IDC ANALYZE THE FUTURE

IDC TECHNOLOGY SPOTLIGHT

Sponsored by: StorageCraft

Disasters and data loss events are a virtual certainty. Businesses should be asking themselves how they plan to react and minimize downtime "when" a disaster strikes, not what they might do "if" a disaster strikes. Increasingly, organizations are turning to cloud disaster recovery services to implement automated, cost-effective solutions.

Cloud-Based Disaster Recovery Services Help Organizations Achieve Business Resilience

December 2020

Written by: Andrew Smith, Research Manager, Cloud Infrastructure Services

Almost Half of Enterprises Do Not Have a Fully Functioning Disaster Recovery Solution or Plan

IDC estimates that up to half of all organizations would be unlikely to survive if hit by a disaster that rendered their datacenter unusable. In part, this is because, on average, less than half (48.4%) of applications are covered by a disaster recovery (DR) plan. The primary reason that organizations do not have a complete DR plan is cost. The traditional DR method is either having duplicate datacenters with redundant failover or contracting with a third party for the redundant infrastructure. In most cases, these solutions nearly double the organization's infrastructure cost and can quickly be interpreted by the business as an overpriced insurance policy rather than a critical enabler of enterprise IT operations.

The second reason for DR deficiencies is complexity. Most organizations have dozens or hundreds of applications with complex permutations of interrelated infrastructure. This complexity means that many organizations with DR plans can see them become outdated or obsolete overnight as business operations evolve, new systems are added, and old systems are decommissioned.

To address the fundamental DR challenges of cost and complexity, many organizations are moving to adopt disaster recovery as a service (DRaaS) solutions. DRaaS is a cloud-based DR solution that provides on-demand access to storage, networking, and compute resources to execute application failover in the event of a disaster. DRaaS providers also add modern tools such as workload migration, user self-service portals, automated alerts, data replication, and recovery orchestration to dramatically simplify the process of recovering virtualized workloads in secondary locations. This analysis provides a high-level overview of the technical aspects of modern DRaaS solutions and what buyers should look for in a competitive solution/services set. In addition, we provide readers with an overview of the growth forecast for the DRaaS market and how it compares with the growth forecast for the traditional data replication and protection (DR&P) software market.

AT A GLANCE

KEY TAKEAWAYS

- Many organizations still see DR as an unnecessary expense, and as a result, less than half of enterprise apps are covered by a DR plan today.
- DRaaS solutions address cost and complexity associated with traditional DR through managed service, automation, and cloud.
- For many organizations, DRaaS makes DR a reality where it was previously cost prohibitive, opening an opportunity to rethink their disaster planning and business resilience strategy.

Disaster Recovery as a Service: Why It Matters, Key Features/Functions

A successful DR plan is much more than an IT exercise. IT-driven DR efforts are necessary to ensure application availability, and they can be accomplished exclusively through the IT team. However, fully developed DR efforts involve the entire organization (i.e., people, process, *and* technology). Disasters do not discriminate; they affect line-of-business (LOB) workers and operations as much as they affect IT systems and operations. For this reason, organizations must take a holistic approach to DR planning that includes both IT and LOB as the potential impact of downtime will affect the entire enterprise. DRaaS solutions are designed to achieve this goal, combining technology and operational capabilities in cloud-delivered services. Due to the cost and complexity factors outlined previously, many organizations will not have the manpower or the funds to execute their DR efficiently. Increasingly, DRaaS providers help organizations of all sizes fill this gap with solutions tailored to their specific size, industry, or application(s).

What Is Enterprise DRaaS? Key Elements of the Service and a Comparison with Traditional DR

DRaaS is a cloud-based service whereby IT organizations can subscribe to the compute, storage, and networking infrastructure corresponding to their application requirements. A key element of the solution is the scalable, on-demand nature of these infrastructure-as-a-service (IaaS) resources. All modern DRaaS solutions offer IaaS resources that can be provisioned, scaled, and paid for on demand as part of the overall subscription service.

When comparing DRaaS with traditional DR solutions, organizations should keep in mind the following three key differentiators:

1. Unlike traditional DR, with DRaaS, the organization doesn't need to stand up and bear the cost of its alternative infrastructure in a second datacenter. This is important both for enterprises that wish to reduce their datacenter footprint and for smaller enterprises that do not have the facilities or operational capacity to manage their offsite resources. Cloud-based DR addresses a wide range of greenfield opportunities because it enables DR for this segment of smaller enterprises where it was previously cost prohibitive.
2. When considering traditional DR services, the organization must contract a specific set of systems and system resources, which may lay idle when not in use. With DRaaS, IT organizations will usually stage data at the DR site using periodic data replication methods. Typically, this storage incurs an ongoing, nominal fee. In the event of a disaster failover, the organization would provision the needed additional infrastructure (e.g., compute, networking, additional storage) on demand and begin the process of workload migration. Only then will organizations incur additional billing for the extra resources used to fail over.
3. DRaaS allows enterprises to adopt a wide range of adjacent security, compliance, and application services that go above and beyond what might be considered "core" DR capabilities such as threat analysis, runbook creation, and failover testing. These adjacent services can include both advanced analytics capabilities to optimize infrastructure resource allocation as well as detect security breaches and advanced encryption and compliance tools. Unlike traditional software solutions, which must be licensed and installed separately, most DRaaS providers deliver these adjacent services natively on their platform for an additional subscription charge, which can simply be switched on/off.

From a technical perspective, DRaaS solutions are commonly (but not always) built around the following components:

- **Data movers.** This is the core technology used to stage data from the primary system to the DR location. Data movers typically come as a backup/recovery software solution or as replication software.
- **Workload migration tools.** These tools facilitate the movement of workloads from the primary site to the DR site across the virtual infrastructure. Such tools may abstract the workload from the underlying infrastructure, including the hypervisor.
- **Orchestration tools.** These tools automate the process of bringing applications back online. They can typically start application services, boot systems in the proper sequence, and so forth.
- **Cloud infrastructure resources.** These resources consist of compute, network, storage, security, and all related hardware and software necessary to run the application environment.
- **User portals.** The DRaaS provider may set up portals to allow users to provision systems and manage their environment in a self-service manner.
- **Appliances.** Physical/virtual appliances are optional, but some cloud service providers choose to use them. If used, the appliance sits in the data path and resides physically or virtually at the primary location. The machine will hold the most recent backup data for immediate restore while facilitating the data migration. Appliances may also fulfill other essential data services such as compression, encryption, and deduplication to eliminate any stress on production systems while minimizing the size of data transfers and any protocol translation between sites. A corresponding appliance may be in the DR datacenter but is not always necessary.

Along with the previously listed components, some DRaaS providers will offer additional capabilities, many of which are actual value-added services. These may include:

- **Threat analysis.** This accounts for all of the primary site considerations, such as the nature of neighboring businesses, transportation considerations, climate/geography, power grid feeds, and regulatory requirements. Threats should be mapped to mitigating DR contingencies.
- **Runbooks.** These documents describe the process of who needs to do what under which conditions and when. Effective runbooks should be very detailed such that, if one of the individuals concerned is not available, someone else could step into that role. Runbooks can quickly become out of date, so updating them should be part of the IT change management process.
- **Testing.** Under traditional DR efforts, testing involved a complex process of physically failing over production systems, requiring Herculean efforts by IT staff and disruption to the organization. For that reason, testing was conducted once a year at best. With DRaaS, many cloud service providers offer virtual (simulated) testing and failover to eliminate the need for physical failover. For periodic physical failover, most organizations will fail over specific applications or groups of servers to limit the test's scope and impact.
- **Analytics.** Analytical tools are mostly focused on infrastructure usage, consumption, and costs but may also assist with forecasting and "what if" planning.

- **Reporting.** DRaaS reporting systems should monitor SLA attainment and alert when SLAs are out of compliance. Reporting systems will also provide audit trails for testing and system coverage to assist in the audit process.
- **Workplace and datacenter recovery.** Significant natural disasters often affect the IT staff, preventing them from assisting in the DR failover. When area or regional disasters hit, the IT staff may need to attend to their homes and families rather than system recovery. Some cloud service providers offer to have their staff trained to assist in recovery and carry out specific functions of restarting systems according to runbooks. Some full-service cloud service providers also offer workspace facilities and temporary living quarters for both IT and non-IT staff. Some temporary office suppliers also offer DR office space on a contract basis.

The Relationship Between DRaaS and Business Resilience

Many organizations erroneously believe that disaster recovery is simply a response to unplanned natural disasters such as fire, earthquake, flood, hurricanes, and tornadoes. However, many other threats can also trigger a disaster response. Such threats may include the spread of hazardous fumes (e.g., from a truck or train accident), power outage/grid failure, snowstorms that prevent worker access to business facilities, terrorist attacks, and national emergencies. More likely, though, are threats from attacks such as malware, ransomware, or employee sabotage. And even more likely are data loss events caused by simple human error or accidental deletion. While much less catastrophic or malicious, these threats can still render systems unusable and require that affected applications be restarted under different infrastructure.

It is impossible for organizations to predict and prevent this multitude of disaster scenarios and data loss events. Overall, IDC research has found that 84.6% of organizations have experienced a malware and/or ransomware attack within the past 12 months; many reported multiple attacks. Of these organizations, 89% suffered a successful attack, and 56% reported an unrecoverable data event within the past three years. Organization leaders cannot take solace in the idea that disasters always happen to other companies or that they are not in a high-risk location geographically. Certainly, COVID-19 has taught us that disaster scenarios (e.g., a global pandemic) are impossible to predict and impact almost all business operations, as well as the global economy in which these businesses operate, in some way.

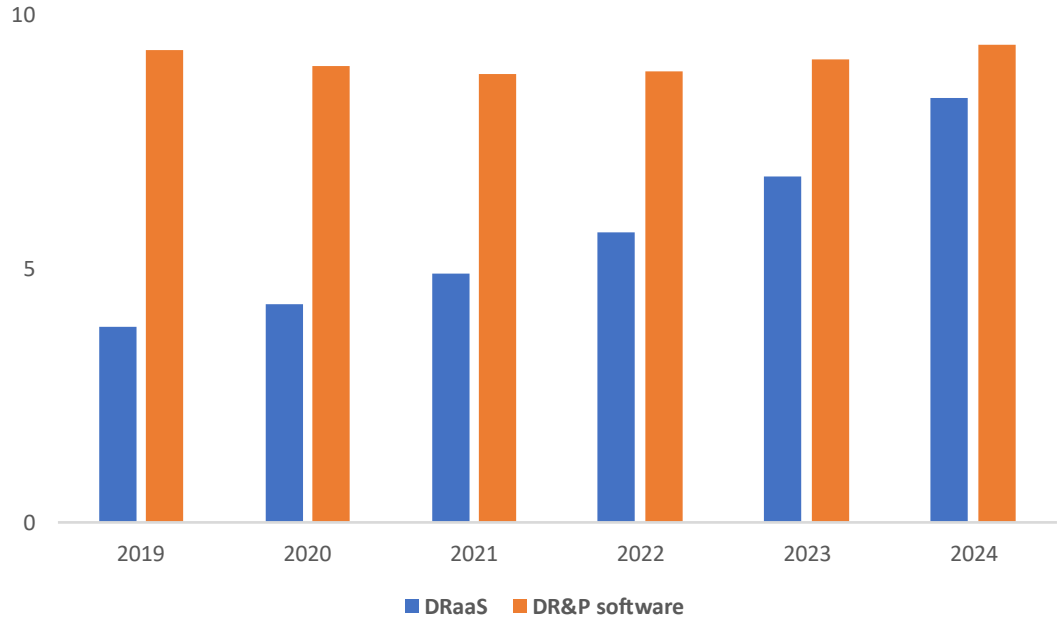
84.6% of organizations have experienced a malware and/or ransomware attack within the past 12 months; many reported multiple attacks. Of these organizations, 89% suffered a successful attack, and 56% reported an unrecoverable data event within the past three years.

Disasters and data loss events are a virtual certainty at some point in an organization's life. Businesses should be asking themselves how they plan to react and overcome "when" a disaster strikes, not what they might do "if" a disaster strikes. The former approach is increasingly implemented by organizations within the umbrella of business resilience. We recommend organizations begin implementing a strategy for business resilience that includes DRaaS as a critical element. Advanced contingency plans must be made if workers cannot access their typical workplaces or devices due to a natural disaster. DRaaS solutions can help organizations achieve this access by providing a means to fail over and host applications for extended periods using distributed cloud resources, giving workers a mechanism to access their data and applications remotely and continue operating.

DRaaS Market Sizing and Growth Trends — Impact of COVID-19

IDC estimates the DRaaS market totaled $3.9 billion in 2019 and grew 22% annually from 2018. This market grew significantly faster than the traditional DR&P software market, which we estimate grew approximately 5% in 2019 (see Figure 1). IDC forecasts that the DRaaS market will reach $8.4 billion by 2024, representing a compound annual growth rate of 16.7%.

FIGURE 1: ***Forecast Growth of DRaaS and DR&P Software Markets ($B)***



Source: IDC's Worldwide Semiannual Software Tracker, 1H20 Forecast Release and IDC's Worldwide Data Protection as a Service Forecast, 2020–2024

IDC estimates that more than 2,000 cloud service providers offer a DRaaS solution. Some providers have a national scope or an international scope, but many provide local or regional coverage. Some focus on specific applications or IT ecosystems, while others focus on serving specific industry verticals. Cloud service provider offerings can range from bare-bones, do-it-yourself (DIY) infrastructure to full-service "white glove" solutions that assist not just with technology but also with people and process. The continued expansion of this long tail of service providers will be a critical contributor to DRaaS market growth. The DRaaS market is expected to continue growing throughout the forecast period because of several additional factors. Three of the most impactful factors are as follows:

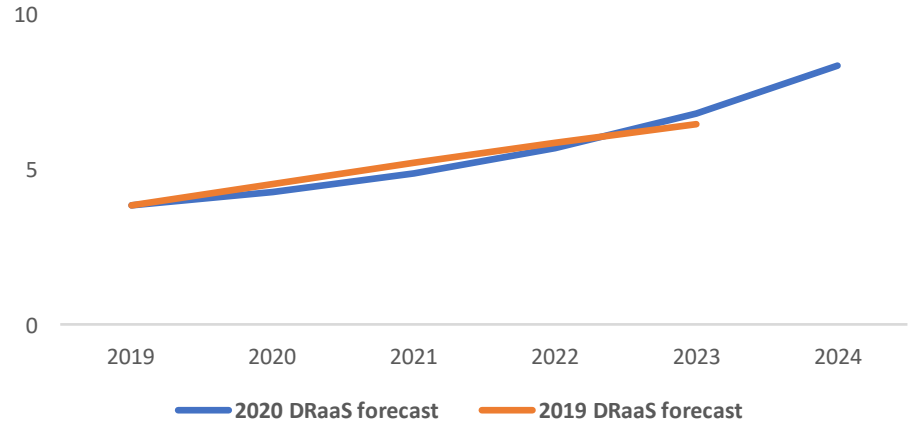
1. Enterprises continue to adopt cloud-based IaaS solutions, specifically compute and storage resources. These resources are often integrated with DR, backup, recovery, and archiving services because of their scalability and cost-effectiveness.
2. Secondary storage workloads (backup, disaster recovery, archive) are consistently high on the list for IT departments to automate or offload, giving them room to focus on higher-value tasks.
3. Enterprises face a constant battle to manage growing volumes of data in a way that keeps this data secure and accessible. Adoption of DRaaS helps achieve this goal without requiring datacenter expansion or significant capex outlay.

COVID-19 Is Changing the Way Enterprises Think About Data Protection and Business Resilience

The DRaaS market will remain largely unaffected by COVID-19 in the long term (see Figure 2). We do expect the slower growth seen in 2020 to be a short-term trend, with the DRaaS market recovering throughout 2021 and returning to previously forecast levels of revenue and growth by 2024. IDC's forecast assumptions regarding COVID-19's impact on DRaaS include:

- In the post-COVID-19 era, organizations will look for ways to increase their agility and velocity. Cloud infrastructure services will continue to play a critical role in those efforts.
- COVID-19 may accelerate specific areas of opportunity associated with DRaaS, such as workplace recovery, business continuance planning, pandemic contingency planning, and enterprise initiatives to develop digital resilience.
- COVID-19 will not negatively impact the proliferation and growth of enterprise data and devices. New ways of working and collaborating because of COVID-19 (e.g., videoconferencing, file sharing to enable an influx of remote work) will only contribute to data generation and the need to ensure data protection, availability, and recovery.
- Although COVID-19 negatively impacted business planning and expenditure in the short term, we believe that over time, the legacy of COVID-19 will be used by organizations to strategically reassess their digital business policies with a focus on data protection, resilience, and compliance.

FIGURE 2: ***Forecast Growth of DRaaS Pre- and Post-COVID-19 ($B)***



Source: IDC's Worldwide Data Protection as a Service Forecast, 2020–2024

Considering StorageCraft Disaster Recovery as a Service

StorageCraft has offered a cloud DRaaS solution for over five years, and this service builds on the vendor's expertise with on-premises backup and DR solutions, specifically ShadowXafe, ShadowProtect, and OneXafe Solo. StorageCraft's DRaaS solution sits within the provider's broader Cloud Services portfolio, including a comprehensive set of cloud data protection and backup services (e.g., backup for specific apps such as Office 365 and G Suite). This approach allows StorageCraft to offer DRaaS as one element of a more comprehensive cloud data protection and business resilience portfolio, extending to SaaS application backup and recovery as well as ransomware protection.

StorageCraft DRaaS is built from the ground up to support cloud-based disaster recovery using snapshot-based replication. StorageCraft DRaaS is engineered to track only incremental changes after an initial image is captured,

improving the service's cost profile, performance, and operational efficiency. All DR and application failover activity is executed in StorageCraft's cloud datacenters.

In terms of DRaaS service levels, StorageCraft offers three tiers of performance based on customer requirements:

1. **Cloud Basic** offers secure offsite storage of business backups with full-system restore via a BMR drive (a BMR drive contains the user's stored ShadowXafe or ShadowProtect images and enables users to restore the system to replacement hardware onsite).
2. **Cloud Plus** offers Cloud Basic capabilities, plus immediate file and folder recovery (download from the cloud).
3. **Cloud Premium** offers the capabilities of Cloud Plus and adds instant virtualization of user systems and data in the cloud (multiserver and network failover is possible, meaning the service can temporarily act as a virtual office space during a disaster).

As mentioned previously, the adjacent features/services offered by DRaaS providers are an essential area of differentiation and value-add for customers that require unique tools or deployment options depending on their industry, application, or compliance requirements. Table 1 provides a detailed overview of the tools and features of StorageCraft DRaaS.

TABLE 1: ***StorageCraft DRaaS Features***

Feature	Description
Fault tolerance	» StorageCraft DRaaS cloud is designed to provide 99.999% uptime. Cloud Services is monitored and managed 24 x 7 x 365 by the StorageCraft Network Operations Center.
Security and redundancy	» Each StorageCraft datacenter architecture is built with enterprise-grade hardware and redundant firewalls and meets or exceeds Telecommunications Infrastructure Standards (TIA-942) and tier 3 datacenter requirements. All data in StorageCraft's Cloud is encrypted using the AES-256 standard.
Account alerts	» Individual account alerts can be set to notify users when uploads become inactive or data growth exceeds established thresholds. Notifications can be created to flag when new machines are added or deleted or when VMs are running. » Alerts can be set to notify users about seed and BMR drive request updates.
Account permissions	» Account permissions allow clients to access files, folders, or entire systems from the cloud portal.
Networking	» In addition to customizing recovery network firewalls, users can update recovery networks through OpenVPN or IPsec to enable site-to-site, single-user, or entire organization virtual private network (VPN) connections. » Additional networking features include port forwarding, port blocking, network control options such as DHCP, independent and isolated recovery networks, static public and private IP address reservations, a dynamic private IP address available at the time of a disaster, and custom VPN configurations.
Self-service portal	» StorageCraft provides a dashboard for the status of all accounts, machines, seed drives, BMR drives, virtual machines, and account space used. Users can download entire image recovery files from the portal with no additional fees.

Source: StorageCraft, 2020

StorageCraft Key Differentiators

StorageCraft DRaaS is engineered to serve small and medium-sized businesses (SMBs) and enterprise organizations that are protecting their environments and managed services providers that wish to build an extended platform of cloud data protection and DR services for their customers. We believe the following are key differentiators:

- **Virtual machine (VM)–based billing and annual freemium.** StorageCraft employs a VM-based billing policy. In other words, users are licensed according to the number of VMs protected. Each VM license includes 1TB of virtual storage and 30 days of operation on StorageCraft's cloud per year. This "freemium" period of operation should be seen as an important differentiator for organizations that are adopting DRaaS for the first time and are unsure of their infrastructure consumption and cost profile. Organizations can leverage this model to failover test and develop a more accurate estimate of billing for cloud DR over the long term.
- **No additional cost for data recovery.** Unlike many public cloud services that charge extra for downloading data back from the cloud, StorageCraft includes recovering data from the datacenter to on premises as part of the service fees. Customers don't incur any additional cost.
- **One-click DRaaS orchestration.** Pre-stage sitewide failover processes enable testing without disrupting the production environment and allow true failover with a single click. Customers can preconfigure the sequence, order, and timing for each mission-critical server/system and virtualize them in the cloud using the patented Virtual Machine Policy.
- **Recent integration with Google Cloud Platform (GCP).** StorageCraft's recent partnership with GCP is designed to capitalize on a number of synergies, including improved performance with accelerated replication to the cloud, scalability and elasticity to handle on-demand growth, and high availability with reliability across multiple regions. Organizations can now replicate StorageCraft backup images reliably to GCP as often as they need to achieve their recovery point objectives (RPOs), giving them access to additional infrastructure and software tools they need to keep their operations running.

Challenges

- The reliance of StorageCraft on its cloud datacenter resources was one of the more significant challenges. However, the company's recent partnership with GCP changes this dynamic by integrating directly with public cloud IaaS resources/datacenters as well as providing access to adjacent cloud data services from GCP. This partnership will help StorageCraft better address this challenge, specifically with customers that require solutions that accommodate hybrid (a mix of cloud and noncloud resources) and/or multicloud (cloud services from more than one cloud service provider) deployments.
- Another challenge applies to StorageCraft and all DRaaS providers: cost optimization. Customers don't expect to pay as much for a cloud service as they would for a full-featured enterprise storage array or purpose-built backup appliance. The economics of cloud services is both a blessing and a curse for DRaaS providers. In many cases, the provider is expected to deliver increased functionality over time at the same or lower base subscription price. StorageCraft sells appliances, software, and cloud services. It must continue to balance the cost models and customer expectations of each while educating customers and partners that may be moving from legacy on-premises solutions to cloud about how these new models will impact their bottom line. This is a significant challenge for any provider and one of the main reasons why refresh and migration of backup/DR technology can be such a lengthy process.

Conclusion

The necessity for system failover is a virtual certainty, regardless of what form a disaster takes. Nevertheless, the need for DR and business continuance planning is not always intuitive to business leaders outside the IT ecosystem. They may not appreciate the extent to which planning is necessary. The risks of downtime significantly outweigh the benefits of a cloud-based DR plan, and there is no reason for any organization not to have sufficient DR capabilities to rapidly recover from minor events (planned or unplanned) and ensure organizational survival from significant events. IDC sees DRaaS providers as an essential, enabling partner in this context, helping organizations update their DR strategies and capabilities, develop business resilience plans, and align with customer expectations for flexible, scalable, cloud-delivered IT services.

About the Analyst

Andrew Smith, *Research Manager, Cloud Infrastructure Services*

Andrew Smith is a Research Manager within IDC's Enterprise Infrastructure Practice. Andrew's research focuses on public cloud infrastructure-as-a-service platforms and solutions, with specific focus on storage services. Andrew contributes to market sizing and forecast efforts across IDC's Public Cloud IaaS segments, as well as adjacent markets like multicloud data management, data protection as a service, and public cloud cold storage.

MESSAGE FROM THE SPONSOR

For nearly two decades, StorageCraft has been innovating advanced data management, protection, and recovery solutions. Together with our channel partners, we ensure medium and small organizations can keep their business-critical information always safe, accessible, and optimized.

We have shifted the paradigm of traditional data protection by converging data platforms for primary and secondary storage while integrating data protection. Our customers benefit from category-leading intelligent data protection and management solutions for converged scale-out storage platforms, and world-class cloud backup and DRaaS services.

Regardless of whether an organization relies on on-premises, cloud-based, or a hybrid IT environment, StorageCraft solves the challenges of exploding data growth while ensuring business continuity through best-in-class protection and recovery solutions. For more information, visit ***storagecraft.com***

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.

5 Speen Street
Framingham, MA 01701, USA

T 508.872.8200

F 508.935.4015

Twitter @IDC

idc-insights-community.com

www.idc.com