Power Generation

Security Workplace: FILE SANITIZER
Reliability - Security - Compliance

Removable Media Risk Mitigation

The Risk Factors: "Trusted Files from Trusted Insiders"

A top cyber threat vector against your Plant control environment is the trusted insider or contractor who unintentionally introduces malicious software (malware) by means of an "infected" file or USB firmware (BadUSB) transferred through removable media (flash drive, DVD). Unfortunately, you are wide open to a targeted attack whenever you import files into your Operational Technology ("OT") environment, from any source, period.

The attack method of preference, due to its success rate, is to embed or hide malware into common file types such as CAD, Visio, PDF's, video, images and Microsoft Office documents (doc, ppt, xls) and deliver them via email (phishing attacks), special interest web sites (watering holes) or removable media (flash drives). This malware is designed to evade anti-virus scans and other common detection technologies and to stealthily execute its mission.

A recent wave of attacks against Industrial Control Systems (ICS) dubbed the "Dragonfly Campaign" compromised OEM websites, infecting "trusted" files that provide software downloads for their customers. The end users, using administrative rights, then authorized these "trusted" software files to execute on their computers, essentially evading all security controls such as firewalls, whitelisting and anti-virus.

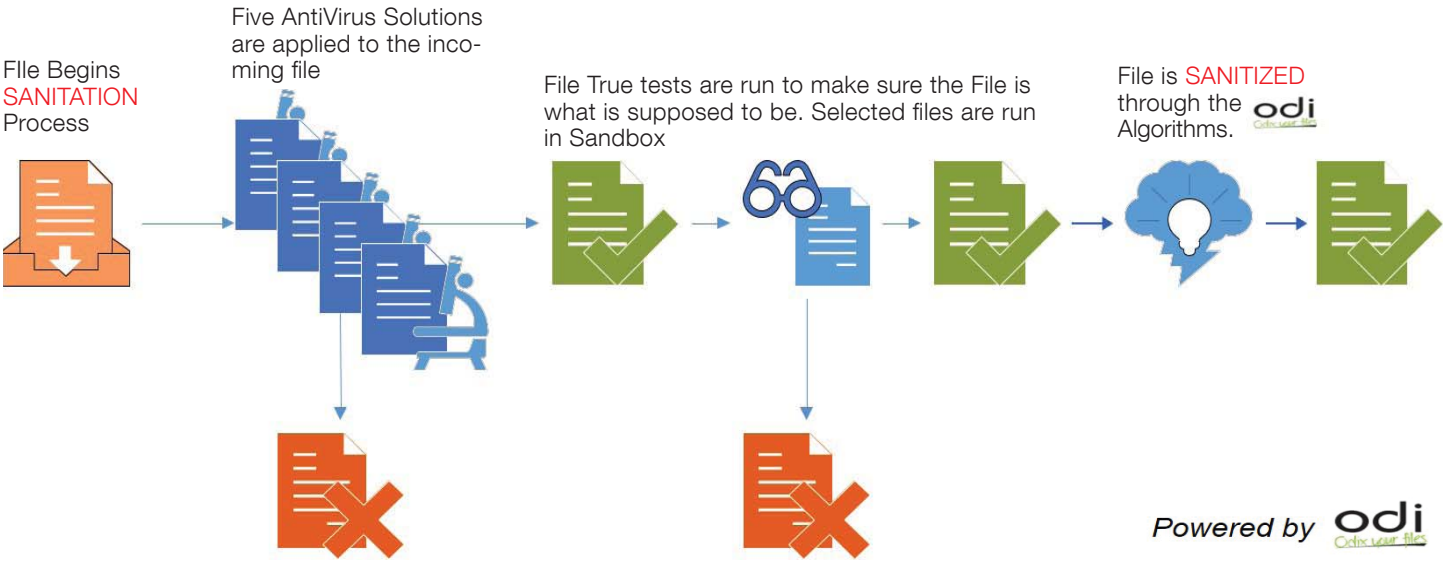
Who then should you trust to provide malware-free files when you require essential software or security patch updates? Your OEM, IT department or MicroSoft? No one! All sources and files should be considered un-trustworthy.

The Solution: ABB Security Workplace FILE SANITIZER Powered by the ODIX Process

To mitigate the risk from introducing an infected file into your OT environment, ABB has introduced the **FILE SANITIZER** powered by the ODIX process that sanitizes files by neutralizing and removing undetectable malware at the speed of business. But how do you neutralize something that you can't detect?

The ODIX process uses a three (3) stage sanitation process to rapidly produce trusted files. Stage 3 of this process employs sophisticated algorithms, custom designed by file type, which allow the **FILE SANITIZER** to "scramble" or remove malicious code from the file without corrupting the integrity of that file. These algorithms depend on knowing the mathematical construct of the file type, not the identification of malicious code. This proprietary method is the only proactive approach in use today that does not rely on detection or identification.

FILE SANITIZER Process



Power and productivity for a better world™

ABB

Security Workplace
Removable Media Protection

The **ABB** FILE SANITIZER solution can be deployed in an air-gapped environment or connected to the plant network and centrally managed. Depending upon the desired architecture, the sanitized files can be transferred to read-only media (CD-ROM) using the appliance or to a file server.

The **ABB** FILE SANITIZER appliance provides a controlled environment which physical devices such as flash drives, IDE drives or DVD/CD can be inserted into the system (meets NERC CIP v5 CIP-010-2 R4). This hardened appliance is resistant to any attack including BadUSB and will then process all selected files from the removable media and deliver only those that have been sanitized.

2VAA00000 Power Generation 0514

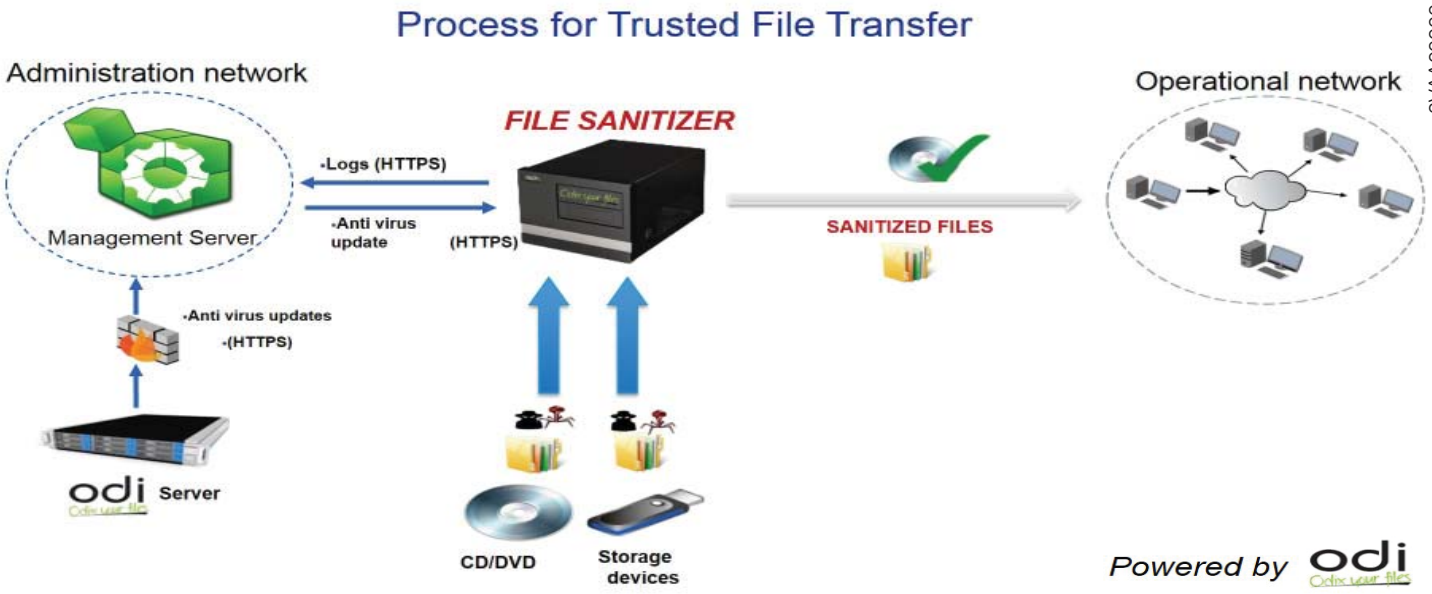


ABB is recommending only files that have gone through the FILE SANITIZER be introduced to the Distributed Control System (DCS) via CD-ROM or networked file transfer from the FILE SANITIZER. Due to the BadUSB threat, we discourage the use of flash drives for this purpose since there is no effective defense from USB attacks.

System Description & Benefits

- **Unique process based on proprietary algorithms**
- **Sanitizes all files from known & unknown malware.**
- **Operating system hardening – FILE SANITIZER boots from a LIVE CD.**
- **Modular design allows adding more appliances by demand.**
- **Operates under Linux Operating System.**
- **Full treatment in rooted office files.**
- **Virtual environment for each filtering process.**
- **5 different anti-virus engines.**
- **User authentication, permissions, policies and logs.**
- **Audit trail of every file installed on your ABB DCS.**

Contact Us

For more information please contact:

Mike Radigan
ABB Inc.
Senior Advisor, Cyber Risk Management, Power Generation
Wickliffe, Ohio, USA
Phone +1 614 398 6241
E-mail: mike.radigan@us.abb.com

www.abb.com/powergeneration

Power and productivity
for a better world™