servicenow

GLOBAL SURVEY INSIGHTS

How future-ready manufacturers manage OT risk

Ensure your OT security is up to the task

servicenow

Contents

Executive summary

Securing operational technology in the face of increasing cyber threats

The convergence of operational technology (OT) and IT has increased security risks for manufacturers—and while IT security is on the radar, OT security is often left behind.

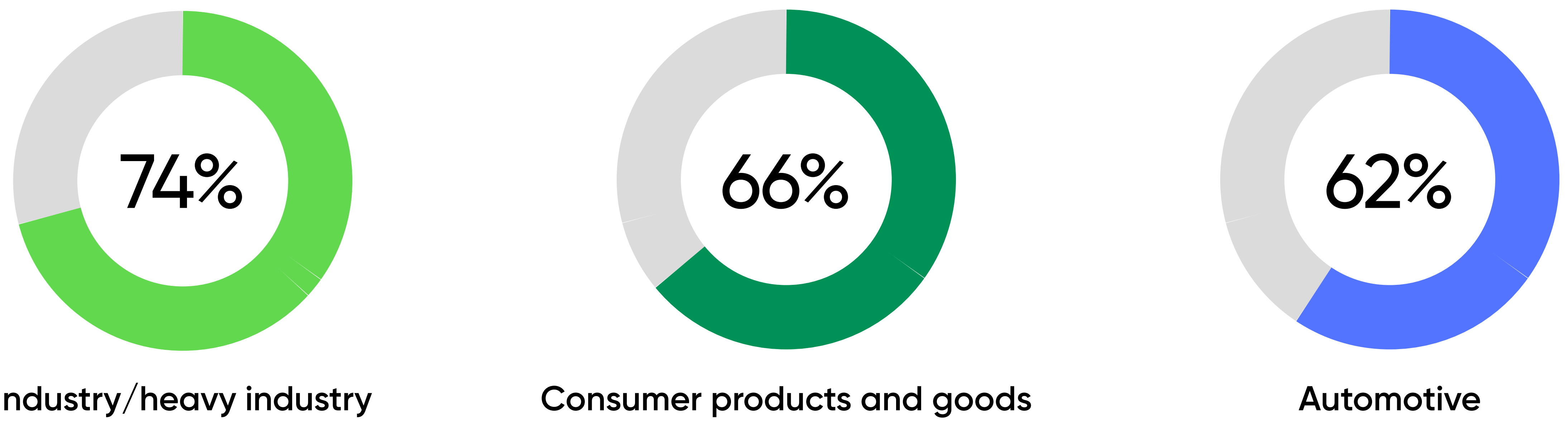
To secure your enterprise, a dual focus on both OT and IT security is imperative.

While IT skills are essential, they cannot seamlessly be transferred to OT environments—therefore, a comprehensive security strategy must include developing best practices and investing in tools across teams to effectively manage their landscape.

In 2023, ServiceNow led a survey of 1,900 manufacturing leaders globally to uncover the level of OT risk manufacturers face, levels of progress in reducing risks, barriers to progress, and how leaders are implementing winning strategies to increase resilience.

Our research shows that manufacturers need fundamental alignment between OT and IT security teams to ensure enterprisewide security. They must also invest in emerging OT technologies to advance proactive vulnerability response.

Top 3 sub-verticals that rate a “high” OT security risk in the next two years



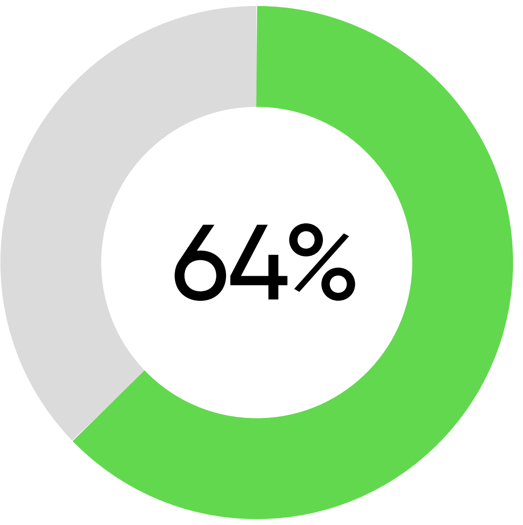
> **“Businesses must make significant investments in cybersecurity protection of their networks and data as they increasingly rely on digital tools.”**
>
> Chief Technology Officer, Automotive Manufacturer, Germany

A high focus on improving OT security but progress is limited

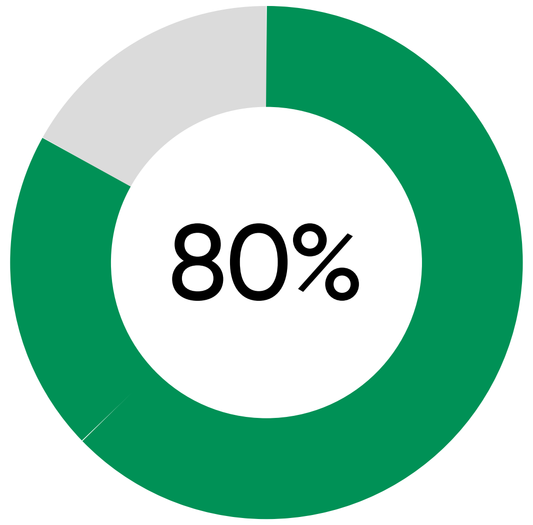
The high stakes of OT security

Globally, 64% of manufacturers say they face a high risk in OT security. OT risk is not news to manufacturers. Incredibly, 80% of respondents in our survey place a high priority on improving OT security. However, more must be done to manage risks, as only one-third (33%) of respondents have made significant progress securing their OT systems.

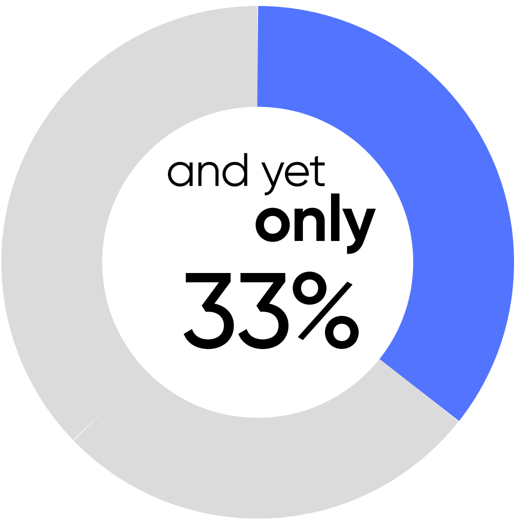
Manufacturers are investing in OT security, but progress does not match ambitions



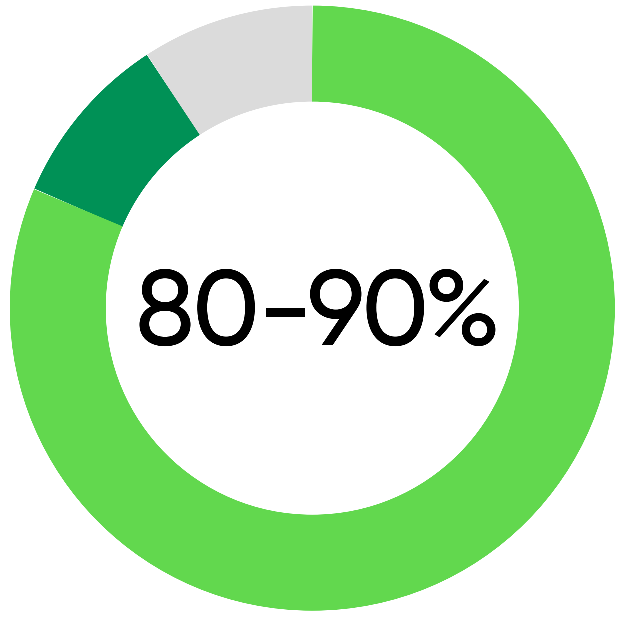
rate the level of OT security risk they face as high.



have a high level of focus or investment on improving OT security.



have made significant progress improving the security of OT assets.



C-suite spotlight

80-90% of CIOs/CTOs/COOs place a high to very high focus on investing or improving OT security

servicenow

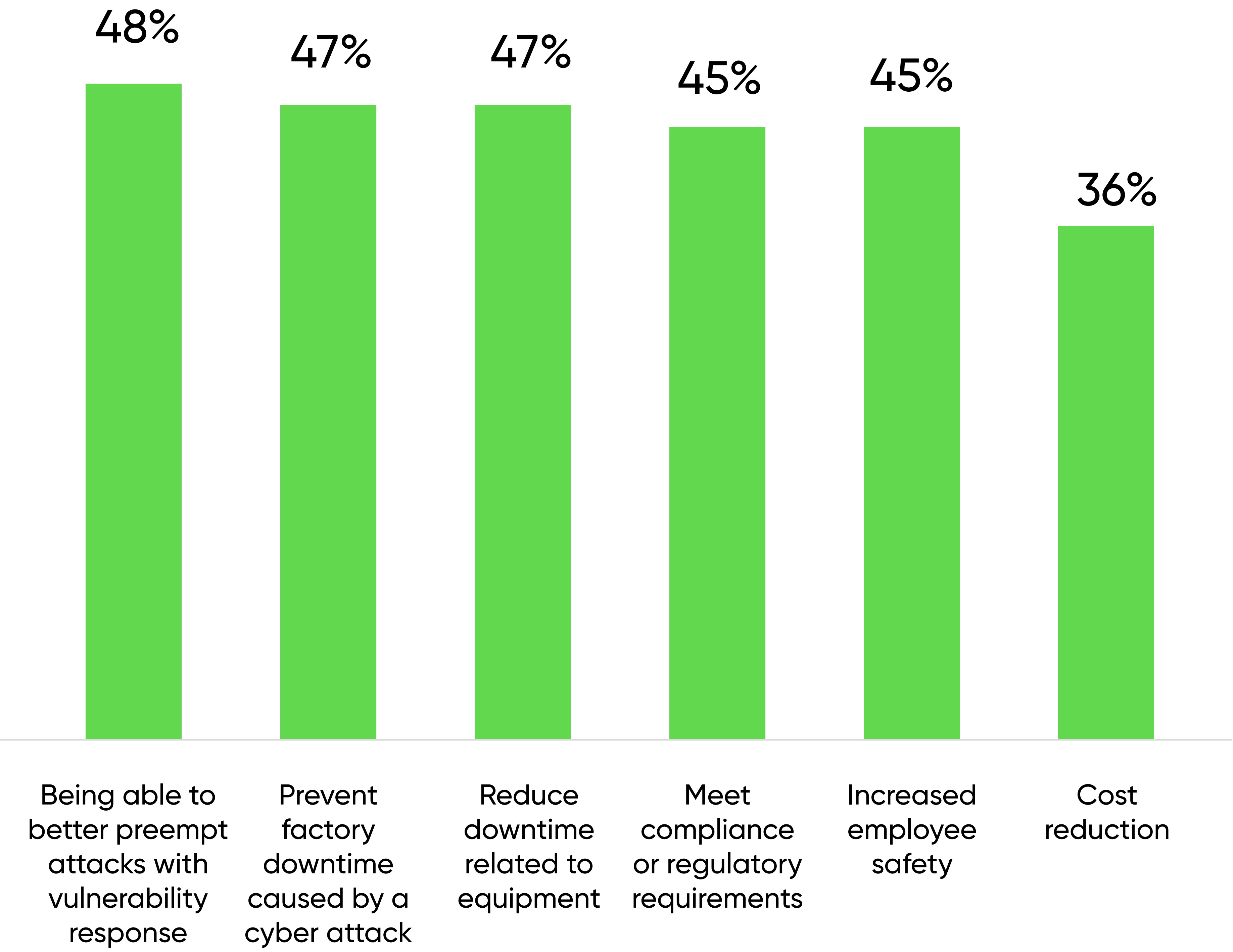
Proactive vulnerability response and reducing downtime are top priorities for manufacturers

Unplanned downtime caused by a breach can cost hundreds of thousands of dollars, impacting productivity and profitability. But a breach can be even more disastrous.

Attacks on critical services and infrastructure that rely on OT—such as emergency services, water treatment plants, and traffic management—can lead to severe economic damage. When these operations are at risk, so are the lives of workers and the public. As OT technology advances, manufacturers recognize they must proactively preempt attacks to reduce risks.

Prioritized outcomes from improving OT security

(% of total)



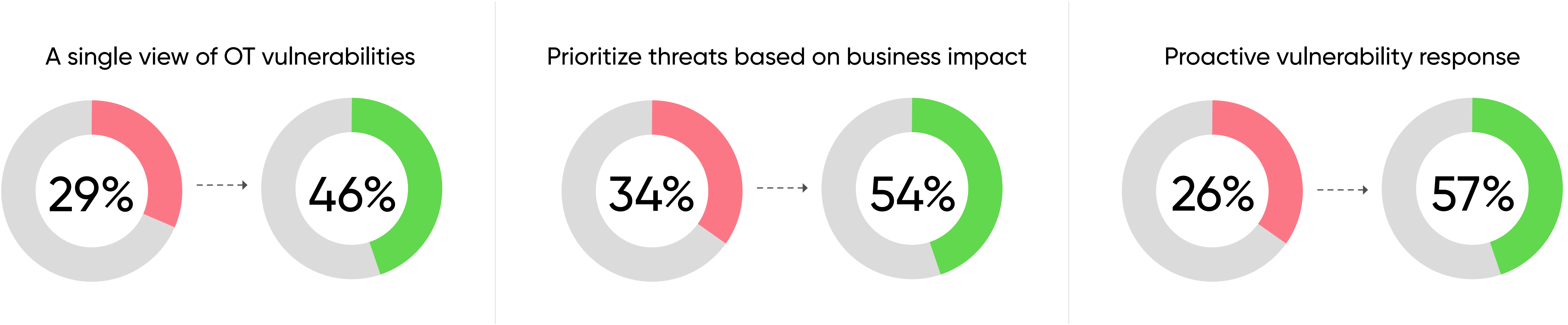
You can't protect what you can't see

Visibility of vulnerabilities is paramount to building a resilient OT security strategy. Without visibility into threats, proactive resolution will be prevented. When a breach does occur, manufacturers often cannot quantify the impact. In some instances, manufacturers may not even understand how the breach happened or how to resolve it.

Despite evidence of increased visibility of threats and vulnerability response, numbers are still low

Our research shows that overall, just over one-third (35%) of survey respondents say they've made significant progress in achieving a single, comprehensive view of all OT vulnerabilities. Only 36% say they have made considerable progress in proactive vulnerability response.

Leaders vs. laggards: Significant progress reported in the following areas



Laggards: Manufacturers that report none to some progress improving the security of their OT assets

🟥 Laggards 🟩 Leaders

Leaders: Manufacturers that report significant progress improving the security of their OT assets

Top 3 reported barriers to improving OT security:

- Lack of know-how, skills, and talent
- Organizational silos
- Lack of data analytics to inform business decisions

33%

of manufacturers still use spreadsheets to manage OT security.

OT and IT. Better together.

Manufacturers making the most progress improving OT security have something in common: They are more likely to embrace the convergence of OT and IT. Seventy-two percent of respondents who have significantly boosted their OT security manage OT and IT assets together and show increased capabilities across OT security.

Know your OT and IT assets and how they interact

Manufacturers need visibility of their OT assets before they can identify vulnerabilities. But OT environments are complex. There are hundreds of different technologies on the factory floor creating potential blind spots across your OT and IT landscape.

Gaining a full, contextual view of the interdependencies between all OT and IT assets in production is the first step to identifying underlying causes of issues and potential vulnerabilities.

72%

of respondents who have significantly boosted their OT security manage OT and IT assets together.

Where do manufacturers see opportunities to improve OT security?

Automate end-to-end OT service management. This is the top reported improvement area for manufacturers. Using automation and intelligent routing, manufacturers can accelerate vulnerability response and change management to proactively resolve vulnerabilities before a breach happens. Yet, only 37% of manufacturers report they are currently using automation to improve OT security.

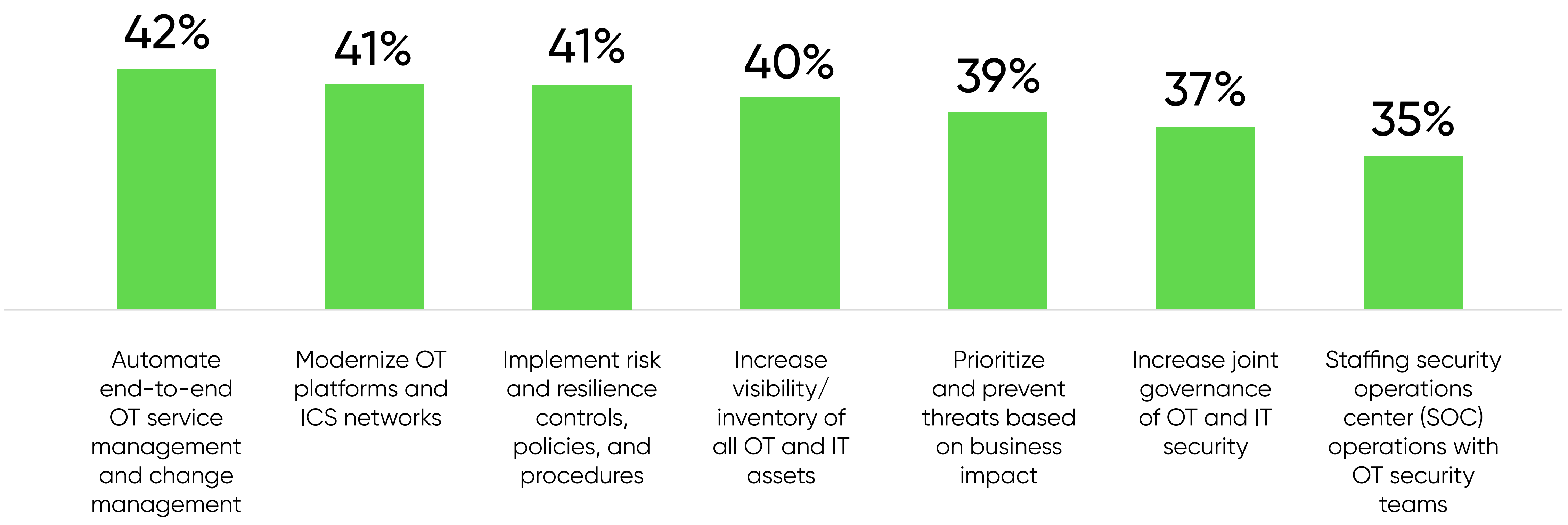
Increased visibility across OT and IT. Even though leaders are more likely to manage OT and IT assets together, only 40% of manufacturers recognize the need to increase visibility of all OT and IT assets to improve security.

Prioritize threats based on business impact. Ensure you fix critical vulnerabilities first. Manufacturers need to gauge and prioritize the security vulnerabilities that need immediate attention.

Manufacturers also recognize that modernizing OT platforms remains vital and helps to reduce the risk of legacy technology that pose vulnerabilities.

Improvement targets in OT security to reduce risk

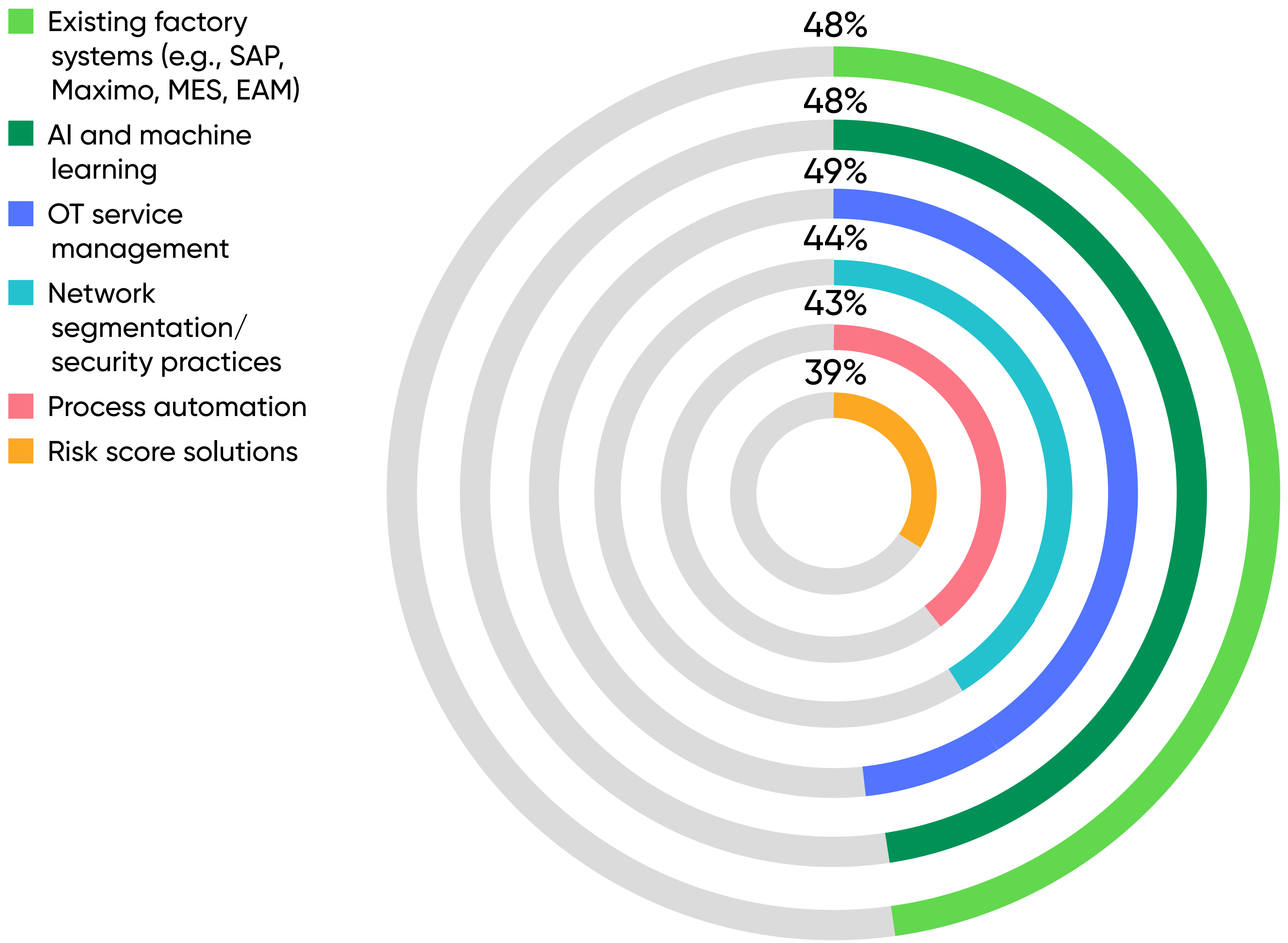
(% of total)



Leaders lean into technology

Our research shows that manufacturers making the most progress improving OT security are more likely to leverage AI and machine learning, OT service management, and process automation.

Digital technology solutions currently utilized to increase OT security



Karan Shrivastava

Director, Product Management, ServiceNow

Bridging the gap between OT and IT security

What you can't see you can't protect, making it difficult to put together any security boundaries. For convergence with IT, there are best practices that have matured over the last couple of decades, yet there is an inherent difference. IT is managed at an enterprise level, while OT is managed at a factory or a site level. At the same time, for visibility, prioritizing vulnerabilities and mitigating security instances—the best practices remain the same. Customers should look at the IT environment to figure out what works to incorporate on the OT side.

Many manufacturers today find it imperative for the offices of CIOs or CSOs to figure out a uniform strategy across OT and IT to safeguard devices, which begins at the C-suite level from a strategy and vision perspective.

We have seen many different best practices from manufacturing customers, but there can be inherent confusion about OT and IT convergence with respect to security. One of the most common questions we get is, "Do I need to merge my OT and IT department to obtain the level of convergence required in the industry?" and the answer is "no". It's about adoption of best practices between OT and IT to better secure your OT environment.

To overcome some challenges with OT and IT security integration, manufacturers must determine what their internal best practices are. From OT and IT domain separation, visibility, or on a single pane of glass, incidents or changes attacking assets and vulnerabilities—those differences must be identified early.

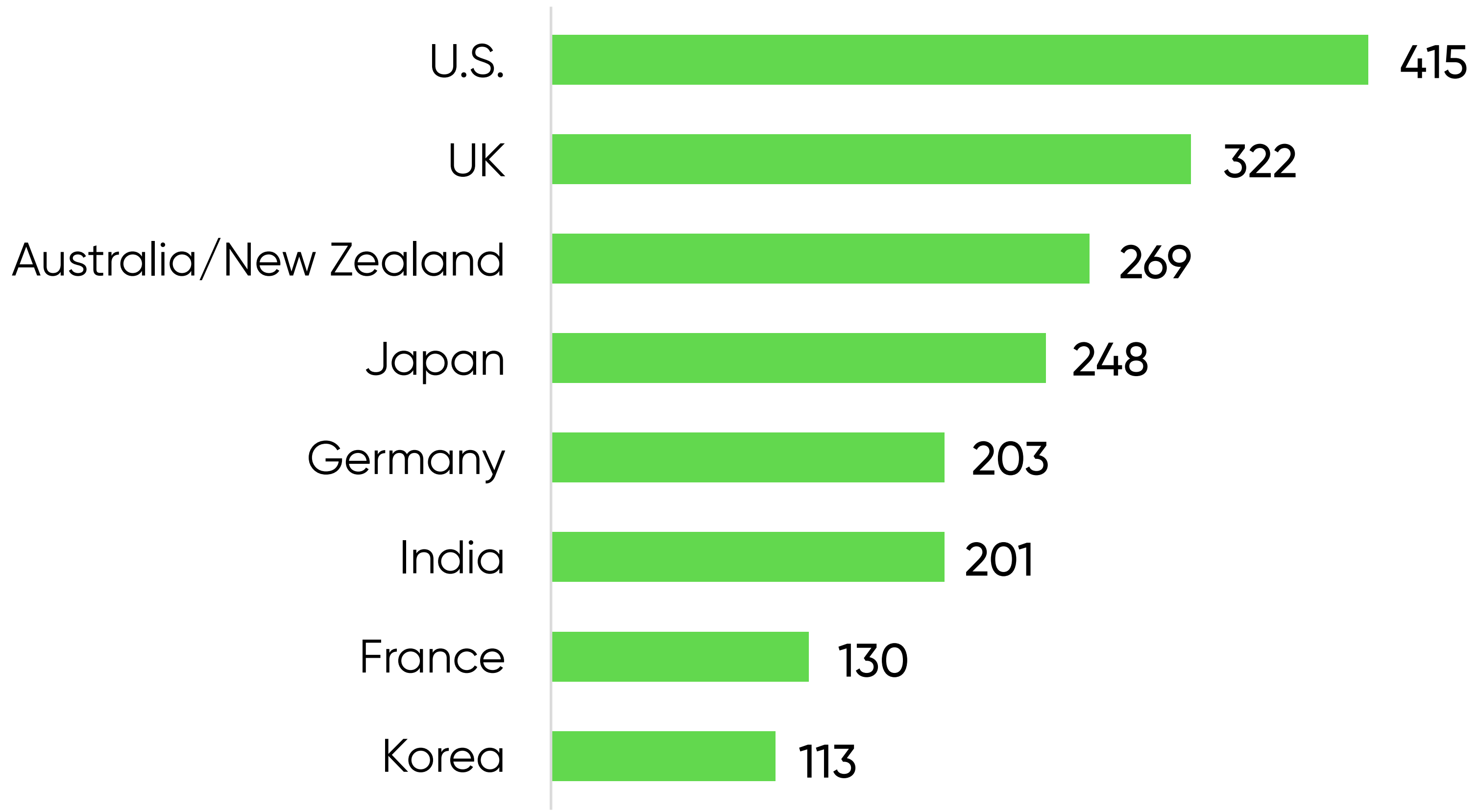
About this study

ServiceNow engaged Dynata to conduct a global survey of manufacturing executives, evaluating how manufacturers are leveraging digital transformation to drive outcomes and manage macro uncertainty across the value chain.

Methodology

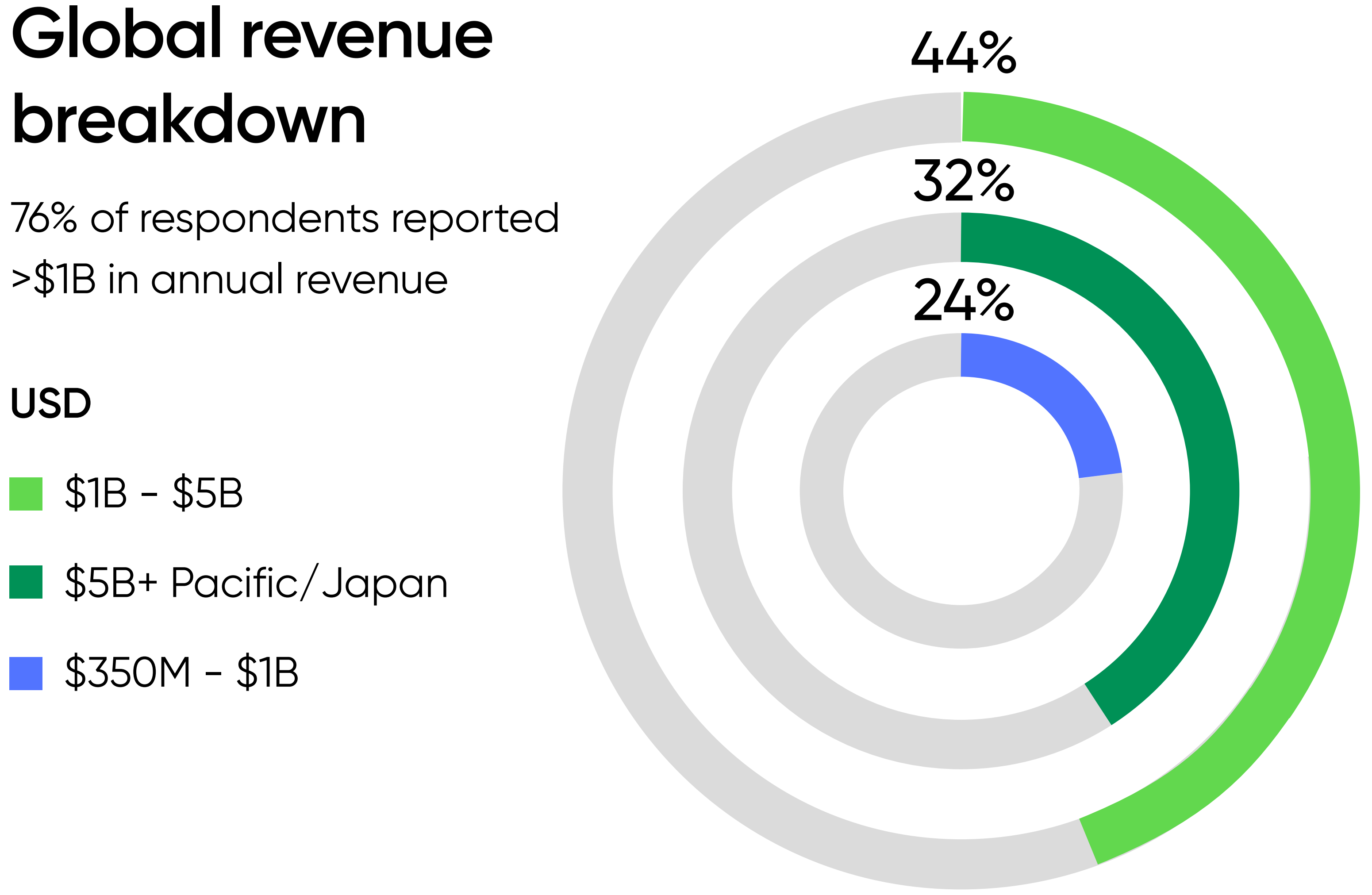
Survey responses from 1,901 respondents were collected via online surveys conducted between March 13 and April 13, 2023.

Global respondents

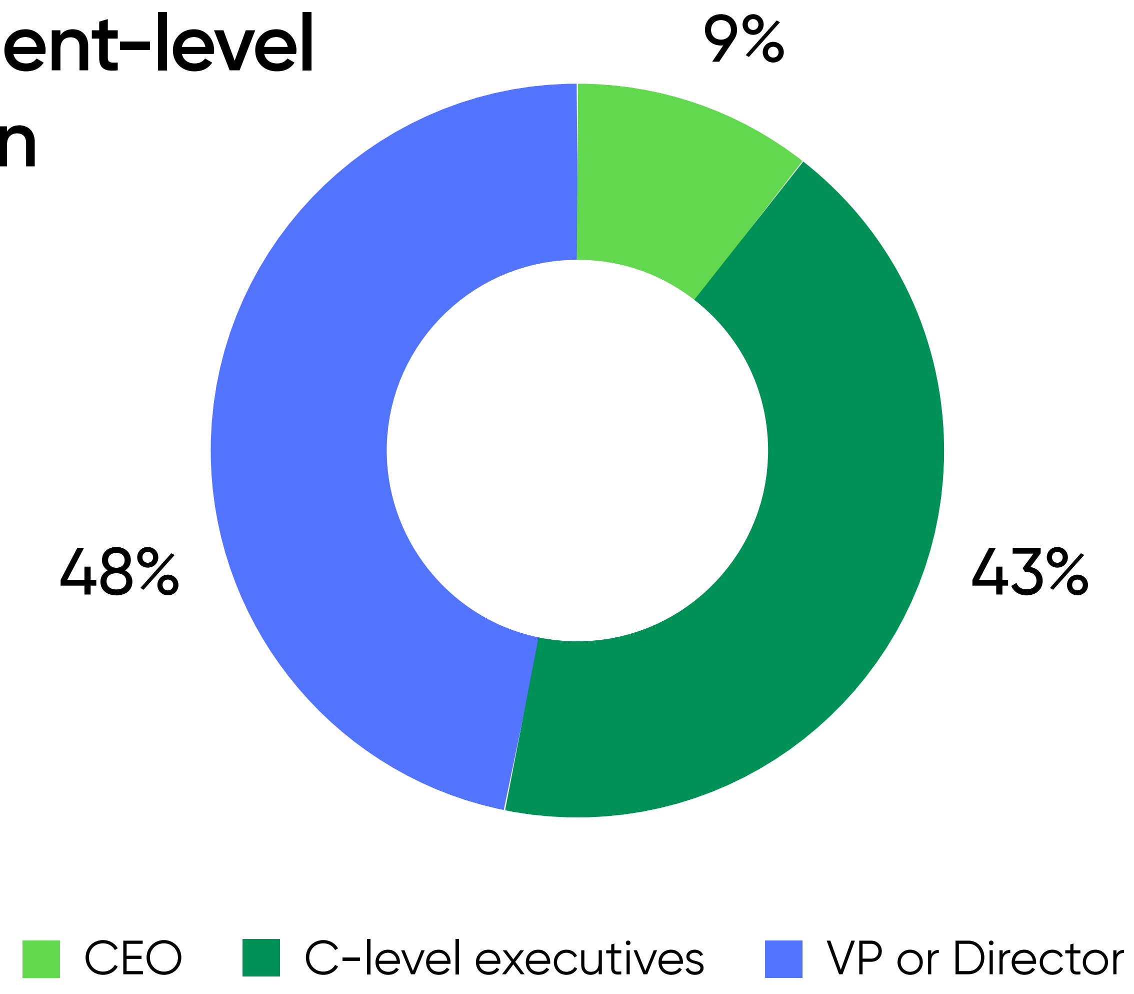


Global revenue breakdown

76% of respondents reported >$1B in annual revenue

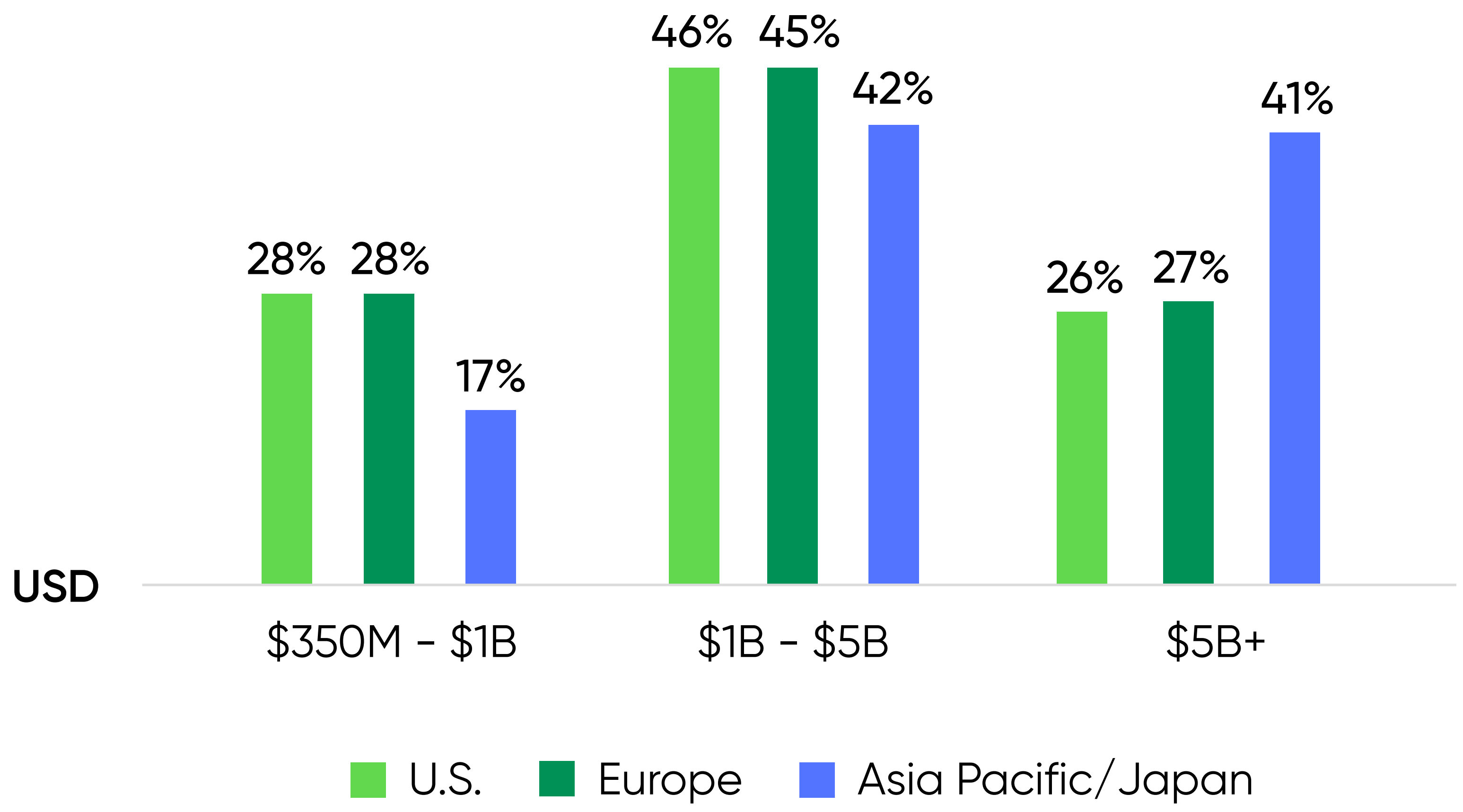


Management-level breakdown



C-level executives: COO, CFO, CIO, CTO, CISO, CHRO, CRO

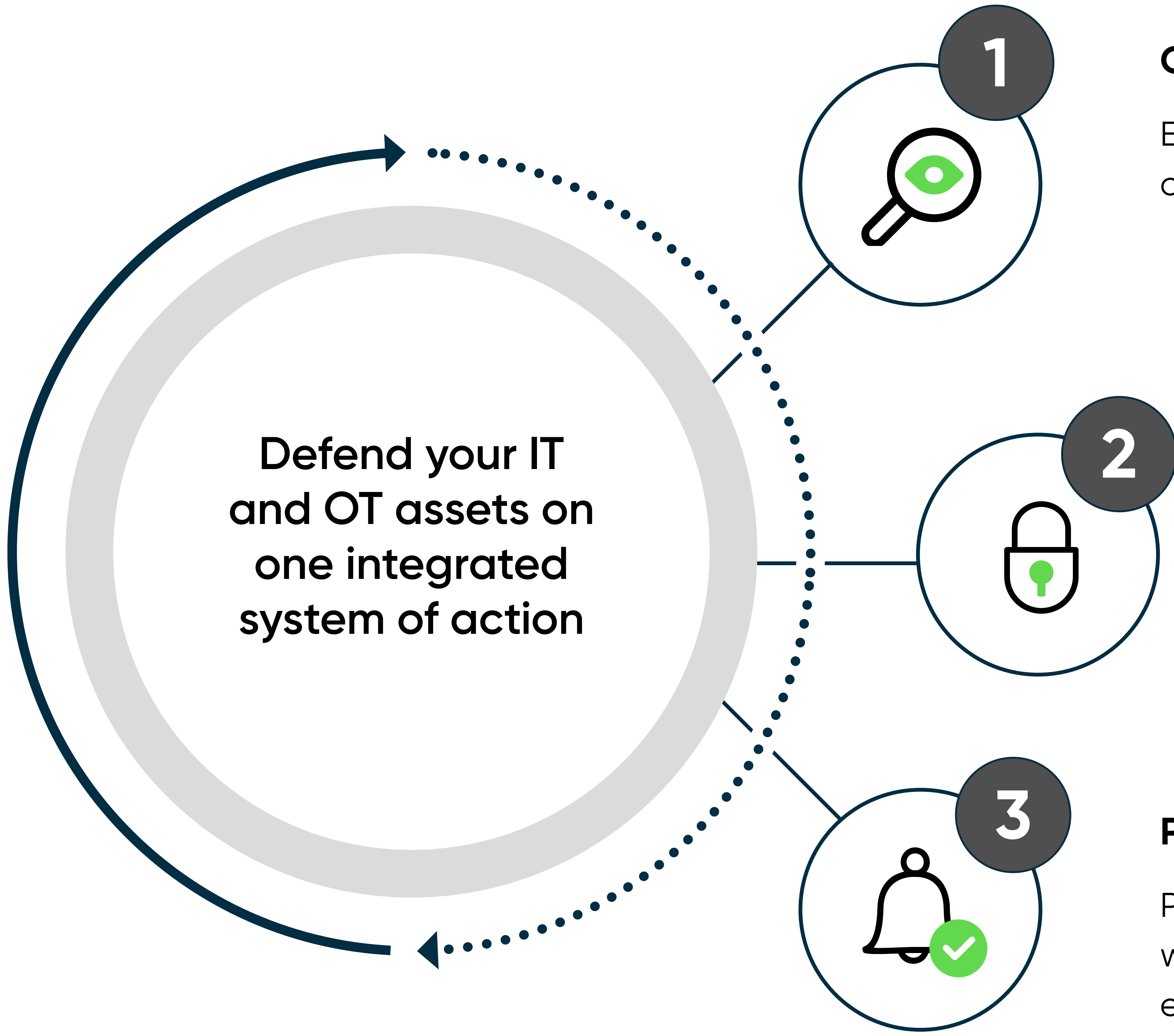
Regional revenue breakdown



servicenow.

Secure your digital factory and manufacturing enterprise

ServiceNow is a single system of action that enables you to drive enterprisewide security starting with end-to-end visibility of the OT and IT ecosystem.


Defend your IT and OT assets on one integrated system of action
1
2
3

Gain visibility into your IT and OT environment

Eliminate blind spots with a complete, contextual view of all IT and OT assets and any interdependencies.

Assess the vulnerability of your environment

Identify, assess, and prioritize security vulnerabilities to maintain system security and availability.

Proactively manage and respond to OT risks

Prevent costly downtime by connecting operations with production processes and digital workflows that expedite and automate threat response.

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:

3 steps to secure the digital factory

The convergence of IT and operational technology (OT) systems has fundamentally altered the security landscape for manufacturers. Read this ebook to learn how manufacturers can identify and prevent potential breaches to counter the increased sophistication of attackers.

Read Ebook

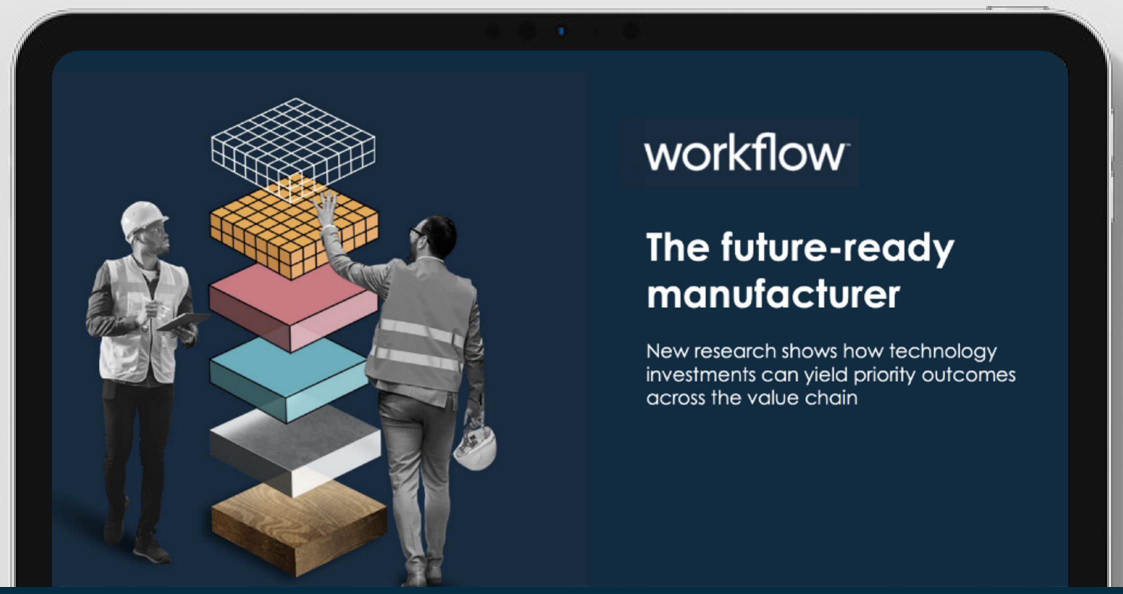
servicenow.

3 steps to secure the digital factory

The future-ready manufacturer

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 Ebook



workflow

The future-ready manufacturer

New research shows how technology investments can yield priority outcomes across the value chain

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

servicenow

CUSTOMER INSIGHTS

Manufacturing Industry Testimonials

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.