White Paper

Three Mistakes to Avoid When Moving to the Cloud — A Unified Security Policy Guide

Sponsored by: Fortinet

Frank Dickson Philip Bues Jay Bretzmann

June 2021

INTRODUCTION/EXECUTIVE SUMMARY

Trust. Capabilities. Guidance. These are the hallmarks of successful cloud deployment. Digital transformation was accelerated by the pandemic made possible by the advent of the public cloud and cloud marketplaces. Customers now search for independent software vendor products and services that easily integrate with these cloud platforms, to the delight of many security practitioners. This new software delivery model enables the best of both worlds: best-in-breed solutions that are easy to find, test, buy, and deploy. In this paper, IDC explores the current unprecedented migration to the cloud through the lens of Fortinet and its marketplace partner, Amazon Web Services (AWS). We'll cover common migration mistakes, how the reality of cloud for many may be a hybrid architecture, and the various opportunities and challenges to effectively securing your critical systems in the face of an unprecedented cybersecurity talent shortage and an increasing attack surface with new threats and vulnerabilities around every corner of your organization (including your kitchen).

SITUATION OVERVIEW

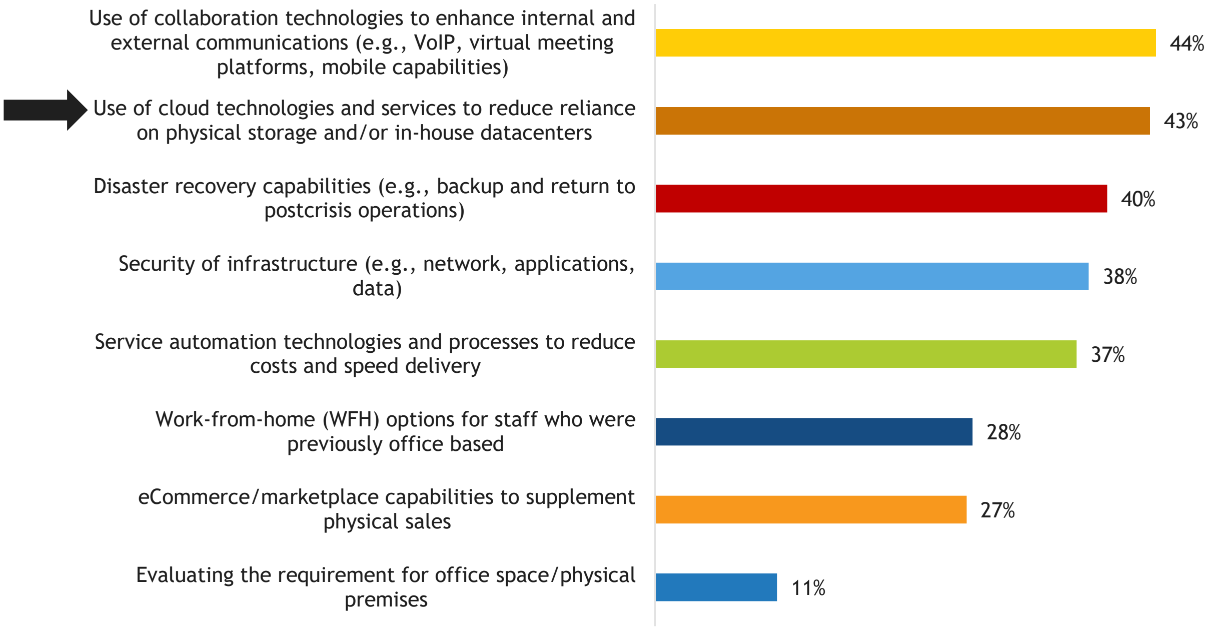
As businesses map out their cloud journey, they see cost savings on technology infrastructure, faster deployments, enhanced productivity, near limitless scalability, trained security practitioners, and the list goes on. Organizations seldom move to "the" cloud; rather, they create a hybrid cloud architecture with a heavy emphasis on the cloud but retain some functions and workloads on premises. As shown in Figure 1, 43% of respondents in IDC's *Service Provider Pulse, 1Q21: Survey Findings* indicate that they have moved to or are considering cloud technologies and services to reduce reliance on, not entirely replace, physical storage and/or in-house datacenter.

Defining your cloud environment, determining your deployment model, partnering with the right cloud provider, and preparing your security audit road map will determine which fork on the road leads to nirvana; so choose wisely. Not only does cloud migration have several security challenges to consider but security in general is provisioned differently in the cloud. Granular policy-based IAM and authentication, zero trust controls across logically isolated networks, and next-generation web application firewalls are just some of the features/differences and advantages. Also, inherent is the shared responsibility model (SRM) with your public cloud provider. In general, the SRM means that a cloud service provider (SP) is responsible for the security of the cloud and the users (customers) are responsible for securing the data they put in the cloud.

FIGURE 1

Reduced Reliance in On-Premises Datacenters Is Here to Stay

Q. You indicated that the COVID-19 pandemic has caused you to reconsider or develop your organization's business resiliency plans. What specific aspects have you changed or are considering? [Choose all that apply.]



n = 183

Source: IDC's *Service Provider Pulse, 1Q21: Survey Findings,* March 2021

As organizations leverage hybrid cloud to digitally transform, the implementation choices can complicate or facilitate trust. Taking time up front to establish a security baseline is the first step in ensuring the confidentiality, integrity, and availability (CIA) of your systems. In fact, as shown in Figure 2, to meet customer requirements, 49% of respondents ranked investment in cybersecurity protection as the top priority.

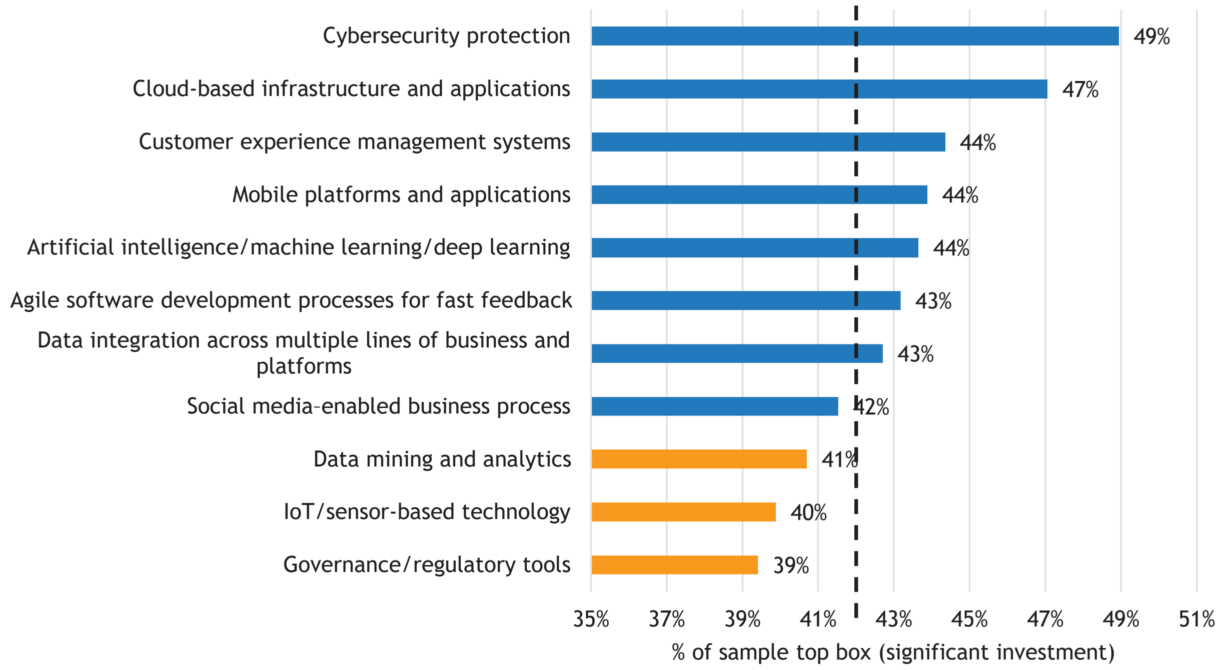
Many benefits drive the movement to the cloud such as:

- Agility, speed, and efficiency
- Rapid testing and development for launching new products and services
- Deploying resources quickly in response to changing business conditions
- Full scalability and visibility in real time

FIGURE 2

Cybersecurity Requires Investment, and Customers Agree

Q. Rate the level of investment in the following services over the next 24 months to meet your customers' requirements (0 = No investment, 10 = Significant investment) (Randomize.)



n = 850

Source: IDC's *Service Provider Pulse, 1Q21: Survey Findings,* March 2021

Essential Guidance

As stated previously, the implementation choices made during our cloud migration can complicate or facilitate trust. Taking time up front to establish a security baseline is the first step in ensuring the confidentiality, integrity, and availability of your systems. As companies look to plan their cloud migration strategy, IDC has identified three common missteps (discussed in the sections that follow) to avoid in moving to the cloud.

Bringing Your Legacy Security Deployment Model with You to the Cloud

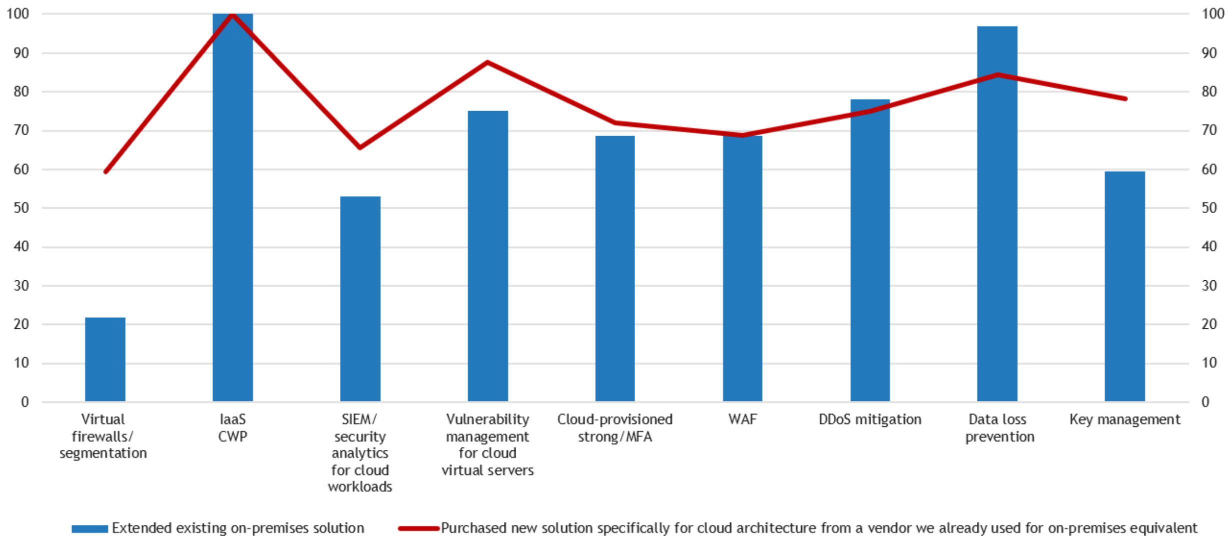
The keyword here is legacy. Regardless of how cool the code name may be for your particular deployment model, a legacy system by its very definition is "outdated." Now that doesn't mean that you shouldn't take advantage of the institutional knowledge and training that internal resources and partners have developed over time on your tools. In fact, cloud service providers and marketplace vendors offer several options to extend on-premises data stores and security and governance policies. Just as lifting and shifting on-premises IT architectures to the cloud creates a "clunky" cloud deployment, lifting and shifting on-premises security to the cloud is suboptimal as cloud is all about agility and your security operations should reflect this reality. As shown in Figure 3, many still extend existing on-premises solutions to the cloud.

When organizations shift on-premises products into the cloud instead of extending security architectures to the cloud, IDC survey data shows that organizations later replace the solution. Unless internal staff have the necessary skills and training, not having the right partner in place to manage that transition and optimize your current tools without a rip and replace can cause data loss and downtime and be cost prohibitive when trying to scale among multiple sites and geographies.

FIGURE 3

Protection of Workloads/VMs in IaaS

Q. Thinking about security solutions for cloud architecture (PaaS, IaaS), when your company first adopted cloud architecture, how did you choose to secure it? In other words, for each of the security functions below, how did your organization primarily apply them to the new cloud architecture?



n = 204 (organizations with 2,500+ employees)

Source: IDC's *Cloud Security Survey,* 2018

Cloud is not just another environment — it's a different way to provision IT. Hardware and software are built in with the cloud platform along with the additional products and services offered by partners, allowing for greater customization. Auto updates reduce error and the need for internal resources. Scalability is on demand and services are pay as you grow (PAYG). Remote support is a given. These are not checkbox items for on-premises infrastructure. On-premises tools protect on-premises infrastructure. Cloud tools protect assets in software-defined compute infrastructure, regardless of when the virtualization happens in the datacenter or IaaS. The key is to have a singular set of policies that unify across all infrastructure (one set of policies to rule them all) extending on-premises policies to cloud-native tools.

In this case, IDC recommends a holistic security approach to integrate and optimize these protections both at the workload and at the edge. This is made possible by leveraging those existing frameworks that will speed the enablement of a stable cybersecurity posture. A greater emphasis may be placed on protections at the edge, releasing the burden at the workload and providing that critical "endpoint" protection. While there is no single vendor that can provide a full SASE solution, threats and vulnerabilities are better addressed by SASE "buckets" such as integrating software-defined wide area network (SD-WAN), network firewall, and secure web gateway technologies.

By 2024, 25% of organizations will improve business agility by integrating edge data with applications built on cloud platforms, enabled by partnerships across cloud and communications service providers (see prediction number 9 in *IDC FutureScape: Worldwide Cloud 2021 Predictions,* IDC #US46420120, December 2020).

The key is to not simply replicate the on-premises model in the cloud. The key is to have security tools that are software defined and that can be deployed and can scale and operate in a dynamic, cloud-native way; that automate the protection of ephemeral cloud resources that are appearing, multiplying, and disappearing on a permanent basis; and that integrate with a new and evolving system of cloud tools and services.

Not Reengineering SecOps for a Hybrid Cloud Environment

Lower risk and easy to manage are some of the benefits that come with the cloud. It's an all-in-one solution that doesn't leave you looking for that one last piece of the puzzle – it's already put together. As enterprises grow, private clouds become necessary to augment public clouds. These virtual private clouds are also available within a public cloud. At this stage, every part of your application life cycle should be reengineered to take advantage of the agility unlocked by moving to the cloud and optimizing cloud-native applications that have been designed "for the cloud." This effectively increases the speed at which you can innovate, deploy, and update so you can bring your solutions to market faster.

The cloud is also open to the internet by default making it completely dynamic, so security must be provisioned differently. Cloud service providers offer a level of assurance that's hard to replicate. Security staff and resources (both virtually and physically) are available 24 x 7 protecting your information. Redundancy, backups, and disaster recovery help you sleep better at night. Patching and auto update remediation are available through ML and AI. Encryption is made simple to prevent data exposure. They are constantly retraining and hiring so staff is on the edge of the latest technology.

Not Excising Legacy Business Processes

At the end of the day, on-premises security models that were designed to protect monolithic applications are simply not intended or optimized for the cloud. Today's emphasis is on agile operations and extending policies and rules to the cloud. Leveraging security models that are reengineered for the cloud lets you take full advantage of all that the cloud has to offer. You can't go half way – you have to lean all the way in.

The cloud migration benefits we've seen and commented on are vast including cost cutting, reduced TCO, and access to emerging technologies and partner ecosystems. The procurement model must also be reengineered, where previous security buying decisions may have been predicated partly on a list of wants. Now it's all about goals and outcomes. So the financial model must recognize this now as opex, not capex. It's a reality for the future. And it's not just procurement models – the entire application life cycle has to be reengineered for the cloud (design, build, release, operate, support, and so forth).

Moving away from legacy business processes also brings a new level of transparency to procurement and performance. Leveraging your cloud SP marketplace in this way will be sure to bring a smile to any procurement department. Customers can now enjoy buying cloud security like they buy cloud, based on usage. It's a pay-per-usage model.

Some of the new ways in which marketplaces are increasing visibility and cost optimization for enterprises is by enabling organizations to associate cloud and cloud spending to specific projects, allowing for security costs to be linked with lines of business. Security then becomes a pass-through expense rather than a cost center. Attributing this to a line of business is a game changer and allows teams to optimize and forecast for better planning.

Additional savings on the marketplace can also be seen through the private offer features. This allows you to negotiate terms and discounts that are not publicly available. Private offers allow sellers and buyers to negotiate custom prices and end-user licensing agreement (EULA) terms for software. Private offers can include a free trial enabling flexibility and cost management while minimizing risk to the customer.

Solution

To maintain pace with today's complex and fast-evolving threat landscape, enterprises need to feel safe in the hands of a proven cybersecurity platform. A security architecture that can truly help "realize the promise of cloud" with dynamic services elevates the security baseline and posture but also fits within the construct of reducing infrastructure sprawl with elegant design offerings. Enter Fortinet and AWS integrations. Fortinet comes with a mature security fabric and a pragmatic approach to cloud security, realizing that organizations that move to the cloud also stay on premises. This is a hybrid cloud reality.

Fortinet not only provides cloud migration guidance but also offers a proven security blueprint to extend and translate rules and policies to the cloud. All of this takes place through its software-defined security that operates in a cloud-native manner. These solutions identify, assess, and mitigate cloud risks and allow your on-premises and cloud resources to coexist leveraging cloud-as-a-platform benefits to delivering agile security services. FortiGuard is able to ingest over 100 billion security events every day to generate intelligence on known threats and those being seen for the very first time. Offerings such as AWS Network Firewall with Fortinet Managed IPS Rules are powered by that threat information, auto updated, and deployed. There are multiple rule set options to choose from covering common use cases such as malware detection and vulnerabilities across application, network, IoT, and server/OS.

Organizations look to security vendors to help minimize the complexity created by the hybrid architectures that they implement. Fortinet and AWS collaborated and brought to market solutions that do just that — simplify. Fortinet Security Fabric for AWS provides visibility across the attack surface. FortiGate-VM Next-Generation Firewall (NGFW) integration with AWS Gateway Load Balancer helps organizations simplify and secure their Amazon VPC environments. The Fortinet Adaptive Cloud Security provides native multilayered security from across clouds and datacenters to AWS.

Fortinet looks to leverage the investment customers made in on-premises security measures by extending the security context policies and rules to cloud offerings for a consistent and uniform security architecture. These are not legacy systems being repurposed but rather a simplification of a unified policy framework.

Next-generation fire walls, web application firewalls (WAF), secure email gateways, sandbox, and workload protection are integrated in a single platform. Fortinet removes a lot of the complexities for customers as they grow as well. This can be seen when a customer begins on a native AWS WAF but then opts for the Fortinet FortiWeb Cloud WAF-as-a-service AWS subscription-based solution. To Fortinet, cloud is about agility and enabling security practitioners to embrace automated workflows directly from their consoles. Also, it's worth noting that these solutions come with bring-your-own-license (BYOL), pay-as-you-grow, and 14-day trial options.

The Fortinet Security Fabric approach makes the most out of agile cloud benefits:

- Single-pane-of-glass control and management across on premises and cloud
- Visibility and control native to AWS, in addition to working across all cloud platforms
- Integration and uniform protection across the entire attack surface

Fortinet has made an investment in the AWS partnership as a long-term partner, with 44 products on the AWS marketplace. As a result, organizations gain in-depth cloud-native visibility and control into AWS application deployments and workloads.

Challenges

Fortinet is not the only security company on the AWS marketplace, nor is the marketplace the only place in which security solutions can be found. With each passing day, there is yet another new security company that may or may not add value to an organization's security architecture. Frankly, the multitude of vendors creates a lot of noise; and the noise can be deafening. Perceiving differentiation among the vendors is key. IDC recommends focusing on the benefits offered to an organization's individual use case. Benefits measured in terms of impact on security personnel are recommended as security professionals are an organization's most precious asset.

In addition, Fortinet and any other security vendor can only mitigate so much complexity for an organization as organizations create their own complexity. Cloud often means "freedom" — freedom to implement different solutions and different security tools. Just because an organization is free to choose and use as many security tools as it likes does not mean it is a best practice. In IDC's recent presentation at IDC Directions 2021, IDC established that complexity is the enemy of security and measures of complexity positively correlate with breaches. Fortinet is constrained by an organization's willingness to proactively manage complexity. It cannot save an organization from itself.

CONCLUSION

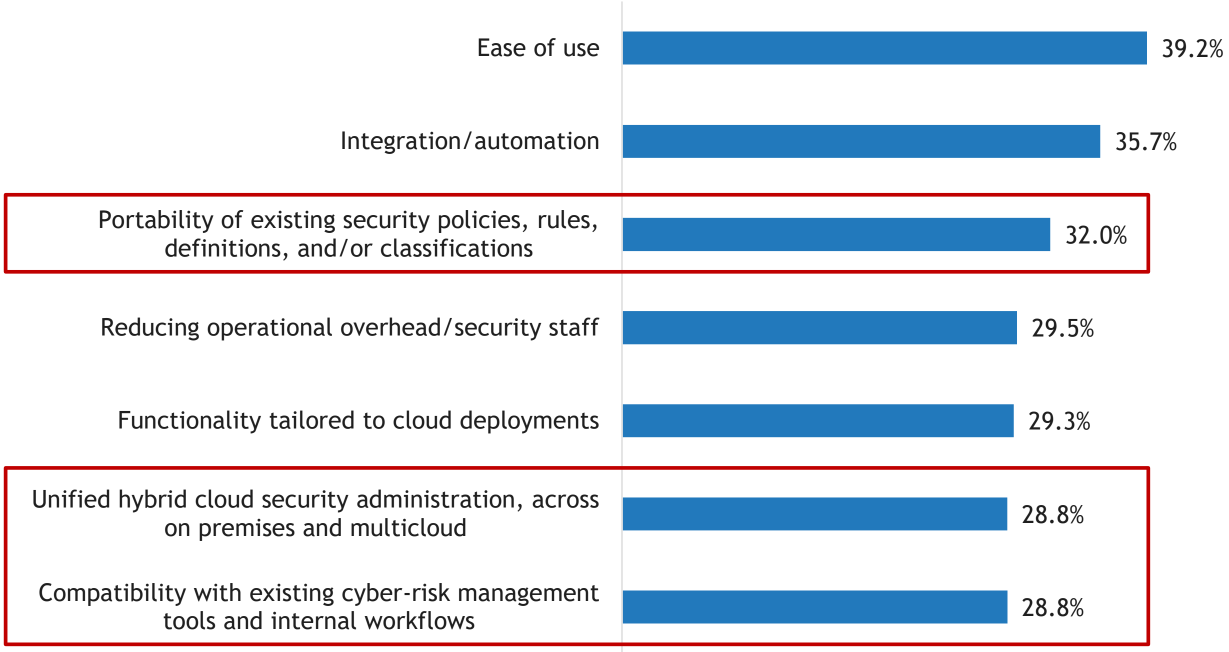
The cloud is different. The promise of cloud is real. The cloud for Fortinet is wherever a service edge can be software defined. Independent software vendors want to bring the cloud service providers such as AWS and their customers closer around that edge — no matter where that exists — so they too can offer their services.

On premises and cloud should not be mutually exclusive. As an IDC survey called out, hybrid cloud is the new reality (see Figure 4). Just because configurations, controls, and tools are different, the goal is not to create two completely disconnected security architectures.

FIGURE 4

Cloud Workload Security Selection Criteria

Q. Please rank the top 5 reasons for selecting [Q1 vendor] as your primary supplier of cloud workload security.



n = 403 (organizations with 2,500+ employees)

Source: IDC's *Cloud Security Survey,* December 2020

Security tools should extend across cloud and on premises to reduce complexity and increase efficacy. Nonintegrated solutions just cause headaches and unnecessary work for the already overburdened IT staff. Policies and rules should be consistent but adapted to each environment and controlled by a singular, unified console: the single pane of glass.

Implementation choices made during our cloud migration can complicate or facilitate trust. Intentional and deliberate planning is key in cloud migration strategy to avoid the three common missteps in bringing your legacy security deployment model with you to the cloud, not reengineering SecOps for a hybrid cloud environment, and not excising legacy business processes.

MESSAGE FROM THE SPONSOR

Fortinet secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments. Fortinet is a top global supplier of security appliances shipped worldwide and more than 500,000 customers trust Fortinet to protect their businesses.

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.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com