nuvolo

# OT Security for Life Sciences: **Protecting Your Assets**

# Understand OT Security Risk

Operational technology (OT) is defined as all non-IT equipment connected to the network, including equipment that may be air-gapped or physically isolated from the internet. While IT security has been in place for over 20 years, and the tools to protect these devices work reasonably well, connected OT devices are newer and often do not have the same security protocols in place.

Security threats are a challenge for all companies, but regulated industries, like life sciences, are especially at risk and must protect manufacturing and lab equipment, clinical trial data, product specification, and methods that underlie patents, trade secrets, and scientific know-how.

In 2020, the average cost of a pharmaceutical data breach was $5.06 million. Of the 17 industries surveyed, pharmaceuticals ranked fourth in average cost. The average time to identify and contain a breach in this industry was 257 days, putting companies and consumers at prolonged risk. [1]

This ebook provides an understanding of how modern OT security works and why it is important to select, deploy, and operationalize these capabilities to protect equipment supporting current good manufacturing processes (cGMP) processes and your reputation on a sustainable and cost-effective basis.

## $5.06 million

**was the average cost of a pharmaceutical data breach in 2020.**

## 257 days

**was the average response time to identify and contain a breach.**

Manufacturing pharmaceuticals and medical devices requires a wide variety and large volume of OT technologies, devices, and applications to support cGMP processes. This creates a challenge in defining and implementing coherent security policies across the equipment, which can require more resources to achieve a maturity level comparable with IT. The complexity in monitoring and maintaining security levels increases exponentially with this scale and criticality of life sciences global operations.

Air-gapped systems are certainly more secure by virtue of fewer attack avenues. However, these systems are still vulnerable despite being disconnected from the internet. Organizations that employ these kinds of systems should address all possible gaps in security to ensure that their air-gapped infrastructure is indeed secure. But no level of investment can ensure 100% protection, and improperly managed lab and manufacturing equipment can result in:

**Reduced and unanticipated equipment availability**

**Decreased safety**

**Financial exposure**

**Reputational and public relations risk**

**Loss of revenue**

**Compliance and regulatory issues**

**Product shortages**

There is a growing realization that addressing threats and vulnerabilities requires deep commitment and collaboration across all people, processes, and technology involved in producing pharmaceuticals and medical devices. This is easier said than done due to the complex nature of the life sciences industry.

# OT Security Challenges in Life Sciences

**Decentralized Inventory:** Equipment information is stored in multiple inventories

**Compliance False Assurance:** There is false assurance that compliance means a strong OT security posture

**Integration with Legacy Systems:** Newly commissioned OT delivered with legacy or unpatched operating systems

**Sophisticated Environment:** Equipment is managed by different systems and vendors

**Lack of Orchestration:** Difficult to tie security events to detailed asset context for effective remediation

**IT Governance:** IT security controls rarely cover OT areas that are related to manufacturing and lab equipment

**Multiple Manufacturing Sites:** Each manufacturing site is autonomous and has unique processes and protocols

# Close the Gap in OT and IT Security

Securing traditional IT devices is generally a high priority for an organization. In contrast, for life sciences, the teams overseeing cGMP equipment had no historical security mandate and mostly focused on device resiliency and performance.

However, life sciences companies have entered a new era, where collaboration between business device owners and IT is essential to meet growing security threats. While IT security teams have the benefit of mature active monitoring capabilities, vulnerability management tools, and nearly universal remote remediation capabilities for IT devices, many of these tools and resources are not available or cannot be used for manufacturing and lab equipment security. Instead, the life sciences industry must adhere to other processes and requirements:

- Passive monitoring is the standard and can provide needed data without interacting directly with an asset. Specialized passive monitoring tools sniff the network and can identify and classify asset signatures. This is an alternative to active monitoring, which cannot be performed on most cGMP equipment because the installed operating system is often not configured to withstand active monitoring tools. In many cases, active monitoring may cause the equipment to crash or become unresponsive.
- Security remediation for assets can only be executed by authorized, trained, and certified technicians and engineers—not IT security teams.
- Specialized skills, training, tools, and experience are required for security remediation.
- Physical access to these devices is often highly restricted due to their locations within clean rooms, aseptic spaces, and wet labs.
- In some cases, OEM or third-party service providers must be utilized to perform lab and manufacturing equipment security corrective maintenance activities versus internal device technicians or IT security teams.

**IT security teams have the benefit of mature active monitoring capabilities, vulnerability management tools, and nearly universal remote remediation capabilities for IT devices, but many of these tools and resources are not available or cannot be used for manufacturing and lab equipment security.**

These issues can be complicated by the historical gaps—culturally and organizationally—between your IT team and supply chain teams responsible for day-to-day maintenance of cGMP equipment. Additional training required to enter and operate within a cGMP space further complicates securing devices. Closing the gap is critical as more sophisticated and determined attackers are actively exploiting network-connected assets as a new and highly vulnerable entry point into your enterprise. The threat is real and growing, and a new era of cooperation is essential.

# People, Process & Technology

In life sciences, because security events directly impact the accessibility and availability of equipment and processes, fundamental questions must be answered as part of maintaining a strong security posture.

- How can you confirm the availability of your manufacturing and lab equipment?
- How do you make sure your manufacturing and lab equipment are accessible when you need them?

### People

The teams responsible for cGMP equipment maintenance need accurate reporting on OT inventory with information reflecting condition, calibration, validation, disposition, and location of all assets. The security operations center (SOC) needs monitoring information that empowers them to monitor lab and manufacturing equipment security and activity on the network.

### Process

You need a way to accurately capture the cGMP asset lifecycle, as part of a standard equipment onboarding process. Without this, it's difficult to determine asset suitability for cGMP use, installation, validation, disposition, calibration, maintenance, use, and security. When a security threat, vulnerability, or exploit occurs, timely remediation can be difficult or impossible to achieve in the absence of a common data model for matching, contextualization, and security event correlation. The process of creating a standard data model enables the technology to perform to expectations. Without this process commitment, the technology will not meet expectations and risk will remain persistent.

### Technology

Multiple CMMS, EAM, IWMS, or other service management technologies will prevent an organization from achieving a successful security posture. Consolidating legacy maintenance software onto a single modern inventory and service management platform provides consistent, accurate data and is a key first step for the enterprise.  Without this commitment, the business will struggle and accrue security risk over time.

Managing your lab and manufacturing equipment profile data and network information in different systems adds enormous complexity, cost, and risk when a security event takes place. How can your assets be matched to security threats if there is no standard data model? How can your cGMP equipment support teams understand what other assets are potentially at risk without a common data model? It is essentially impossible at scale to manage security across multiple inventory and service management technologies with disparate data. Consolidation and a common, standard data model are the only options.

## Pain Points

- Disparate & Unmanaged Inventory Data
- Ineffective Manufacturing & Lab Asset On-Boarding Process
- Non-Standard Naming Conventions & Location Data

# Discovery - Intersecting OT & IT

How do you discover and monitor network-connected lab and manufacturing equipment that live on your network? The most common option is to implement new asset discovery technology. The key to success is then pairing your selection with a single, modern service management platform for cGMP assets that you own and operate. The service management platform is where the security discovery data is added, contextualized, and acted upon in a way that mitigates threats and drives remediation work activities. The service management platform must be authoritative in nature and have within it the trusted inventory.

A single, trusted inventory system helps your organization manage the full network connected lab and manufacturing equipment lifecycle. Regular, ongoing updates to inventory data take place when the lab and manufacturing equipment teams perform routine preventive maintenance (PM) or corrective maintenance (CM), provision new assets, or update firmware or software.

The inventory system includes, but is not limited, to data such as:

- Owner
- Location
- Site
- Serial number
- Asset make
- Department
- Latest software version
- Asset model
- Usage
- Maintenance history

When a security event happens, the discovery payload is received by system and enriched by the service management and inventory data. This enrichment process enables the data security, IT, and device support teams to all be operating with the same data for the very first time. Having everyone on the same page is essential for visibility and rapid remediation of security events.

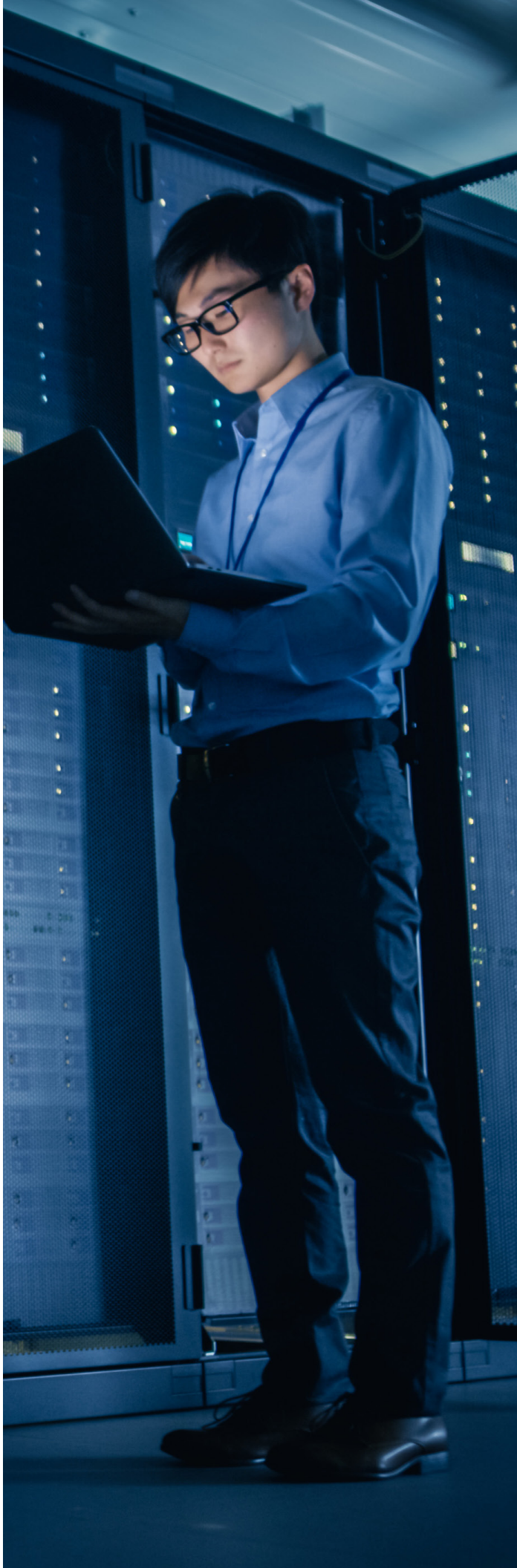
# Trusted Device Data with Monitoring & Remediation

An essential part of safeguarding network connected lab and manufacturing equipment is ensuring persistent visibility using new discovery tools. The goal is to prevent security blind spots. Monitoring and discovery should be a standard everyday activity for security professionals, with an appreciation and understanding of the growing importance of these devices as part of business operations.

These resources help analyze vulnerabilities and provide a security event assessment and remediation recommendations. It is critical that only trained, certified, and authorized resources are utilized or dispatched to remediate affected cGMP assets. A key driver here is regulatory mandates. For example, an equipment manufacturer may require only certified, authorized personnel to work on the asset for warranty or compliance reasons. Likewise, standard operating procedures (SOPs) must be followed to adhere to validated manufacturing processes.

When a security event takes place, the IT security team can see the full context. They'll know who the equipment owner is and what remediation process must be followed, so a work order can be dispatched to a qualified technician. Using a single, modern platform, all activities are tracked, time stamped, date stamped, and available as data for reporting and compliance purposes. In this model, information security, IT, and the support teams have full visibility and reporting on all activities for remediation.

This combination of expertise, modern technology, and well documented and operationalized processes help keep the connected lab and manufacturing equipment accessible and available in the face of a rapidly growing security threat.



# Lab & IT Teams - Using the Same Data Means Faster Remediation

When there are thousands of connected manufacturing and lab assets in use in your organization, it's critical to have a scalable, orchestrated, and automated response process to security events. Nuvolo encourages an automated response as outlined below:

### Intelligence Hub

- Supports all OT Discovery Tools
- Device Profiles in Common Data Model
- IT & OT Teams can see the Same Threat Data

### Automation

- Correlation
- Orchestration
- Automates Intake of OT Security Events

### Workflow

- Collaboration
- Gain Context

### Response

- Work Dispatching
- Work Order Management

Nuvolo OT Security for life sciences provides:

- Single system of inventory
- Common asset data model
- Workflow and orchestration
- Matching capability for "like" affected assets
- Dispatch
- Tracking and reporting

# Conclusion

Nuvolo provides a single, trusted inventory system that helps the life sciences industry manage the entire connected lab and manufacturing equipment lifecycle. Regular, ongoing updates take place when the support team performs tasks such as routine planned or corrective maintenance, provisioning new devices, or installing firmware or software updates.

When cGMP equipment is connected to the network or a security event takes place, Nuvolo receives that information from asset discovery and monitoring tools, creating an intelligence hub of asset and event information. This allows Nuvolo to leverage an existing discovery tool, natively embedded as part of the solution. Alternatively, if the enterprise has already purchased and operationalized a discovery tool, the intelligence hub allows for easy integration.

When a security event takes place, the key is that both the information security and support teams can see the full context of the device. The intelligence hub also helps facilitate full knowledge and visibility of the affected asset including theater of operation, owner, designation, and many other attributes as well as the remediation process to be followed.

Nuvolo enables this seamless approach, accelerates remediation, and improves quality and safety when security events occur.

[1]https://www.ibm.com/security/digital-assets/cost-data-breach-report