greatly alleviating your patch management burden as we have been for over ten years. Our Patch Availability Program analyzes and categorizes assets as follows:

- **REPORT READY**
  Item is included on monthly Patch Availability Report.
- **CREDENTIALS REQUIRED**
  FoxGuard requires contract credentials to access patch data.
- **NOT IDENTIFIABLE**
  Item lacks required information to determine if it can be patched. FoxGuard works with you to clarify and/or remove the item from the list.
- **END OF SUPPORT (EOS)**
  FoxGuard works with vendors to determine that an item is no longer supported and provides documentation as evidence.
- **NOT APPLICABLE**
  Item does not receive security patch releases. FoxGuard provides you with proper documentation to support this finding.

DON'T EVEN KNOW WHAT YOU HAVE?

FoxGuard can help with that too. We have a team of patching engineers ready and able to help you identify and clean up your baseline of assets.

WHY FOXGUARD?

- **EXPERIENCE**
  Leverage over 10 years experience with thousands of information and operational technology items. We know the industry’s assets because we have analyzed, documented and provided patch details for these items.
- **ONE SOURCE**
  We aggregate all of your assets and vendors into one source - eliminating the need for you to contact and follow up with all of your vendors every month.
- **ONE CALENDAR**
  Because you have only one source, your compliance calendar of 35 days for the subsequent NERC CIP-007-6 R2.1, R2.2, R2.3 and R2.4 requirements stops and starts at the same time. Just one calendar to manage instead of 10’s or 100’s. Every month.
- **SECURITY VS. NON-SECURITY**
  Our trained engineers analyze patch details to determine if a patch addresses a security vulnerability, even if the patch vendor doesn’t make this declaration. This allows you to prioritize the patches that are needed to secure your critical systems.
- **SECURE STORAGE OF YOUR ASSET INFORMATION**
  Not all patches are readily available on the Internet, so we have the ability to work directly with your vendors to access patch status and subsequent details on your behalf and securely store the appropriate asset information.
- **INTEGRATION**
  Have some form of an automated Asset Management System or Compliance Tool? We can work with your vendor to automatically integrate our reports into your system, automating the process of digesting newly released patches. Want to know if we work with your provider? Just ask us.
- **EOS DOCUMENTATION**
  Not every product lives forever. When a vendor declares an item as “End of Support”, you need documentation to show why you are no longer monitoring patches for that item. We’ve got that covered.
- **SAVE VALUABLE TIME**
  Trust us. This work is complicated and takes well-trained professionals. Save the time of your valuable resources to focus on your business and leave the patch management work to the experts. Us.