GlobalData.

SUMMER 2023

End-to-end management across your IT and OT estate

AUTHORS

David Bicknell, GlobalData

SPONSORED BY

TANIUM

Contents

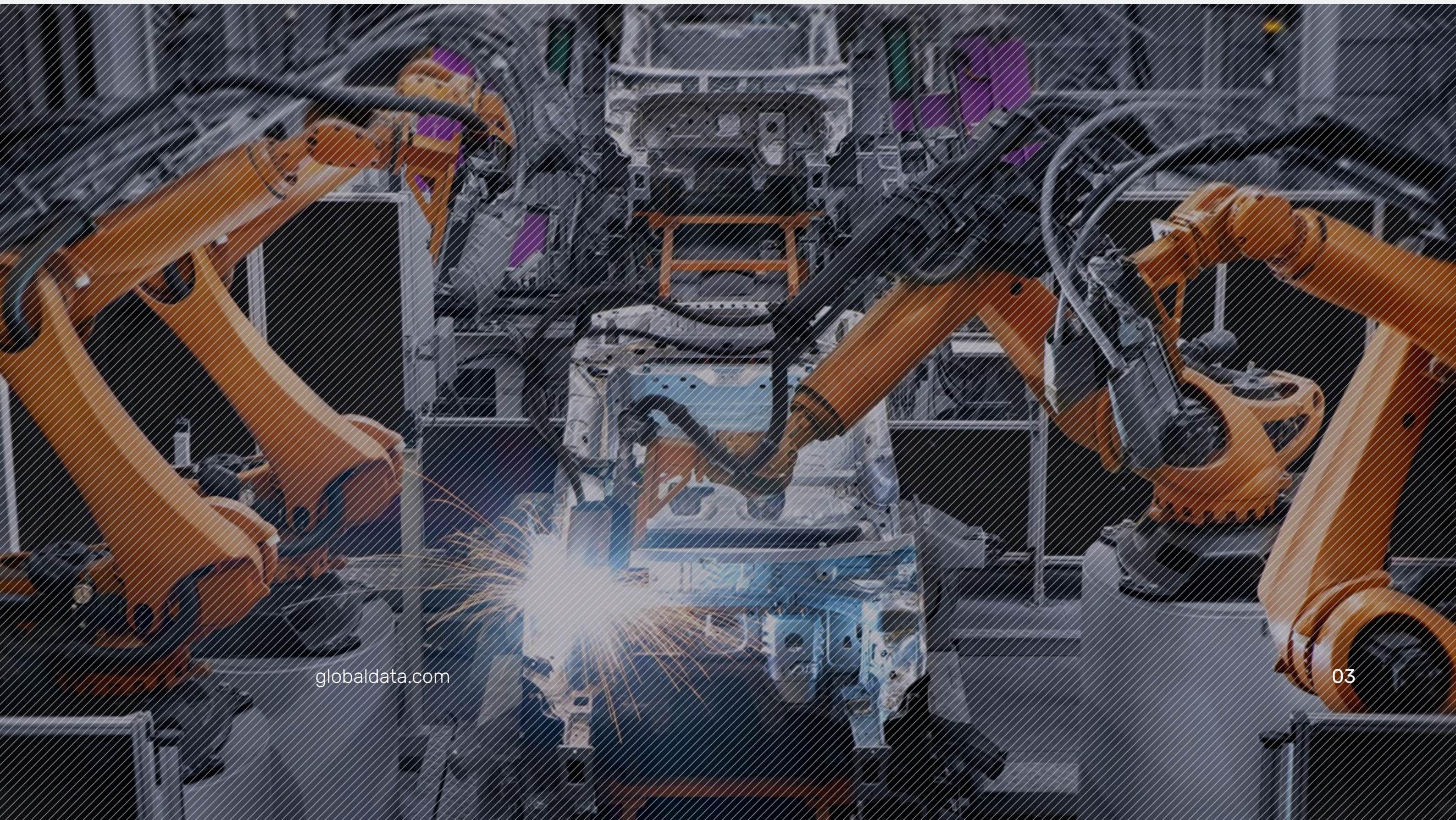
Introduction

Ransomware groups are increasingly attacking manufacturers to fracture the backbone of global supply chains and cause widespread disruption, typically for either profit or political goals. Ransomware attacks on industrial infrastructure organizations nearly doubled in 2022. Ransomware activity is rising in frequency and ferocity, with attacks typically being made through the vulnerable information technology (IT) - operational technology (OT) corridor. OT today is broken and the cause of the fracture is a lack of visibility and control.

The problem is that the legacy OT technology sitting on manufacturing floors can be easily attacked. The equipment is of high criticality with a lot of dollars and safety risk tied to it. In many cases, the technology itself is ancient. Typically, the equipment uses legacy protocols that are very hard to communicate with and discover. Consequently, identifying such devices is difficult. The challenge for organisations is finding a way of gaining that much-needed IT and OT visibility and control.

That incidents in the manufacturing environment can cause critical safety incidents is serious enough. But that is compounded by the economic cost of manufacturing disruption and downtime, which can be of the order of millions of dollars a day. Cyberattacks cause manufacturers to experience unplanned operational downtime, damaging revenues and brand image. According to Forbes, **the average automotive manufacturer loses $22,000 per minute if the production line stops**. This becomes a significant challenge in an industry where maintenance windows for critical systems can be extremely tight, reducing the time security teams have to test and deploy crucial patches.

But manufacturing typically hasn't helped itself. Historically, it appeared that the shopfloor and the data centre were on different pages and were destined never to meet. The two domains ran independently, with different skillsets and different types of technology creating a natural barrier between them. Fear of disrupting operations has therefore led to a 'moat-and-drawbridge' approach to protecting plants and a reluctance to make changes to the technology supporting the operating tools. Such functional silos within IT and manufacturing led to tenuous relationships between manufacturing, engineering, and IT teams.



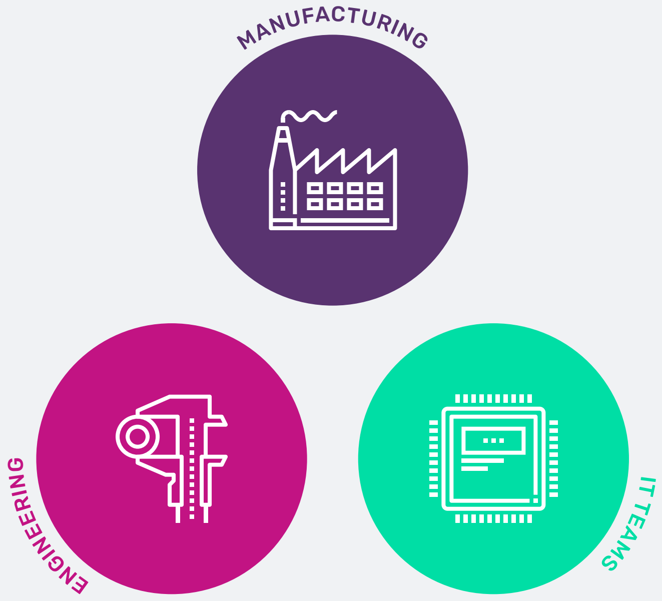
Benefits of removing barriers

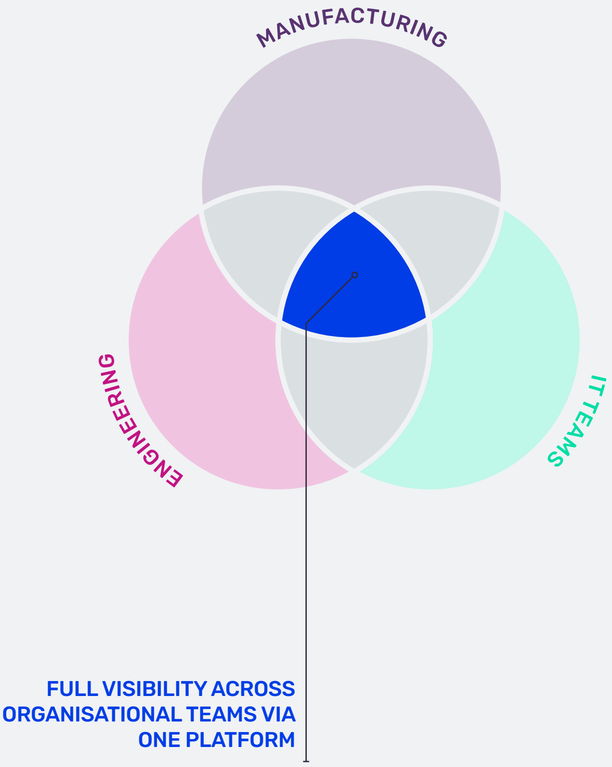
Things have changed over the past few years. Industry 4.0, and connectivity to the internet, means manufacturing environments are now beginning to be more connected to IT environments, though it might be a stretch to describe technology and manufacturing domains as inextricably connected and interdependent. The good news is that a removal of barriers enables companies to operate more efficiently and mitigate risk more effectively. The bad news is that manufacturing is now a prime target for bad actors.

According to the Dragos ICS/OT Cybersecurity Year in Review 2022, there was a 27 percent increase in vulnerabilities in 2022. Despite the material increase, this represented a slowdown in the growth rate. Improvements in the rate of mistakes and risk ratings were a very positive signal. The standard information technology (IT) approach to vulnerability mitigation is a patch. But patching in the OT world often requires system and plant shutdowns.

The Dragos report recommends adopting the SANS "Five ICS Cybersecurity Critical Controls" for industrial cybersecurity as a reference framework to evaluate progress. But there is much work to be done. One critical control, ICS Network Visibility, continues to be a challenge. 80 percent of environments had little or no visibility into traffic and devices in ICS/OT environments. While in 2022, there was an improvement of 600 basis points from 2021, the vast majority of environments still find it challenging to detect and investigate issues, and much less maintain accurate asset inventory.

Another critical control is Secure Remote Access which also showed a negative trend, with users in 54 percent of environments using the same credentials for IT systems as OT systems. Remote access is the most common way for threat groups to penetrate OT systems, and sharing the same credentials only makes it much easier for threats to cross from IT to OT systems.




MANUFACTURING
ENGINEERING
IT TEAMS
FULL VISIBILITY ACROSS ORGANISATIONAL TEAMS VIA ONE PLATFORM

Manufacturing challenges

As well as cyber challenges, manufacturers are suffering ongoing macroeconomic and compliance ones. Supply chain disruption is compounded by inflation, narrowing cost margins (driven for example by the rising cost of raw materials and energy prices), and the availability of materials. The next few years will see increasing compliance headaches as manufacturing regulation and standards get the oversight and rigour that has been lacking for years.

The supply chain dilemma

Supply chain vulnerabilities have been exposed by several recent events, including COVID-19, chip shortages, and the Russia-Ukraine war. Geopolitical conflicts and China's Zero Covid policy have also had a knock-on effect on the way supply chains operate. Supply chain disruption is the new normal, as GlobalData's social media datasets indicate. In 2023, social media mentions of supply chains reached 1,389, a seven-fold increase from 2019.

Although ongoing disruptions have led to many more companies considering reshaping their supply chains, that is easier said than done. Even companies of the size of Apple have found the challenge of reengineering their supply chain extremely difficult due to its inherent complexity. It is a major project for boards to seriously consider relocating supply chains to other countries, and entirely another to go ahead and do so with all the short-term disruption that can cause.

Complex supply chains also bring more risk. Often, corporations will have no visibility of their suppliers' cybersecurity procedures and protection. If there is a breach in a supplier's network, this can leave other corporations in the supply chain vulnerable. If a key supplier is hit by a cyberattack, operations across the supply chain will be affected, causing financial and reputational damage.

The end-to-end challenge: getting efficiencies across IT and OT asset management

Complex supply chains bring more risk. Often, corporations will have no visibility of their suppliers' cybersecurity procedures and protection. If there is a breach in a supplier's network, this can leave other corporations in the supply chain vulnerable. If a key supplier is hit by a cyberattack, operations across the supply chain will be affected, causing financial damage.

Companies that have the far-sightedness to apply good technology and manufacturing governance to their operations will reap efficiency rewards. There is a path of technology governance benefits that start with being able to discover, monitor and accurately track all your OT assets and combine them with IT assets in one place.

Consider these questions about effectively managing and securing your IT/OT estate. Can you answer yes to them?

- Do you have visibility into all of your devices and endpoints?
- Can you view and manage all of these devices/ endpoints from one platform?
- Can you identify vulnerabilities and breaches in real-time?
- Do you have clear workflows and processes to follow in the case of an incident?
- Are you able to issue updates and patches remotely?

If so, then your estate is probably benefiting from having unified asset inventory across IT and OT; visibility across multiple vendor environments; and enhanced security and ability to quickly respond high-criticality vulnerabilities across devices.

By increasing OT vulnerability and remediation, that then starts to yield centralized IT and OT management efficiencies, which in turns leads to greater, broader manufacturing efficiency, and ultimately stronger manufacturing governance and automation.

Regulation and compliance

What has been lacking is the motivation for companies to take steps to protect themselves and their partners. But now, belatedly, regulators are starting to take compliance seriously. When regulators start talking about penalties for compliance failure, suddenly corporate budgets miraculously open up to fix those failures.

Standards such as NIST SP 1800-10B, German supply chain security reporting standards, UN R155/156 in the automotive sector, the international standards ISA/IEC62443, which addresses current and future security vulnerabilities in industrial automation and control systems, and the Cybersecurity Maturity Model Certification (CMMC), which applies to any company doing US federal government business, must all be addressed by manufacturers.

The chart below shows the ISA/IEC62443 standards adopted by the International Electrotechnical Commission (IEC), which provides a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems.

The next few years will see increasing regulatory requirements being enforced with penalties and board level accountability. The time to start tackling this is now.

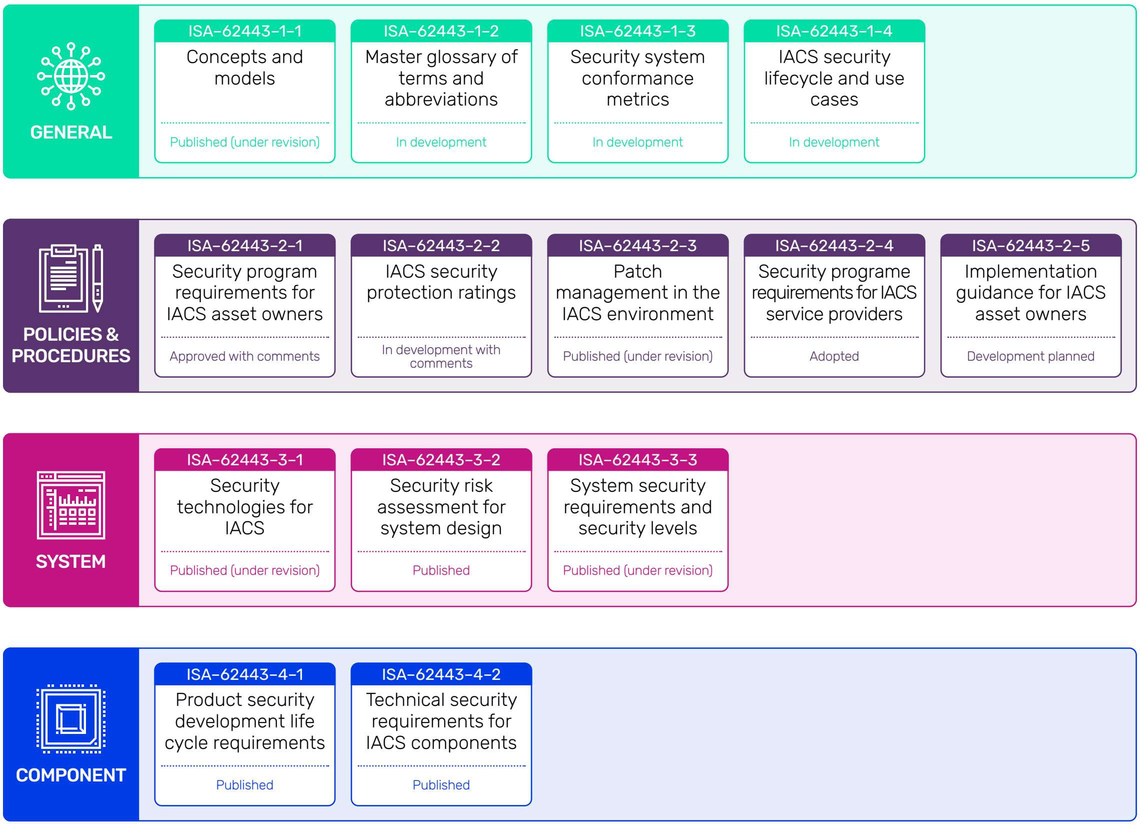
Dealing with digitalisation

Digitalisation and automation offer a double-edged sword for manufacturers. They have brought significant advantages that can lead to greater efficiencies and reduced operating costs. For example, digital tools help manufacturers to centralise and manage the entire manufacturing process in one software platform, opening up opportunities to collect and analyse data across the digital manufacturing lifecycle.

But at the same time, digitalisation has widened the attack surface area and arguably created a complex and potentially unmanageable technological architecture, with new technologies deployed alongside legacy systems. New industry 4.0 technologies, including the Internet of Things (IoT) have themselves created more entry points for attackers, as every sensor is an endpoint that can potentially be exploited.

Figure 1

The ISA/IEC 62443 Series of Standards



GENERAL
- ISA-62443-1-1: Concepts and models — Published (under revision)
- ISA-62443-1-2: Master glossary of terms and abbreviations — In development
- ISA-62443-1-3: Security system conformance metrics — In development
- ISA-62443-1-4: IACS security lifecycle and use cases — In development

POLICIES & PROCEDURES
- ISA-62443-2-1: Security program requirements for IACS asset owners — Approved with comments
- ISA-62443-2-2: IACS security protection ratings — In development with comments
- ISA-62443-2-3: Patch management in the IACS environment — Published (under revision)
- ISA-62443-2-4: Security programe requirements for IACS service providers — Adopted
- ISA-62443-2-5: Implementation guidance for IACS asset owners — Development planned

SYSTEM
- ISA-62443-3-1: Security technologies for IACS — Published (under revision)
- ISA-62443-3-2: Security risk assessment for system design — Published
- ISA-62443-3-3: System security requirements and security levels — Published (under revision)

COMPONENT
- ISA-62443-4-1: Product security development life cycle requirements — Published
- ISA-62443-4-2: Technical security requirements for IACS components — Published

Source:
https://www.tripwire.com/state-of-security/isa-iec-62443-framework

> *"As industries are accelerating into digitalisation, there is a growing interdependency between the traditional technology domains of IT, manufacturing, and embedded product technology. On the one hand we are seeing significant innovation and transformation. On the other hand, it is creating increased regulatory and cost pressure. As technology environments are becoming more complex, companies need to find ways to reduce the cost to operate and protect them. Streamlining the technology estate often means modernising, and many companies are looking to integrated platform approaches to replace outdated technology and the quagmire of point solutions that are used to manage it."*

Tom Molden, CIO of Global Executive Engagement at Tanium

What are the risks?

IT-OT convergence and the challenges of securing legacy manufacturing systems

When we talk about IT-OT convergence, the IT systems refer to the systems used for data-centric computing, usually in a corporate setting, and the OT systems are those that monitor industrial operations. IT-OT convergence involves the integration of these two systems into one cohesive system, using networking and computational technologies to provision OT systems, and collect data across operational equipment and systems.

IT-OT convergence provides the foundations for advanced technologies in the manufacturing world, but at the same time, by widening the attack surface area, it increases potential pathways for hackers. The problem comes from connecting Industrial Controls Systems (ICS) to the internet and to IT networks and systems, which creates new weak points. IT and OT systems were built to operate independently. The problem is how to protect them in this converged world. When they are converged without properly unifying the security stack, that causes weak points to emerge which can be exploited by attackers, creating open access to the entire IT and OT suite.

Tom Molden explains: "With the rapidly evolving convergence of IT and OT, companies are looking for ways to get end-to-end visibility, management, and protection of technology assets across the manufacturing space. In most companies, corporate IT and manufacturing engineering have run independently for years: the combined solution space is not mature and lacks holistic solutions. Experienced practitioners on both sides know you cannot simply copy and paste IT methods into the OT environments. Outdated operating systems, narrow change windows, thin hardware specs, and network segmentation are all traditional challenges. However, with recent advances in technology and increased collaboration between functions, progressive companies are increasingly able to reduce risk and improve operability, without impact to production."

IT and OT-based attacks are not imaginary, they are real. The Colonial Pipeline attack in the US in May 2021 took advantage of weaknesses in IT-OT convergence. Ransomware attackers targeted the fuel pipeline's IT billing system, rather than its operational technology. But Colonial was still forced to shut down its physical operations, because its IT systems were in close proximity to its OT systems. Continuing physical operations posed too much of a risk of an IT attack turning into an OT attack, debilitating operations even further. Damage to physical operations would have lasted longer, cost more, and could have endangered employee lives.

Lack of visibility to manufacturing assets

You cannot manage what you cannot see; and in today's world, you cannot protect it if you cannot manage it. In the legacy manufacturing world, asset inventory processes involved manual steps and were heavily dependent on spreadsheets. But as more and more new asset types have been brought into the plant environment, many were not captured using such traditional scans. In some worst-case scenarios, operators would simply unplug a device when it was time for a scan and then plug it back in afterward. For years, this outdated, incomplete information was accepted because it was more important to focus on the things that kept the operation running. Now, times have changed. Today's CIOs and heads of manufacturing understand the value of real-time visibility and a need to provide a simplified, comprehensive view of assets across the corporate and manufacturing technology estates.

Acting globally on compliance

Business is global and organisations with ambitions to compete in other countries will have to tackle their compliance requirements. It does not matter where organisations do business in the world, they have to attest to being compliant with the relevant security surveys and assessments. The threat is compounded by the formation of new auditing bodies being created with auditors keen and hungry to make their mark. For the next few years, auditors will be hard-nosed out of the gate on new regulations. These standards are now hitting manufacturing because hackers know systems are old and unpatched: a treasure trove offering low hanging fruit. These enforcements now oblige manufacturers to fix the problems that they have either ignored, or worse, swept under the rug.

> *"While these different standards sound daunting, many of the controls are the same. Therefore, effort applied to meeting one of these compliance frameworks automatically earns credit towards the others. Regardless of the letters and numbers on the controls, the end goal is a secure environment of people, process, and tools."*
>
> Ashley McGlone, Technology Strategist for Manufacturing at Tanium

Recommendations

1

IMPROVED SCANNING OFFERS BETTER VISIBILITY AND CONTROL ACROSS DOMAINS:

Those organisations that can deliver for themselves real-time visibility of endpoints will benefit from improved safety and traceability. At the heart of that visibility is having a single source of truth and unified security and operations. More effective surveying of devices is the long-term goal.

2

VISIBILITY OF THIRD-PARTY ASSETS IS PARAMOUNT. REGULATORY COMPLIANCE IS KING:

The best way to manage supply chain risk is to start by having visibility of all corporate IT assets and third-party IT assets. This is the first step to manage supply chain risk, assessing third party dependencies, assessing supplier security maturity, and knowing how third parties use your company data. A quantitative approach is needed, combined with third-party attestation and valuations, and compliance with all necessary regulatory standards, to assess supply chain risk and protect against potential breaches. It is hard to get visibility into third party assets, but doing so and putting effective governance around it is a necessity.

3

ADOPT AN EFFECTIVE PLATFORM TO BRIDGE THE IT-OT GAP AND DRIVE GREATER EFFICIENCIES:

Manufacturers should aim to reduce the impact of silos to gain a holistic view, enabling them to get their arms around the key concept of ‘knowing what you know, knowing what you don’t know.’ A single platform provides a simple solution, creating a single source of truth across endpoints, bridging the IT-OT gap across manufacturing companies’ developing digital infrastructures. That then drives converged IT/OT environments even across complex supply chains, and ultimately greater manufacturing efficiencies through automation.

4

RATIONALISE APPLICATIONS:

Taking steps to rationalise applications will help avoid software bloat, reduce both total cost of ownership and complexity, and help bridge the gap between IT and OT. This makes systems safer and reduces potential manufacturing disruption, with a simplified system architecture allowing easier monitoring and to identify critical dependencies.

Sponsor

Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale.

Tanium has been named to the Forbes Cloud 100 list for six consecutive years and ranks on Fortune's list of the Best Large Workplaces in Technology. In fact, more than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

Visit www.tanium.com
Follow us on Linkedin: Tanium
Follow us on Twitter: @Tanium

GlobalData.

We are the trusted gold standard intelligence provider to the world's largest industries

We have a proven track record in helping thousands of companies, government organizations, and industry professionals profit from faster, more informed decisions.

Our unique data-driven, human-led, and technology-powered approach creates the trusted, actionable, and forward-looking intelligence you need to predict the future and avoid blind spots.

Leveraging our unique data, expert analysis, and innovative solutions, we give you access to unrivaled capabilities through one platform.

HEAD OFFICE

John Carpenter House
7 Carmelite Street
London
EC4Y 0AN
UK

Tel: +44 20 7936 6400

GlobalDataPlc
GlobalDataPlc
GlobalData.com

DISCLAIMER

All Rights Reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publisher, GlobalData. The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions and recommendations that GlobalData delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. As such, GlobalData can accept no liability whatsoever for actions taken based on any information that may subsequently prove to be incorrect.