VERITI

VERITI FOR MANUFACTURING

AUTOMATED SECURITY CONTROL OPTIMIZATION

Proactively monitor and remediate security gaps and misconfigurations across your security stack, without sacrificing business uptime.

Today, production methodologies have undergone a transformative shift, embracing flexibility, customization, and cost-effectiveness. This evolution, driven by the integration of Operational Technology (OT), Information Technology (IT), Internet of Things (IoT), automation, and digital transformation, has heralded unprecedented opportunities for enhanced efficiency and productivity. However, within this landscape of progress lies a challenging terrain of cybersecurity concerns and unparalleled cyber risks.

Concealed within the intricate fabric of modern manufacturing operations are hidden vulnerabilities and security gaps that lurk in the shadows, awaiting exploitation. These latent threats, coupled with the everyday risks stemming from network or process misconfigurations, operational oversights, and resource utilization spikes, collectively cast a looming shadow over the productivity and security of manufacturing organizations.

WHY SECURITY FOR MANUFACTURING IS SO CHALLENGING

The challenge of OT security revolves around the delicate balance between vulnerabilities and a shortage of cybersecurity talent. As operational technology and IoT assets grow exponentially, the scarcity of specialized experts hinders the effective identification and management of vulnerabilities. Relying on manual assessments, while necessary, can be time-consuming and prone to errors. Business continuity is at stake as traditional vulnerability mitigation methods can disrupt critical infrastructures. Moreover, the ever-present threat of downtime due to daily misconfigurations and operational errors poses a significant risk to productivity, often overshadowing external cyberattacks. Distinguishing between genuine threats and false positives is crucial to maintaining operational efficiency, as an influx of false positives can lead to unnecessary disruptions. In essence, the challenge of OT security involves these interconnected issues of talent shortage, business continuity, downtime, and accurate threat assessment.

2,170
INDIVIDUAL CVES AFFECTING ICS AND OT

56
VULNERABILITIES DISCOVERED IN OT PRODUCTS FROM 10 DIFFERENT VENDORS

56%
HAVE OT DEVICES CONNECTED TO THE INTERNET AND 51% HAVE THE OT NETWORK CONNECTED TO THE IT NETWORK

VULNERABILITIES

BUSINESS CONTINUITY

TALENT SHORTAGE

EMERGING THREATS

VERITI

VERITI'S AUTOMATED SECURITY CONTROL OPTIMIZATION

Veriti provides a consolidated security platform that seamlessly integrates with your existing security infrastructure, enabling proactive assessment and monitoring for hidden gaps and misconfigurations across the entire security stack. With Veriti, you can move beyond subjective assessments and embrace data-driven security measures, ensuring unwavering confidence in your organization's security resiliency. It automatically analyzes, detects, triages, and remediates security gaps while ensuring zero business disruptions.

By addressing risks, ensuring business continuity, fostering cross-team collaboration, and mitigating false positives, Veriti delivers tangible value to organizations in the manufacturing sector.

KEY FEATURES

Virtual Patching - Rapid response to mitigate known and emerging threats across all security solutions.

IoT Vulnerability Mitigation - Seamlessly integrates with your IoT fabric, identifying vulnerabilities across devices and sensors.

Zero False Positives -Simplify investigations, identify high-risk events, and dramatically lower Mean Time to Remediate (MTTR).

KEY BENEFITS

PROACTIVE HARDENING OF OT DEVICES

Veriti assesses, identifies gaps and automatically creates a remediation plan to reduce risk to OT devices and systems

ULTRAPRACTICAL INTELLIGENCE

Convert threat intelligence to action – consolidating data from all vulnerability assessment tools into one unified platform.

NON-DISRUPTIVE REMEDIATION

With a single click, Veriti enables organizations to swiftly address vulnerabilities and security gaps without causing disruptions to critical business operations.