

NIS2 Readiness: A Guide for Organizations in Europe



Mark Child
Associate Research Director,
European Security, IDC



Ralf Helkenberg
Senior Research Manager,
European Privacy and Data
Security, IDC



Dominique Bindels
Consulting Manager,
Custom Solutions Europe, IDC

NIS2 Readiness: A Guide for Organizations in Europe



In the face of escalating cyberthreats and the evolving digital landscape, the implementation of the Network and Information Systems Directive 2 (NIS2) has become an urgent imperative for organizations in Europe.

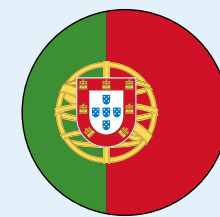
With its expanded scope and stringent requirements, NIS2 aims to enhance cybersecurity resilience across critical sectors and ensure a unified approach to risk management.

However, the tight timelines for compliance present significant challenges to organizations, requiring them to quickly assess their current cybersecurity postures, identify gaps, and develop comprehensive implementation plans to ensure compliance.

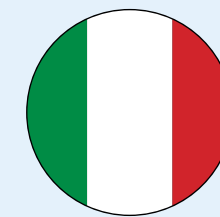
Countries included in the research



Spain



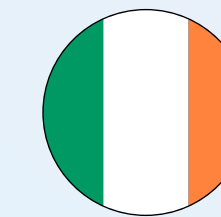
Portugal



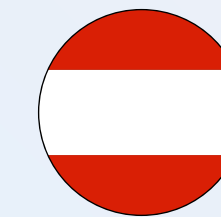
Italy



Nordics



Ireland



Austria



Belgium

The research conducted for this report, sponsored by Microsoft, plays a crucial role in assisting CISOs in navigating this complex and time-sensitive process.

This research provides valuable insights into the readiness of organizations across different countries in Europe. It serves as a benchmark for organizations to evaluate their own progress and prioritize actions. It also highlights the most prevalent challenges and areas of concern, enabling CISOs to focus their efforts on critical aspects and effectively allocate resources.

Furthermore, the research offers recommendations that CISOs can use to accelerate their NIS2 implementation journeys.

NIS2 Readiness Framework

An organization's readiness for NIS2 can be assessed across the four categories below. IDC's survey, sponsored by Microsoft, asked organizations in Europe a range of questions across these categories to explore factors like awareness, NIS2 compliance ownership, challenges, and reliance on partners.



Region Overview: Readiness Levels

The percentages below show the share of organizations in each of the five readiness levels.

NIS2 Readiness Levels

Aware

9%



Organizations at this level have a basic understanding of NIS2. They are beginning to recognize its importance and are **aware** of the need to align with its requirements. This stage is about gaining knowledge and understanding the scope of what needs to be done.

What they are lacking:

Lacking a comprehensive understanding and implementation of NIS2 requirements. They need to move beyond basic awareness to actionable steps.

Capable

17%



At this stage, organizations have moved beyond basic awareness and are **capable** of taking action. While they have started to put policies and procedures in place to meet some NIS2 requirements, there is still work to be done to ensure full compliance.

What they are lacking:

Missing full compliance and robust procedures. They need to enhance their policies and procedures to meet all NIS2 requirements.

Equipped

33%



Organizations scoring in this range are **equipped** to handle most of the challenges presented by NIS2. They have a solid grasp of the directive and have implemented a significant number of measures. They are well on their way to achieving a strong cybersecurity posture.

What they are lacking:

Lacking capabilities to address all challenges and achieve a strong cybersecurity posture. They need to implement more measures and improve their cybersecurity strategies.

Advanced

27%



These organizations are **advanced** in their preparedness. They have not only addressed the majority of the NIS2 requirements but also put robust processes and technologies in place. They are likely to be seen as leaders in cybersecurity within their industries.

What they are lacking:

Lacking continuous improvement and integration of NIS2 requirements. They need to focus on refining their processes and technologies.

Ready

14%




Organizations at the **ready** level exhibit the highest degree of preparedness. They have fully integrated NIS2 requirements into their operations and are continuously improving their cybersecurity measures. They serve as benchmarks for best practices in the field.


What they are lacking:

Lacking the ability to set benchmarks and best practices. They need to maintain and enhance their high level of preparedness and serve as industry leaders.


NIS2 Readiness: Region Overview

NIS2 Readiness

 **Moderate awareness of NIS2.**

 **Moderate coverage by the first NIS.**


 **High interest in the use of GenAI.**

 **Highly reliant on security technology providers.**

Expected Effect of NIS2 on Compliance Costs

 **42%**
Higher

 **23%**
Same

 **36%**
Lower

Awareness and Knowledge



- 44%** — Have a moderate awareness of NIS2
- 49%** — Are aware of the penalties for non-compliance
- 42%** — Are aware of the core cybersecurity risk management measures recommended in NIS2
- 42%** — Are aware of the national authorities responsible for auditing and enforcing the directive

Compliance and Governance



- 76%** — Are already covered under the first NIS directive
 - 68%** — Are not yet fully compliant with the new NIS2 directive
 - 58%** — Of boards are not engaged about NIS2 compliance
 - 73%** — Have set up a project team to explore and ensure compliance with NIS2
- AND**
- 27%** — Say this team is led by IT
 - 26%** — Say this team is led by the CISO
 - 22%** — Say this team is led by the data protection officer (DPO)

Risk Management and Security Practices



- 91%** — Are considering GenAI to automate and improve the efficiency of security operations
- BUT**
- 58%** — Do not currently have or are only planning to develop a strategy to secure sensitive data when using GenAI for cryptography and encryption
- Most challenging to comply with:**
- 23%** — Risk management and information system security policies
 - 23%** — Policies and procedures to assess the effectiveness of security risk management measures
 - 26%** — HR security, access control policies, and asset management

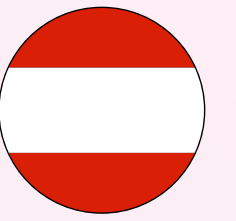
Strategic Alignment and Information Channels




- 89%** — Expect the offerings of their strategic security providers to align with their NIS2 compliance efforts
- 28%** — Rely on their organization's security technology providers for information and guidance on NIS2
- 16%** — Rely on the ministry for their sector for information and guidance on NIS2


Country Deep Dives

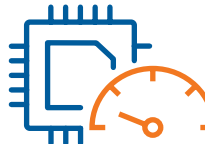
NIS2 Readiness: Country Deep Dive — Austria




NIS2 Readiness

 **Moderate awareness of NIS2.**

 **Moderate coverage by the first NIS.**

 **Limited interest in the use of GenAI.**

 **Highly reliant on security technology providers.**

Expected Effect of NIS2 on Compliance Costs



Awareness and Knowledge



52% — Have a moderate awareness of NIS2

62% — Are aware of the penalties for non-compliance

62% — Are aware of the core cybersecurity risk management measures recommended in NIS2

42% — Know nothing about when the directive will come into force

Compliance and Governance



71% — Are already covered under the first NIS directive

77% — Have set up a project team to explore and ensure compliance with NIS2

78% — Are not yet fully compliant with the new NIS2 directive

68% — Say their organization's board is not engaged regarding NIS2 compliance

Risk Management and Security Practices



81% — Have a policy in place to communicate security risks and incidents to stakeholders

97% — Are considering GenAI to automate and improve the efficiency of security operations

32% — Have supply chain IT security audits or assessments in place

Most challenging to comply with:

- 29%** — Policies and procedures to assess the effectiveness of security risk management measures
- 26%** — Incident handling and management
- 26%** — Risk management and information system security policies

Strategic Alignment and Information Channels



77% — Expect the offerings of their strategic security providers to align with their NIS2 compliance efforts

36% — Rely on their organization's security **technology** providers for information and guidance on NIS2

16% — Rely on their industry's regulator to receive information and guidance on NIS

NIS2 Readiness: Country Deep Dive — Belgium

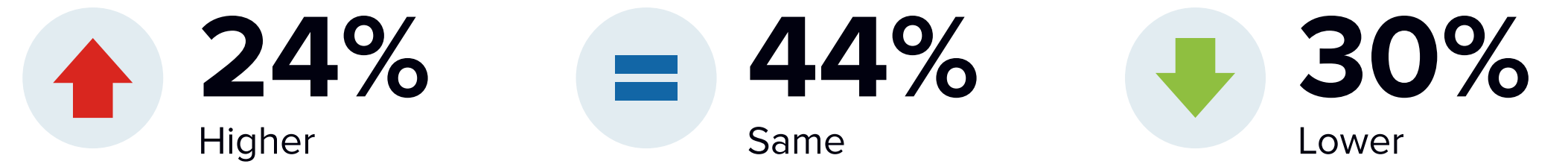


NIS2 Readiness

- Limited awareness of NIS2.
- High coverage by the first NIS.

- High interest in the use of GenAI.
- Highly reliant on security technology providers.

Expected Effect of NIS2 on Compliance Costs



Awareness and Knowledge



- 47%** — Are aware and know something about the core cybersecurity risk management measures recommended in NIS2
- 44%** — Have low or no awareness of NIS2
- 32%** — Are aware of the penalties for non-compliance but know nothing about them

Compliance and Governance



- 82%** — Are already covered under the first NIS directive
- 71%** — Believe they are not or only partially compliant with NIS2
- 71%** — Say their organization’s board is not engaged regarding NIS2 compliance
- 62%** — Have set up a project team to explore and ensure compliance with NIS2
- AND**
- 38%** — Say this team is led by the CISO

Risk Management and Security Practices



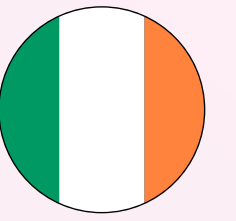
- 82%** — Are considering GenAI to automate and improve the efficiency of security operations
- BUT**
- 68%** — Do not currently have or are only planning to develop a strategy to secure sensitive data when using GenAI for cryptography and encryption
- Most challenging to comply with:**
- 35%** — HR security, access control policies, and asset management
- 21%** — Multifactor authentication (MFA), continuous authentication, and secure communications
- 18%** — Security in the acquisition, development, and maintenance of network and information systems

Strategic Alignment and Information Channels




- 79%** — Expect the offerings of their strategic security providers to align with their NIS2 compliance efforts
- 41%** — Rely on their organization’s security **technology** providers for information and guidance on NIS2
- 38%** — Rely on the ministry for their sector to receive information and guidance on NIS

NIS2 Readiness: Country Deep Dive — Ireland



NIS2 Readiness

 Moderate awareness of NIS2.

 High coverage by the first NIS.

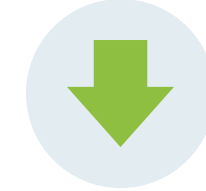
 High interest in the use of GenAI.

 Highly reliant on security service providers.

Expected Effect of NIS2 on Compliance Costs

 **53%**
Higher

 **17%**
Same

 **30%**
Lower

Awareness and Knowledge



67% — State they have low or moderate awareness of NIS2

57% — Are aware of the penalties for non-compliance and know **something** about them

33% — Are aware of the core security measures recommended within the directive but know **nothing** about them

32% — Are aware of the penalties for non-compliance but know **nothing** about them

Compliance and Governance



83% — Are already covered under the first NIS directive

70% — Believe they are not or only partially compliant with NIS2

63% — Say their organization's board is not engaged about NIS2 compliance

68% — Have set up a project team to explore and ensure compliance with NIS2

AND

45% — Say this team is led by the CISO

Risk Management and Security Practices



87% — Are considering GenAI to automate and improve the efficiency of security operations

BUT

63% — Do not currently have or are only planning to develop a strategy to secure sensitive data when using GenAI for cryptography and encryption

Most challenging to comply with:

30% — Security in the acquisition, development, and maintenance of network and information systems

23% — Incident handling and management

23% — Risk management and information system security policies

Strategic Alignment and Information Channels



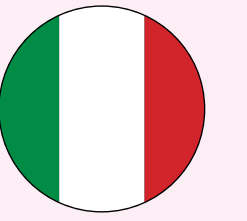
90% — Expect the offerings of their security provider to align with their NIS2 compliance efforts

20% — Rely on their organization's security **technology** provider for information and guidance about NIS2


30% — Rely on their organization's security **service** provider

40% — Rely on security conferences, publications, and independent experts

NIS2 Readiness: Country Deep Dive — Italy



NIS2 Readiness

 **Moderate awareness of NIS2.**

 **Medium coverage by the first NIS.**


 **High interest in the use of GenAI.**

 **Highly reliant on security service providers.**

Expected Effect of NIS2 on Compliance Costs

 **42%**
Higher

 **28%**
Same

 **26%**
Lower

Awareness and Knowledge



- 67%** — State they have low or moderate awareness of NIS2
- 50%** — Are aware of the national authorities responsible for auditing and enforcing NIS2 and know **something** about them
- 47%** — Are aware of the penalties for non-compliance and know **something** about them
- 42%** — Are aware of the core security measures recommended within the directive and know **a lot** about them

Compliance and Governance



- 77%** — Are already covered under the first NIS directive
- 97%** — Believe they are already partially or fully compliant with NIS2
- 56%** — Say their organization’s board is aware and engaged about NIS2 compliance
- 73%** — Have set up a project team to explore and ensure compliance with NIS2
- AND**
- 32%** — Say this team is led by IT
- ONLY**
- 16%** — Say this team is led by the CISO

Risk Management and Security Practices



- 92%** — Are considering GenAI to automate and improve the efficiency of security operations
- AND**
- 53%** — Are developing a strategy to secure sensitive data when using GenAI for cryptography and encryption
- Most challenging to comply with:**
- 27%** — Policies and procedures to assess the effectiveness of security risk management measures
- 23%** — MFA, continuous authentication, and secure communications
- 23%** — Risk management and information system security policies

Strategic Alignment and Information Channels





- 95%** — Expect the offerings of their security provider to align with their NIS2 compliance efforts
- 30%** — Rely on their organization’s security **service** provider for information and guidance about NIS2
- 28%** — Rely on their organization’s security **technology** provider for information and guidance about NIS2
- 40%** — Rely on security conferences, publications, and independent experts

NIS2 Readiness: Country Deep Dive — Nordics



NIS2 Readiness

 **Moderate awareness of NIS2.**

 **Moderate coverage by the first NIS.**


 **High interest in the use of GenAI.**

 **Highly reliant on security service providers.**

Expected Effect of NIS2 on Compliance Costs

 **44%**
Higher

 **23%**
Same

 **32%**
Lower

Awareness and Knowledge



- 75%** — State they have low or moderate awareness of NIS2
- 62%** — Are aware of the penalties for non-compliance and know **something** about them
- 57%** — Are aware of the national authorities responsible for auditing and enforcing NIS2 and know **something** about them
- 34%** — Are aware of the core security measures recommended within the directive and know **a lot** about them

Compliance and Governance



- 75%** — Are already covered under the first NIS directive
- 95%** — Believe they are already partially or fully compliant with NIS2
- 63%** — Say their organization's board is aware of and engaged about NIS2 compliance
- 79%** — Have set up a project team to explore and ensure compliance with NIS2
- AND**
- 32%** — Say this team is led by IT
- 27%** — Say this team is led by the DPO
- 27%** — Say this team is led by the CISO

Risk Management and Security Practices



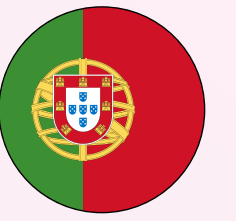
- 95%** — Are considering GenAI to automate and improve the efficiency of security operations
- AND**
- 43%** — Are developing a strategy to secure sensitive data when using GenAI for cryptography and encryption
- Most challenging to comply with:**
- 28%** — Policies and procedures regarding use of cryptography and encryption
- 23%** — Supply chain IT security audits and assessments
- 21%** — Risk management and information system security policies

Strategic Alignment and Information Channels




- 92%** — Expect the offerings of their security provider to align with their NIS2 compliance efforts
- 33%** — Rely on their organization's security **service** provider for information and guidance about NIS2
- 23%** — Rely on their organization's security **technology** provider for information and guidance about NIS2
- 33%** — Rely on regional or local authorities for information and guidance about NIS2

NIS2 Readiness: Country Deep Dive — Portugal




NIS2 Readiness

 **Limited awareness of NIS2.**

 **High uncertainty if they are covered by the first NIS.**


 **High interest in the use of GenAI.**

 **Highly reliant on security technology providers.**

Expected Effect of NIS2 on Compliance Costs

 **42%**
Higher

 **23%**
Same

 **36%**
Lower

Awareness and Knowledge



- 47%** — State they have no or low awareness of NIS2
- 38%** — Are aware of the core security risk management measures recommended within the directive but know **nothing** about them
- 34%** — Are aware of the penalties for non-compliance but know **nothing** about them
- 31%** — Are aware of the national authorities responsible for auditing and enforcing NIS2 but know **nothing** about them

Compliance and Governance



- 60%** — Are already covered under the first NIS directive
- 25%** — Do not know if they were already covered under the first NIS directive
- BUT**
- 90%** — Believe they are already partially or fully compliant with NIS2
- 60%** — Say their organization’s board is not engaged about NIS2 compliance
- 60%** — Have set up a project team to explore and ensure compliance with NIS2
- AND**
- 42%** — Say this team is led by the CISO
- 26%** — Say this team is led by IT

Risk Management and Security Practices



- 90%** — Are considering GenAI to automate and improve the efficiency of security operations
- BUT**
- 75%** — Do not yet have a strategy to secure sensitive data when using GenAI for cryptography and encryption
- Most difficult to comply with:**
- 25%** — Policies and procedures regarding use of cryptography and encryption
- AND**
- 25%** — MFA, continuous authentication, and secure communications
- 22%** — Supply chain IT security audits, and assessments

Strategic Alignment and Information Channels



- 94%** — Expect the offerings of their security provider to align with their NIS2 compliance efforts
- 9%** — Rely on their organization’s security **service** provider for information and guidance about NIS2
- 28%** — Rely on their organization’s security **technology** provider for information and guidance about NIS2
- 28%** — Rely on their national cybersecurity center or agency

NIS2 Readiness: Country Deep Dive — Spain



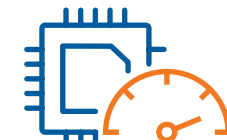
NIS2 Readiness



High awareness of NIS2.



Moderate coverage by the first NIS.

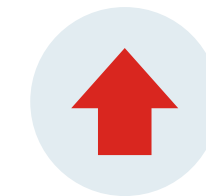


High interest in the use of GenAI.

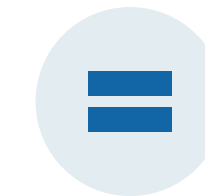


Highly reliant on security technology providers.

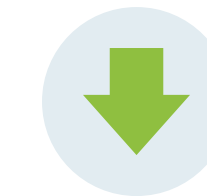
Expected Effect of NIS2 on Compliance Costs



42%
Higher



23%
Same



36%
Lower

Awareness and Knowledge



- 79%** — State they have moderate or high awareness of NIS2
- 50%** — Are aware of the national authorities responsible for auditing and enforcing NIS2 and know **something** about them
- 48%** — Are aware of the penalties for non-compliance and know **something** about them
- 40%** — Are aware of the core security risk management measures recommended within the directive and know **something** about them

Compliance and Governance



- 79%** — Are already covered under the first NIS directive
- 94%** — Believe they are already partially or fully compliant with NIS2
- 69%** — Have set up a project team to explore and ensure compliance with NIS2
- AND**
- 26%** — Say this team is compliance officer-led
- 20%** — Say this team is led by IT
- 20%** — Say this team is led by the DPO
- 18%** — Say this team is led by the CISO

Risk Management and Security Practices



- 90%** — Are considering GenAI to automate and improve the efficiency of security operations
- AND**
- 92%** — Are already developing or planning to develop a strategy to secure sensitive data when using GenAI for cryptography and encryption
- Most challenging to comply with:**
- 27%** — Risk management and information system security policies
- 27%** — Incident handling and management
- 26%** — Business continuity and crisis management

Strategic Alignment and Information Channels



- 87%** — Expect the offerings of their security provider to align with their NIS2 compliance efforts
- 40%** — Rely on the ministry for their sector for information and guidance about NIS2
- 35%** — Rely on security conferences, publications, and independent experts for information and guidance about NIS2
- 26%** — Rely on their organization's security **technology** provider for information and guidance about NIS2

Next Steps for Organizations in Europe



Awareness and Knowledge

Deepen the understanding of NIS requirements and obligations

- **Monitor the transposition of the NIS2 directive** into national laws. Italy, Ireland, Portugal, and Spain have yet to publish draft legal texts.
- **Engage directly with your organization's strategic security provider** for a specific understanding of what NIS2 means for you.



Compliance and Governance

Engage the board and drive awareness across the organization

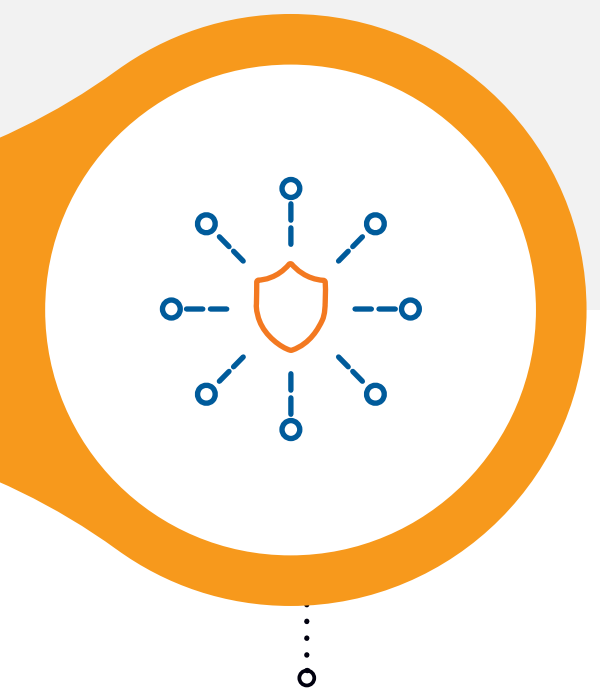
- **Ensure that company leadership, including the board, is part of the NIS2 compliance process** and communicate clearly what NIS2 means for the organization.
- **Project teams should have a diverse membership** consisting of DPO, CISO, legal, and compliance leaders due to the various aspects of the incoming directive.



Risk Management and Security Practices

Identify challenges now and develop action plans

- **Conduct a gap analysis** to identify where your organization's security measures do not meet NIS2 requirements and determine a remediation road map.
- **The directive mentions a risk-based system** for determining measures and specifically refers to European and international standards. Conformance with security standards such as ISO 27001 can help organizations meet NIS2 requirements.



Strategic Alignment and Information Channels

Engage technology and service partners to overcome challenges

- **Deepen your relationship with strategic security providers** as they can serve as useful sources for information and guidance as well as pro-active partners in ensuring compliance.

Message from the Sponsor



NIS2 is EU-wide legislation designed to strengthen Europe's cybersecurity resilience at a time when cyberattacks are becoming more sophisticated. Achieving NIS2 compliance represents an opportunity for organizations to future-proof their security postures and build trust with their customers and stakeholders.

Microsoft provides a host of integrated solutions to help customers achieve NIS2 compliance efficiently and confidently.

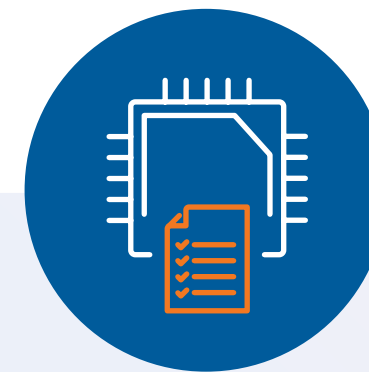
To learn more, please visit:

[Microsoft Security](#)



Risk Management:

Microsoft Defender and Microsoft Purview help with identifying, preventing, and mitigating external and internal security risks.



Incident Reporting:

Microsoft Sentinel simplifies incident reporting requirements by providing intelligent security analytics.



Staff Training:

Microsoft 365 offers tools like phishing simulations and learning paths to empower employees.



This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell, and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

© 2024 IDC Research, Inc. IDC materials are licensed for external use, and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.



IDC UK

5th Floor, Ealing Cross, 85 Uxbridge Road, London, W5 5TH, United Kingdom

T 44.208.987.7100

[X @idc](#)

[in @idc](#)

[idc.com](#)

© 2024 IDC Research, Inc. IDC materials are licensed [for external use](#), and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

[Privacy Policy](#) | [CCPA](#)