servicenow

3 steps to secure the digital factory

Drive a stronger security posture with OT management

servicenow

Contents

Bridging IT and OT for a future-ready, secure manufacturing ecosystem

The convergence of IT and operational technology (OT) systems has fundamentally altered the security landscape for manufacturers.

In the age of IIoT (industrial internet of things), the factory is more connected and automated than ever. Manufacturers are using IIoT to inspire growth and drive widespread efficiencies at scale, but this requires rethinking their approach to security to thrive in the new digital landscape.

As complex IT and OT systems converge, new attack vectors are laid bare, exposing vulnerable OT systems. Because IT security enjoys more advanced treatment at a higher priority, OT security often doesn't receive the same level of attention and investment. The OT threat landscape is also an uncharted one, requiring a completely different mindset and approach to security and risk management.

What's more, OT failure isn't always due to a malicious breach. An inadvertent employee error can cause an entire factory to shut down.

The consequences of any OT failure or breach can be severe. A halt in production can cost millions of dollars per hour, not to mention the serious risk to employee safety. An OT failure can damage not only the factory floor but also the entire enterprise, by allowing hackers a gateway into IT operations.

How, then, can manufacturers identify and prevent potential breaches to counter the increased sophistication of attackers? Success relies on a fundamental shift in their approach to OT security, from both technological and operational mindsets. Only then can OT and IT security work together to form a complete, robust, and resilient risk posture across the entire enterprise.

64%

of organizations rate the level of OT risk they face as high, but only 33% have made significant progress toward improving OT asset security. [ServiceNow]

servicenow

Why are manufacturers struggling to secure OT?

OT and IT convergence has matured significantly over the past 20 years, yet there are still inherent differences—namely, IT being managed at enterprise level and OT security governed locally in the factory or on-site.

Encouragingly, the two share many best practices—such as refining risk visibility, prioritizing vulnerabilities, and mitigating security instances—meaning manufacturers must calculate which tactics from their IT environment will translate best into an OT security setting and where they must invest in skilled OT security teams and new technologies.

Success relies on a uniform strategy across OT and IT to safeguard devices, and this change management starts at the C-suite with tighter collaboration between the CIO and CSO.

However, significant challenges remain. For example, the rise of remote access to OT networks through third-party vendors expands the attack surface and creates even more vulnerabilities.

When it comes to security tools to harden attack surfaces and thwart attackers, manufacturers have many options. However, overinvestment in security tools often creates more alerts for staff to investigate—an additional challenge when security experts are already in short supply.

Overall, manufacturers are less aware of the OT security risks within their organization. As a result, OT just doesn't enjoy the same budget or investment as IT security.

Often, teams must rely on cumbersome and time-consuming manual processes to manage security. Many manufacturers still use spreadsheets to manage OT security—one of many manual measures that simply cannot scale to the demands of modern digital manufacturing.

Here, we explore three critical steps manufacturers can take to secure the digital factory and enterprise with a connected OT and IT security strategy.

72%

of organizations making the most significant progress improving OT security manage OT and IT assets together. [ServiceNow]

YET

Only 37%

of manufacturers are targeting improvement or investments to increase joint governance of OT and IT security. [ServiceNow]

1 Know what you need to protect

To avoid unplanned downtime, keep costs low, and secure assets, manufacturers must possess a single, integrated view of their IT and OT estates in one unified location.

However, OT environments are complex—layering legacy and new connected technologies over time—with hundreds of different technologies on the factory floor, such as robotic arms, HMIs, SCADA systems, and sensors.

Know how OT and IT asset relationships impact your vulnerability

True visibility goes well beyond asset lists, helping manufacturers determine exactly which devices are in play and how they're communicating. One device has the potential to bring down an entire factory.

Manufacturers can use a singular data model to discover not only OT assets through industrial security integrations, but also IT assets within OT environments. This way, they can aggregate data from various sources into a multisource CMDB (configuration management database) while still meeting the highest industry standards.

Using this class model, CMDBs build and map visual representations of OT and IT assets, defining the relationships between them across different levels of critical infrastructure and how each asset ties into the production line.

Contextual visibility helps manufacturers to assess potential production impacts faster, helping untangle the web of visible—and often invisible—dependencies between devices, applications infrastructure, and third-party integrations.

44%

of manufacturers have real-time or precise inventory and visibility of OT assets. [ServiceNow]

2 Find and prioritize your vulnerabilities

For manufacturers looking for OT weaknesses, it quickly becomes overwhelming to interrogate all infrastructure, cloud technology, and applications—largely because multiple scanners and teams are often involved.

Prioritizing what to patch is key, and threat intelligence represents one of the most effective methods. With only 2% to 7% of published vulnerabilities exploited in the wild, manufacturers must prioritize weaknesses with known exploits. Importantly, they need to do this before a breach occurs.

Assess weaknesses at the asset or factory level with risk scores

Risk scores add vital business context to any potential OT and IT vulnerabilities, determining the importance of particular assets and calculating the potential impact on production.

A CMDB brings together all asset information, automatically triaging the data in order to process and prioritize each insight. Manufacturers can easily see which assets require immediate attention by automatically factoring in contextual asset information—including hardware, criticality, and other attributes.

Remember, though, every organization is different. The right platform and service provider uses a prioritization calculator to focus on what's most important to each individual manufacturer—whether that's vulnerabilities on premises, in the cloud, in applications, or in OT devices.

Only 39%

of manufacturers are targeting investments or improvements to prioritize threats based on business impact. [ServiceNow]

3 Remediate efficiently with end-to-end service management

To mitigate vulnerabilities and prevent OT security breaches, manufacturers should connect automated, digital workflows to their production processes.

Doing this through a single platform, especially one that uses machine learning to group and assign tasks to the appropriate people across OT and IT teams, increases efficiency.

Issues are prioritized and assigned to the correct people for remediation—and a single, accessible system makes it easy to manage all vulnerabilities, regardless of the source.

By automatically identifying vulnerabilities, remediation teams can also streamline decisions and speed up the resolution process.

Power your operational resilience with a centralized platform

Workflows are a vital part of the remediation process, supporting change management, incident management, and new installations.

Digital workflows help manufacturers to plan, expedite, and automate the proactive maintenance, change management, and threat response of OT and IT ecosystems.

A single platform serves as a single point of action: all parties have access to real-time information on every alert, including its level of significance and how to resolve it.

With IT and OT security working together on the same platform, each task possesses a tracked service-level agreement (SLA), making it almost impossible for jobs to slip between the cracks.

According to the 2023 ServiceNow and Dynata global survey of 1,900 manufacturing leaders, implementing or automating end-to-end service management is the highest reported area manufacturers aim to target reduce OT risk.

42%

of manufacturers are targeting investments or improvements in automating end-to-end service management and change management. [ServiceNow]

Only 35%

of manufacturers report significant progress in proactive vulnerability response. [ServiceNow]

Secure your digital factory and enterprise

As the attack surface grows, it's no surprise that many teams are overwhelmed trying to keep up. To have a successful, proactive security program across the enterprise, manufacturers need to integrate OT and IT strategies and teams involved to see the bigger picture and understand risks.

Workflows and automation help teams work effectively to prioritize and remediate issues before they breach. A single platform enables manufacturers to combine their data, technology, and teams, helping everyone work faster to mitigate risks across OT and IT.

Learn more about OT management

It all starts with OT management at ServiceNow. We're already building the future of manufacturing with digital workflows on a single, unified platform. We're now extending these benefits to the OT world.

Our ServiceNow® Operational Technology Management product helps you prevent factory downtime by enabling you to see, strategize, and protect your operational technology. Unlocking OT visibility in this way, our single system of action empowers manufacturers to lower operating costs, quickly resolve security issues, and act with confidence.

By streamlining the overall process, ServiceNow allows manufacturers to confidently navigate the challenges of a hyperconnected era. With ServiceNow, you're not just secure; you're future-ready.

To learn more about how ServiceNow can help you improve your OT management, please visit **www.servicenow.com/otmanagement**.

The world's most powerful platform for automating work

The Now Platform® includes generative AI, machine learning frameworks, natural language understanding, search and automation, and analytics and process mining that work together to seamlessly enhance employee abilities and customer experiences. Generative AI uses computer algorithms to generate outputs in a variety of content forms—unlocking near-limitless use cases for the Now Platform.

For manufacturers looking to ensure uptime and empower factory teams, generative AI on the Now Platform can:

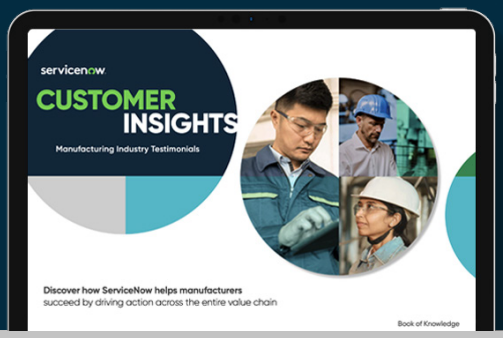
- Personalize and approve checklists for production workers based on SOPs and manuals.
- Help mitigate factory floor downtime with assistants that help with requests and asset management tasks.
- Generate remediation playbooks based on input from factory floor workers and approval from SMEs.

For a deeper exploration of ServiceNow solutions, we recommend the following content:

Customer insights—manufacturing industry testimonials

Discover the manufacturing strategies our customers are implementing to achieve business outcomes, and drive action across the entire value chain.

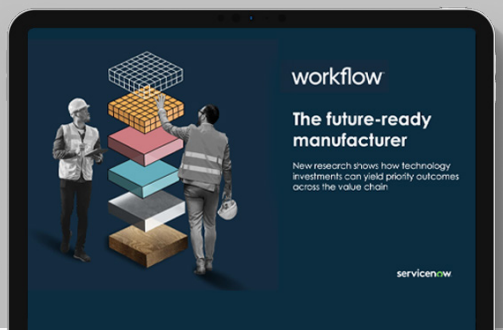
Read Ebook



The future-ready manufacturer report

Gain access to insights from over 1,900 manufacturing leaders, and discover how manufacturers can harness technology investments to navigate present and future macro challenges.

Read Report



About ServiceNow

ServiceNow (NYSE: NOW) makes the world work better for everyone. Our cloud-based platform and solutions help digitize and unify organizations so that they can find smarter, faster, better ways to make work flow. So employees and customers can be more connected, more innovative, and more agile. And we can all create the future we imagine. The world works with ServiceNow™. For more information, visit www.servicenow.com.