Meeting the Growing Need for Holistic Workload Protection

Sponsored by:
Cisco Systems

Author:
Brad Casemore

January 2019

IDC OPINION

As enterprises adopt multicloud postures and strategies, their distributed application environments will increasingly require holistic workload protection. While adoption of multicloud certainly confers undeniable business benefits, such an environment also brings larger attack surfaces and a proliferation in points of vulnerability.

Consequently, enterprises will need to pervasively implement modernized security mechanisms and models across both legacy and cloud-native workloads, regardless of the infrastructure on which workloads run and irrespective of whether workloads reside on-premises or in public clouds.

Across this spectrum of needs, most enterprises currently use a range of point products to address different use cases. These tools either have failed to remain relevant in the context of multicloud or function as fragmented and disconnected elements that fall short of providing holistic workload protection — hence the need for a more comprehensive strategy and an all-encompassing approach to security.

In this white paper, which features data from a worldwide survey as well as insights from interviews with enterprise customers, IDC explains why there is strong interest in a platform-based approach to holistic workload protection across a wide range of use cases. This white paper also explores how Cisco's Tetration platform specifically addresses the use cases and requirements that customers have identified relating to holistic workload protection in a multicloud world.

SITUATION OVERVIEW

In the context of digital transformation, applications have attained unprecedented importance, serving as the digital lifeblood for organizations worldwide. Applications increasingly represent the face of business, generating revenue, facilitating engagement with customers and other stakeholders, driving business outcomes and, ultimately, differentiating organizations from their competitors.

As these applications have gained in business importance, they are also evolving into dynamic deployments, leveraging virtualization, containerization and microservices, and workload mobility technologies. Consequently, communication patterns between application components change constantly as the east-west traffic within and between datacenters proliferates to the point where such traffic now predominates, marking a fundamental change from the north-south traffic patterns of the client/server era. This technological shift has contributed to an increased attack surface and new attack vectors that take advantage of extensive lateral movement across datacenter infrastructure.

IDC
ANALYZE THE FUTURE

Indeed, applications are now distributed, no longer residing solely in an on-premises datacenter. Enterprises are embracing hybrid IT and multicloud, choosing to run new and existing applications in public and private clouds while maintaining legacy business applications in on-premises datacenters. That last point warrants additional emphasis: Even as enterprises advance, embracing innovation accelerators in pursuit of digital transformation, they maintain bridges to what has come before — to previous investments in knowledge and technology and to legacy application environments that will remain relevant for years to come.

At the same time, the imperative to innovate will remain relentless. Innovation will only be amplified by the rise of microservices, which in turn will yield a growing number of business-critical applications developed with the inherent attributes of elasticity and portability. Microservices will make it possible for developers to construct highly distributed application environments in which application tiers and data services are increasingly spread across datacenters and public clouds.

Need for Holistic Workload Protection

These distributed application environments will create an unprecedented need for holistic workload protection. To be sure, in the context of hybrid IT and multicloud — where the legacy environments remain relevant even as enterprises charge headlong into a future with cloud-native microservices — workload protection is of paramount importance. Legacy workloads must be protected, of course, but the advent of multicloud introduces larger attack surfaces and manifold points of vulnerability. What's more, the ascent and primacy of applications mean the integrity and security of workloads, irrespective of where they reside and how they were architected, are chief concerns for all enterprises. That's why it's essential for modern security mechanisms and models to be pervasive across legacy and cloud-native workloads.

Today, enterprises have procured and use a range of point products to address a variety of use cases. For example, they have separate tools to address application discovery, policy enforcement and microsegmentation, compliance and audit, security forensics, simulation, container security, software vulnerability, and process behavior. Unfortunately, these disparate tools, even when they have kept pace with evolving requirements, function as discrete and disconnected puzzle pieces that provide only partial and fragmented elements of workload protection. Point products also inherently lack the ability to deliver ***"network effects,"*** in which a product or technology is used systemically across a growing number of use cases, with benefits and value multiplying as it addresses each additional use case.

Perhaps this is why IDC has noted growing enterprise interest in a more comprehensive and systematic approach to addressing the challenge of workload integrity and protection.

A Platform-Based Approach

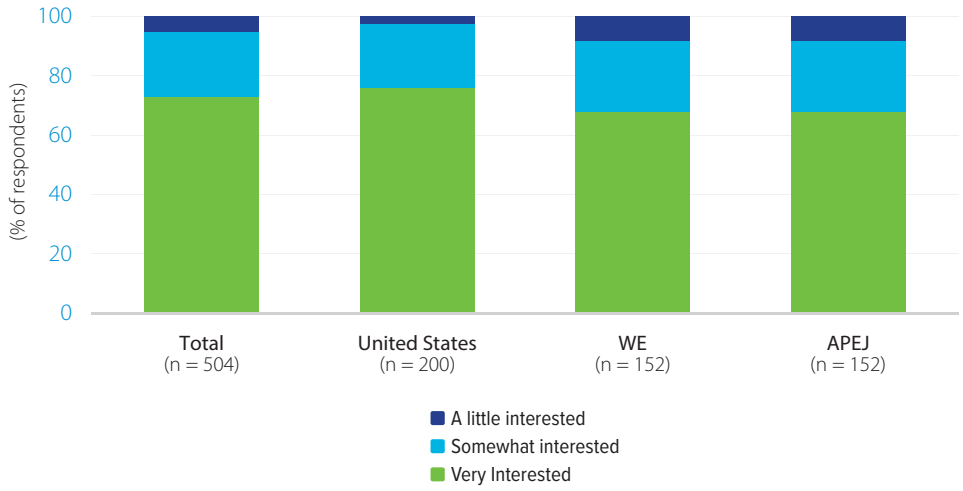
Overall Interest

In a recent worldwide survey commissioned by Cisco, IDC found that enterprise respondents expressed considerable interest in a platform-based approach that could address several of the aforementioned use cases. In fact, 72% of respondents indicated they were ***"very interested"*** in a platform-based approach, which was defined as one that addressed three or more use cases that included application discovery, security forensics, network security (microsegmentation), and visibility. The 72% of respondents that were ***"very interested"*** in a platform-based approach were well represented across geographies and other survey demographics. What's more, most respondents indicated that they will adopt a platform-based approach within the next 12 months (see Figure1).

FIGURE 1

Level of Interest in a Platform-Based Approach

Q. *How interested would your organization be in adopting a platform-based approach?*



n = 504

Source: IDC's Platform Solution Survey, 2018

IDC ANALYZE THE FUTURE

Point Products Deployed Today

- **Point product count:** Currently, the majority of survey respondents (72%) indicated that they had three or four point products, although regional differences surfaced. Respondents in Western Europe (WE) were more likely to have three point products, those in the United States had three to four point products, and those in Asia/Pacific (excluding Japan) (APEJ) reported with greater frequency than other regions that they had five or more point products.
- **Types of point products:** Point products in use cited most frequently include application dependency mapping and cloud workload protection (including microsegmentation):
  - Regional variations are notable: For application dependency mapping products, 77% of APEJ respondents indicated they had purchased such products compared with 62% of U.S. respondents and just 45% of WE respondents. Similarly, for container security products, 62% of APEJ respondents said they had purchased such products, while the percentages for WE and U.S. respondents were at 45.5% and 35.5%, respectively. For cloud workload protection products, the pattern was similar, with nearly 69% of APEJ respondents indicating they had purchased such products, whereas the percentages for the United States and WE were 61% and 55%, respectively.
- **Frequency of point product use:** Most respondents reported that they used their point products on a weekly basis, at minimum, and 42% of respondents indicated they used these products on a daily basis. Interestingly, those respondents who indicated they were ***"very interested"*** in a platform-based approach also tended to be daily users of point products. Perhaps not surprisingly, those who used point products on a daily basis also tended to have the greatest number of physical servers among respondents.
- **Satisfaction with current point products:** Interestingly, those respondents ***"very interested"*** in a platform-based approach also indicated they were very satisfied with their point products' implementation, integration, ongoing operations, and user/operator productivity. This might seem paradoxical, but it demonstrates that respondents are seeking an approach that is more comprehensive and holistic than what they have today. It also suggests that respondents are searching for better and smarter ways to work. What's more, those respondents ***"very interested"*** in a platform-based approach, as well as the broader population of respondents, indicated they were least satisfied with their products' costs, in terms of both initial up-front costs and ongoing annual costs.
- **Perceived benefits of a platform-based approach:** Although many respondents voiced concerns about a potential quality compromise in adopting a platform-based approach, they anticipate significant benefits accruing from adoption, including operational efficiencies (48%), cost savings (capex and opex) (42%), and a ***"network effect"*** (44%), where the value of the platform multiplies as it is used for more use cases and sometimes by more users (see Figure 2). Further:
  - Another factor that favored a platform-based approach involved the degree or level of expertise within respondent organizations. Respondents expect a platform-based approach to extend a single learning curve across a wide range of use cases pertaining to cloud workload protection versus point products, which tend to necessitate more lengthy training cycles and daunting learning curves.

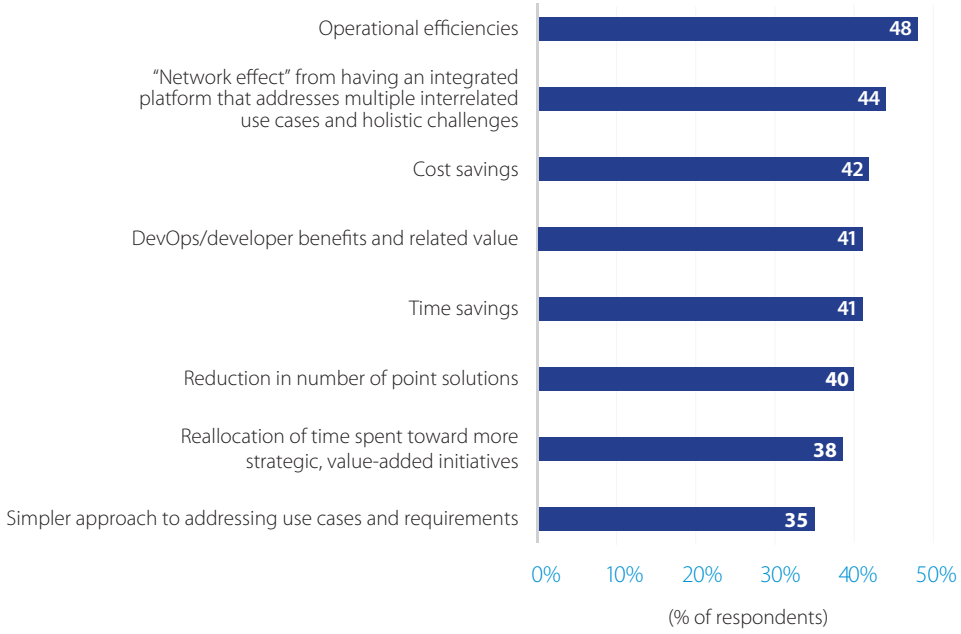
» **Preferred form factor of a platform-based solution:** Given the nature of increasingly distributed application workloads at enterprises today, it should come as no surprise that survey respondents expressed a desire for a platform that could support all deployment options, including on-premises, private cloud, and multiple public clouds:

- There is no clear favorite, although an on-premises physical appliance finished slightly ahead of other options. U.S. respondents had a clear preference for on-premises physical appliances, aligning closely with their workload placement, while WE respondents tended to prefer on-premises virtual appliances and APEJ respondents were more inclined toward software as a service (SaaS). Again, these preferences were in general alignment with each region's cloud orientation and workload placements.
- Deployment scenario is where security features for cloud workload protection emerge as prominent considerations, as the use cases must be addressed not only in on-premises datacenters but also in private clouds and public clouds. Point products typically are inherently limited in their ability to both address multiple use cases and consistently address the increasingly distributed nature of multicloud workload placement.

FIGURE 2

Benefits Anticipated from Platform Adoption

Q. *What benefits do you anticipate from the adoption of a platform-based approach?*



n = 504
Source: IDC's Platform Solution Survey, 2018

CISCO TETRATION'S APPROACH TO ADDRESSING HOLISTIC WORKLOAD PROTECTION

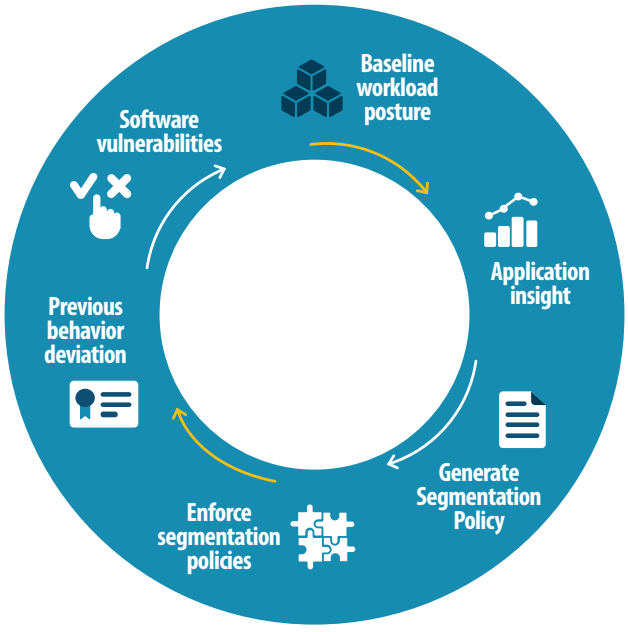
The Cisco Tetration platform has evolved steadily since its inception. It now implements a zero-trust model through segmentation as part of its ability to provide holistic workload protection across multicloud environments. The objective is to enable organizations to quickly identify security incidents, contain lateral threat movement, and reduce attack surfaces. As a platform, Tetration provides an infrastructure-agnostic approach that supports workloads that reside on-premises or in multiple public clouds.

In the multicloud datacenter, Tetration supports **pervasive workload protection** using white list-based segmentation, the foundation of a zero-trust security model, as well as behavior baselining for analysis and identification of process deviations. Moreover, the Cisco Tetration platform provides baselining for analysis of traffic flow deviations, including signs of data exfiltration. It also facilitates detection of common vulnerabilities and exposures associated with software packages installed on servers, and it provides the ability to take **proactive security measures**, such as dynamically quarantining servers when vulnerabilities are detected and similarly blocking communication upon detection of policy violations.

In addition, Tetration can use the Cisco AnyConnect NVM module to collect telemetry from endpoint devices such as laptops, desktops, and smartphones, providing insights into application access behavior, including which users and user groups are accessing what applications (see Figure 3).

FIGURE 3

Cisco Tetration — Hybrid Cloud Workload Protection



Source: Cisco, 2019

The creation of automated white list policy for segmentation is supported through real-time telemetry from application components and behavior analysis algorithms. **The continuous telemetry makes it possible to keep policies relevant and up to date.**

The Cisco Tetration platform is designed to fully address these challenges using comprehensive traffic telemetry data collected directly from the application servers. Indeed, Tetration is an integral component of Cisco's intent-based network for multicloud datacenter, working in conjunction with Cisco's Application Centric Infrastructure (ACI), Nexus 9K datacenter switches, and Cisco Network Assurance Engine. When ACI and Tetration are used together, the former provides intent-based fabric automation and segmentation, whereas the latter also delivers segmentation, as well as policy-informing visibility and holistic workload protection. To be clear, though, Tetration is also capable of providing segmentation on its own, independent of ACI, giving the customer the flexibility to choose the type of infrastructure it wants to employ to achieve this objective without constraint or restriction.

Tetration performs advanced analytics using an algorithmic approach that includes unsupervised machine learning techniques and behavioral analysis. The platform provides functionality across the use cases mentioned previously in this white paper and in the survey of worldwide enterprise respondents, namely discovery, security enforcement and microsegmentation, compliance and audit, network forensics, simulation, network visibility, container security, software vulnerability, and process behavior.

The Tetration platform not only addresses the requirements of hybrid IT and multicloud — supporting on-premises workloads, private clouds, and multiple public clouds — but also **provides customers with a range of form factors, including on-premises physical appliances, virtual appliances, and a software-as-a-service delivery option.**

CUSTOMER EXPERIENCES WITH THE TETRATION PLATFORM

This section features two interviews with Tetration customers, focusing on the capabilities of Tetration and the value it has provided. This section also examines how Tetration has extended its purview within these customers' environments, typically first addressing a single use case of primary importance and then gradually addressing other use cases as the platform evolved and as customers grew increasingly confident in Tetration's capabilities.

Healthcare Services Provider: From Segmentation to Broader Workload Protection

A large provider of healthcare services originally deployed the Cisco Tetration platform when the provider was in the midst of moving a datacenter. The architecture was a bit dated, and the healthcare provider wanted to use Cisco ACI for segmentation. The problem was, the provider lacked visibility into application dependencies and wasn't sure which policies to implement for segmentation purposes.

The customer had also attempted segmentation previously, running into numerous challenges. The customer had, for example, used a NetFlow tool for packet capture, which provided static snapshots of network traffic but not real-time telemetry flow. This meant that policy and rule definition were imprecise and subject to error.

It was at this point that Cisco introduced the customer to Tetration. Indeed, the customer was one of the first to deploy a full-rack Tetration cluster, and its initial attraction to Tetration was for policy creation and segmentation. Initial evaluation of Tetration took place in late 2016, and the platform was fully deployed early in 2017.

After using Tetration first for the use case of policy and segmentation, the customer recognized that it also could be used for other purposes. A follow-on use case involved application troubleshooting and remediation, with visibility into application dependencies and whether latency issues were attributable to the application or the network.

The customer also looked at how Tetration could be used for visibility into and control over host-based firewalls, enforcing intent-based policy with hardware and software visibility and detection across physical and virtual infrastructure. In addition, the customer is looking at how Tetration could be used with host-based firewalls to migrate workloads to the cloud while ensuring that consistent security policies can be applied holistically.

Tetration has yielded several benefits, starting with a reduction in man-hours associated with the datacenter migration, particularly through making it easier and faster to determine what belongs to each group involved in the move. Application troubleshooting, which helps identify whether latency issues are attributable to the application or the network, has resulted in faster remediation and better application availability and performance.

Another benefit has come from the ability to use Tetration to apply policy modeling on live traffic. This enables the proactive simulation of traffic patterns and application dependencies to understand the impact of new policies before they're put into production.

Tetration's greatest impact has been in segmentation enforcement and understanding the consequences of policy and policy changes. The customer is also looking at extending Tetration to multicloud scenarios for holistic workload protection.

In summary, the customer had the following to say about the Tetration platform:

> ***"When you drop something on the network, you need to go in and understand what it needs to speak with and how it needs to speak with it. The rules and policies need to be appropriate, and you need to ensure that things are done securely. Tetration provides a fountain of data, and it's in a unique place to tell you about that data and influence traffic."***

> ***"Tetration is a fantastic product, and we've been impressed with Cisco's willingness to enhance it. It's been impressive to see it developed and enhanced from its inception to address use cases that weren't envisioned when we first adopted it."***

Large Financial Institution: Mean Time to Innocence and Workload Protection

One of the largest financial institutions in Africa said its initial interest in the Tetration platform could be summed up emphatically in three words: ***"visibility, visibility, visibility."***

The visibility was essential because the network was continually and reflexively blamed for application performance problems and outages, invariably in the absence of proof that the network was at fault. In adopting Tetration, the customer wanted to expedite ***"mean time to innocence"*** by demonstrating incontrovertibly that the network was not to blame for performance issues that had other root causes, such as a faulty web server.

The Tetration platform gave the customer a single view into the network and applications for a use case that was centered on troubleshooting and remediation. Now, though, with ***"mean time to innocence"*** addressed, the financial institution is using Tetration for policy formulation and definition.

As the customer said, ***"If we didn't have Tetration, we wouldn't have the capability of doing SDN."***

Other use cases have developed, too, notably workload protection. The customer said that Tetration's workload protection functionality has allowed it to retire point products. The customer had been using a variety of tools for visibility, network monitoring, and network access control, and many of those tools have now been displaced in favor of a platform-based approach.

The customer also emphasized the ***"network effect"*** associated with Tetration: The more that team members use Tetration, the more use cases and benefits the customer associates with it. As that happens, additional point product tools will be retired. In that respect, the customer observed that Tetration, for example, might be used by the SecOps team in conjunction with vulnerability scans to better manage firewall rules.

The customer said: ***"Now we're opening up Tetration to all the IT shops in the company, not just my platform and team. The more people that use Tetration, the more tools that we'll get rid of."***

The financial institution first started using Tetration about 18 months ago, but it has been using the platform more extensively within the past year. The customer first deployed Tetration across 1,000 servers, and now it's used across about 5,500 servers. With Tetration demonstrating tangible benefits and business outcomes, the IT team's investment in Tetration has won the confidence and buy-in of the business. The customer said: ***"It's showing value that nothing else in this environment could have delivered."***

The environment itself is complex. The financial institution is a venerable bank, and it runs an extensive array of legacy and new applications. As the customer described it, ***"From an application and infrastructure standpoint, you name it and we've got it."***

In that environment, Tetration is implemented across networks, security services, and a growing constellation of other infrastructure. The server team initially had reservations about Tetration agents running across its infrastructure, but the team members changed their minds after seeing the results achieved on the first 1,000 servers.

These results included troubleshooting and remediation processes that were reduced from hours or days to mere minutes. Tetration gave the customer the ability to resolve firewall issues on servers that ran open source monitoring tools. In these scenarios, the rogue process or issue was something that those tools didn't monitor.

Tetration is now used across a range of use cases, starting with visibility and now extending to policy definition and formulation, workload protection (including security detection and enforcement), vulnerability management, and change previews and replays in which the customer can simulate moves of load balancers or firewalls to understand the implications. As the customer explained it, ***"Now I test what I want to change in Tetration before I make the change."***

Tetration will be used in other use cases too. The customer expects additional value of using Tetration in the security realm, identifying and checking anomalous behavior. In addition, as the financial institution embraces containerization and microservices, Tetration will play a role in providing cloud-native workload protection, including behavior modeling of cloud applications in a multicloud environment.

Even before then, however, the platform capabilities of Tetration have resulted in displacement of point products at the financial institution. An APM tool, for example, has been retired, principally because Tetration offered a comprehensive view of east-west datacenter traffic, allowing operations to see what happened and what changed in real-time flows. Other point products, too, are being displaced by Tetration, including network monitoring tools and other visibility offerings.

As noted previously, a primary benefit the financial institution has gained from Tetration is ***"mean time to innocence,"*** which derives from the platform's ability to quickly ascertain, through troubleshooting and remediation, whether performance-related problems are attributable to application or server issues rather than network issues.

CHALLENGES/OPPORTUNITIES

For enterprises, the principal challenge is how to provide holistic workload protection in an increasingly multicloud world. Today, as the survey results have shown, enterprises typically use several tools and point products to achieve their objectives, and though many of those point products offer familiarity and value to those that have procured and use them, they sometimes fall short in areas where new functionality is required, and they each entail learning curves and expertise. What's more, point products typically operate in isolation from one another and fail to deliver comprehensive or holistic insights, which are increasingly important as applications become distributed across on-premises and cloud environments.

For Cisco, the challenge is persuading these customers that a platform-based approach delivers the holistic workload protection without compromising functionality across use cases, infrastructure, and application environments. Cisco also must ensure that prospective customers understand the full array of benefits, including the aforementioned ***"network effects,"*** that Tetration can provide.

Conversely, Cisco's opportunity manifests in successfully positioning Tetration as an indispensable platform for holistic workload protection within the context of multicloud. If Cisco is successful, Tetration will become a cornerstone element in how its enterprise customers defend and maintain the integrity of applications and infrastructure in the cloud era. For customers, of course, the opportunity is in gaining that comprehensive workload protection and in the ability to confidently and securely execute their digital transformation initiatives and multicloud strategies.

CONCLUSION

Increasingly complex and distributed application environments are a consequence of enterprises embracing hybrid IT and multicloud. This development has yielded a need for holistic workload protection that has the breadth and depth to cover a full range of use cases across legacy and cloud-native applications, all forms of infrastructure, and applications residing both on-premises and in public clouds.

IDC survey data confirms strong enterprise interest in holistic workload protection through a platform-based approach. Survey respondents perceived several benefits stemming from platform adoption including operational efficiencies, cost savings, and a significant network effect, in which the value of the platform increases as it used more extensively. Those benefits, as well as others, were also cited in interviews with customers that have adopted and use the Cisco Tetration platform.

In opting for a platform-based approach to holistic workload protection, enterprises have been adamant: They don't want to compromise on quality when it comes to functionality and use cases. Enterprises also want a platform-based approach to support all deployment options, including on-premises, private cloud, and multiple public clouds. Enterprises also expressed interest in form factors that extend from on-premises physical and virtual appliances to SaaS delivery options.

The Cisco Tetration platform addresses the aforementioned requirements for holistic workload protection across the multicloud landscape, effectively responding to enterprise demands at a time when workloads are more directly related to business outcomes than ever before.

IDC Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC
ANALYZE THE FUTURE