HostedBizz

# DISASTER RECOVERY AS A SERVICE

## AN OUTLOOK REPORT FROM STORAGE STRATEGIES NOW

By Deni Connor and Earl Follis

VEEAM StorageStrategies NOW TARGETED ANALYSIS

WHITE PAPER
06.20.2016

# Contents

## Editor's Note

This report is aimed at IT pros working in organizations from small businesses with fewer than 25 employees, all the way up to multi-national corporations with thousands of employees. The unique value proposition offered by Disaster Recovery-as-a-Service (DRaaS) makes it a viable option for most — but not all — disaster recovery (DR) scenarios.

In particular, DRaaS offers sophisticated availability strategies to guard against loss of data during natural or man-made disasters. DRaaS is a solution that all IT pros should consider when and where DR requirements, budget and complexity cannot be addressed by traditional DR options. This report expands on the capabilities of DRaaS and where it best fits in an IT DR portfolio.

**Deni Connor**

dconnor@ssg-now.com

**Earl Follis**

efollis@ssg-now.com

## Executive Summary

Cloud-based disaster recovery, also known as Disaster Recovery-as-a-Service (DRaaS), presents a significant opportunity for companies of all sizes to save money on their disaster recovery (DR) capabilities or expand those capabilities at the same price.

DRaaS offers companies a plethora of benefits over traditional DR strategies, including reduced complexity, quicker recovery configuration and processes, lower costs through better allocation of resources, reduced capital expenditures, less upfront financial risk and self-service capabilities that enable the effective governance of data.

DRaaS offers companies a plethora of benefits over traditional DR strategies, including reduced complexity, quicker recovery configuration and processes, lower costs through better allocation of resources, reduced capital expenditures, less upfront financial risk and self-service capabilities that enable the effective governance of data.

Given the potential for cost savings in a DRaaS environment, many companies are saving money compared to their traditional DR costs, while expanding their DR capabilities far beyond traditional DR approaches. Considering the compelling economic argument presented by DRaaS, every company in the world should weigh their options for a DRaaS plan that assures timely restoration of IT software and services in the event of a downtime event. SMBs have always struggled with the lack of IT expertise required to formulate an effective DR strategy while enterprise-scale IT shops have the expertise but possibly not the budget or bandwidth to ensure end-to-end availability of their applications following a natural or manmade disaster.

The first economy DRaaS provides is an economy of scale due to the virtualized cloud infrastructure required to support DRaaS services. Migrating services such as DR to the cloud distributes that infrastructure over thousands of companies who reside in that same DRaaS cloud. The fact that DRaaS infrastructure is virtualized and supports multi-tenancy leads to additional cost savings, because utilization of cloud resources will typically be extremely high in a shared DRaaS infrastructure. If you have elastic cloud resources available on-demand, any time you need it, it's likely that IT organizations will no longer be motivated to over-provision your DR planning due to the scarcity of resources in a traditional DR architecture.

When considering DR strategies and vendors, we strongly recommend that you evaluate DRaaS enablement technologies that serve as the technological backbone of a DRaaS offering.

When considering DR strategies and vendors, we strongly recommend that you evaluate DRaaS enablement technologies that serve as the technological backbone of a DRaaS offering. Many offer unlimited, continuous snapshots of virtual machines (VMs), applications and databases. Many offer comprehensive DR capabilities for specific mission-critical applications, such as Microsoft Exchange.

DR strategies normally infera host-to-host replication quick and seamless failover and failback, but in some instances DRaaS providers consider storing a backup in a cloud repository as DR although it requires custom steps to failover and failback. Some DRaaS vendors include a virtual sandbox where ad hoc DR tests can be performed with the click of a mouse. DRaaS is a natural fit for most companies, if not as a complete DR strategy at least providing cost-effective DR coverage for many common environments, applications and databases. This report covers the history of DRaaS, common (and uncommon) features and capabilities of DRaaS, as well as recommended best practices for companies looking to evaluate and implement DRaaS solutions.

## Driving Issues, Trends, History

Online backup and restore capabilities have been available for more than 10 years, though the development of cloud-based data services over the last five years has accelerated the exponential growth of DRaaS offerings in the high-tech market.

One of the biggest drawbacks of online backup and recovery schemes 10 years ago was the relatively slow link between the computers being backed up and the online storage mechanism. Now, with high-speed internet being both ubiquitous and relatively cheap, transporting data from a local environment to a cloud storage facility is far easier and cheaper than ever before.

DRaaS is a term that specifically pertains to the ability to quickly and easily restore applications and data in a timely fashion after a downtime event with little to no downtime or end user disruption.

### Off-site backups

Historically, online backup and restore services always required IT admins to make a full backup of the data to be protected, copy that backup to one or more tapes or disks, then ship them off to the backup facility. Once the original full backup was populated in the online repository, all future differential backups could proceed directly across whatever wide-area network (WAN) link connected the on premises environment to the online repository. Though most DRaaS vendors still support the mail-in or drive over initial full backup technique called seeding, a much more common approach is to simply send that initial full backup to the online repository via the existing network connection between backup source and the online repository. Depending on your connection speed to the online repository and the amount of data in the initial backup set, it might take several days or longer to upload that full backup. However, that typically takes no longer than it takes to run the full backup, store the data to suitable media, ship the media, and then wait for your online backup service to load that data into the repository.

Many companies, particularly smaller companies, have a very difficult time resuming revenue-generating operations following a downtime event, even if they have a DR plan and strategy in place. That's where BC plans come into play.

If your company's data falls into one of the categories of companies that cannot or should not store its data in a public cloud, you will find DRaaS options on the market that support a private cloud architecture. More on this point in a bit.

## DRaaS and Business Continuity Planning

DRaaS is a term that specifically pertains to the ability to quickly and easily restore applications and data in a timely fashion after a downtime event with little to no downtime or end user disruption. By contrast, business continuity (BC) refers to not just restoring lost data and application functionality following a downtime event, but also to restoring every aspect of a company's infrastructure so that business operations can resume as soon as possible. Many companies, particularly smaller companies, have a very difficult time resuming revenue-generating operations following a downtime event, even if they have a DR plan and strategy in place. That's where BC plans come into play.

***For instance, BC planning includes considerations such as:***

- Where will employees physically work following damage to their office or workspace? Will displaced employees have a computer to use? Will they be able to connect to the corporate network?
- How will a company restore internal and external telephone communications if a natural disaster floods company facilities or causes physical damage to company locations?
- How will a company process payroll, write checks, pay its bills or maintain supply chain communications following an unplanned outage?

As you can see, BC considerations are a superset of what we've always thought of as DR. Restoring user, server and application data is certainly an important step following a downtime event, but BC is the key to fully restoring company operations — not just company data. Many DRaaS offerings include sophisticated BC capabilities as well.

## The cloud makes DRaaS a reality, but a cloud is not required

DRaaS doesn't necessarily mean storage of DR data solely in a public cloud. There are private cloud and hybrid DRaaS solutions that might be a better fit in some cases, particularly where governmental rules and regulations require special protection of data that includes personally identifiable information (PII), or if an organization is looking to build a more personable relationship with their DRaaS provider. If your company's data falls into one of the categories of companies that cannot or should not store its data in a public cloud, you will find DRaaS options on the market that support a private cloud architecture. More on this point in a bit.

A key factor in the value proposition for DRaaS services is that ability to pay only for what you use and need.

Many DRaaS providers also make it easy for companies to add or subtract DR services via a self-service portal where protected devices can be self-managed. This is an important part of your DRaaS planning and evaluation process when looking for suitable DRaaS solutions for your company.

### DRaaS offers pay-as-you-go pricing

A key factor in the value proposition for DRaaS services is that ability to pay only for what you use and need. Traditional DR services consist of paying annual fees to guarantee access to physical servers and network infrastructure residing in a shared DR data center in the event of a disaster. Or, if you are looking to build and manage a second facility for DR, it can be an expensive upfront investment. This was an extremely expensive and inefficient model because though you might pay to protect your entire data center, you might only need to restore some fraction of your computing infrastructure in the event of a disaster. DRaaS drastically improves this situation by allowing companies to pay only for the DR availability they need. This also allows large IT shops to divide their DR strategy between traditional DR providers, say for mainframe or other specialty devices, while common server and end-user protection can leverage the cost-savings and convenience of DRaaS services. They can also set certain RTOs for particular applications and data, prioritizing business critical systems and driving additional costs savings with lower RTOs for less business-critical systems.

### DRaaS and elastic provisioning

Another benefit of DRaaS is that you can easily expand or contract your DR platform as needed. Traditional DR providers would only guarantee application availability following a disaster for the exact number of computers and other devices being paid for. Adding additional servers could produce sizable increases in DR costs, while decommissioned computers and devices could typically only be removed from your DR services contract at renewal time. DRaaS offers companies DR availability that can expand and contract as a company's computing and network resources changes, which for most companies can be a very regular occurrence. This is an important consideration when evaluating DRaaS providers: How flexible is the DRaaS provider when you need to expand or contract your DR coverage? Most DRaaS providers have a flat fee for DR protection based on processor count, physical servers protected or VMs. Many DRaaS providers also make it easy for companies to add or subtract DR services via a self-service portal where protected devices can be self-managed. This is an important part of your DRaaS planning and evaluation process when looking for suitable DRaaS solutions for your company.

Hybrid DRaaS approaches also offer an excellent opportunity for a phased implementation of cloud-based DRaaS, where data is gradually migrated from a local datastore to a cloud-based DRaaS data store. This allows companies to control the timing and velocity of migrating data from a local data center to a public cloud DRaaS provider.

## DRaaS Essentials

### Local versus cloud DRaaS

As mentioned earlier in this report, there are a variety of DRaaS architectures and strategies available for companies that do not want or cannot store some or all of the data in public clouds. The first strategy is to utilize a local or private cloud, owned and operated by a service provider. This is the best option for companies who must ensure that no third party has access to PII or other high-value or protected classes of data. Hacks of public cloud infrastructures are rare, but there is still always an exposure anytime your data leaves your company premises. Many solutions offer in-flight and at-rest encryption to add an additional layer of security in situations when your data leaves your company's on-premises infrastructure. As an example of how hardened public clouds have become, the Central Intelligence Agency (CIA) decided in 2013 to host their data on a private cloud engineered by and based on a public cloud architecture. But the point is that if the CIA is comfortable with the available security of the private cloud that the public cloud service provider built for the agency, your non-regulated data will likely be plenty secure in a public DRaaS environment. This is assuming, of course, that your company follows applicable security processes and procedures for storing your DRaaS data in the cloud: proper protection of passwords, encryption, two-factor authentication, etc.

### What is hybrid DRaaS

Another option for companies looking for the best of both worlds between the economics of public cloud DRaaS and the highly secure — but more expensive — model of local or private cloud DRaaS is the possibility of a hybrid DRaaS approach. In a hybrid DRaaS scenario, high-value data or data containing PII can be kept in a local cloud controlled by a service provider, while less critical data, e.g. end-user backups or other non-mission-critical data, can be kept in the cheaper environs of a public DRaaS cloud. Many DRaaS vendors understand the appeal of a hybrid DRaaS architecture and build features into their service offerings that allows companies to seamlessly integrate local data stores and cloud data stores, allowing their customers to choose the appropriate destination for each category or class of DRaaS data. Hybrid DRaaS approaches also offer an excellent opportunity for a phased implementation of cloud-based DRaaS, where data is gradually migrated from a local datastore to a cloud-based DRaaS data store. This allows companies to control the timing and velocity of migrating data from a local data center to a public cloud DRaaS provider.

Some DRaaS vendors only support one or two hypervisor platforms because the majority of the hypervisor market is dominated by two main players, so be sure to ask questions about hypervisor support as part of your evaluation process if you use a lesser supported hypervisor.

### DRaaS in virtual environments

Most companies run some — or all — of their IT server, database and application infrastructure on virtual servers supported by hypervisor platforms such as VMware vSphere, Microsoft Hyper-V or Citrix XenServer. Considering that most DRaaS clouds also run on virtualized servers, there is a natural synergy between customers using VMs and protecting those VMs via DRaaS. That said, the compatibility of your virtual server environment with your DRaaS provider's supported virtual platforms is an important consideration when evaluating your DRaaS options. If your virtual server environment runs on VMware, be sure that your DRaaS provider also supports the same version of VMware. This hypervisor compatibility ensures that your VM images will run seamlessly in the DRaaS environment you select. Some DRaaS vendors only support one or two hypervisor platforms because the majority of the hypervisor market is dominated by two main players, so be sure to ask questions about hypervisor support as part of your evaluation process if you use a lesser supported hypervisor.

# Implementing DRaaS

The process of implementing a DRaaS solution starts where all IT projects (should) start, with gathering of all applicable requirements. Be sure to include all stakeholders, both internal and external (suppliers, logistics, etc.) in your requirements-gathering process.
Your DRaaS requirements list is a living document that ensures whichever DRaaS solution your company chooses will meet all current and foreseeable needs for DR availability.

Be sure to communicate regularly with your chosen DRaaS provider during the implementation process to ensure that all project requirements are met in a timely fashion. That said, you will find that DRaaS hides much of the complexity of DR planning while leveraging cloud capabilities to simplify both the planning process as well as the procedures utilized during an actual disaster. Note that migrating some or all of your applications and infrastructure to a cloud-based DRaaS provider may also require additional network capacity, the implementation of network traffic grooming or other infrastructure upgrades that should be factored into your project timeline.

With the blurring of traditional lines between various IT admin roles, ease-of-use is no longer just a trite phrase: It is truly becoming a critical part of any software implementation, and DRaaS is no different.

### End-user DRaaS self-service saves time and money

With the blurring of traditional lines between various IT admin roles, ease-of-use is no longer just a trite phrase: It is truly becoming a critical part of any software implementation, and DRaaS is no different. Recognizing that many IT staffs struggle to perform their daily workload as it is, ease of configuration and operation helps DRaaS solutions reduce the load on IT staff, while simultaneously reducing the need for additional investments in hardware, software or personnel. DRaaS solutions with a self-service portal offer data governance that is comprehensive and easy to manage.

### DRaaS is competitively priced

The price advantage of cloud-based DRaaS is mainly because the cost of the DR infrastructure can be spread across many different client companies. This ability to spread out DRaaS infrastructure costs results in DRaaS being one of the best bargains in the IT services market.

Competitive pricing makes DRaaS an attractive alternative for medium and enterprise companies, while also making comprehensive DR availability a reality for millions of small companies that have thus far been unable to afford a DR solution

Traditional DR providers typically include in their pricing one or more DR tests per year to be performed in the actual DR recovery center, though tests can usually be performed via remote access.

Competitive pricing makes DRaaS an attractive alternative for medium and enterprise companies, while also making comprehensive DR availability a reality for millions of small companies that have thus far been unable to afford a DR solution. Once again, as DRaaS providers sell to smaller companies, ease-of-use becomes a key differentiator because smaller firms likely do not have the technical expertise to implement traditional DR solutions, even if small firms can afford such services.

### Automating virtual DR tests

Traditional DR providers typically include in their pricing one or more DR tests per year to be performed in the actual DR recovery center, though tests can usually be performed via remote access. The concept of annual tests is the only valid way to validate that your DR plans and recovery infrastructure will meet your company's requirements in the event of an actual disaster. But such physical DR tests are extremely expensive in terms of the fees paid to access the DR data center for the test, as well as the onerous amount of time and labor it takes to successfully perform such tests.

Many DRaaS providers offer a better option for testing your DR preparedness: virtual recovery tests. Depending on the services offered by your specific DRaaS provider, you may be able to recover part or all of your protected infrastructure in an isolated sandbox environment. Once your recovery is underway in the sandbox, you can then test whether or not the recovery process works as expected. You can simultaneously test your human recovery procedures as part of a virtual DR test — i.e., can users log in, do your applications come back up as expected and does the recovered environment meet the goals of your DR plan? In a sandbox recovery scenario, you can even use your production network configuration with the real IP addresses and configurations of all servers and network services. For application or database DRaaS, you can recover and test those application and database servers can just as you would during a real disaster.

Many DRaaS provider also allow you to perform ad hoc DR tests of specific servers or services at the click of a mouse. Just as backups are worthless without a verified restore process, your DR process is only good as your DR test results. Fortunately, DRaaS providers are making DR tests easy and quick to perform, with little or no extra cost from the DRaaS perspective. As a result, the ease of DR testing should be a key requirement for your DR planning process and DRaaS evaluation criteria.

As you can see from the capabilities and features we've described thus far, DRaaS is an integral part of your BC planning process. Some DRaaS vendors explicitly offer BC services on top of their DRaaS services to include things such as cloud-based telephony and remote access schemes so that employees can work from home in the event of a disaster.

By combining DRaaS planning with BC planning, you can be sure that your IT infrastructure and the business activities that rely on those services will work in unison to recover from an incident in the shortest possible time and at the lowest cost.

### RPOs and RTOs

Recovery point objectives (RPOs) and recovery time objectives (RTOs) are two terms that have been used in the traditional DR world for many years. RPO represents a goal of the maximum time period that you can afford to lose data in the event of a disaster. For instance, if your company's business operations require no more than four hours of downtime following an incident or disaster, then obviously daily backups will not be sufficient to meet that RPO goal. RPOs should only be set following discussions with your company's business experts, not based on the capabilities of your backup and restore process. RTO is the maximum amount of time that the recovery process can take before the lack of operable IT infrastructure or data will produce an unacceptable gap in business continuity. Once again, define the RTO with your business leaders before you devise a DR strategy to meet those goals. Business requirements always dictate the RPO and RTO for a company, not the capabilities of IT to restore data and service. That said, the setting of RPOs and RTOs will likely be a balance of cost, IT capabilities and business needs. Of course, no downtime is the preferable RTO for your business users but that is only a theoretical option. We suggest that you define the business RPO and RTO goals first and then devise a DR recovery plan that meets that RPO and RTO. Also, remember to communicate to all DR stakeholders that the O stands for objective, not guarantee.

### Bare metal restores

Bare metal restores are critical for restoring physical servers that have to be rebuilt form the ground up. For instance, if a server loses its internal hard drive to a crash, it is usually quicker to perform a bare metal restore by creating a bootable disc that can be used to restore the entire contents of that server, including the operating system (OS). With that in mind, obviously a bare metal restore disc that allows a server to boot up, connect to the recovery environment and start the recovery process will have to be created in advance. This process allows for the timely booting and rebuilding of a server that has been repaired following a hardware failure or other hard crash.

### How DRaaS complements business continuity planning

As you can see from the capabilities and features we've described thus far, DRaaS is an integral part of your BC planning process. Some DRaaS vendors explicitly offer BC services on top of their DRaaS services to include things such as cloud-based telephony and remote access schemes so that employees can work from home in the event of a disaster. BC is a step beyond simply recovering from a downtime event: It provides a method and plan for getting your company back in business, generating revenue and serving your customers. By combining DRaaS planning with BC planning, you can be sure that your IT infrastructure and the business activities that rely on those services will work in unison to recover from an incident in the shortest possible time and at the lowest cost.

# Best Practices for the Implementation of DRaaS

We've covered quite a few best practice recommendations in this report, but we've accumulated the most important of those recommendations and best practices below.

**Vendor**

HostedBizz & Veeam

**DRaaS Solution**

HostedBizz Cloud Infrastructure as a Service and DRaaS plus Veeam® Cloud Connect Replication (included in Veeam Availability Suite™ v9, Veeam Backup & Replication™ and Veeam Backup Essentials™)

**Link to more information:**

https://www.veeam.com/disaster-recovery-as-a-service-draas.html

- Don't take DR planning lightly, whether utilizing DRaaS, traditional DR services or a combination of the two. Generate a project plan, include stakeholders in all phases of planning, and be sure to address any and all concerns before you start to evaluate your options.
- Develop a DR requirements list and circulate that list to all stakeholders. Be sure that you document all reasonable requirements and explain to your stakeholders why requirements might not make the list (cost, complexity, etc.).
- If applicable, include business continuity planning as part of your DR planning process, even you end up addressing those problems separately. DR and BC are usually intertwined aspects of a company's overall survival plan in the event of a downtime event or disaster.
- Your DRaaS solution should be easy-to-use, with applicable support available in the event of an incident requiring recovery activities.
- Self-service portal for end users will greatly reduce the amount of time IT admins will have to spend supporting restore requests. Be sure that your DRaaS solution allows help desk personnel to assist end users with routine restoration tasks.
- Remember that RTOs and RPOs should be negotiated with IT and the business entities within your company. Also, remember that these are objectives, not guarantees.
- Identify any physical servers that will require bare metal restores and be sure that your bare metal restore images are continually updated.
- Being able to perform ad hoc virtual DR tests quickly and easily is an important consideration when evaluating DRaaS providers. Be sure to run such tests on a regular basis to ensure that your recovery process will run as expected should disaster strike.
- A hybrid DRaaS solution is a great fit for companies that store PII or other protected data. Hybrid DRaaS can also be a valid strategy for a phased migration from traditional DR to a DRaaS approach.

HostedBizz & Veeam make disaster recovery simple and easy to deploy with Cloud Connect Replication by including its capability in its recently announced Veeam Availability Suite v9. Enabled by service providers and resellers, Veeam Cloud Connect Replication lets Veeam customers create, configure and manage disaster recovery operations for their VMware vSphere and Microsoft Hyper-V VMs without having to build or maintain a second site for DR.

Setting up Veeam Cloud Connect Replication is easy. From the Veeam console, the user selects HostedBizz as its service provider, enters the credentials provided by HostedBizz and then provisions the targets (cloud host) that their production host will replicate to.

Via Veeam Cloud Connect Replication and Veeam Availability Suite, customers can set up a hybrid environment that consists of on-site availability via backups and snapshots and off-site disaster recovery by simply replicating HostedBizz - a Veeam Cloud & Service Provider (VCSP).

Setting up Veeam Cloud Connect Replication is easy. From the Veeam console, the user selects HostedBizz as its service provider, enters the credentials provided by HostedBizz and then provisions the targets (cloud host) that their production host will replicate to.

From the service provider with Cloud Connect Replication, the customer is able to failover specific VMs or entire sites and failback VMs with little to no downtime or disruption to users. (The recovery point and time objective [RTPO™] is less than 15 minutes for all applications and data, according to Veeam's claims.)

As a VCSP partner, powered by Veeam Cloud Connect Replication, HostedBizz provides the cloud and handles multi-tenancy for multiple customers or departments, the orchestration and network extension. Built-in WAN acceleration is supported, yet optional, to the end user.

Within the cloud host are allocations for CPU, RAM, storage and networking resources, which allow the customer to initiate full-site failovers to a remote DR site in just a few clicks and partial site failovers to switch over to selected VM replicas instantly. Full-site failovers can even be initiated from a cell phone via the Veeam Cloud Connect web portal.

During replication, Veeam Cloud Connect Replication encapsulates and encrypts all network traffic — for management, replication and inter-VM communication — to transmit data securely over a single port using SSL/TLS.

Both full site failovers and partial failovers will leverage built-in network extension appliances, which will simplify networking complexity and preserve communication between running VMs regardless of physical location — even without having to make any changes to replica TCP/IP settings before, during or after failover.

Veeam counts in its ranks over 170,000 customers, 34,500 partners and 10,000 service providers, 1,000 of which are providing Cloud Connect within the first 12 months of it inception.

Finally, built-in WAN acceleration allows the service provider to allow DRaaS services to customers with slow or unreliable WAN connections or a large number of VMs. Replica seeding is also available for easy ramp-up.

Veeam Cloud Connect Replication is included in Veeam Availability Suite v9, Veeam Backup & Replication and Veeam Backup Essentials at no additional charge and with no additional licensing required for all traditional end-user customers. However, these end users will need a subscription with the VCSP partner to provide their cloud host. The customer is then charged for the disaster recovery service by the service provider, based on the pricing and licensing terms of the service provider.

### About Veeam

Veeam was founded in 2006 by president and CEO Ratmir Timashev, formerly of Quest Software and Aelita. It has received minority funding of an undisclosed amount from Insight Venture Partners. The company's headquarters are in Baar, Switzerland.

Veeam counts in its ranks over 170,000 customers, 34,500 partners and 10,000 service providers, 1,000 of which are providing Cloud Connect within the first 12 months of it inception. The company's base of customers is growing by an average of 4,000 customers a month. Its software currently protects over 10 million VMs.

### About HostedBizz

Founded in 2012, HostedBizz is an all Canadian Cloud Infrastructure as a Service provider for the IT industry. Located in Canadian Tier 3 data centers, HostedBizz's enterprise grade cloud platform delivers public and private cloud infrastructure along with hosted applications and services including virtual servers, virtual desktops, data backup and disaster recovery solutions that easily scale with organizational needs.

### About Storage Strategies NOW™

Storage Strategies NOWTM (SSG-NOW) is an industry analyst firm focused on storage, server, cloud and virtualization technologies. Our goal is to convey the business value of adopting these technologies to corporate stakeholders in a concise and easy-to-understand manner.