Deploying the Right Data to the Right Cloud in Regulated Industries

RESEARCH BY:

Adelaide O’Brien
Research Director, Government Digital Transformation Strategies, IDC

Christina Richmond
Program Vice President, Security Services, IDC
## Executive Summary

Deploying the Right Data to the Right Cloud in Regulated Industries

## Methodology

Situation Overview

- Growing Concern with Data Security, Privacy, and Innovation
- Confidential and Restricted Data Is Vulnerable in a Public Cloud
- Concerns Go Beyond Security
- The Case for Repatriation
- Growing Need for Sovereign Cloud Solutions

## Essential Guidance

- Develop a Data Strategy
- Shift from Cloud First to Cloud Smart
- Find a Trusted Multicloud Partner

## Appendix

- Summary Survey Demographics

## About the Analysts
Executive Summary

Cloud and cloud-centric operating models have grown to become integral components of the modern IT environment. Controlling the actual location of data in the cloud to comply with data privacy regulations has become an important task for CIOs and CISOs and should be a key evaluation criterion in choosing cloud services that handle private, confidential, and restricted data.

With data privacy and residency regulations being put in place across the globe, such as General Data Protection Regulation (GDPR) in Europe and similar laws in the United States, India, Brazil, China, and Russia, CIOs need to be savvy about how to protect data and control the flow of data across boundaries and how to contain data in certain regions. As data privacy regulations are likely to change over time, CIOs will need to continuously evaluate their assessment of data risk management and require vendors to meet current and future organizational requirements and national laws, policies, and mandates. While protecting and controlling data is the primary concern of CIOs, organizations face a broad range of challenges managing critical data, including data availability, integrity, access, and innovation.

As data privacy regulations are likely to change over time, CIOs will need to continuously evaluate their assessment of data risk management and require vendors to meet current and future organizational requirements and national laws, policies, and mandates.
IDC conducted a global survey to determine whether decision makers in regulated industries (i.e., public sector, healthcare, and financial services) recognize the limitations in jurisdictional control and authority over data as well as security risks for critical data in commercial public clouds. In addition, IDC wanted to determine whether respondents understood the benefits of locally or regionally delivered sovereign clouds to protect critical data and whether there is a corporate and/or national policy mandate to improve data privacy and economic innovation with sovereign clouds.

**IDC's global survey findings include:**

- Data security is not just a corporate or organizational issue; 50–60% believe there is a national mandate to improve data security, privacy, and innovation.

- Approximately 50% of regulated industry organizations are using commercial public cloud for confidential and restricted data.

- Security, compliance, and risk mitigation are the top reasons why organizations choose cloud environments for confidential and restricted data; however, respondents are not confident about storing confidential and restricted data in commercial public clouds. Sixty-nine percent of respondents feel confidential data is very/extremely vulnerable when stored in a commercial public cloud.

- Global respondents are very/extremely concerned about critical data being managed by U.S. cloud providers given a changing geopolitical landscape and emerging global threats.

- Forty-two percent of respondents are very/extremely concerned about the authority of the U.S. CLOUD Act compelling United States–based cloud providers under certain circumstances to disclose data whether located within or outside the United States.

- Sixty-three percent of respondents say it is very/extremely important to have a cloud solution that provides complete jurisdictional control and authority over data.

- Customers are repatriating workloads, driven by security and data privacy requirements, as well as to improve latency. Thirty-five percent have already repatriated all data and workloads from commercial public clouds — with more planned.

These findings suggest that some survey respondents’ needs and concerns are not being fully addressed by commercial public clouds when it comes to storing confidential and restricted data and that customers are looking for alternative cloud solutions.
Methodology

IDC recently completed a sovereign cloud survey of 508 respondents in the public sector, financial services, and healthcare (regulated) industries globally. This white paper examines current and planned cloud usage for various data types, existence of an organizational cloud strategy based on data criticality and classification, perceptions of data vulnerability, and difficulties of protecting data against evolving and emerging security threats, as well as concerns about legitimate access by foreign authorities and changing geopolitics.

The definitions of cloud used in the survey include:

- **Commercial public cloud** is an industry-standard public cloud that provides infrastructure as a service (IaaS) and/or platform as a service (PaaS) on demand to multiple tenants in a shared environment, typically over the internet. Data resident in a public cloud, even if deployed in one country, may be subject to lawful collection by another country (e.g., U.S. CLOUD Act), and metadata (e.g., service accounts, host name, events, tokens, security groups) and ticket/escalation data may not be resident on sovereign soil.

- **Sovereign industry cloud/compliant public cloud** is typically targeted at specific private sector industries with regulated workloads (e.g., healthcare, financial services) and may also be referred to as a “community cloud” or “industry cloud.” It includes all features of commercial public cloud plus deeper and embedded security services, data protection services, compliance services, and restricted network access. Compliant clouds provide data sovereignty. Single jurisdictional control and legal authority can be asserted over resident data. All customer data, metadata, and escalation data is resident on sovereign soil.

- **Sovereign government cloud/sovereign public cloud** is typically targeted at public sector agencies with sensitive or classified data. It includes all features of compliant cloud plus air-gapped infrastructure, separate datacenters/regions, additional physical security controls, security clearances for operators, restricted connectivity to government networks, and additional network segmentation/firewalls, and may even include tenant screening. Sovereign clouds provide data sovereignty. Single jurisdictional control and legal authority can be asserted over resident data. All customer data, metadata, and escalation data is resident on sovereign soil.
→ **Public data** refers to unclassified data for public use.

→ **Confidential data** refers to personally identifiable information (PII), corporate IP, and regulated data.

→ **Restricted data** refers to classified data, secret/top-secret data, and government data.

→ **Data residency (locality)** refers to the physical and geographic location where customer data is stored and processed.

→ **Data sovereignty** refers to the idea that data is subject to the data privacy laws and governance structures within the nation where the data is collected.
Growing Concern with Data Security, Privacy, and Innovation

Decision makers in regulated industries (i.e., public sector and regulated private sector including financial services and healthcare) believe that in addition to being a corporate/organizational issue, there are national mandates to improve data security, privacy, and innovation (see Figure 1).

→ Sixty-two percent of respondents believe there is a national mandate to improve protection of critical corporate or national data with a more robust cybersecurity regime.

→ Fifty percent of respondents believe there is a national mandate to leverage clouds that provide complete data sovereignty versus data locality to protect critical national/corporate data.

**FIGURE 1**
Respondents Believe There Are Corporate and National Mandates and Debates Across a Broad Set of Data Sovereignty Issues (% of respondents)

Q. Do you believe that there is a corporate or national mandate and debate about any of the following?

<table>
<thead>
<tr>
<th>Corporate mandate/debate</th>
<th>National mandate/debate</th>
<th>Both</th>
<th>Neither</th>
</tr>
</thead>
<tbody>
<tr>
<td>To improve protection of critical corporate or national data with a more robust cybersecurity regime</td>
<td>35%</td>
<td>26%</td>
<td>36%</td>
</tr>
<tr>
<td>To improve data privacy laws and regulations and ensure better enforcement and controls</td>
<td>36%</td>
<td>30%</td>
<td>32%</td>
</tr>
<tr>
<td>To fuel economic growth and unlock innovation by pooling critical data in cloud and leveraging advanced data services</td>
<td>32%</td>
<td>35%</td>
<td>25%</td>
</tr>
<tr>
<td>To leverage clouds that provide complete data sovereignty versus data locality to protect critical national or corporate data</td>
<td>33%</td>
<td>26%</td>
<td>24%</td>
</tr>
</tbody>
</table>

n = 508

Source: IDC’s VMware Sovereign Cloud Survey, March 2021
Confidential and Restricted Data Is Vulnerable in a Public Cloud

Seventy-five percent of organizations have a cloud strategy based on data criticality and classification such as public data, confidential data, and restricted data. Approximately 50% of respondents are using commercial public clouds for confidential and restricted data, while the other 50% are using private clouds.

At the same time, up to nearly 70% of respondents feel that confidential and restricted data is very/extremely vulnerable when stored in a commercial public cloud (see Figure 2). Organizations indicate they face a broad range of difficulties with protecting data against evolving and emerging security threats and ensuring data availability and integrity. In addition, over two-fifths of survey respondents are very/extremely concerned that data in a commercial public cloud may not remain on sovereign soil even when using a local region (see Figure 3 next page).

FIGURE 2
Confidential Data Is Very/Extremely Vulnerable When Stored in Commercial Public Cloud (% of respondents)

Q. In your opinion, how vulnerable are the following types of data when stored in a commercial public cloud?
FIGURE 3
Forty-Five Percent of Respondents Are Very/Extremely Concerned That Data in a Commercial Public Cloud May Not Remain on Sovereign Soil
(% of respondents)

Q. Whether or not your organization uses a commercial public cloud, how concerned are you that some types of data in a locally delivered commercial public cloud may not remain on sovereign soil? For example, customer data may be resident locally, but metadata (e.g., service accounts, host name, events, tokens, security groups) and ticket/escalation data (e.g., contacts, configuration) may not be resident?

58% of healthcare respondents very/extremely concerned
Followed by:
43% education
43% financial services
43% state/local government
Concerns Go Beyond Security

While data security and privacy are top of mind, organizations face a broad range of challenges with managing critical data. At least 40% of respondents struggle with data access and agility, keeping up with new data protection laws and regulations, and unlocking data insights and innovation (see Figure 4).

FIGURE 4
Organizations Face Broad Difficulties with Data (% of respondents)

Q. In your opinion, how difficult are the following for your organization?

- Protecting data against evolving and emerging security threats: 42%
- Ensuring data availability and integrity: 42%
- Improving data agility and access: 42%
- Keeping up with new and changing data protection laws and regulations: 40%
- Unlocking data insights and innovation: 40%
- Scaling data: 36%

57% of North American respondents find protecting data against emerging threats difficult, much higher than other regions:
- 46% Latin America (LATAM)
- 42% Asia-Pacific (APAC)
- 34% Europe

Difficulty with data agility is highest in:
- 61% LATAM
- 51% North America
- 40% Europe, the Middle East and Africa (EMEA)
- 34% APAC

Source: IDC’s VMware Sovereign Cloud Survey, March 2021
Moreover, 79% of global respondents are moderately to extremely concerned about critical data being managed by U.S. cloud providers given a changing geopolitical landscape (see Figure 5).

**FIGURE 5**

Seventy-nine percent of Respondents Are Moderately to Extremely Concerned About Critical Data Being Managed by U.S. Cloud Providers

(% of respondents)

Q. How concerned are you about critical data being managed by U.S. cloud providers given a changing geopolitical landscape and emerging global threats (e.g., growing trade disputes and nationalism, pandemics and supply chain management, need to control critical national infrastructure)?

![Pie chart showing concern levels](chart.png)

In addition, 42% are very/extremely concerned about the U.S. legislation, The Clarifying Lawful Overseas Use of Data Act, or CLOUD Act, enacted in 2018. The CLOUD Act enables the U.S. and foreign law enforcement partners to obtain electronic evidence from global cloud service providers (SPs) based in the United States. It authorizes the U.S. government to enter into executive agreements with foreign nations under which each country would remove any legal barriers that may otherwise prohibit compliance with qualifying court orders issued by the other country. Both nations would be able to submit orders for electronic evidence needed to combat crime directly to cloud SPs, without involving the other government and without fear of conflict with U.S. or the other nation’s law (see Figure 6 next page).
The Case for Repatriation

Workload and data repatriation have become an integral part of the cloud migration journey as organizations find optimal deployment locations to run applications and protect critical data. For some organizations, cloud repatriation might mean converting workloads back to an on-premises model, while for others it might mean migrating to more sophisticated types of hybrid cloud architectures but not abandoning the cloud altogether. Buyers increasingly understand that cloud workload deployment is not one and done. It is a journey. Further, decision makers in regulated industries recognize that the right data must be deployed into the right cloud. As organizations embrace hybrid and multicloud strategies, they are repatriating data and workloads from commercial public clouds to a variety of cloud architectures that meet their data requirements. Security, data privacy, and latency are top reasons for data and workload repatriation (see Figure 7 next page).
FIGURE 7

Security and Data Privacy Are Top Reasons Why Organizations Repatriate Workloads and Data (% of respondents)

Q. Why did or would your organization repatriate workloads and data?

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>For enhanced security</td>
<td>58%</td>
</tr>
<tr>
<td>For increased data privacy</td>
<td>57%</td>
</tr>
<tr>
<td>To improve latency</td>
<td>45%</td>
</tr>
<tr>
<td>For regulatory compliance</td>
<td>36%</td>
</tr>
<tr>
<td>Owing to geopolitical concerns</td>
<td>31%</td>
</tr>
<tr>
<td>To improve cost</td>
<td>26%</td>
</tr>
</tbody>
</table>

n = 409
Source: IDC’s VMware Sovereign Cloud Survey, March 2021

Broad acceptance of a hybrid approach has made repatriation more likely as decision makers begin to appreciate that it is not possible nor financially viable to transform all workloads into modern applications or migrate them to SaaS environments. The market is at an inflection point where repatriation is happening for both early and late cloud adopters following a review of their deployments. IDC research indicates that 35% of survey respondents have already repatriated all data out of the public cloud, 46% have repatriated some data, and 18% are actively planning or considering repatriation (see Figure 8 next page).
FIGURE 8
Many Organizations Still Have Data and Workload Repatriation Work Ahead of Them
(% of respondents)

Q. Regarding your organization’s use of commercial public cloud, has your organization considered or is it considering workload and data repatriation?

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, already repatriated all data and workloads</td>
<td>35%</td>
</tr>
<tr>
<td>Yes, already repatriated some data and workloads</td>
<td>46%</td>
</tr>
<tr>
<td>Planning to repatriate data and/or workloads within 18 months</td>
<td>11%</td>
</tr>
<tr>
<td>Considering repatriating but have not done so yet</td>
<td>7%</td>
</tr>
<tr>
<td>No plans and not considering repatriation</td>
<td>2%</td>
</tr>
</tbody>
</table>

n = 417
Source: IDC’s VMware Sovereign Cloud Survey, March 2021

Growing Need for Sovereign Cloud Solutions

Our study discovered that not all clouds are the same. Decision makers in regulated industries need to be aware of cloud risks and options as currently buyers are utilizing public clouds for confidential and restricted data but are also extremely concerned about sovereignty and security. IDC believes the emergence of locally or regionally delivered sovereign clouds offers additional choice to the buyer to deploy the right workload/data in the right cloud.

Survey respondents deploy a hybrid cloud approach, with 91% of organizations using public cloud and 45% using private cloud to store and process data. Beyond ensuring data security and integrity, 62% of customers state they need a cloud option that provides data sovereignty with complete jurisdictional control and authority over data. Sixty percent need a cloud operated by certified staff that typically are citizens with security clearances. Fifty-eight percent need a cloud with air-gapped infrastructure or regions (Availability Zones (AZs)) on sovereign soil (see Figure 9 next page).
FIGURE 9
Important Features Beyond Ensuring Data Security and Integrity
(% of respondents)

Q. Whether or not your organization uses a sovereign industry cloud or sovereign government cloud, please rate the importance of the following features.

Data sovereignty with complete jurisdictional control and authority over data, air-gapped infrastructure, and operator control are of top importance in sovereign cloud

Complete jurisdictional control and authority over data

Air-gapped infrastructure or cloud regions (AZs) on sovereign soil

Operated by certified staff

Not at all to somewhat important

Very/extremely important

n = 508
Source: IDC's VMware Sovereign Cloud Survey, March 2021

For these buyers, it is clear from the relative similarity of data points shown in Figure 10 that they consider a broad range of features important for sovereign public cloud.
FIGURE 10
Organizations Find a Broad Range of Features Important for Sovereign Public Cloud; Embedded Data Protection and End-to-End Security Are Most Important (% of respondents)

Q. Whether or not your organization uses a sovereign public cloud, please rate the importance of the following features.

<table>
<thead>
<tr>
<th>Feature</th>
<th>% of respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded data protection services (e.g., disaster recovery)</td>
<td>66%</td>
</tr>
<tr>
<td>End-to-end security (e.g., from data and apps to workspaces and devices)</td>
<td>65%</td>
</tr>
<tr>
<td>Restricted network access (e.g., healthcare or government network)</td>
<td>64%</td>
</tr>
<tr>
<td>Compliance certifications and attestations</td>
<td>64%</td>
</tr>
<tr>
<td>Data life-cycle management (e.g., eventual deletion of data)</td>
<td>63%</td>
</tr>
<tr>
<td>Embedded security services (e.g., micro-segmentation)</td>
<td>63%</td>
</tr>
<tr>
<td>Data sovereignty with complete jurisdictional control and authority over data</td>
<td>62%</td>
</tr>
<tr>
<td>Continuous compliance monitoring, management, and auditing</td>
<td>62%</td>
</tr>
<tr>
<td>Advanced data management services (e.g., big data, analytics, ML)</td>
<td>62%</td>
</tr>
<tr>
<td>Operated by certified staff</td>
<td>60%</td>
</tr>
<tr>
<td>Air-gapped infrastructure or cloud regions (Availability Zones (AZs)) on sovereign soil</td>
<td>58%</td>
</tr>
</tbody>
</table>

n = 508
Base = respondents who rated the feature as either “important” or “very important”
Source: IDC's VMware Sovereign Cloud Survey, March 2021

In addition, organizations responded that they use identity and access management (IAM), vulnerability management capabilities, and network segmentation more often in sovereign clouds today (see Figure 11 next page). While IAM and vulnerability management will remain critical in the future, data encryption and cloud security will become increasingly important in the coming 12–18 months. Beyond security controls, buyers require data management capabilities such as data warehousing, data storage, and data lakes as the top must-haves for a sovereign cloud solution.
FIGURE 11
Organizations Use Identity and Access Management, Vulnerability Management, and Network Segmentation Significantly More in Sovereign Government Cloud than Other Cloud Environments
(% of respondents)

Q. Does your organization use any of the following security products as part of the following environments today?

<table>
<thead>
<tr>
<th>Security Product</th>
<th>Sovereign government cloud</th>
<th>Commercial public cloud</th>
<th>Sovereign industry cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAM</td>
<td>100%</td>
<td>77%</td>
<td>76%</td>
</tr>
<tr>
<td>Email messaging security</td>
<td></td>
<td>92%</td>
<td>93%</td>
</tr>
<tr>
<td>Web content security</td>
<td></td>
<td>98%</td>
<td>92%</td>
</tr>
<tr>
<td>Vulnerability management and assessment</td>
<td></td>
<td>66%</td>
<td>81%</td>
</tr>
<tr>
<td>Firewalls/next-generation firewalls (NGFW)/</td>
<td></td>
<td>58%</td>
<td>89%</td>
</tr>
<tr>
<td>unified threat management (UTM)/Network (NW) security</td>
<td></td>
<td></td>
<td>88%</td>
</tr>
<tr>
<td>Load balancing</td>
<td></td>
<td>58%</td>
<td>88%</td>
</tr>
<tr>
<td>Cloud security</td>
<td></td>
<td>80%</td>
<td>93%</td>
</tr>
<tr>
<td>Network and/or micro-segmentation</td>
<td></td>
<td>80%</td>
<td>35%</td>
</tr>
<tr>
<td>Endpoint security</td>
<td></td>
<td>87%</td>
<td>78%</td>
</tr>
<tr>
<td>Distributed denial of service (DDoS)/Web</td>
<td></td>
<td>67%</td>
<td>83%</td>
</tr>
<tr>
<td>application firewall (WAF)/internet defense</td>
<td></td>
<td></td>
<td>96%</td>
</tr>
<tr>
<td>Encryption, data loss prevention (DLP), and data security</td>
<td></td>
<td>52%</td>
<td>55%</td>
</tr>
<tr>
<td>SIEM/analytics</td>
<td></td>
<td>53%</td>
<td>48%</td>
</tr>
<tr>
<td>Secure access service edge (SASE)</td>
<td></td>
<td>34%</td>
<td>37%</td>
</tr>
<tr>
<td>5G network slicing</td>
<td></td>
<td>6%</td>
<td>5%</td>
</tr>
</tbody>
</table>

Base: respondents who indicated they are using/planning to use commercial public cloud
Source: IDC’s VMware Sovereign Cloud Survey, March 2021

n = 417
Essential Guidance

Develop a Data Strategy

Identify and ensure compliance with data privacy laws and industry regulations. Identify whether there is a national data strategy or sovereign cloud mandate for your country. Develop a data strategy that aligns to both, including data classification. Conduct an application, data discovery, and data protection impact assessment (DPIA) before adopting a cloud. For organizations that have not done so, consider creating a new role: chief data officer or data guardian. Engage your legal and security teams early to ensure your organization complies with organizational and national mandates and minimizes risk.

For national policy leaders, strategic plans should address how to protect and unlock the value of national data and how to build a national capability for the digital economy.

Shift from Cloud First to Cloud Smart

Develop a cloud migration strategy based on the aforementioned data strategy and assessment. Not all clouds are created equal. Deploy the right workload into the right cloud. Most organizations today have a multicloud strategy to reap the benefits of a specific cloud for a specific workload.

Data locality or residency is not true data sovereignty. Sovereign cloud options can provide buyers with greater data sovereignty and jurisdictional control of confidential and restricted data within their cloud environment as well as data independence and mobility, improved data access and integrity, and data security and compliance.

Have a cloud exit strategy. Data and workloads migrated to public clouds do not need to reside there permanently. Consider the security sensitivity of your data and required compliance as well as the impact of security breaches. IDC has observed that data and workloads may be in the process of moving between deployment locations until the organization is satisfied it is in compliance with current organizational regulations and national laws in addition to discovering the right functionality for specific data sets.

For national policy leaders, consider how sovereign clouds can help you execute national mandates regarding the protection of critical data, improving data privacy, pooling critical data to fuel economic growth, and building digital capabilities and skills within your nation.
Find a Trusted Multicloud Partner

Investigate how locally or regionally delivered sovereign clouds can help your organization achieve security and data sovereignty needs better than commercial public clouds. Conduct market research and consider cloud vendors you may not be using today but that have deep industry expertise across multiple clouds (including commercial public clouds) and understand national laws and corporate regulations regarding data sovereignty, data security and compliance, and data independence and technology interoperability.

Many organizations will benefit from engaging managed service providers to assist them with these recommendations as they are complicated and require an understanding of all the different types of cloud options available and which one will suit the organization.
Appendix

Summary Survey Demographics

Industry
- Government: 40%
- Education: 20%
- Financial services: 20%
- Healthcare: 14%
- Life science: 6%

Organization size by number of employees
- 500 – 999: 10%
- 1,000 – 4,999: 44%
- 5,000 – 9,999: 26%
- 10,000+: 20%

Decision authority
- Primary decision maker: 14%
- Part of a team that makes IT decisions: 76%
- IT decision influencer: 10%

Region
- North America: 16%
- Latin America: 11%
- Europe, the Middle East and Africa: 33%
- Asia/Pacific: 41%
About the Analysts

Adelaide O’Brien
Research Director,
Government Digital Transformation Strategies, IDC

Adelaide O’Brien is Research Director for IDC Government Insights responsible for Government Digital Transformation Strategies. Ms. O’Brien assists clients in understanding the full scope of efforts needed for digital transformation, and focuses on technology innovations such as Big Data, AI, cognitive, and cloud in the context of government use cases such as customer experience, data-driven benefits and services, and public health protection. Ms. O’Brien's research also includes a particular emphasis on journey maps that assist clients in understanding the full scope of efforts required to achieve outcomes, and she has benchmarked the maturity of deploying cloud and Big Data and analytics in the federal government. Her research also includes the threats and opportunities now facing government’s ecosystems in leveraging agency information as a critical asset, allowing stakeholders to make better decisions, provide better services and experiences for constituents, and react in real time to limit liabilities and manage risks.

More about Adelaide O’Brien

Christina Richmond
Program Vice President,
Security Services, IDC

Christina Richmond is the Program Vice President for IDC’s Security Services research practice. She is responsible for the day-to-day management of the program. Core research coverage for the team includes, but is not limited to, security consulting, integration, and managed services. In addition, the team looks at services that help organizations adopt emerging technologies like Cloud, Edge, and IoT as well as key focus areas such as Risk, Data Privacy, and Compliance. Christina brings a wealth of security services expertise and knowledge to the position and is frequently sought after by IT security executives to share her research and insights on dynamics and trends in the security industry.

Christina also focuses on the global IDC Technology for Social Good program which examines technology innovation and best practices, trends, portfolio offers, and initiatives developed by technology vendors and social entrepreneurs. The practice seeks to highlight technology that works to solve society’s largest challenges with Climate Impact, Environmental Sustainability, Diversity & Inclusion, and Communities at Risk.

More about Christina Richmond
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.