

Media Contact:  
Michelle Meyer  
Marketing Manager  
MDT Software  
678.297.1016  
[Michelle.Meyer@MDT-software.com](mailto:Michelle.Meyer@MDT-software.com)



## **MDT AutoSave Now Includes Cybersecurity Features to Track Firmware Versions in Automation Devices**

*This capability expands AutoSave's protection and recovery solutions to help manufacturers identify vulnerabilities in their automation layer*

**ALPHARETTA, Georgia, November 28, 2018** – MDT Software, the world leader in change management solutions for automated manufacturing assets, today announced a new cybersecurity feature in AutoSave. AutoSave can now track data such as firmware, software and CPU versions in automation devices from the following vendors: Siemens, Schneider, Mitsubishi and Rockwell; support for additional device types and automation vendors will be added soon. The capability to easily and automatically identify this information, for comparison against published threat reports, will greatly aid automation users to address vulnerabilities in their devices.

Manufacturing is the second most commonly targeted industry by attackers and many attacks are successful due to the many vulnerabilities that exist in the manufacturing environment. One method hackers use to attack these facilities is through a device's firmware. Once security threats are identified by the device manufacturer, a new software or firmware release is issued to address the risk. In using AutoSave to identify the device's current versions, the plant can easily identify which devices need to be upgraded to the newly issued version.

MDT AutoSave also helps mitigate risks to the automation device's program data. One of the easiest and most successful ways to launch an attack in a manufacturing facility is to change an automation device program, however, this risk to a plant's safety is not addressed by data access and network monitoring applications. MDT AutoSave provides the ability to:

- Secure your program intellectual property: AutoSave saves a copy of each program revision in a central repository. Access to program folders and programs is managed by via a flexible privileging system.
- Detect changes made outside the change management system: AutoSave compares the latest program copy on file in AutoSave with the program running in each device to identify any differences. If differences are found, the appropriate people are notified with an email highlighting the differences.

- Rapidly recover from unauthorized changes: With an archive of all program revisions, the latest approved program can be quickly restored after an unauthorized change.

“Effective management of Industrial Control Systems must be part of the security plan for any manufacturing facility and utility operation,” explains Gary Gillespie, Vice President, MDT Software. “An inventory of program configurations, code and firmware versions will greatly aid in implementing solutions to protect a plant from threats and recover quickly from unauthorized changes to program logic.”

**About MDT Software, Inc.**

MDT Software is a world leader in change management solutions for automated manufacturing devices. MDT’s flagship product, AutoSave, empowers users to protect, save, restore, discover, and track changes in industrial programmable devices and plant-floor documents. AutoSave supports the most comprehensive range of devices and editors in the industry from Schneider Electric, Siemens, Mitsubishi, GE, Rockwell Automation and others. For more information on MDT and AutoSave, visit [www.MDT-Software.com](http://www.MDT-Software.com).