VERVE
A ROCKWELL AUTOMATION COMPANY

CASE STUDY

70% LABOR COST REDUCTION

How a Pharmaceutical Giant Transformed OT Security and Optimized Resources

SUMMARY

Our client, a global pharmaceutical manufacturer with 55 facilities, faced significant challenges securing its OT environment. Verve Industrial implemented its unified security platform, Verve Security Center, resulting in a 70% reduction in security-related labor costs, streamlined threat response, and a shift to a proactive security posture. The solution also improved regulatory compliance and allowed the reallocation of resources to revenue-generating activities.

CHALLENGES

The pharmaceutical manufacturer faced significant challenges in securing its OT environment. The primary issue was the use of traditional IT security tools, which were not designed for the unique requirements of OT systems. OT systems, often older and proprietary, prioritize continuous operation over the data confidentiality typically emphasized in IT. This mismatch resulted in a lack of visibility into the OT network, leaving large portions unmonitored and vulnerable.

LACK OF VISIBILITY

This lack of visibility made it difficult to maintain accurate asset inventories and identify potential vulnerabilities. To compensate, the company relied on time-consuming manual processes for asset management, vulnerability assessments, and patching, increasing the risk of human error and delaying crucial security updates.

AT A GLANCE

INDUSTRY
Pharmaceutical Manufacturing

COMPANY SIZE
Fortune 500 global enterprise

LOCATION
Headquarters: Deerfield, Illinois
55 global facilities across multiple countries

CHALLENGES

- Fragmented OT asset inventory
- Manual, error-prone security processes
- Limited visibility into site-specific risks

VERVE'S SOLUTION

- Deployment of Verve Security Center
- Enterprise-wide asset management with risk scoring
- Centralized controls with local execution

KEY OUTCOMES

- 70% reduction in security-related labor costs
- Streamlined, automated threat response
- Comprehensive OT asset and risk visibility

GLOBAL SCALE

The company's global scale, with 55 diverse facilities worldwide, further complicated matters. Maintaining consistent security policies and practices across such a varied landscape proved challenging. The constant pressure to prioritize production uptime also clashed with the need for robust security measures.

STRICT REGULATORY REQUIREMENTS

The pharmaceutical industry's strict regulatory requirements added another layer of complexity. Adhering to strict change control processes to ensure product quality and safety often slowed down the implementation of necessary security measures.

URGENT NEED FOR SECURITY REFORM

All these factors combined hindered the company's ability to respond quickly and effectively to emerging threats. The lack of visibility, coupled with slow manual processes and regulatory constraints, resulted in prolonged response times and extended periods of vulnerability. It also became difficult to prioritize security efforts due to a lack of understanding of the criticality of different assets.

An infrastructure assessment revealed additional vulnerabilities, including inadequate network segmentation, unauthorized remote access, poor access control, and insufficient backups. These findings highlighted the need for a complete overhaul of the company's OT security strategy to address these weaknesses and establish a consistent, robust security framework across all operations.

SOLUTION

To tackle the complex OT security challenges, the pharmaceutical manufacturer partnered with Verve to implement a comprehensive solution. This solution centered on deploying Verve Security Center across all 55 facilities.

VERVE'S UNIQUE APPROACH

Verve's approach stood out during the evaluation process due to its unique Tech-Enabled Assessment (TEA) methodology. This TEA process involves mining deep, contextual data to extract multiple gaps and security issues across people, processes, and technology. By leveraging this comprehensive analysis, Verve demonstrated its ability to address the intricate security landscape of operational technology environments, making it the standout choice for this business partnership.

IMPLEMENTATION PROCESS

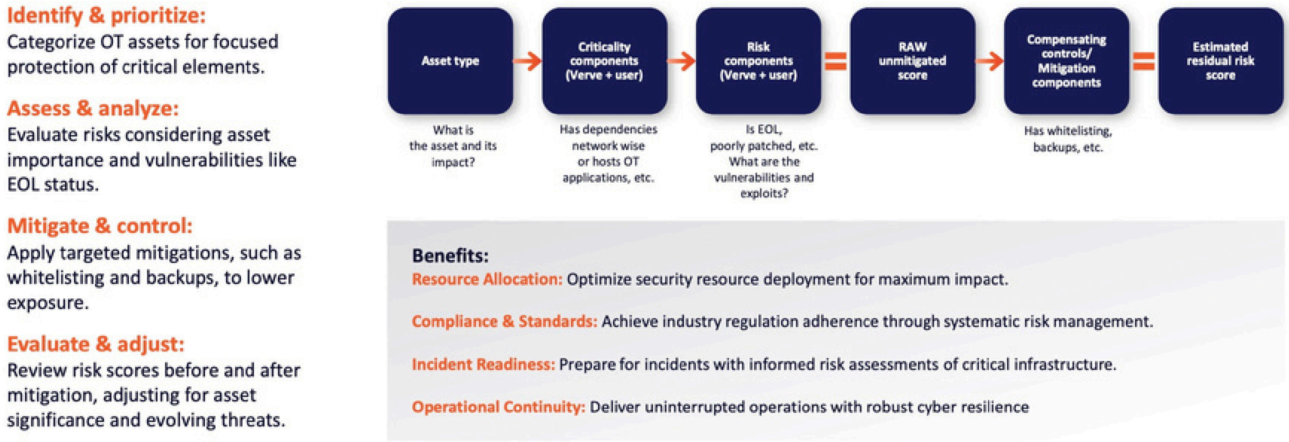
The implementation started with a pilot phase in four production facilities. This initial rollout allowed for a thorough evaluation of the system and informed the development of a detailed roadmap for improvements across people, processes, and technology. The lessons learned from the pilot were then applied to the subsequent rollout to the remaining 52 sites, ensuring a refined and practical approach.

CONTEXTUAL RISK SCORING AND AUTOMATION

Verve Security Center provided the company with a much-needed comprehensive view of its OT assets across the entire enterprise. It offered contextual risk scoring, a feature lacking in the previous fragmented approach, allowing for more effective prioritization of security efforts based on potential operational impact.

The solution also automated many previously manual processes, including inventory management, vulnerability assessments, and patch coordination. This automation streamlined security operations, reducing the risk of human error and freeing up valuable resources.

Contextual Risk Scoring Process



Identify & prioritize: Categorize OT assets for focused protection of critical elements.

Assess & analyze: Evaluate risks considering asset importance and vulnerabilities like EOL status.

Mitigate & control: Apply targeted mitigations, such as whitelisting and backups, to lower exposure.

Evaluate & adjust: Review risk scores before and after mitigation, adjusting for asset significance and evolving threats.

Asset type
What is the asset and its impact?
Criticality components (Verve + user)
Has dependencies network wise or hosts OT applications, etc.
Risk components (Verve + user)
Is EOL, poorly patched, etc. What are the vulnerabilities and exploits?
RAW unmitigated score
Compensating controls/ Mitigation components
Has whitelisting, backups, etc.
Estimated residual risk score

Benefits:

Resource Allocation: Optimize security resource deployment for maximum impact.

Compliance & Standards: Achieve industry regulation adherence through systematic risk management.

Incident Readiness: Prepare for incidents with informed risk assessments of critical infrastructure.

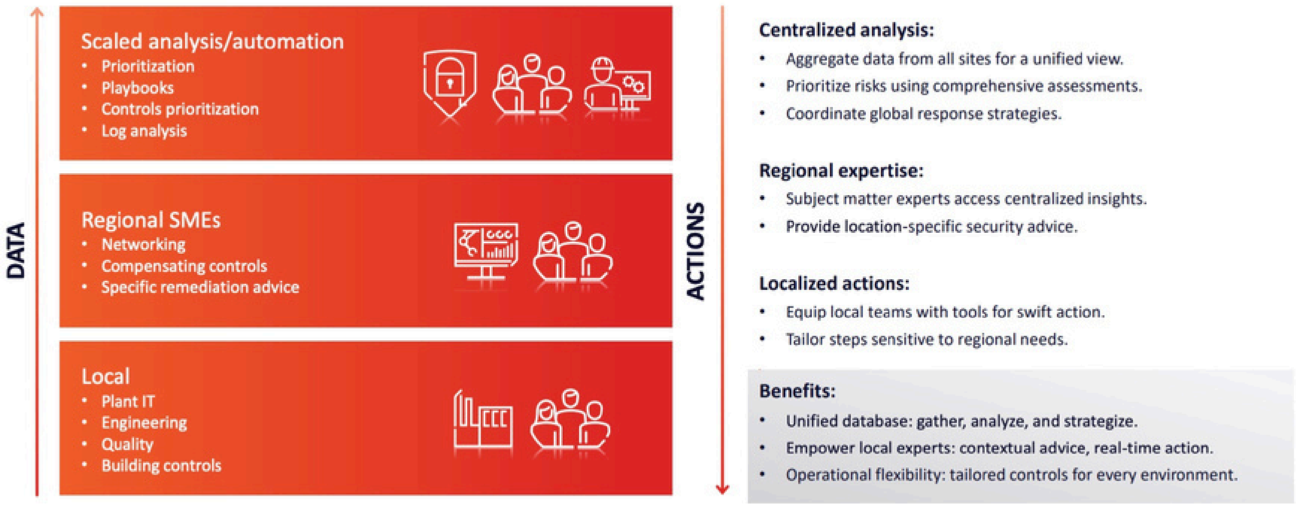
Operational Continuity: Deliver uninterrupted operations with robust cyber resilience

This image outlines Verve's systematic approach to operational technology (OT) security risk management. It illustrates a step-by-step process for identifying, assessing, mitigating, and evaluating risks to OT assets. The workflow progresses from asset identification through risk assessment to mitigation strategies and residual risk evaluation. The diagram also highlights key benefits of this approach, including optimized resource allocation, improved compliance, enhanced incident readiness, and ensured operational continuity. This framework provides a holistic view of how organizations can effectively manage and reduce cybersecurity risks in their OT environments.

THINK GLOBAL, ACT LOCAL APPROACH

A key advantage of the implementation was the balance between centralized control and localized execution, otherwise known as Think Global, Act Local (TGAL). The TGAL approach allowed for coordinated security efforts tailored to each facility's specific needs. For instance, patching schedules could be adjusted to fit each site's maintenance windows, minimizing disruption to production.

THINK GLOBAL, ACT LOCAL APPROACH



Scaled analysis/automation
- Prioritization
- Playbooks
- Controls prioritization
- Log analysis

Regional SMEs
- Networking
- Compensating controls
- Specific remediation advice

Local
- Plant IT
- Engineering
- Quality
- Building controls

Centralized analysis:
- Aggregate data from all sites for a unified view.
- Prioritize risks using comprehensive assessments.
- Coordinate global response strategies.

Regional expertise:
- Subject matter experts access centralized insights.
- Provide location-specific security advice.

Localized actions:
- Equip local teams with tools for swift action.
- Tailor steps sensitive to regional needs.

Benefits:
- Unified database: gather, analyze, and strategize.
- Empower local experts: contextual advice, real-time action.
- Operational flexibility: tailored controls for every environment.

Think Global, Act Local: A Comprehensive Approach to OT Security Management. This image illustrates Verve's multi-tiered strategy for managing operational technology (OT) security across large organizations. It demonstrates how centralized analysis and automation at the top level inform and guide regional subject matter experts (SMEs), who in turn support local teams. This hierarchical structure enables a balance between standardized, enterprise-wide security practices and tailored, site-specific actions. The approach combines the benefits of centralized data analysis with regional expertise and local execution, allowing for both comprehensive risk management and adaptable, context-aware implementation of security measures.

SECURITY ENHANCEMENTS

The deployment also included improvements in network segmentation, access control, and backup capabilities, addressing weaknesses identified in the initial assessment. These enhancements significantly strengthened the overall security of the OT environment.

IMPROVED THREAT RESPONSE

By providing a more efficient and comprehensive approach to threat response, the solution dramatically reduced the time and resources needed to address vulnerabilities. This allowed the organization to react much faster to potential threats, minimizing the window of exposure.

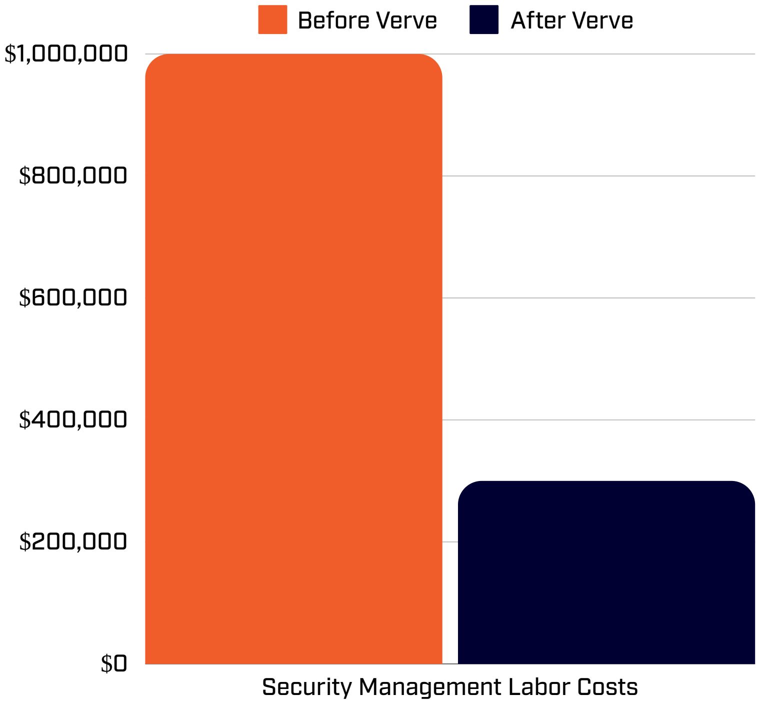
REGULATORY COMPLIANCE

Importantly, the implementation of Verve Security Center was designed to meet the strict regulatory requirements of the pharmaceutical industry. The platform provided robust change management capabilities, detailed audit trails, and comprehensive reporting features, making it easier to comply with Good Manufacturing Practice (GMP) standards and other regulations. This alignment of security practices with existing quality management systems further streamlined the organization's approach to regulatory compliance.

OUTCOME AND BENEFITS

SIGNIFICANT COST SAVINGS

The pharmaceutical manufacturer's implementation of Verve Security Center resulted in substantial improvements. The company saw a significant 70% reduction in labor costs related to security management, saving nearly $700,000 annually. This was achieved by automating previously manual tasks, such as vulnerability assessments and patch management, which had previously cost the company almost $1 million per year.



ENHANCED THREAT RESPONSE

The solution drastically improved the company's ability to respond to emerging threats. Instead of the labor-intensive, multi-day process previously required to address vulnerabilities, the company could now rapidly assess and respond in real-time, thanks to the comprehensive view of OT assets and associated risks provided by Verve Security Center.

IMPROVED VISIBILITY AND RISK MANAGEMENT

The enhanced visibility across the OT environment eliminated blind spots, allowing for proactive security management. The contextual risk scoring feature helped prioritize security efforts, ensuring resources were allocated to the most critical vulnerabilities first.

RESOURCE OPTIMIZATION

The automation of manual processes not only improved accuracy but also freed up significant engineering resources. Staff were able to shift their focus from routine security tasks to revenue-generating activities and innovation, boosting overall productivity.

ROADMAP FOR CONTINUOUS IMPROVEMENT

The implementation also provided a roadmap for continuous improvement in OT security. The detailed, multi-phase plan developed during the project outlined a clear path for ongoing enhancements across people, processes, and technology.

TRANSFORMING OT SECURITY FROM REACTIVE TO PROACTIVE

In summary, the Verve Security Center implementation transformed the company's approach to OT security. It moved the company from a reactive to a proactive stance, significantly reducing cyber risk while improving efficiency and ensuring regulatory compliance.

> *“This implementation marks a pivotal shift for the pharmaceutical manufacturer. With Verve Security Center, they've transitioned from a reactive to a proactive security posture based on contextual risk information, enabling early threat detection and prevention.”*

> **— *R*ick Kaun, VP of Solutions**
> **Verve Industrial**

READY TO TRANSFORM YOUR OT SECURITY?

Discover how Verve Security Center can help your organization transition from reactive to proactive security, reduce costs, and ensure compliance. Our experts are ready to guide you through your OT security transformation.

CONTACT US

To learn more, visit www.verveindustrial.com or contact us at info@verveindustrial.com