G00298161

Critical Capabilities for Disaster Recovery as a Service

Published: 10 October 2016

Analyst(s): Ron Blair, John P Morency, Mark Thomas Jaggers

Gartner has identified seven critical capabilities and four use cases with which to assess DRaaS offerings from 20 service providers. IT leaders should determine which of these DRaaS vendors offer products that align with their organization's recovery needs, and consider smaller, flexible providers.

Key Findings

- There are more than 250 providers in the disaster recovery as a service market, with more than 50,000 active production instances. On average, the 20 vendors that have been evaluated in this research demonstrate service capabilities that merit scores of near-excellent or better across the board.
- The DRaaS market remains fragmented, and the wide array of DRaaS provider options can be overwhelming, making side-by-side comparisons difficult.
- Hybrid configurations, which combine virtual and physical servers, are becoming the norm. Hybrid recovery configurations often require a custom recovery time objectives SLA, especially when the number of in-scope servers is on the order of hundreds.
- There is a strategic shift by many DRaaS providers to a highly channel-centric sales model. In addition, the number of provider channel partners in the market that are reselling and white-labeling DRaaS services is steadily increasing.

Recommendations

- IT leaders with complex environments, a high percentage of non-x86 workloads, a need to integrate with legacy physical assets or a requirement for mainframe recovery should narrow their focus to providers that score high for production and application recovery.
- IT leaders with highly virtualized, x86-based environments should engage providers based on their needs in terms of self-service versus fully managed.

- IT leaders contemplating midsize and large implementations (i.e., 100 to more than 400 servers) should exclude providers that offer only one option for recovery (i.e., a "one-size-fits-all" solution). This will be too expensive, or it will underserve their business requirements.
- IT leaders with fewer staff that require assistance with run book creation should place a higher premium on smaller providers who often take a high-touch approach to onboarding.

Strategic Planning Assumptions

By 2018, the number of organizations using disaster recovery as a service (DRaaS) will exceed the number of organizations using traditional, syndicated recovery services.

By 2018, 20% of enterprises with a minimum of 5,000 employees will be failing over the operation of one or more production applications to DRaaS, infrastructure as a service (IaaS) or cloud-enabled managed hosting.

What You Need to Know

Gartner's Critical Capabilities for Disaster Recovery as a Service research will assist IT leaders in developing a list of DRaaS provider candidates to evaluate and compare. The vendors' critical capabilities should be considered when making the final selection of a DRaaS provider, subject to the needs of your organization.

DRaaS services are categorized as one of two types. In the first, the service provider is responsible for managing virtual machine (VM) replication and activation, exercise management and servicing customer disaster declarations. Increasingly, this is becoming the preferred model for customers with large, hybrid configurations that include physical, as well as virtual, servers. Here, the provider adds significant value by supporting managed recovery orchestration across an entire set of servers and production applications, rather than just the virtual servers.

In the second, the provider role is relegated to just VM activation and shutdown, and the service customer is responsible for managing replication, exercise management and recovery operations following a disaster declaration. In the service provider descriptions below, Gartner has designated which type of services (e.g., workload management options) are available for each.

Many DRaaS providers also offer hosting, IaaS, cloud-based recovery, backup as a service (BaaS) and cloud-based archival. In addition, some offer virtual desktop and unified communications (UC) recovery. Several DRaaS providers profiled in this research have also moved to a more channel-centric sales model to increase their reach.

Wider Adoption for Large Enterprises

Initially, providers' DRaaS services were primarily attractive to small or midsize businesses (SMBs), because they lacked recovery data centers, and DRaaS freed up time for IT staff in these organizations. However, larger organizations are now increasingly evaluating and, in some cases,

adopting DRaaS. Large enterprises account for more than 13% of production DRaaS instances, but will account for a larger percentage during the next few years. Wider adoption of DRaaS can be attributed largely to the broader proven viability of public-cloud-based solutions. Gartner estimates the size of the DRaaS market to be approximately $1.7 billion, with a compound annual growth rate (CAGR) of approximately 25% through 2018.

Cross-Vertical Interest

DRaaS providers reported adoption and strong interest across a large number of verticals, because the number of knowledge workers has increased and dependence on application and data availability has a direct impact on business performance. The two largest industries in terms of installed base are financial (noninsurance at 18%) and healthcare (at 11%). DRaaS is also attractive to verticals with regulatory and compliance requirements; Gartner observes similar interest among verticals with respect to client inquiries (see "Magic Quadrant for Disaster Recovery as a Service").

Providers have put forth significant efforts to increase security and compliance-related certifications to support widespread adoption. Although some have launched vertical-specific DRaaS offerings, most have focused on horizontal offerings that support scalable expansion through managed service provider (MSP) sales channel approaches. This is typically supplemented by disaster-recovery-related professional services that are generally independent of specific vertical industry business impact analysis facilitation, recovery plan development and exercise plan orchestration.

Global Presence Considerations

Global presence and market share are factors for the "Magic Quadrant for Disaster Recovery as a Service," but less so for Critical Capabilities research. However, all of the DRaaS providers in this research have significant capabilities in the geographic areas on which they focus.

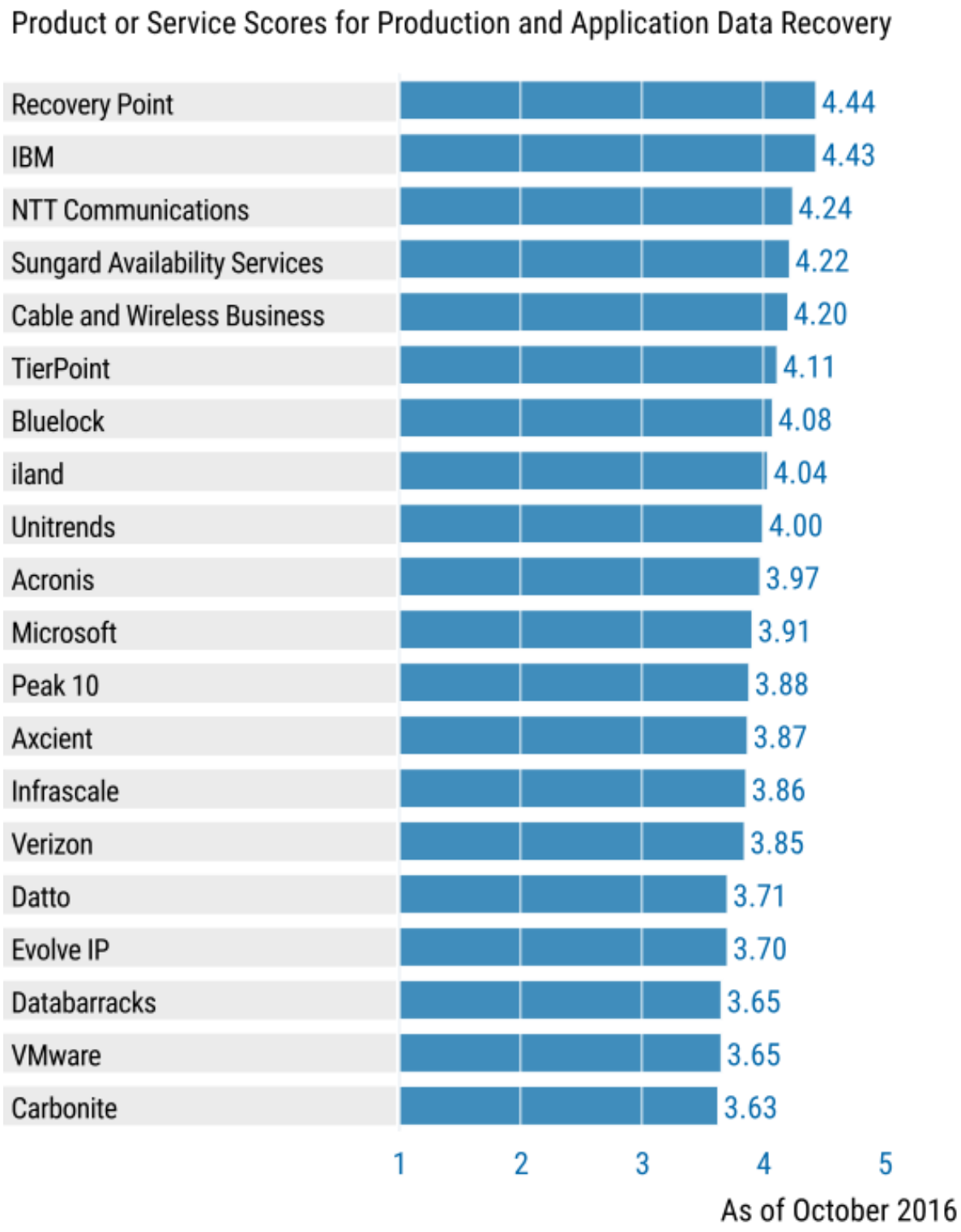
Notable Use-Case Weighting Modifications for 2016

Due to increased adoption by larger organizations with complex environments, the weighting for certain use cases has evolved accordingly to give more credence to those that can accommodate more platform types (e.g., physical/virtual system recovery). Take this into consideration before attempting to compare 2015 scores. If your environment consists primarily of x86 systems and is highly virtualized, then modify the weighting via "Customize the Cases and Weightings" as you deem appropriate for your organization, because all of the DRaaS providers in this research are highly capable of VM recovery.

Analysis

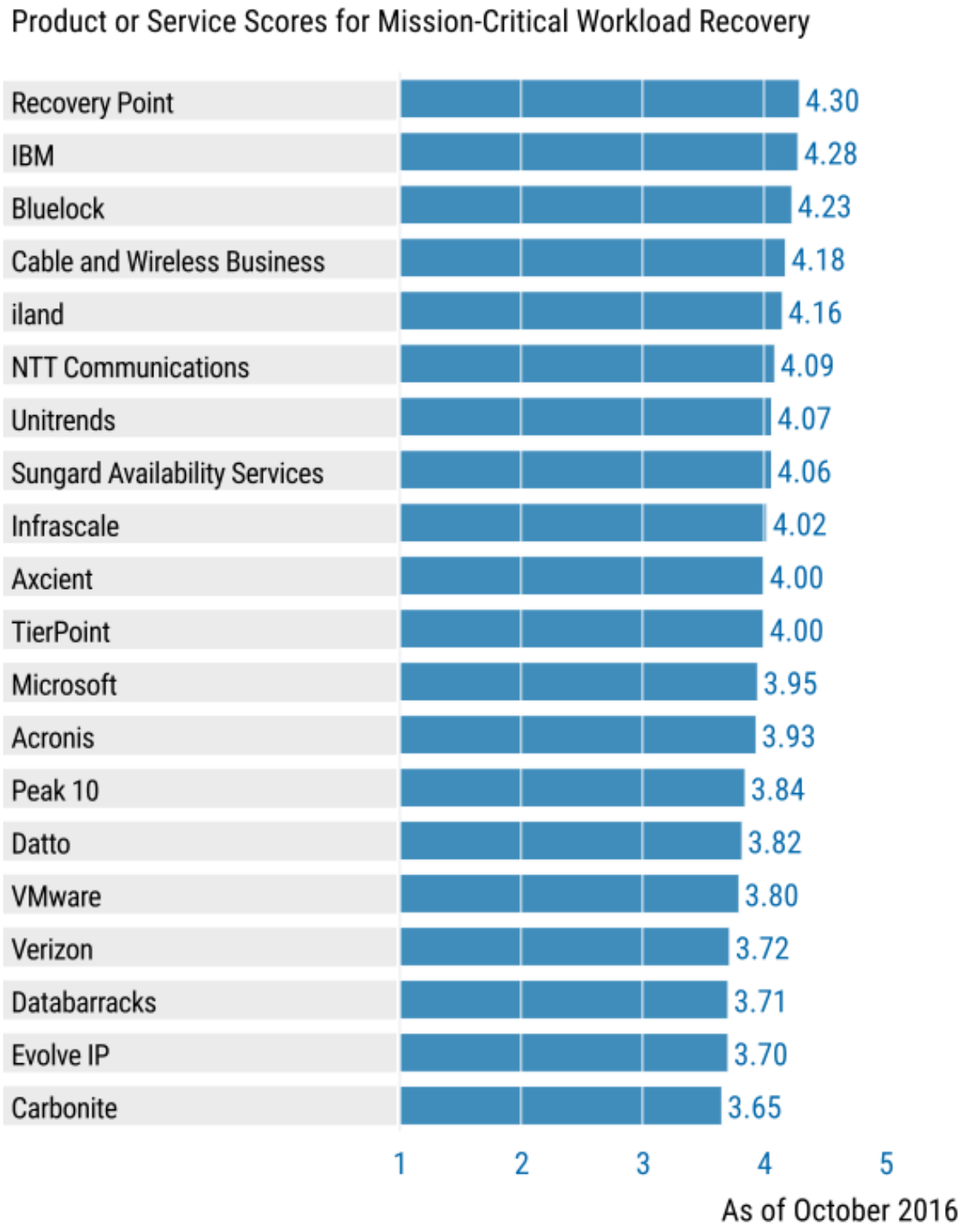
Critical Capabilities Use-Case Graphics

Figure 1. Vendors' Product Scores for the Production and Application Data Recovery Use Case



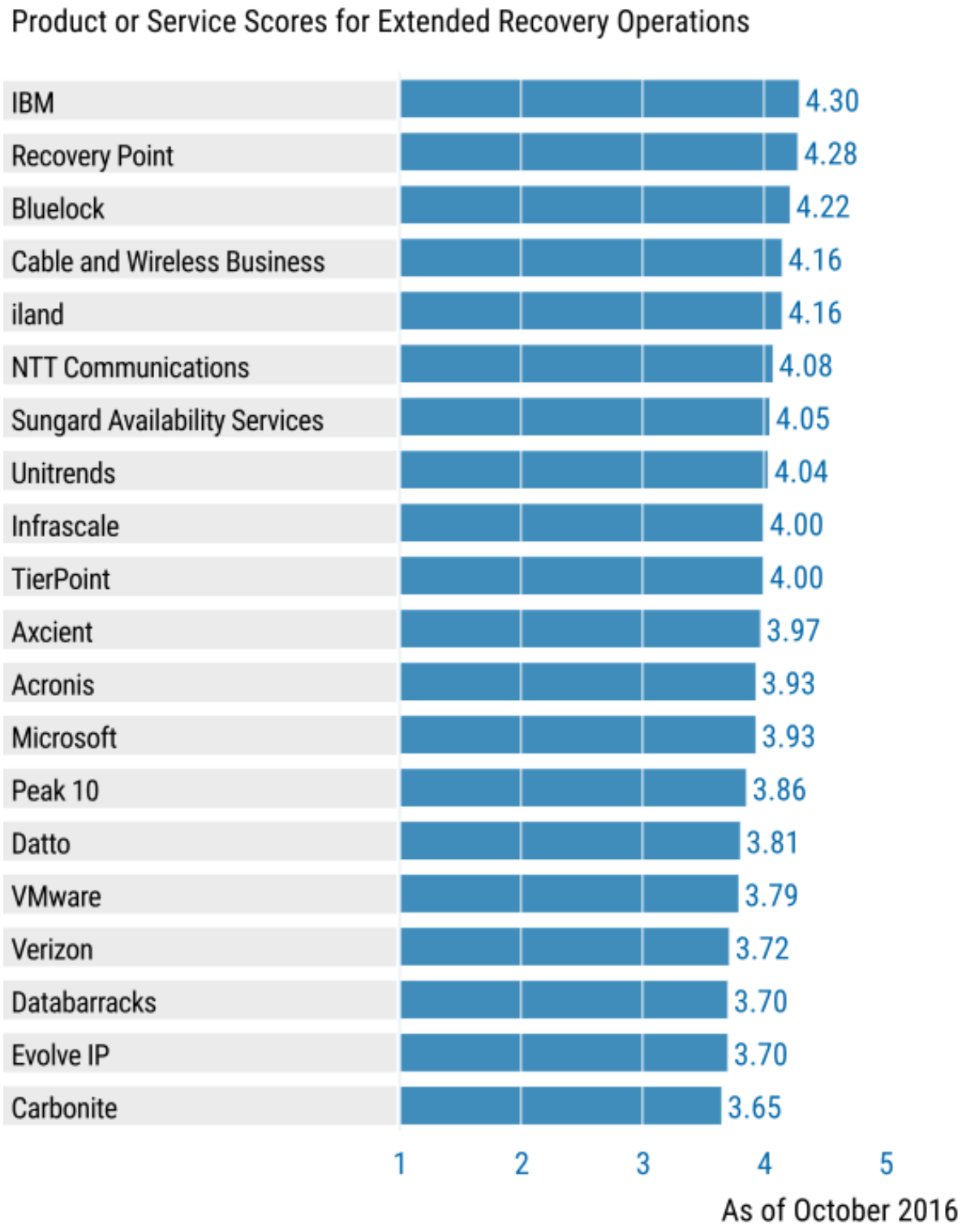
Source: Gartner (October 2016)

Figure 2. Vendors' Product Scores for the Mission-Critical Workload Recovery Use Case



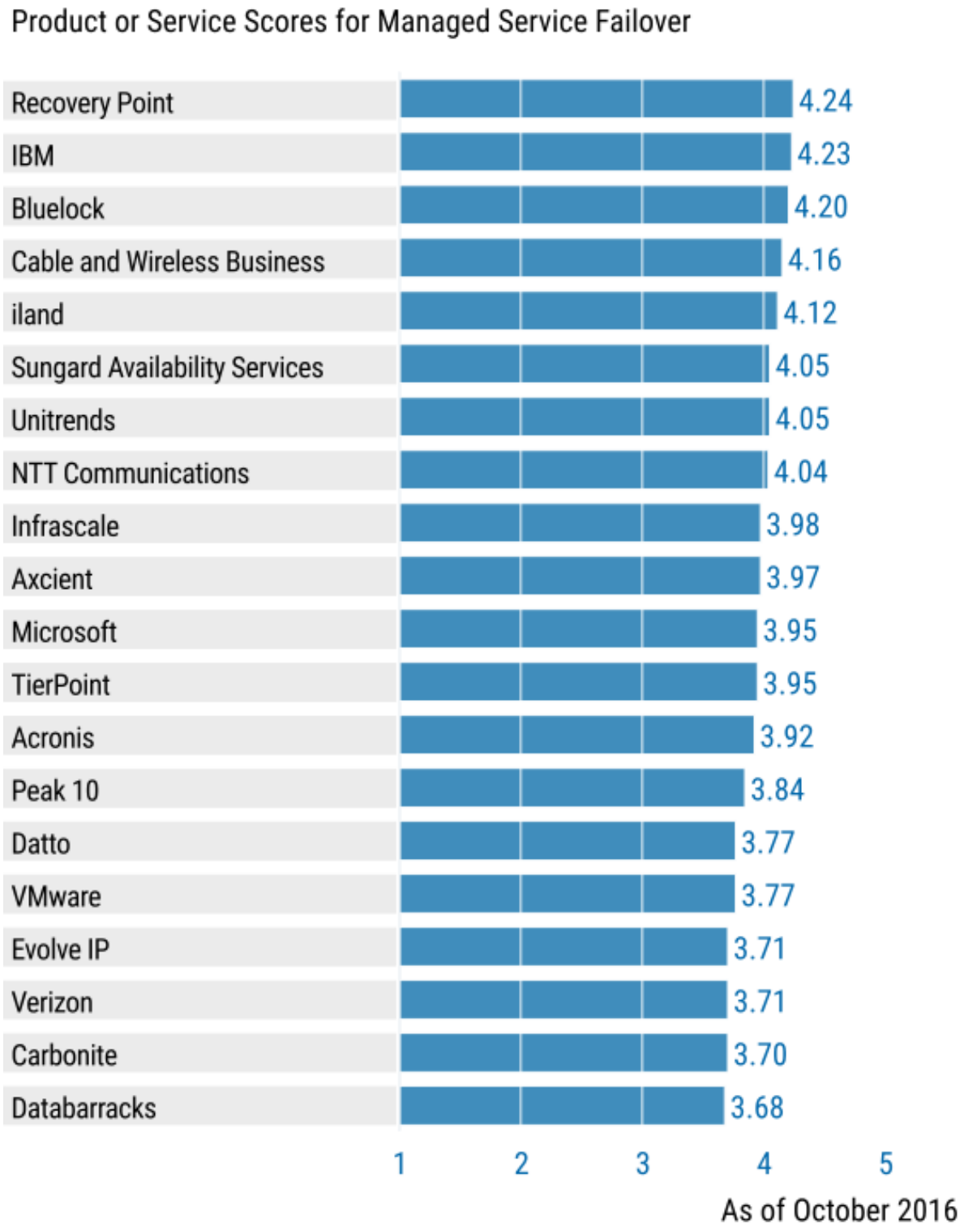
Source: Gartner (October 2016)

Figure 3. Vendors' Product Scores for the Extended Recovery Operations Use Case



Source: Gartner (October 2016)

Figure 4. Vendors' Product Scores for Managed Service Failover



Source: Gartner (October 2016)

Vendors

Acronis

Solution: Acronis Disaster Recovery Service

The Acronis DRaaS service offers a fully featured disaster recovery and backup solution in 145 countries as a self-managed service and a fully managed service through partners. The Acronis Cloud Recovery Console provides many functions that give Acronis' customers or its channel partners service control management, reporting and analytics for their cloud and on-premises data and server protection. The support team is available to provide day-to-day help desk support, to support clients during a disaster failover and to actively assist with the failback process. This support is available 24/365. Almost all of Acronis' current production customers have hybrid recovery configurations.

Acronis Disaster Recovery Service provides multiple availability options: active-active replication via a native data replication method, such as SQL mirroring or Exchange DAG, for most critical systems; regular image snapshot replication for cloud recovery guaranteed SLAs of 15 minutes or less; and image backups and ability to recover it in the Acronis Disaster Recovery cloud for secondary systems. The service also offers multiple testing options, including ad hoc tests for individual systems, regular automated and manual tests of entire infrastructure, and support for disaster recovery exercises.

Acronis earned consistent scores (that is, between 3.92 and 3.97) across Gartner's four use cases: production and application data recovery, mission-critical workload recovery, extended recovery operations and managed service failover. Its highest score (3.97) was for production and application data recovery.

Service Delivery Options: Self-service or fully managed (both via channel partners)

Axcient

Solution: Axcient Business Recovery Cloud

Axcient's DRaaS offering is based on its own technology, which can be sold as a self-managed or a fully managed solution. Although 80% of Axcient's DRaaS revenue is from MSPs, Axcient also has a strong and growing base of SMB customers in the U.S. It has two service delivery data centers — one in the U.S. and one in Canada. Axcient provides a web-based portal, named the Remote Management Console (RMC). MSPs or users can select new devices to be protected, verify their status, receive alerts, recover files and virtualize an entire office instance.

Axcient supports the replication of production VM images and data via an on-site hardware appliance, Axcient Virtual Appliance, or via Axcient's new applianceless service delivery model, Direct to Cloud (D2C), which was launched in 2015. More-recent 2016 enhancements include an "export to VMDK option" for VM backups, enhancements for Linux backups that include bare-metal restore to cloud options and granular restoration of Microsoft SQL backups.

In terms of critical capabilities, Axcient earned a top-five score for customer experience (4.5) and a range of 3.7 to 4.1 for the rest. With respect to use cases, scores ranged from production and application data recovery (3.87) to mission-critical workload recovery (4.00).

Service Delivery Options: Self-service or fully managed

Bluelock

Solution: Bluelock Disaster-Recovery-as-a-Service

Bluelock's Disaster-Recovery-as-a-Service enables customers to support physical servers, VMs and related production data inside a managed cloud. The service family has two variants. The "To-Cloud Disaster Recovery" version supports replication from customer-premises-based data centers into the Bluelock cloud. The "In-Cloud Disaster Recovery" versions support replication from a production hosting environment that is already operational inside the Bluelock cloud. The services are provided fully managed or via assisted service. In the managed service, Bluelock's team is responsible for certified testing, run books, alerts and change management on behalf of the client. With the assisted service, Bluelock provides the training, tools, templates and support for the client to perform those activities themselves.

The services are underpinned by Zerto or Veeam for hypervisor-based workloads and Vision Solutions' Double-Take, Commvault or client-chosen tools for non-hypervisor-based workloads. Support for hybrid recovery configurations, including target recovery times, is defined in a customer-specific support plan. In addition, the unified SaaS control panel (called Bluelock Portfolio and Recovery Assurance) capabilities provide a look at the recovery health of a client's infrastructure and continuous verification of recoverability. Bluelock scored high in customer experience.

In terms of its 2016 critical capabilities results, Bluelock was one of five providers to achieve an average score of 4.2 or higher across the seven core critical capabilities categories. And it had the highest score for customer experience (4.7) and testing and declaration (4.3). For its 2016 use-case results, it earned the third-highest scores for mission-critical workload recovery, extended recovery operations and managed service failover.

Service Delivery Options: Self-service or fully managed

Cable and Wireless Business

Solution: C&W Business Disaster Recovery as a Service (DRaaS)

The C&W Business DRaaS service offering is sold as a fully managed service. It provides support in English and Spanish. This provider uses Geminare's Cloud CORE platform technology as the foundation for its recovery cloud service management system. In addition to DRaaS, the company offers connectivity, managed security, managed network services, IaaS, desktop as a service (DaaS) and colocation services. It has a strong focus on professional services.

In March 2015, Cable and Wireless Communications (CWC) acquired Columbus International. Columbus Business Solutions' (CBS's) DRaaS service was originally included in Gartner's 2015

Disaster Recovery as a Service Magic Quadrant and was rated a Challenger. CWC was rated as a Leader in the "Magic Quadrant for Disaster Recovery as a Service."

The CBS acquisition gave CWC additional presence in the Caribbean/Latin American region, because CBS is present in 42 countries in the region, including the Cayman Islands, Colombia, Panama, Honduras, Guatemala, Puerto Rico, Dominican Republic, El Salvador, Trinidad, Jamaica, Grenada, Curacao and Barbados.

For its 2016 critical capabilities results, C&W Business was one of five providers to achieve an average score of 4.2 or higher across the seven core critical capabilities categories and had no score lower than 4.0. In its 2016 use-case results, C&W Business earned above-average scores in all four use-case categories, with its highest of 4.2 in production and application data recovery, which placed it fifth overall. Its scores for the other three use cases varied between 4.16 and 4.18.

Service Delivery Options: Fully managed

Carbonite

Solution: EVault Disaster Recovery Service

Carbonite (EVault's) DRaaS offering is its highly customizable EVault Cloud Disaster Recovery. EVault Cloud Disaster Recovery is a managed service that supports customer recovery of VMs, bare-metal system images and production data inside a managed cloud. Recovery testing and recovery operations are largely provider-managed, requiring close management coordination between the service customer and technical support. Guaranteed SLA tiers include a one-hour recovery time objective (RTO) and a five-minute recovery point objective (RPO); a 24-hour RTO with an RPO target between four and 24 hours; and a 48-hour RTO tier with a four-to-24-hour RPO SLA.

All provider-managed offerings include an annual disaster recovery test and proactive failover with zero downtime for planned outages. The one-hour SLA is available for Windows Servers, whereas the 24- or 48-hour recovery options are available for Windows, Linux, VMware, and the IBM AIX and i-series, as well as other common platforms, including Microsoft SQL Server, Microsoft Exchange and Oracle Database.

In terms of its 2016 use-case results, Carbonite earned consistent scores (between 3.63 and 3.70) across production and application data recovery, mission-critical workload recovery, extended recovery operations and managed service failover. Its highest score (3.70) was for managed service failover.

Service Delivery Options: Self-service or fully managed

Databarracks

Solution: Databarracks Disaster Recovery as a Service

Databarracks' DRaaS virtual data center is sold in the U.K. directly and through channel partners. The fully managed solution is based on a reserved server pool that is set at a percentage of the

client's normal operations. This is the fixed-resource reservation; however, this reservation is not limited, and a client can increase the allocation of either virtual processors, RAM or storage resources beyond this reservation up to the configuration of any or all of the protected VMs. Databarracks uses technology such as PlateSpin, Veeam, Zerto, Asigra and Commvault to power its DRaaS offering; however, customers are shielded from these details as part of a continuously improving service led by a team of engineers with average experience of more than five years specifically in continuity and data protection.

Databarracks has also developed Cyber-DRaaS as an extension to standard DRaaS to enable fast recovery from cyber threats using DRaaS, rather than backup. The first iteration uses automated recovery and scanning to protect against ransomware, with further development planned for additional cyber threats. Databarracks is seen as possessing strong sector-based knowledge when serving the legal vertical, which accounts for approximately one-third of company revenue.

In the 2016 critical capabilities, Databarracks earned an average score of 3.7. It had relatively consistent scores across the use cases, ranging from production and application data recovery (3.65) to mission-critical workload recovery (3.71).

Service Delivery Options: Fully managed

Datto

Solution: Datto Total Data Protection Platform

Datto builds its solutions in-house and has nine data centers throughout the world with more than 250 petabytes of storage. The Datto product line consists of the Datto SIRIS, Datto Alto, Datto Backupify, Datto Network Appliance (DNA), Datto NAS and Datto Drive. Datto SIRIS is the company's flagship product and is key to its DRaaS offerings, providing protection against downtime, with an on-average six-second recovery of failed servers or lost files. Datto sells 100% of its DRaaS through MSPs. This provides Datto with broad market coverage and the ability to scale rapidly.

Datto supports two user interfaces (UIs). One is the local UI to the on-premises Datto backup appliance, whereby users can manage backup schedules, configure backup alerts and test backups by mounting file restores and spinning up VMs of any recovery points that exist locally on the device. In the cloud, the second UI is supported by Datto's management portal. Customers use this interface to set up alerts for Datto hardware, as well as test and fail over to the Datto cloud. Both UIs enable the user to provide network access to their individual VMs.

In its 2016 use-case results, Datto earned its highest score (3.82) for mission-critical workload recovery. It also had relatively consistent scores (3.71 to 3.81) across Gartner's other use cases: production and application data recovery, extended recovery operations and managed service failover.

Service Delivery Options: Fully managed

Evolve IP

Solution: Evolve IP DRaaS

The Evolve IP DRaaS service offering expands from its core OneCloud value proposition, which provides "one-stop shopping" for customers that want a single provider for desktops and servers, as well as IP phone systems, UC, call centers and IT-managed services. Evolve IP's disaster recovery suite consists of six products, with DRaaS ZT, DRaaS DT and DRaaS VE forming the cornerstones of the DRaaS portfolio. They are provided in a self-service model, with DRaaS ZT powered by Zerto and offered as a Standard Edition with a 24-hour RTO. The Premium Edition has a four-hour RTO.

DRaaS DT is powered by Vision Solutions' Double-Take for the replication of physical server images between two of Evolve IP's four geographically separated Tier 4 U.S.-based locations. Finally, DRaaS VE is offered as a lower-cost Veeam-based solution. Evolve IP was rated a Niche Player in the 2016 DRaaS Magic Quadrant. It may be ideal for clients looking for one cloud provider across servers, storage, desktops, communications and networks.

In terms of its 2016 critical capabilities results, Evolve IP achieved an average score of 3.70 in the seven core categories. Similar scores were achieved for the production and application data recovery (3.70), mission-critical workload recovery (3.70), extended recovery operations (3.70) and managed service failover (3.71) use cases.

Service Delivery Options: Self-service

IBM

Solution: IBM Cloud Virtualized Server Recovery

IBM Resiliency Services is the overarching portfolio, which includes solution areas ranging from Resiliency Consulting; High Availability Services; Business Continuity Management; and Site, Facilities, and Data Center Services to Resiliency Communications. Cloud Virtualized Server Recovery (CVSR) is one of several DRaaS and BaaS options offered by IBM. IBM CVSR is sold as a fully managed service, and there are three service levels to choose from. Its Gold level includes failover within minutes per server, the Silver level includes shared virtual servers provisioned within one hour for automated recovery and the Bronze level includes shared virtual server provisioning within six hours of declaration. IBM has had solid expansion of Resiliency Services into regions such as the Middle East and Africa, Asia/Pacific (APAC) and Latin America. It has 17 CVSR Points of Delivery (PoDs) across 16 countries and six continents, and it is also available in multiple public cloud environments. More than half of IBM's DRaaS customers have hybrid recovery configurations. IBM was rated a Leader in the 2016 DRaaS Magic Quadrant.

With respect to 2016 critical capabilities, IBM Resiliency Services earned scores that placed it first in terms of overall average (4.3). Notable high points were physical/virtual system recovery (4.6) and value-added services (4.6). For use-case categories, it earned the first or second highest scores among this year's DRaaS providers: production and application data recovery (4.43), mission-critical workload recovery (4.28), extended recovery operations (4.30) and managed service failover (4.23).

Service Delivery Options: Fully managed

iland

Solution: iland Disaster Recovery-as-a-Service

iland's DRaaS offering is part of its Enterprise Cloud Services portfolio. It has eight data centers and a presence in the U.S., U.K. and Singapore. iland focuses on ease-of-use via its Enterprise Cloud Services Console, which can also be accessed via mobile devices. The pricing for the services and the service levels is simple and straightforward. The three DRaaS primary offerings are underpinned by Zerto, Veeam or Vision Solutions' Double Take. More-complex hybrid configurations can be accommodated by means of colocation. iland was rated a Leader in the 2016 DRaaS Magic Quadrant.

iland differentiates on the security and compliance of its target cloud and the flexibility of its offering. With a host of security technologies baked-in, and on-demand compliance reports through the console, customers fail over quickly. With options for physical systems, complex networking, bare metal and colocation, iland consults with customers to design a solution to protect the entire data center.

In terms of its 2016 critical capabilities, iland shared highest honors for service manageability (4.2) and earned top five scores in four other areas as well. For the use cases, iland was above average for production and application data recovery (4.04) and achieved top-five scores among this year's DRaaS providers with respect to mission-critical workload recovery (4.16), extended recovery operations (4.16) and managed service failover (4.12).

Service Delivery Options: Self-service

Infrascale

Solution: Infrascale Disaster Recovery

Infrascale provides both BaaS (aka data protection as a service) and DRaaS options for clients. Specific to DRaaS, Infrascale provides recovery services for VMware, Hyper-V, and Windows and Linux bare-metal implementations via an Infrascale cloud service that includes an on-premises virtual or physical appliance. This self-service offering is based on simplicity, affordability and transparency, while providing a guaranteed 15 minutes or less recovery time for critical applications. Infrascale enables clients to replicate to their own on-premises locations; to one of Infrascale's clouds in the U.S., Canada, Australia, England, Ireland, Germany and South Africa; or to "any cloud" of the client's choosing, including Google Cloud Platform, Microsoft Azure or Amazon Web Services (AWS). The associated value proposition for clients is the ability to leverage their existing infrastructure investments and provide options in terms of meeting governmental regulations, such as those regarding data sovereignty. Pricing is straightforward by way of a storage-based monthly fee, and the service includes unlimited recovery testing and disaster declarations, with no additional charges beyond the initial set-up fee. Infrascale was rated a Visionary in the 2016 DRaaS Magic Quadrant.

In terms of its 2016 critical capabilities results, Infrascale shared top honors for resiliency (4.2), was tied for fifth place for customer experience (4.5) and was slightly above average overall. For use cases, Infrascale came in a fraction below average for production and application data recovery (3.86) and slightly above average for the others, including mission-critical workload recovery (4.02), extended recovery operations (4.00) and managed service failover (3.98).

Service Delivery Options: Self-service

Microsoft

Solution: Microsoft Azure Site Recovery (ASR)

Microsoft provides the cloud service (Microsoft Azure) and cloud migration and disaster recovery utility (Azure Site Recovery [ASR]). ASR is natively integrated with Azure and is available as part of the Operational Management Suite, which is a comprehensive cloud management offering that enables customers to manage their disaster solutions and other Azure services, as well as provide hybrid disaster recovery capabilities across multiple platforms. ASR is self-service and enables customers to orchestrate and automate protection of on-premises workloads running on Hyper-V VMs, VMware VMs, and physical servers to Azure or a secondary data center. For the latter, customers download InMage Scout, which is included in the ASR subscription.

ASR is sold by partners and is also sold directly to SMB and enterprise clients. Pricing for ASR is per protected instance and differs depending on whether target recovery is to a customer-owned site or to Azure. To the extent that storage, storage transactions and/or outbound data transfer are required, pricing follows published Azure rates in accordance with the 17 regions (six in the U.S., two in Asia, two in Europe, two in Australia, two in Japan, one in Brazil and two for the U.S. government) that are used by the customer. Microsoft was rated a Leader in the 2016 DRaaS Magic Quadrant.

With respect to 2016 critical capabilities, Microsoft ASR scored well for security and compliance (4.3). Use-case scores were production and application data recovery (3.91), mission-critical workload recovery (3.95), extended recovery operations (3.93) and managed service failover (3.95).

Service Delivery Options: Self-service

NTT Communications

Solution: NTT Cloud Recovery Service

NTT Communications' DRaaS offering is part of its Recovery as a Service Data Protection Suite. The DRaaS service offering is sold as a fully managed service through NTT Communications or its partners. Customers also have the option of self-management. For no additional fee, clients are assigned a DRaaS Technical Account Manager (DRaaS TAM) to ensure successful onboarding and are entitled to unlimited failover and recovery testing. Customized RTO- and RPO-based service levels are supported, with a service delivery infrastructure availability level of 99.97%. Typically, recurring monthly charges include the total amount of computing and storage resources required for

their recovery environment, plus a monthly fee for each replicated VM. Customers can add additional resources in the portal for recovery testing; failover and activated resources are billed to customers on a minute-by-minute basis. NTT Communications was rated a Visionary in the 2016 DRaaS Magic Quadrant.

In 2016, NTT Cloud Recovery Service tied for the second-highest score when it came to physical/virtual system recovery (4.4) and earned consistent scores for the other critical capabilities. In terms of use cases, NTT Communications was third among its peers for production and application data recovery (4.24) and just outside the top five for the remaining categories: mission-critical workload recovery (4.09), extended recovery operations (4.08) and managed service failover (4.04).

Service Delivery Options: Self-service or fully managed

Peak 10

Solution: Peak 10 Recovery Cloud

The Peak 10 Recovery Cloud portfolio includes three Zerto-based service offerings from which customers can select to rightsize business requirements with budget constraints for the recovery of Hyper-V and VMware workloads. Recovery Cloud Essentials and Recovery Cloud Prime are multitenant options that support eight-hour and four-hour RTOs, respectively. Recovery Cloud Premium includes dedicated compute and a two-hour RTO. Disaster recovery testing is separately billable for the Prime and Essentials tiers; however, run book development is included in the base price of every tier, and each customer is assigned a manager for the life of the service engagement.

Peak 10 offers support for on-premises production configuration, production environments colocated in any of its data centers, as well as for production configurations that are already operational in its four cloud clusters located in the eastern half of the U.S. A team of disaster recovery service specialists is available 24/365 to monitor data replication or to execute recovery testing and failovers. Physical Windows and AIX servers are supported as tailored managed services that leverage Vision Solutions' Double-Take and MIMIX. Finally, colocation options are available in 28 data centers across 10 U.S. cities.

Peak 10 earned relatively consistent scores across the critical capabilities, ranging from 3.7 to 4.0. The scoring in terms of use cases was similarly consistent: production and application data recovery (3.88), mission-critical workload recovery (3.84), extended recovery operations (3.86) and managed service failover (3.84).

Service Delivery Options: Fully managed

Recovery Point

Solution: Recovery Point Disaster Recovery as a Service

Recovery Point's core service focus is the delivery of a broad range of recovery and continuity services for organizations with complex data center configurations that include, in addition to Windows and Linux servers, physical systems and servers, such as IBM z Systems, IBM System i, IBM System p and Oracle Solaris. In its early days, Recovery Point's primary customer base was

large federal government agencies; however, it now has hundreds of commercial clients, representing the largest share of its business, as well as many state government agencies. Because of its strong capabilities, Recovery Point was rated a Challenger in its first year of participation in the 2016 DRaaS Magic Quadrant.

Recovery Point tied for the second highest average score across the seven core critical capability categories (4.2). With respect to the use cases, Recovery Point earned the highest grades of the DRaaS field in three categories: application data recovery (4.44), mission-critical workload recovery (4.30), and managed service failover (4.24). The score for extended recovery operations (4.28) was the second highest.

Service Delivery Options: Fully managed

Sungard Availability Services

Solution: Sungard Disaster Recovery Solutions (RAAS)

Sungard Availability Services (AS) combines a broad set of DRaaS offerings with extensive experience in the recovery of multivendor data center configurations. Its multivendor service management capabilities are the direct result of its significant experience during the past 38 years, supporting thousands of recoveries for large and small customers with diverse recovery requirements. For these and a number of other relevant reasons, Sungard AS has been positioned as a Leader in the Magic Quadrant for the second consecutive year.

Sungard AS differentiates through its Managed Recovery Program, which tiers workloads and applies the most-relevant recovery approach by programmatically managing, maintaining and enhancing holistic disaster recovery plans. In 2016, the company introduced new automated features, including Discovery and Dependency Mapping and Recovery Execution Script, which ensures rightsized recovery provision and the faster and more-accurate testing and execution of complete recovery plans. Its broad portfolio includes the Cloud Based Recovery suite across all hypervisors, Oracle and SAP; Data Replication for the x86, iSeries (AS/400); managed vaulting; and traditional recovery services.

In terms of its 2016 critical capabilities results, Sungard AS tied for the third-highest score for physical/virtual system recovery (4.4) and earned the fourth-highest security and compliance. In addition, Sungard AS achieved the fourth-highest score for the production and application data recovery (4.22) use case. The other use-case scores were consistent: mission-critical workload recovery (4.06), extended recovery operations (4.05), and managed service failover (4.05).

Service Delivery Options: Fully managed

TierPoint

Solution: TierPoint Disaster Recovery as a Service

TierPoint Disaster Recovery as a Service takes a consultative approach that enables customers to leverage investments previously made, incorporate technologies already being used and evaluate

different DRaaS options. TierPoint's significant year-over-year investments during the past six years have culminated in 39 interconnected U.S. data center locations across the U.S.

TierPoint has positioned itself as a hybrid IT MSP that can help clients manage multiple technologies and multiple clouds. TierPoint leads with a cloud management platform (CMP) approach to enable the use of private, TierPoint-hosted or hyperscale cloud providers as disaster recovery targets. To that end, the Azure relationship has expanded nationally (for DRaaS and managed services, such as for the Azure infrastructure and Office 365), and additional capabilities for AWS are in development. Underpinning the "Server to Cloud" and "Cloud to Cloud" DRaaS offerings are Azure Site Recovery's Inmage Scout and Zerto, respectively. TierPoint supports other replication products, such as EMC RecoverPoint and non-x86 workloads, such as IBM AIX. TierPoint was rated a Challenger in its first year of participation in the DRaaS Magic Quadrant.

TierPoint's average score in the seven core critical capabilities categories was 4.0. Use-case scores averaged above 4.0 with production and application data recovery (4.11) being its highest. The other use-case scores were consistent: mission-critical workload recovery (4.00), extended recovery operations (4.00) and managed service failover (3.95).

Service Delivery Options: Self-service or fully managed

Unitrends

Solution: Unitrends Disaster Recovery Services

Unitrends' two distinct DRaaS solutions were built or acquired in 2014. Unitrends DRaaS is supported in its own cloud. Customers can add DRaaS workloads that use that data for disaster recovery with a guaranteed one-hour SLA. In addition, Unitrends ReliableDR can be used as a service recovery assurance add-on to automate the testing of its disaster recovery environment in the cloud to guarantee recovery. It also supports additional services, including Unitrends Boomerang, which enables customers to use the virtual processing and storage resources of hyperscale cloud providers (e.g., AWS, Azure, GCP, Open Stack-based clouds and Rackspace) as an alternative to Unitrends' own cloud. Boomerang uses a "pilot light" architecture in AWS or Azure that does not require any charges for computing resources until a disaster is declared. Because it offers customers a fair degree of service choice, Unitrends was rated as a Visionary in its first year of participation in the DRaaS Magic Quadrant.

Unitrends' average score in the seven core critical capabilities categories was 4.0. In addition, it scored at or above 4.0 in all four use-case categories, including production and application data recovery (4.00), mission-critical workload recovery (4.07), extended recovery operations (4.04) and managed service failover (4.05).

Service Delivery Options: Self-service (Unitrends Boomerang) or fully managed (Unitrends DRaaS)

Verizon

Solution: Verizon Cloud Disaster Recovery

Verizon's DRaaS (based on VMware technology) enables customers to recover VMs and production data inside a managed cloud. The service has been available for nearly six years, having been officially launched in November 2010. Recovery testing and recovery operations are primarily provider-managed, requiring close management coordination between the DRaaS customer and Verizon's technical support staff in both cases. Customers can negotiate RPOs for SLAs, which depend on the specific data center configuration. Separate from DRaaS, Verizon offers Cloud IaaS with which clients can leverage add-on services for recovery in a self-service fashion, including automated network and firewall configurations. Because of its relatively large customer base and its support for large configurations (i.e., thousands of servers), Verizon was rated a Challenger in the 2016 DRaaS Magic Quadrant.

In terms of its 2016 critical capabilities results, Verizon achieved an average score of 3.7 across the seven core critical capability categories. In the four use-case categories, Verizon's scores were production and application data recovery (3.85), mission-critical workload recover (3.72), extended recovery operations (3.72) and managed service failover (3.71).

Service Delivery Options: Fully managed

VMware

Solution: vCloud Air Disaster Recovery

VMware's vCloud Air Disaster Recovery offering is sold as a self-service solution or as a managed service offering that is delivered by one of its many partners. Its management integration with vCenter eliminates the need for customers to familiarize themselves with a separate provider portal interface. vCloud Air supports a broad level of regulatory compliance, including ISO 27001, SSAE 16 (SOC 1, SOC 2 and SOC 3), Health Insurance Portability and Accountability Act [HIPAA], and the Health Information Technology for Economic and Clinical Health (HITECH) Act. vCloud Air Disaster Recovery provides unlimited testing capabilities and nondisruptive failover testing with full networking capabilities. One of the unique features of vCloud Air Disaster Recovery is that a vCloud Air contract term can be as short as one month. Because of its growing customer base and expanded service capabilities, VMware was rated a Challenger in the 2016 DRaaS Magic Quadrant.

In the 2016 critical capabilities assessment, VMware achieved an average score of 3.8 across the seven core critical capability categories. In the four use-case categories, its scores were production and application data recovery (3.65), mission-critical workload recovery (3.80), extended recovery operations (3.79) and managed service failover (3.77).

Service Delivery Options: Self-service

Context

DRaaS became mainstream in 2015, with many providers experiencing double-digit revenue growth. DRaaS production instances have climbed from approximately 30,000 in 2015 to more than 50,000 thus far in 2016. However, DRaaS is increasingly becoming a subset of a broader hybrid data center enablement.

Among providers of DRaaS, there continues to be a wide variance in experience, service capabilities and pricing mechanisms, as well as other key differentiating factors. Data center managers should use this research to identify and evaluate specific DRaaS providers with capabilities that align with their organizations' recovery needs.

Product/Service Class Definition

For this Critical Capabilities assessment, DRaaS services are classified as two types. In the first, the service provider is responsible for managing VM replication, VM activation, exercise management and servicing customer disaster declarations. Increasingly, this is becoming the preferred model for customers that have large, hybrid configurations that include physical and virtual servers. Here, the provider adds significant value by supporting managed recovery orchestration across an entire set of servers and production applications, rather than just the virtual servers. In the second, the provider role is relegated to just VM activation and shutdown, and the service customer is responsible for managing replication, exercise management and recovery operations following a disaster declaration.

Critical Capabilities Definition

The pricing policy critical capability has been removed for this year's 2016 Disaster Recovery as a Service Critical Capabilities research. Future research will cover some of the nuances across the virtual and physical pricing options, as well as associated tipping points.

Physical/Virtual System Recovery

This capability involves the recovery of virtual, physical and hybrid configurations.

The criteria in this category assess VM support breadth; service alternatives for supporting on-premises VM and production data replication (including the use of SAN-to-SAN replication, as well as hypervisor and VM guest-based replication); the activation of physical servers via a bare-metal restore process; and support for hybrid configurations composed of activated VMs and physical server and storage equipment. In this category, higher scores were given to providers that support the most diverse set of replication options and have the most experience supporting hybrid configurations.

Testing and Declaration

This capability involves recovery testing and disaster declaration.

This capability is specific to the support for and incremental costs of recovery testing and disaster declaration. Vendors that provide the greatest amount of recovery testing flexibility at the lowest cost received higher scores.

Service Manageability

This capability involves seamlessly providing a fully managed service, regardless of customer configuration.

This refers to the degree to which the provider manages RTO- and RPO-based service levels, flexibly supports processor and storage resource bursting, and can support recovery testing for configurations that are split between cloud- and non-cloud-based data centers. It also includes the extent to which on-premises operations management utilities can manage recovery configurations in the cloud, and support postrecovery operations failback from the cloud to the primary production data center. Once again, support for all these criteria resulted in a high score.

Resiliency

This capability ensures the ability to restore operations through well-defined processes, tools and SLAs.

In this category, higher scores were given for built-in backup of replicated VM images and related production data, clear customer credit policies for missed service levels, and a demonstrated and successful track record of availability management. This category also includes a set of well-defined management processes and supporting tools for failover operations among cloud service data centers, should primary service delivery data center operation be disrupted for any reason.

Security and Compliance

This capability involves the security of operations and compliance with industry standards.

Scores were determined based on the existence and use of provider operations controls for identity management, data eradication, role-based access and compliance with standards, such as SSAE 16 SOC 2, DoD 5220.22-M, NIST 800-88, ITAR, FISMA, HIPAA and PCI.

Value-Added Services

This capability involves professional services that are not included as part of the standard DRaaS offering.

Providers were assessed based on the set of available services that supplement the DRaaS offering. Examples include data backup and archive management services; services specific to industry verticals, such as healthcare, government or financial services; support for additional hardware that may be required by a customer, but is not part of the standard service offering; and support for private, virtual private or hybrid network service offerings, as well as the breadth and depth of global technical support services.

Customer Experience

This capability involves the customer experience and customer satisfaction with the DRaaS provider.

Providers were assessed based on collected feedback on DRaaS offerings. Data was collected through the customer reference process for the "Magic Quadrant for Disaster Recovery as a Service" and from Gartner end-user inquiry feedback.

Use Cases

Production and Application Data Recovery

This involves the providers' ability to provide a single recovery solution for a hybrid combination of virtual and physical systems.

Providers were assessed in terms of their ability to supply a single recovery service solution for a combination of VM and non-VM-based systems, physical server and storage systems, and the backup and recovery of data that was not otherwise contained in a VM's virtual file store. These requirements are reflected in the relatively high evaluation weightings that were used in the physical/virtual system recovery (60%), testing/declaration (10%) and customer experience (10%) categories.

Mission-Critical Workload Recovery

This involves assessment of providers' ability to recover and manage mission-critical applications.

Here, the focus was on a provider's ability to effectively recover and manage production applications that would be considered mission-critical by the service customer. In this use case, the highest weighting percentages were used in the physical/virtual system recovery (20%), security and compliance (20%) and customer experience (20%) categories.

Extended Recovery Operations

This involves assessing providers' ability to successfully support postrecovery application operations for extended periods of time.

Operations failover for the service customer is an absolute minimum service prerequisite. It is also important to assess a provider's ability to support postrecovery application operation for an extended period of time, which may be several days, weeks or perhaps even months. For this use case, the highest weightings were given to physical/virtual system recovery (18%), customer experience (17%) and security and compliance (17%).

Managed Service Failover

This involves assessment of providers' ability to successfully support managed application failovers.

Not all events that disrupt IT service operations are major disasters. Most are localized events that occur inside the data center itself and do not affect all production operations. When these events occur, it is useful to fail over the operations of the affected applications to a separate set of servers and storage. In this use case, we assessed each of the providers on the extent to which they can effectively support managed application failovers. In this category, the capabilities considered most critical are resiliency (17%), physical//virtual system recovery (17%), service manageability (17%), security and compliance (17%), and testing/declaration (17%).

Vendors Added and Dropped

Added

The following providers were added to the 2016 Critical Capabilities research:

- Carbonite (via its acquisition of EVault)
- Datto
- Evolve IP
- Infrascale
- Microsoft
- Recovery Point
- TierPoint
- Unitrends

Dropped

Windstream, which was part of the 2015 Critical Capabilities research, is not included in 2016, because its DRaaS business has been acquired by TierPoint.

Inclusion Criteria

Specifically targeted and marketed as a DRaaS offering, as defined in the Market Definition/ Description section of this research.

The vendor must provide its DRaaS service in one of two ways:

- The service provider is responsible for managing VM replication, VM activation, exercise management and customer disaster declarations.
- The provider role is responsible for just VM activation and shutdown, and the service customer is responsible for managing replication, exercise management and recovery operations following a disaster declaration.

The in-scope services must have been in general availability for at least six months, as of 4 January 2016.

The vendor must have at least 25 discrete production customers as of 4 January 2016.

The vendor must be determined by Gartner to be a significant player in the market via market presence and/or technology innovation.

Table 1. Weighting for Critical Capabilities in Use Cases

Critical Capabilities	Production and Application Data Recovery	Mission-Critical Workload Recovery	Extended Recovery Operations	Managed Service Failover
Physical/Virtual System Recovery	60%	20%	18%	17%
Testing and Declaration	10%	12%	10%	17%
Service Manageability	8%	11%	14%	17%
Resiliency	5%	12%	11%	17%
Security and Compliance	5%	20%	17%	17%
Value-Added Services	2%	5%	13%	5%
Customer Experience	10%	20%	17%	10%
Total	**100%**	**100%**	**100%**	**100%**
As of October 2016				

Source: Gartner (October 2016)

This methodology requires analysts to identify the critical capabilities for a class of products/services. Each capability is then weighed in terms of its relative importance for specific product/service use cases.

Critical Capabilities Rating

Each of the products/services has been evaluated on the critical capabilities on a scale of 1 to 5; a score of 1 = Poor (most or all defined requirements are not achieved), while 5 = Outstanding (significantly exceeds requirements).

Table 2. Product/Service Rating on Critical Capabilities

Critical Capabilities	Acronis	Axcient	Bluelock	Cable and Wireless Business	Carbonite	Databarracks	Datto	Evolve IP	IBM	iland	Infrascale	Microsoft	NTT Communications	Peak 10	Recovery Point	Sungard Availability Services	TierPoint	Unitrends	Verizon	VMware
Physical/ Virtual System Recovery	4.0	3.7	3.9	4.2	3.6	3.6	3.6	3.7	4.6	3.9	3.7	3.9	4.4	3.9	4.6	4.4	4.2	3.9	4.0	3.5
Testing and Declaration	4.0	4.1	4.3	4.2	3.8	3.6	3.8	3.7	4.2	4.2	3.9	3.9	3.8	3.9	4.2	4.0	4.0	4.0	3.4	3.8
Service Manageability	3.8	4.1	4.2	4.2	3.7	3.6	3.7	3.7	4.0	4.2	3.9	3.9	4.0	3.9	4.1	3.9	3.9	4.1	3.7	3.7
Resiliency	3.9	3.9	4.2	4.1	3.9	3.7	3.7	3.7	3.9	4.0	4.2	3.9	3.8	3.7	3.8	3.9	3.6	4.3	3.8	3.8
Security and Compliance	3.8	3.8	4.1	4.0	3.7	3.8	3.7	3.8	4.3	4.0	3.9	4.3	4.1	3.8	4.4	4.2	3.8	3.7	3.7	3.8
Value-Added Services	4.0	3.7	4.2	4.0	3.6	3.6	3.8	3.7	4.6	4.2	3.9	3.7	4.0	4.0	4.2	4.0	4.0	3.7	3.7	3.7
Customer Experience	4.0	4.5	4.7	4.4	3.4	3.9	4.3	3.6	4.3	4.6	4.5	3.8	4.2	3.8	4.4	3.8	4.3	4.6	3.6	4.2
As of October 2016																				

Source: Gartner (October 2016)

Table 3 shows the product/service scores for each use case. The scores, which are generated by multiplying the use case weightings by the product/service ratings, summarize how well the critical capabilities are met for each use case.

Table 3. Product/Service Score in Use Cases

Use Cases	Acronis	Axcient	Bluelock	Cable and Wireless Business	Carbonite	Databarracks	Datto	Evolve IP	IBM	iland	Infrascale	Microsoft	NTT Communications	Peak 10	Recovery Point	Sungard Availability Services	TierPoint	Unitrends	Verizon	VMware
Production and Appli-cation Data Recovery	3.97	3.87	4.08	4.20	3.63	3.65	3.71	3.70	4.43	4.04	3.86	3.91	4.24	3.88	4.44	4.22	4.11	4.00	3.85	3.65
Mission-Critical Workload Recovery	3.93	4.00	4.23	4.18	3.65	3.71	3.82	3.70	4.28	4.16	4.02	3.95	4.09	3.84	4.30	4.06	4.00	4.07	3.72	3.80
Extended Recovery Operations	3.93	3.97	4.22	4.16	3.65	3.70	3.81	3.70	4.30	4.16	4.00	3.93	4.08	3.86	4.28	4.05	4.00	4.04	3.72	3.79
Managed Service Failover	3.92	3.97	4.20	4.16	3.70	3.68	3.77	3.71	4.23	4.12	3.98	3.95	4.04	3.84	4.24	4.05	3.95	4.05	3.71	3.77
As of October 2016																				

Source: Gartner (October 2016)

To determine an overall score for each product/service in the use cases, multiply the ratings in Table 2 by the weightings shown in Table 1.

Editor: please add the following boilerplate text below the table, “To determine an overall score for each product/service in the use cases, multiply the ratings in Table 2 by the weightings shown in Table 1.”

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Magic Quadrant for Disaster Recovery as a Service"

"10 Strategic Questions to Ask Potential DRaaS Providers"

"Five Pragmatic Questions to Ask Potential DRaaS Providers"

"How Products and Services Are Evaluated in Gartner Critical Capabilities"

Critical Capabilities Methodology

This methodology requires analysts to identify the critical capabilities for a class of products or services. Each capability is then weighted in terms of its relative importance for specific product or service use cases. Next, products/services are rated in terms of how well they achieve each of the critical capabilities. A score that summarizes how well they meet the critical capabilities for each use case is then calculated for each product/service.

"Critical capabilities" are attributes that differentiate products/services in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

In defining the product/service category for evaluation, the analyst first identifies the leading uses for the products/services in this market. What needs are end-users looking to fulfill, when considering products/services in this market? Use cases should match common client deployment scenarios. These distinct client scenarios define the Use Cases.

The analyst then identifies the critical capabilities. These capabilities are generalized groups of features commonly required by this class of products/services. Each capability is assigned a level of importance in fulfilling that particular need; some sets of features are more important than others, depending on the use case being evaluated.

Each vendor's product or service is evaluated in terms of how well it delivers each capability, on a five-point scale. These ratings are displayed side-by-side for all vendors, allowing easy comparisons between the different sets of features.

Ratings and summary scores range from 1.0 to 5.0:

1 = Poor or Absent: most or all defined requirements for a capability are not achieved

2 = Fair: some requirements are not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

To determine an overall score for each product in the use cases, the product ratings are multiplied by the weightings to come up with the product score in use cases.

The critical capabilities Gartner has selected do not represent all capabilities for any product; therefore, may not represent those most important for a specific use situation or business objective. Clients should use a critical capabilities analysis as one of several sources of input about a product before making a product/service decision.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp