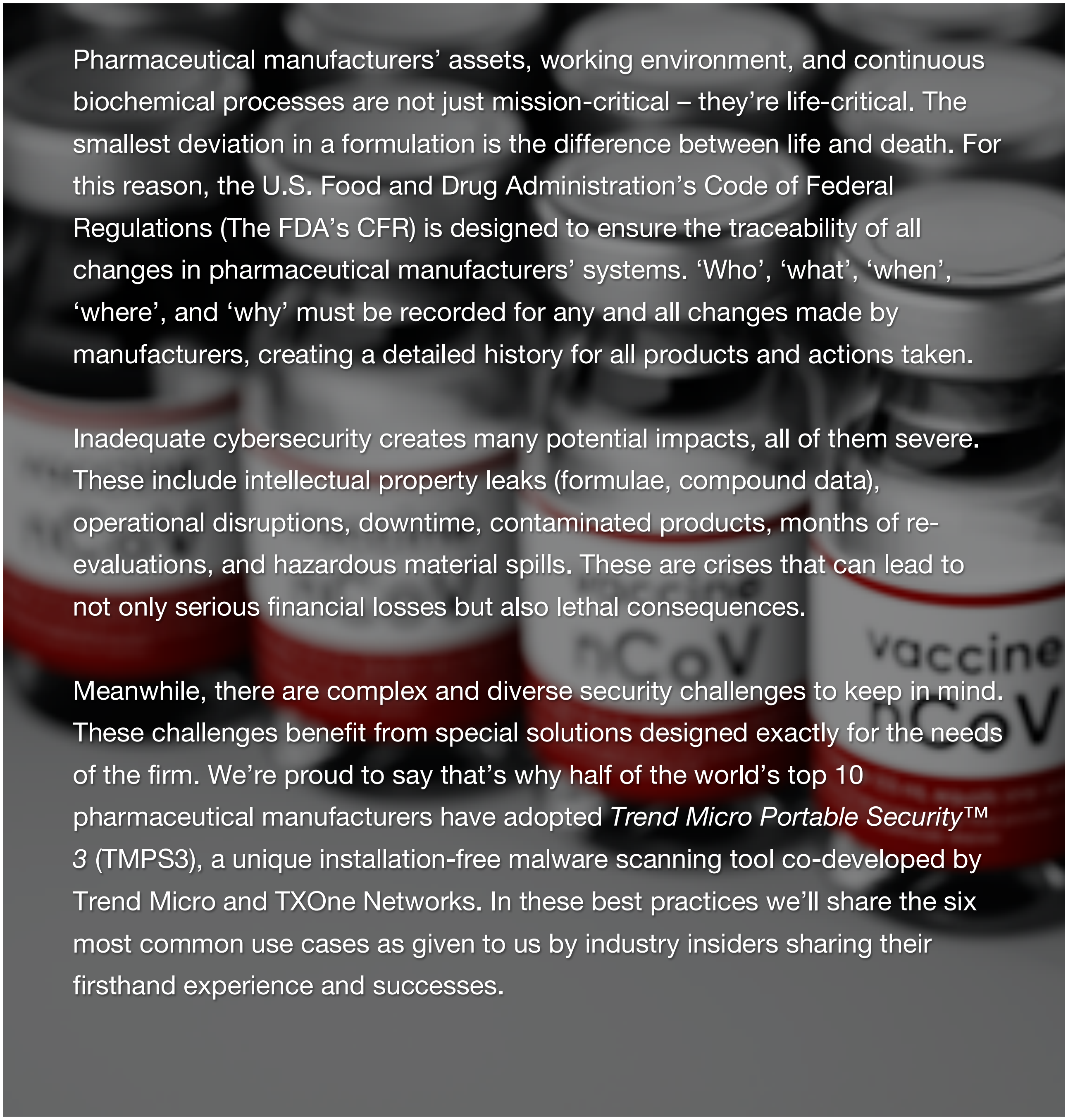
Best Practices for Pharmaceutical Manufacturers: Trend Micro Portable Security™ 3

Michael Cheng

Max Farrell

Content

Executive Summary



Pharmaceutical manufacturers' assets, working environment, and continuous biochemical processes are not just mission-critical – they're life-critical. The smallest deviation in a formulation is the difference between life and death. For this reason, the U.S. Food and Drug Administration's Code of Federal Regulations (The FDA's CFR) is designed to ensure the traceability of all changes in pharmaceutical manufacturers' systems. 'Who', 'what', 'when', 'where', and 'why' must be recorded for any and all changes made by manufacturers, creating a detailed history for all products and actions taken.

Inadequate cybersecurity creates many potential impacts, all of them severe. These include intellectual property leaks (formulae, compound data), operational disruptions, downtime, contaminated products, months of re-evaluations, and hazardous material spills. These are crises that can lead to not only serious financial losses but also lethal consequences.

Meanwhile, there are complex and diverse security challenges to keep in mind. These challenges benefit from special solutions designed exactly for the needs of the firm. We're proud to say that's why half of the world's top 10 pharmaceutical manufacturers have adopted *Trend Micro Portable Security™ 3* (TMPS3), a unique installation-free malware scanning tool co-developed by Trend Micro and TXOne Networks. In these best practices we'll share the six most common use cases as given to us by industry insiders sharing their firsthand experience and successes.

Introduction

Pharmaceutical manufacturing carries the legal requirement that technicians provide a special level of care to every asset. Complying with regulations from organizations like the FDA, EMA, GMP, and GAMP, as well as following the requirements necessary to avoid voiding the warranty, complicates procedures that might normally be routine, such as installing software on the ICS or evaluating changes to assets for impact on products and operation. Since TMPS3 is installation-free and has a very low operational footprint, it has no impact on manufacturing and can be used without voiding your ICS warranty.

When partners, vendors, or consultants come on-site for maintenance, they'll need to connect their potentially infected laptops or USBs to the ICS network or assets. TMPS3 is easy to use, allowing it to conduct quick scans of incoming devices at your checkpoint. No IT expertise is required. Asset owners or operators just plug it in then follow the intuitive onscreen procedure to scan and secure.

Consistently and securely maintaining an up-to-date inventory introduces many potential risks. TMPS3 makes maintaining such records much more convenient – its companion Management Program provides a company-wide view of security. TMPS3's logfiles provide proof of compliance to satisfy the stringent requirements of regulations such as the FDA's *CFR Title 21 Part 11, Electronic Records and Signatures.*

Best Practices

With all this in mind, we've discovered six key best practices that we can whole-heartedly recommend to pharmaceutical manufacturers.

1. Enhance existing inventory management

TMPS3 fits perfectly into your SOP for scanning assets during regular maintenance. TMPS3 provides 4 different scan types. Scan all local folders during maintenance to ensure the ICS is clean and safe.

2. Make security checks to detect threats and document all results

Use 'log-only' scan settings – which create a log file of what was discovered but do not take action – for mission critical asset scans. Record the scan result from TMPS3's logs, and, regardless what the scan finds, fill out an inspection form. Contact the asset owner or asset vendor to confirm what action to take on suspicious or malicious files discovered by TMPS3.

3. Check for endpoint vulnerability caused by unpatched assets or end-of-life operating systems

Your organization's security team should use asset info collected by TMPS3 during the scan to understand what patches and applications are installed. This helps extend your OT visibility, especially for standalone devices, and make it easier to manage your ICS.

4. Conduct an in-depth plug-and-scan security inspection on all devices entering or exiting your work site

Partners, vendors, and consultants will all bring their own assets that must be scanned before they connect to the ICS environment, unless they can show they were given pattern updates and scanned recently. “Recently” for your firm should be a specific number of days that you’ve set and agreed on, for example two days. TMPS3 makes these kinds of routine and “checkpoint” scans a snap. The scan setting “All Local Folders” scans all folders on the target endpoint, or you can choose “Quick Scan” to scan only the folders most vulnerable to system threats (such as the Windows System folder).

5. Centrally log asset information and scan results to streamline the audit process

Transfer scan logs to the Management Program to create a factory-wide or even company-wide view. This can be used to create an audit trail for compliance as well as communicating security timelines and documentation to stakeholders on the supply chain including hospitals, pharmacies, and other crucial healthcare providers.

6. Extend the visibility and utility of your security operations center

You can centrally organize logs and events, regardless of the make of the devices you’re tracking, by employing an SIEM. Logs can be exported or transferred to SIEM such as QRadar or Splunk. This supports your need for data integrity, helping your organization to satisfy legal necessities as well as the need for patient safety.

Conclusion

Half of the top 10 global pharmaceutical manufacturers have already discovered that *Trend Micro Portable Security™ 3* is streamlined and refined with the special needs of pharmaceutical manufacturers in mind.

For more information about *Trend Micro Portable Security™ 3*, please visit https://www.txone-networks.com/en-global/products/index/tmps3.