
BIOS
Be secured. Be assured
What's your plan?

“If you fail to plan, you are planning to fail!”

Benjamin Franklin

What can a real disaster mean to you?

- What would you do if your most important equipment went down tomorrow?
- Would you be able to work without your most important server? Would your employees?
- How much data can you afford to lose?
- How would you go about getting systems back on track if you had a failure?
- Do you know which systems are most important to your business?
- What are your recovery time objectives?
- What are your recovery point objectives?
- How often do you test your current recovery plan?

> Gartner studies have shown that 76% of companies experience an outage each year, and 40% of companies go out of business if they cannot access their data within 24 hours.

And it all boils down to:

How much money are you losing while crucial IT systems is down?

What's driving the need to run 24/7/365?

Accountability

Fiduciary responsibility to shareholders and other key stakeholders

Supplier expectations

Suppliers expect agreements and payments to be non-stop

Cost of downtime

Revenue loss, employee productivity loss, cash flow, fines, penalties

Employee and customer expectations

Impacts confidence and retention

Competitive advantage

Downtime creates an opportunity for competitors to seize market share

But a disaster is not just about losing data

What about the cost of downtime?

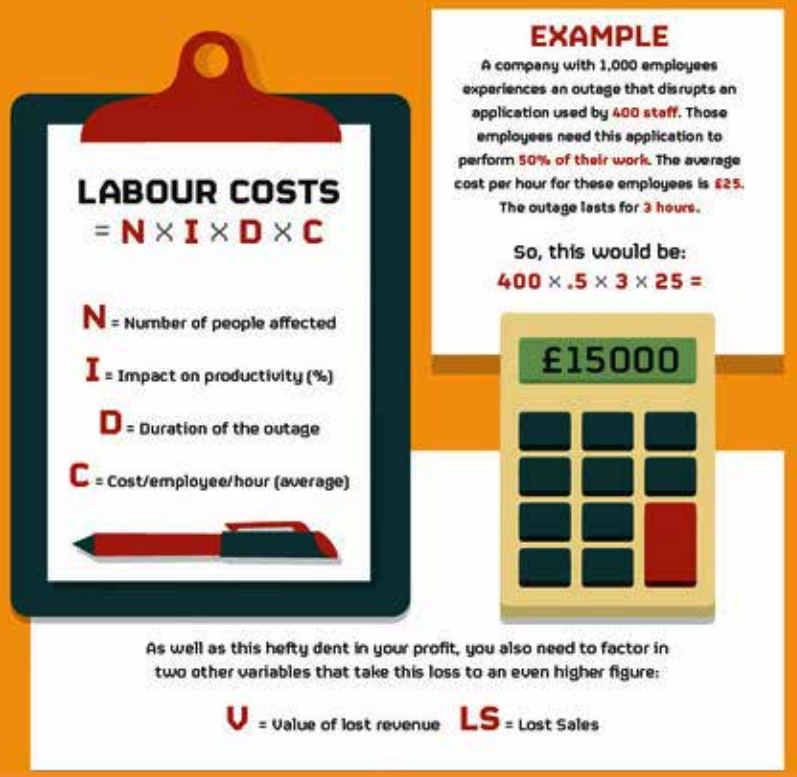
These costs are not only direct revenue losses, the costs of paying employees who can't work but also the costs to the company's brand and goodwill.

In the past:

British airlines IT outage strands thousands. Growing calls to remove the word British from their name.

Wannacry crypto virus takes down hospitals across the global putting lives at risks.

A national Middle Eastern bank's datacenter floods taking down all its ATMs for two days.



The average cost of a critical application failure per hour is

$500,000 to $1 Million

Source: The Real Cost of Downtime - IDC as reported by DevOps.com

The Downtime Iceberg

RBS fined £56m over 'unacceptable' computer failure

Reputational costs aside, what does downtime cost?

	Small Companies		Mid-Sized Companies		Large Companies	
	AED	SAR	AED	SAR	AED	SAR
Average cost/hour	25,358	25,896	271,950	277,723	4,152,750	4,240,907
Occurrences/Year	1.7	1.74	3.5	3.57	3	3.06
Average Length Occurrences (In hours)	2.2	2.25	3.8	3.88	0.8	0.82
Total Cost	94,837	96,952	3,616,935	3,693,717	9,966,600	10,178,177

These figures are based on the wages staff are paid per hour plus the company's productivity per hour.

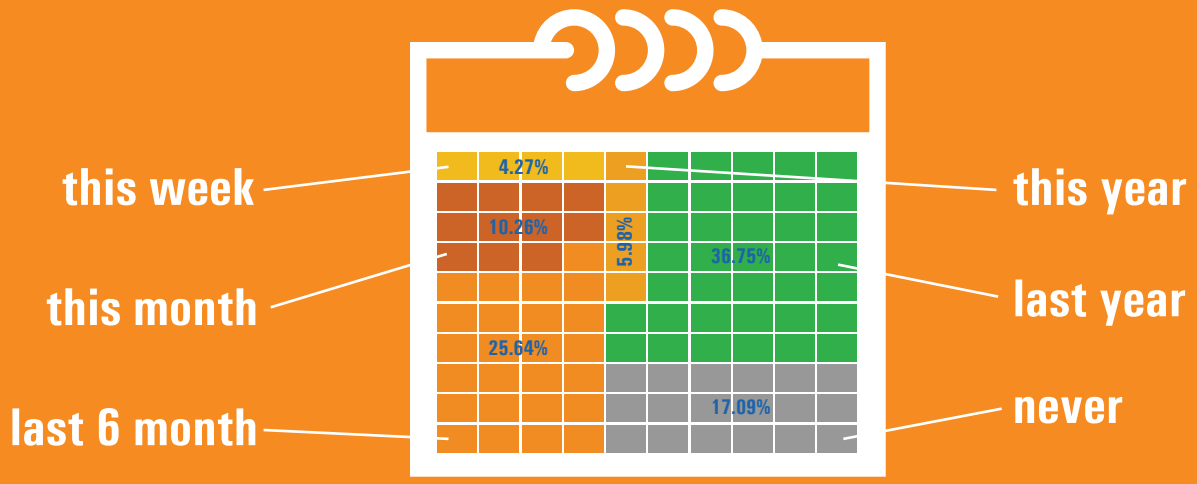

Disasters might
be inevitable,
but data loss and
downtime don’t
have to be.

Is a disaster just about not losing data and being able to recover from downtime?

Absolutely not. It was a big disaster for Sony when their systems were hacked, deleted and their movies posted on the internet.

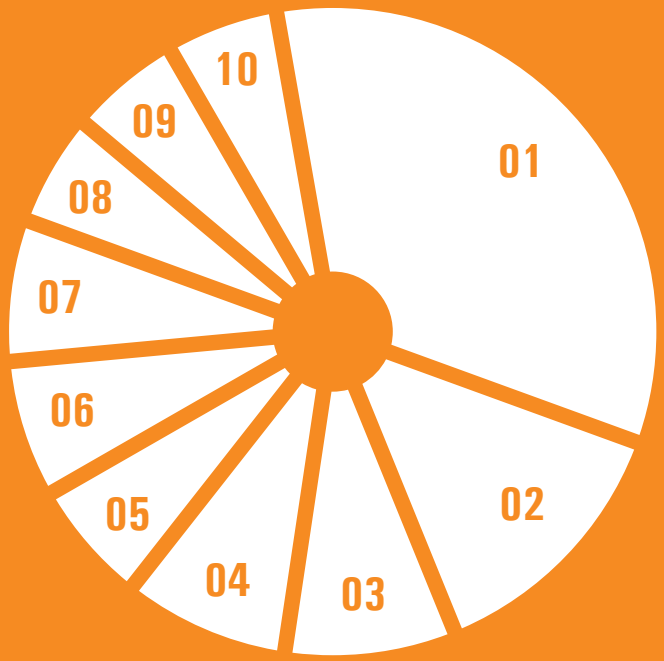
Cyber Security then is a pretty important part of preventing a Disaster.

Approximately **47%** of companies experienced an **outage or downtime this year**



10 typical disasters

01 Human error
02 Physical devices failing
03 Applications failing
04 Weather Related
05 Malware, Ransomware, Viruses
06 Being hacked and data destroyed
07 Datacenters or ISP connectivity outage
08 Denial of Service attack taking your sites down
09 Employee or Employees going 'rogue' and destroying backups and deleting data
10 A city-wide power failure



THE CAUSE OF UNPLANNED OUTAGES

88% HUMAN & MECHANICAL

12% WEATHER RELATED

Data provided by Emerson shows that human and mechanical failures cause the vast majority of unplanned outages in data centers.

The good news

Is it relatively easy to guard against all 10 of these types of disasters.

It is not even expensive. In fact, if a Disaster Recovery Plan prevents an hour of downtime a year it has usually paid for itself!

Our approach to protecting our customers from all 10 of these types of disasters is called Assured Recovery Services. This booklet will outline what Our Assured Recovery Service can do for your business.

Assured Recovery Service

Disaster recovery protects a business from annihilation yet many businesses don't have it, why?

That is because businesses are told they need to invest huge sums to replicate and manage IT enivronment to another location they often don't have.

But with DRaaS from CloudHPT none of that is necessary.
Instead Disaster Recovery can be a consumable monthly service that's fully managed.




Stay in Business. Every Day. **Assured Recovery Service**

Assured Recovery Service from BIOS has 3 elements.
01. CloudHPT: Disaster Recovery as a Service (DraaS)
02. BIOS Assured: Managed Services from our NOC in Dubai
03. BIOS CSI: SIEM as a Service from our SOC in Dubai

The first, DRaaS delivered from our cloud in the UAE and KSA, CloudHPT, and replicates your production environment so it can be brought back up on our cloud in moments.

But what sets us apart is that we understand it is better to prevent a disaster then to be able to recover from it. To achieve this we leverage BIOS Assured to monitor and maintain the health of your production environment. The third and final element of Assured Recovery Service is BIOS CSI which leverages 20 threat intelligence feeds to monitor and prevent malicious activity on your production environment.

Our approach to Disaster Recovery uses a two-pronged approach.

01 Prevent a Disaster (what could be better) and failing that;

02 Recover from a Disaster quickly

> We are immensely proud to have CloudHPT DRaaS recognized as Visionary in Gartner's Global Magic Quadrant.

Disaster Prevention

What is even better than being able to recover from a Disaster? Not having the disaster in the first place.

Too many companies see cyber security and disaster recovery in isolation, when in fact a better approach would be to see them as one and the same. Our Assured Recovery Service includes protecting a customers production environment (on site or in our cloud) with:

- **A patching solution:** failure to patch is the number one reason systems get compromised
- **Managed Detection and Response agents:** Advise us if a machine has been compromised with a persistent foothold, one of the major precursors to malware attack and data theft
- **Managed Anti-virus and DNS security** - to prevent malicious call backs to the internet if a machine is compromised and maintain control over internet usage outside your network
- **Vulnerability scanning and software audits** - know about gaps in your defenses and be able to proactively harden to remove risk
- **XDR agent and SIEM** - log management with ML powered event correlation to highlight suspicious behavior and trends that help catch sophisticated threats

> CloudHPT has a strong focus on disaster avoidance through proactive security information and event management (SIEM) capabilities.
>
> *Gartner Magic Quadrant DRaaS Report*

Disaster Recovery

Disaster Prevention is not enough.

Unfortunately, humans make mistakes. They delete things they don't mean to. They forget to replace backup tapes once a year.

Occasionally they accidently dig up electrical or communication wires. Or unintentionally set fire to buildings by mistake.

Sometimes power stations or sub stations go offline.

Mother nature sometimes sends lots of rain to places we don't expect it and causes flooding we are not prepared for.

Running a business without a Disaster Recovery Plan in place is like operating a shopping mall without a fire protection system in place – not a good idea.

A good disaster recovery plan is in-country

Many of our customers want a Disaster Recovery service that is in country or at least in region.

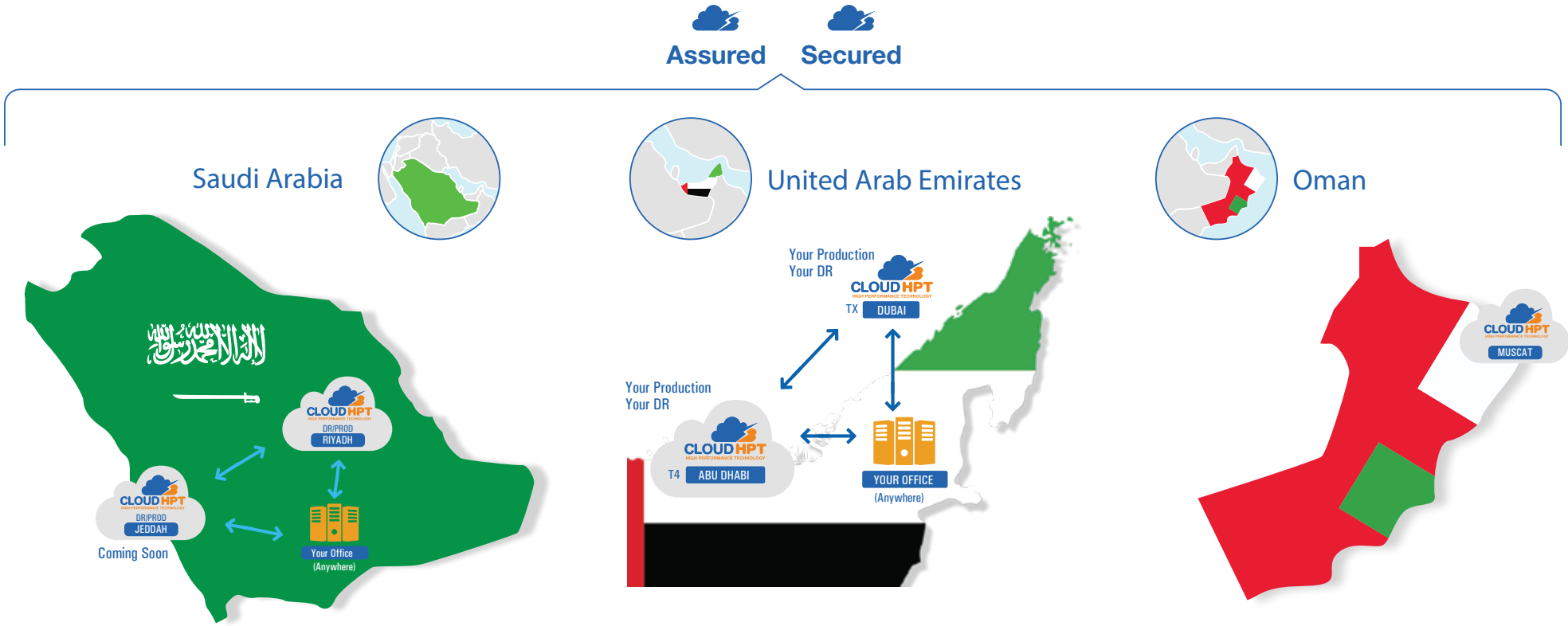
Having a Disaster Recovery site to replicate to on the other side of the world adds delay and interruption.

Our Disaster recovery service leverages our cloud, CloudHPT, which is built in datacenters in UAE, KSA and Oman.

> Keep your data locally in country to comply with data residency laws”
>
> *Gartner Magic Quadrant DRaaS Report*

A good disaster recovery plan protects you from bot net attacks

But what if your services are offline because you are under a Denial of Service (DDOS) attack and the DDOS attack follows your applications to our cloud?
The largest DDOS attack was a botnet attack and recorded 620GB of traffic a second in its peak.
CloudHPT is protected up to 1TB of DDOS – almost twice the largest attack ever.



A good disaster recovery plan includes monitoring your production environment 24x7

What good is a DR plan if you don't know when you are having a disaster in the first place? If something happens at 2am to your datacenter you don't want to only find out about it at 9am the next day when you come to work. That's why we monitor our customers' production environment 24x7 from our NOC (Network Operation Center).

Someone to call, 24/7

While other DRaaS vendors let you deal with it by yourself, we are available 24/7/365 – and ready the instant you need us to execute your recovery, get you back up and running, and assist with any additional updates to your environment.

A good disaster Recovery Service is easy to use

Declaring Disaster

- Your production monitored 24x7
- Auto Alert P1
- Your team confirms or contacts us to declare a disaster
- Disaster declared
- We initiate DR with a single click
- Recovery begins
- Your production is up in our cloud and users connect
- Business continues as usual

15 - 20 MINUTES TO DR FAIL OVER COMPLETE

Disaster Over

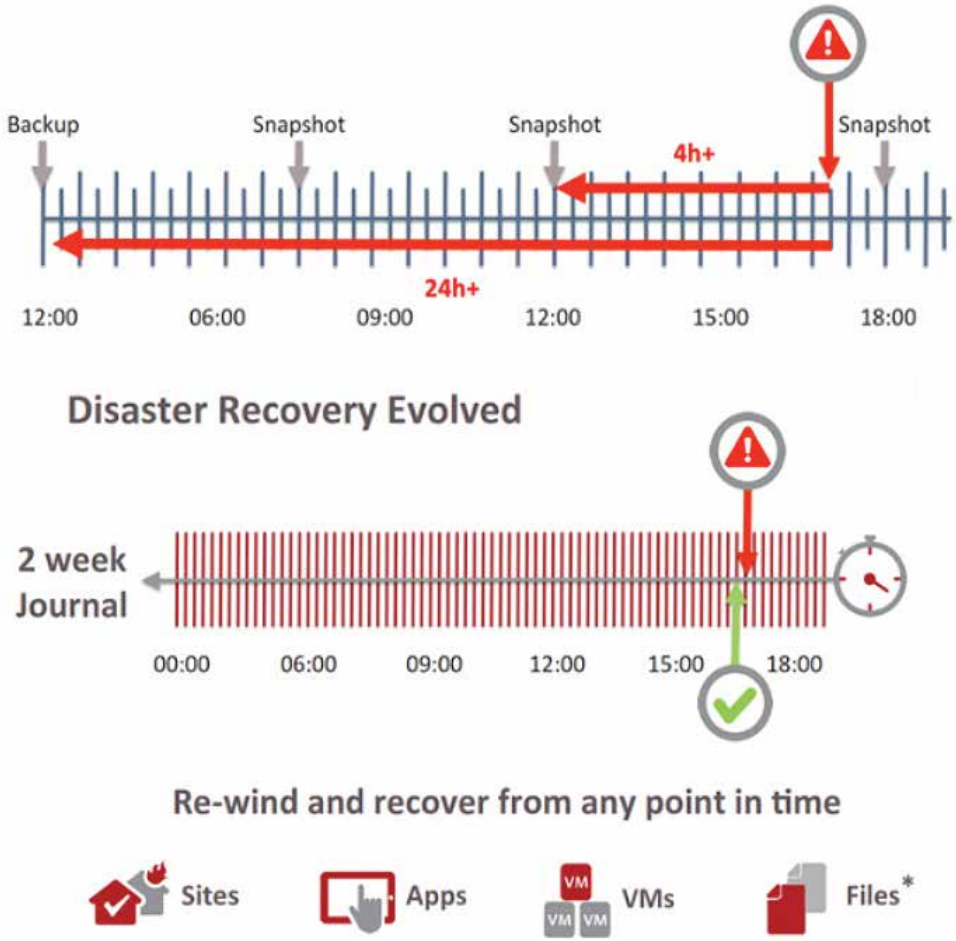
- Our team works with you to get production back online
- Production is confirmed up & monitored
- Production now acts as DR
- Your production resyncs with our cloud
- We fail your cloud environment back to your production
- Business continues as usual

In the event of an extended disaster

- DR is declared for an extended time
- Large changes in data sizes mean resync is not possible
- Your data back to you on removable storage
- Our engineers re-seed and sync to cloud
- Business continues as usual

A good Disaster Recovery Plan means you wont ever Wannacry

We design our Assured Recovery Service around technologies that allow us to roll back to a moment in time. If, for instance, all your files were encrypted by ransomware at 11:52, we could roll back to a 11:51am preventing any loss of data.



A good Disaster Recovery Plan includes detailed processes to follow that can be used for compliance

DR RunBook

When designing you Disaster recovery we build a detailed runbook that acts as an evolving document, constantly being updated. It contains all the information about your network and IT environment, as well as an escalation matrix and what to do in the event of different types of disasters. It also acts as a part of a company's process and compliance.

A good Disaster Recovery Plan includes segregated backups

For example, the sad story of a nice business called code space. Their environment was compromised when they panicked during a DDOS attack because they could not gain access and turned off their 2 factor authentication. Once that was off the hacker was in, first production was deleted and then the disk backups. The business was forced to close.

This is why a segregated backups onto a different domain are taken in addition to a replication of your production environment.

Paranoid is Prepared.

> In summary, most of our data, backups, machine configurations and offsite backups were either partially or completely deleted.

A good Disaster Recovery Plan works during a city-wide power failure

The good news is our services are run from the very best Datacenters.

These datacenters include electrical input from two different substations. In addition the datacenters have enormous diesel generators and 4 weeks worth of fuel as well as best in class UPSs. These generators are tested once every two weeks to ensure when needed, they work.

EFFICIENT COOLING

SECURE RACKS AND BIO METRIC ACCESS

ROBUST POWER

Summary

Always-In Business in an Always-On World

Today's "always-on" world is unforgiving when it comes to business or service disruption. Any downtime, especially in service-oriented industries, is unacceptable with a devastating effect on brand reputation and business credibility.

Many businesses now run real-time applications and maintain an online presence to serve and stay in touch with always-on customers round-the-clock. This makes it even more vital that key business processes and customer touch-points "stay open" even when disaster strikes.

> Although CloudHPT currently reaps the benefits of a specific regional advantage, the roadmap is forward-thinking and includes integration capabilities with respect to hyperscale public cloud providers.
>
> *Gartner Magic Quadrant DraaS*

Myths of Disaster Recovery

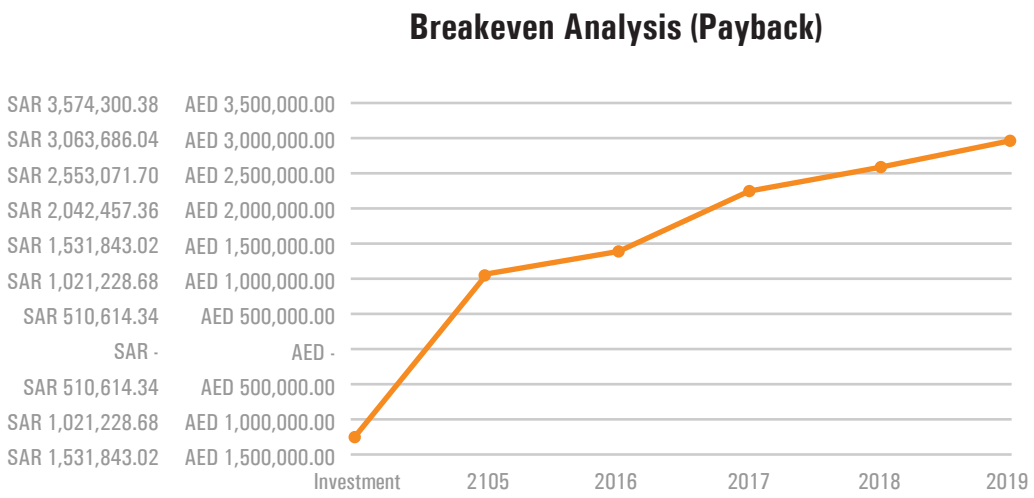
It will be too expensive

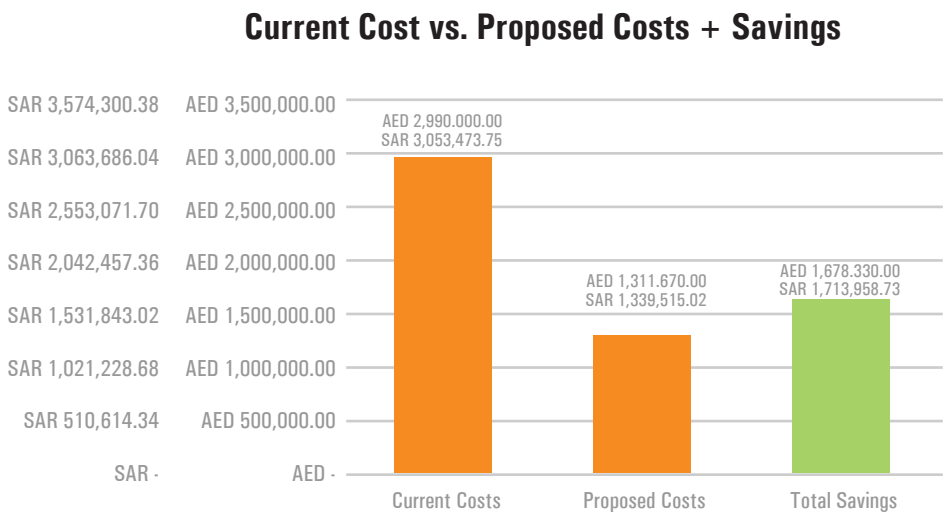
Disaster Recovery used to be expensive, it meant a company would have to build and maintain a secondary data center, including:

- A location unlikely to be impacted
- Infrastructure resources at the secondary site – servers, storage and network
- Maintenance, security and upgrade and replacement costs for those resources
- Staffing needed to manage the secondary site

But with Assured Recovery Service (ARS) that is not the case. ARS has no startup costs and is consumed as a monthly operational cost. In fact we usually see that the cost of just one instance of downtime is more then the cost of ARS for a year.

GCC-based healthcare company design their digital transformation with an exponential Return of Investment





Myths of Disaster Recovery

It is too complex

When you think of all the tasks associated with preventing an outage or responding to an emergency, they can seem a little complex. And, in order to plan for business continuity, you need to consider bandwidth, requirements, application dependencies, network failover, escalation process and the list goes on... Those who have experienced business continuity planning in the past may have suffered through this long process.

For our customers, though, we take that burden on and use our tried and tested planning and delivery process. We will map out the application dependencies, confirm their priority with you, install the required software, conduct a logical test and when we are satisfied, we conduct a full test and sign off on the service. The service will then be managed by our Secured and Assured team. We can usually onboard a complex site within two weeks.

BIOS team in a DR planning and delivery process meeting

Myths of Disaster Recovery

Bandwidth is too limited

Bandwidth costs can be a burden for any company. However, recent advances in Software Defined WAN technology and bandwidth optimizers have driven down these costs. We often find customers even with large data needs can use ADSL. Also, because our service is in country, it means latency is never an issue and we can connect via MPLS to any provider our customers may use.

Myths of Disaster Recovery

Believing a backup is adequate

Having a copy of your data is important. However, being able to fully restore operations and applications quickly and effectively is core to true business continuity.

> By the end of 2016, at least 45% of large enterprises, up from 22% at year-end 2011, will have eliminated tape for operational recovery.

What happens if the backups were corrupted?

What happens if the backup hasn't been working for some time?

What will you restore your backup to if the production environment is damaged? New equipment might take weeks to deliver.

Our view is that if you wouldn't use tape to store your music its probably not a good idea to rely on it as the sole means of protecting your business critical data.

Myths of Disaster Recovery

It can't happen to us

One wouldn't think rain or flooding would be a major issue in the Middle East. But in 2016 one day of rain flooded many datacenters in the UAE and took down a National Bank.

Even if you are not worried about a Natural Disaster, the most common catalysts of IT disasters are cybercrime and human error which know no geographical boundaries.

The UAE and KSA are two of the most targeted countries in the world for cyber crime. In addition, fire, datacenter floods and power cuts can occur. There is even the odd earthquake. In our view Disaster Recovery is vital business insurance no one can afford to be without.

Floods in KSA and UAE in 2016?

Myths of Disaster Recovery

Cloud is not secure.

We can only speak for our cloud, which is built on a validated and certified multi-tenanted architecture from Cisco.

Aside from its physical security – the fact that it resides in cages in the best datacenters in the region – it is also protected by multiple firewalls, IPS, Anti malware devices, monitored 24x7 by our SOC and SIEM, which requires multi-protocol authentication to access.

In addition we have multiple ISPs providing connectivity via diverse routes.

14 reasons why you should consider taking DRaaS from CloudHPT

- Support for each recovery tier (1-4)
- Partial and full failover support and expert help with failback
- Monitored production environment to assist with declaring disaster
- In Region professional services for migration
- UAE NOC and SOC that runs 24x7
- Datacenters in UAE, KSA and Oman
- Physical and virtual machine support for hybrid environments
- Secure environments and solutions to support compliance standards
- Only provider with Assured DR: proven process for onboarding, training, testing and DR Playbook
- Easy-to-use management portal
- Comprehensive testing and validation of DR
- 24/7/365 proactive support team
- Audited Environment and process for compliance
- Certified by Cisco - Cisco Powered

Interested in Assured Recovery Service?

If you are not confident that your current Business Continuity plan would stand up to a major or minor IT disaster we can assess them for you.

If you currently have no Disaster Recovery plan in place, and you care about your business, let's connect and see how we can help.

www.biosme.com

> DRaaS provides the peace of mind that your organization can recover from the unexpected

Gartner®

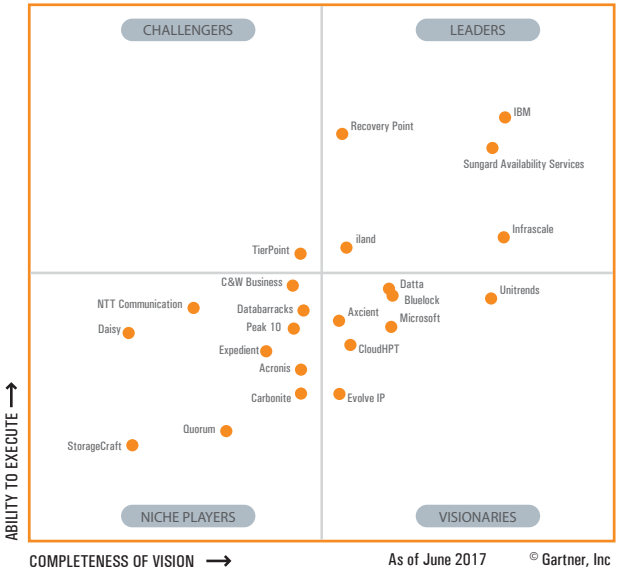
BIOS Middle East, UAE's leading Managed Cloud Provider, has been recognized in the Gartner Magic Quadrant report on Disaster Recovery as a Service (DRaaS), for three years in a row.

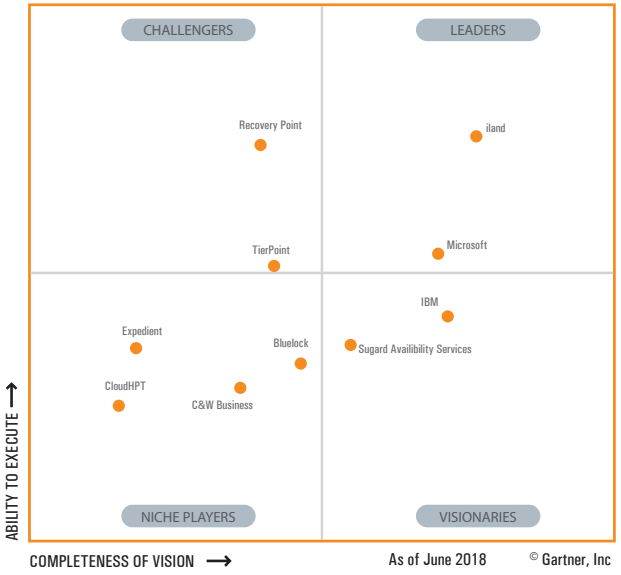
CloudHPT is the cloud solutions division of BIOS Middle East.

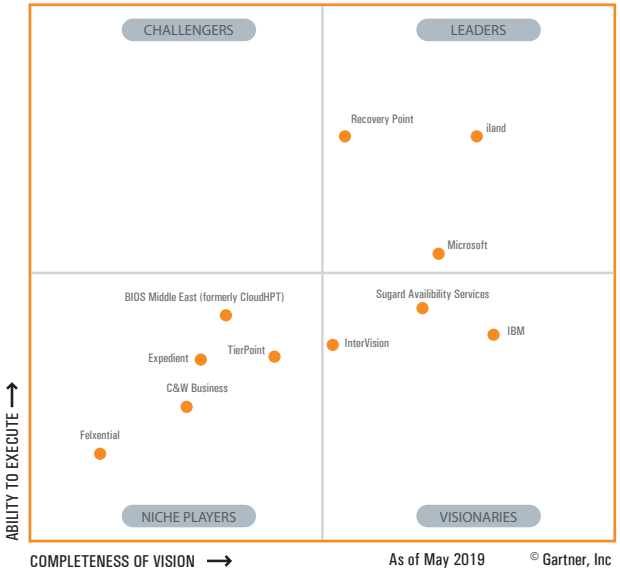
CloudHPT supports multiple tiers of services using distinct technologies for each tier to deliver costs in line with the needed capabilities.

The vendor has a strong focus on disaster avoidance through proactive security information and event management (SIEM) capabilities.

Although CloudHPT currently reaps the benefits of a specific regional advantage, the roadmap is forward-thinking and includes integration capabilities with respect to hyper scale public cloud providers.







Testimonials

أبوظبي للتمويل
ABU DHABI FINANCE

"Migrating our production environment to CloudHPT's in-county cloud eliminated a major capital expenditure and protected us from future technical obsolescence. BIOS helped us determine where to focus our spend for maximum impact. Our data is now secured in T3 datacenters, with enterprise-class security and a 24x7 command center to protect our data."

ALEC
Building Excellence

"As one of the largest and most respected contractors in the Middle East, our clients expect the best. BIOS's in-region infrastructure has made a dramatic improvement in our client experience."

osn

"BIOS Middle East is a partner who really understands our business as the media industry moves very quickly and our deadlines are usually half of what is required in other industries. They came in at the right time to support the design our consolidation of storage, design of our virtualization, and recommended us the right technologies which makes our life easier. They are flexible and their 24x7 NOC team have the right skills and knowledge to fix our issues immediately. We need 99.99% uptime and BIOS gives us that. We managed to reduce power usage by 20%, reduce server space by 80% and more by working with BIOS"

ADNIC
شركة أبوظبي الوطنية للتأمين
ABU DHABI NATIONAL INSURANCE COMPANY

"It's an exciting time for ADNIC, this project was extremely crucial to take the business to the next level of growth and we're delighted to have chosen BIOS Middle East as our partner. I am confident that we will be even more responsive and customer centric now."

Where we are today...

TRUSTED 400 private & public COMPANIES

2020 NPS - 8.65 Customer Satisfaction

10,000 servers & endpoints under management

Assured 24x7 NOC and SOC in Dubai & Banglore

20 years Experience delivering end-to-end technology solutions

100+ Technical Experts

Secured 24x7 SOC
SIEM as a Service
Vulnerability scanning

5 cloud platform in UAE, Saudi Arabia and Oman

UAE's No.1 Cloud & Managed Service Provider

BIOS MULTI-CLOUD

CLOUD HPT HIGH PERFORMANCE TECHNOLOGY

TECHNICAL EXPERTS Azure aws

Cisco Master Managed Service Provider, Gold Partner, Cloud Partner

VEEAM Gold Partner

solarwinds Elite Partner

Zerto Gold Partner

Industry recognition

Gartner Magic Quadrant 3 YEARS RUNNING DRaaS

cisco Service Provider of the year

cisco Cloud Provider of the year

VEEAM Provider of the year

ISO 9001 ISO 27001 ISO 23001 ISO 20001 PCI

Move to the cloud with confidence.
www.BIOSME.com

Dubai Office
Office 1603, Boulevard Plaza Tower 1, Downtown, Po Box 74069 Dubai, UAE
T : 971 4 3789000 | F : 971 4 3789001 | E : info@biosme.com | Toll Free 800 BIOSME | www.biosme.com

Saudi Arabia Office
Grenada Business Park, A4 Tower, 12th floor, East
Ring Road, P.O.Box: 100211, Riyadh 11635,
Saudi Arabia

Oman Office
221-01, Regus Business Center LLC, 2nd Floor
Tamimah Building, Al Nahdah Road, PO Box 395 PC
118 - Muscat, Oman