BIOS

Be secured. Be assured

The emergence of **Multi-Cloud**

Hybrid Cloud

Almost all businesses we see are using some elements of public cloud and have developed a Hybrid cloud strategy. For instance, they may still keep a lot of their production servers on-premise if they are less than 3 years old, but they might leverage the cloud for Disaster Recovery as a Service or for email. In this sense they are already following a Hybrid cloud model.

The rapid growth of a 'Cloud First' approach

Increasingly in recent years, when it comes to the renewal of on-premise datacenters, companies are choosing a 'Cloud First' approach. Whereby, whatever can be put on the cloud is put on the cloud. It is now an accepted fact, that when companies take into the account the operational cost of running their own IT infrastructure and the costs of hardware renewal, warranties and software, cloud is much cheaper than on-premise. More and more businesses are recognizing that cloud is also more secure with cloud providers spending so much on security. The other advantages of cloud vs on premise such as agility and speed of deployment and uptime have been accepted for some time. Most business leaders want their technology teams to focus on driving competitive advantages from developing IP and on cost reductions by leveraging technology, they are not really concerned about managing an IT platform for the sake of it. It is these elements that have led to a 200%+ YoY growth of our managed Cloud services for the past 3 years.

With a 'Cloud First' approach, the first thing many companies focus on is which cloud to use. Different cloud providers might have specific features customers prefer for various workloads, for instance:

1. Many companies use Office 365, so perhaps migrating to Azure is the right answer?
2. The costs of hyper-scale providers can be prohibitively high for standard production workload to be on 24x7 and local regional providers like our own CloudHPT have a significant cost saving advantage for customers.
3. Many developers have a preference for developing applications on AWS or perhaps media companies want to take advantage of AWS Content Distribution Network.
4. Companies looking to do deep data analytics and AI may want to leverage Google cloud
5. Heavy users of Oracle may want to run workloads on Oracle cloud.

So, when considering the best cloud computing solution, companies have to figure out which one is the best option. The obvious answer is to take the best from each provider at the best price.

Finding the perfect balance with Multi-Cloud

Increasingly most businesses are choosing a multi-cloud strategy, taking the best products for the best price from various public clouds and avoiding vendor lock in from any one provider.

An example of Multi-Cloud: A customer chooses our in-country managed cloud, CloudHPT for hosting production workloads. They then use Azure for hosting Office 365 and AWS for their websites. In this way they get the advantages of cheaper managed IaaS from CloudHPT, the world's best email platform from Azure and the Content Delivery Network for webhosting from AWS.

Another examples maybe: Hosting production workloads on a managed affordable platform like CloudHPT, but hosting databases on Azure that inject de-duplicated data and present this Power BI analytics or Azures AI platform.

Reasons to Adopt a Multi-Cloud Strategy

Breadth of capabilities: No single cloud provider offers a comprehensive set of services. Because cloud providers are differentiated, and have strengths, weaknesses and unique capabilities, adopting a multi cloud strategy allows access to best-of-breed capabilities.

Innovation: Cloud providers sometimes leapfrog each other in capabilities. With customers for whom immediate access to the newest innovations is of critical importance, a multi-cloud strategy allows them to quickly take advantage of new capabilities as soon as they are introduced into the market.

Avoid vendor lock in: Some customers believe that placing most of their applications in a single cloud provider creates the risk that a service change could have widespread impact on their overall application portfolio. Some customers are also concerned about the potential for massive outages. For instance, in 2012 and 2014, there were Microsoft Azure outages that impacted nearly all Azure regions worldwide and in 2016 AWS was not accessible for 12 hours on the East Coast of the US.

Cost Savings: Hyper-scale providers come with much innovation and features but at a higher cost than regional providers (who can be up to 50% cheaper) and often for the majority of workloads these features aren't always required. Combining a local provider with a global provider can give a business a significant cost saving. Sometimes Hyper-scale providers try and overcome this by advising clients to power off Applications and Servers out of working hours, but the reality is this is difficult to follow and most businesses are now 24x7x365.

The challenges of Multi-Cloud

There are multiple challenges associated with the multi-cloud model. In addition to selecting the right providers and understanding the cost and platform potential, there is also the issue of security and governance. In a borderless multi-cloud environment, security and governance have to be your priority and not just an after-thought.

Another big challenge is that of complexity. Moving to the cloud does not, as if by magic, remove complexity, in our experience, if appropriate steps are not taken it can increase it.

For instance:

- How are decisions made about what to use and what not to use?
- How do you ensure that the cost is appropriate to the workload and kept under control?
- Do you apply the same processes and procedures to each different cloud provider and how can you ensure that the approach to audit and compliance is the same across all your providers?

When you drill down to an application that spans multiple clouds it can become even more complex. A composite multi-cloud architecture must have solutions for the following challenges:

Networking: Each of the application components on different cloud providers needs to be able to communicate with other application components. The network connectivity needs to be reliable and adequately performant, yet not be excessively expensive.

Data management: Some multi-cloud architectures require data to be replicated across multiple cloud providers, either synchronously or asynchronously. This also requires data integrity and consistency to be maintained across cloud providers. This increases architectural complexity as well as cost.

Security: All components of the application — and all communications between those components — need to be secure. However, there are likely to be components that cannot share a single security context, requiring a tool to unify security visibility across all the components. Identity, authentication and authorization are also likely to be handled differently by the different cloud providers used in the solution.

Regulatory compliance: Every cloud provider involved in the solution needs to meet the regulatory compliance requirements of the application. Data is likely to flow across multiple cloud providers, and the application architect needs to ensure that it does so in a compliant fashion.

Monitoring and tracing: Complex composite multi-cloud applications can be difficult to troubleshoot. The ability to trace application performance in real time across multiple cloud providers and application components is vital.

Availability: The use of multiple cloud providers increases the probability that, at any given point in time, at least one of these providers will be in the midst of an outage. Similarly, each of the integration points between these providers is a potential point of failure. The architect must ensure that the overall design is resilient.

How BIOS is helping to answer the Challenges of Multi-Cloud and unlocking its benefits

In 2012 we opened our Network Operations Center in Dubai. The aim was to focus on providing managed service to companies in the Middle East for their On-premise datacenters. This allowed customers to outsource the monitoring and maintenance of their storage, networking, compute, hypervisors and operating systems and focus instead on the business needs for IT innovation. We called the service BIOS Assured.

In 2014 we launched CloudHPT, an in-country cloud foot print for the UAE based in Dubai and Abu Dhabi. This answered the issues of cross region latency associated with the hyper-scale providers based in the US, Europe and Asia. CloudHPT was and is priced at half the cost of most hyper-scale providers for the commodity components and has an overlay of BIOS Assured.

In 2015 we launched BIOS Secured. A combination of a SIEM and vulnerability platform coupled with 24x7 SOC Services. This service aimed at allowing customers to take a Security as Service for their on-premise or cloud foot print.

In 2017 we became the first company in the world to buy Azure Stack from Cisco, bringing for the first time Azure capabilities in-country for the UAE. Available as a shared or dedicated platform, it is a great opportunity for enterprises to leverage dedicated Azure capabilities in their datacenters and using a shared platform to trial and test the service.
During this time we have provisioned, managed and secured thousands of workloads on our CloudHPT platform, as well as workloads on Azure and AWS. 2019 will be a very exciting year, with in-region services from Azure (Dubai and Abu Dhabi) and AWS (Bahrain) being available for the first time.

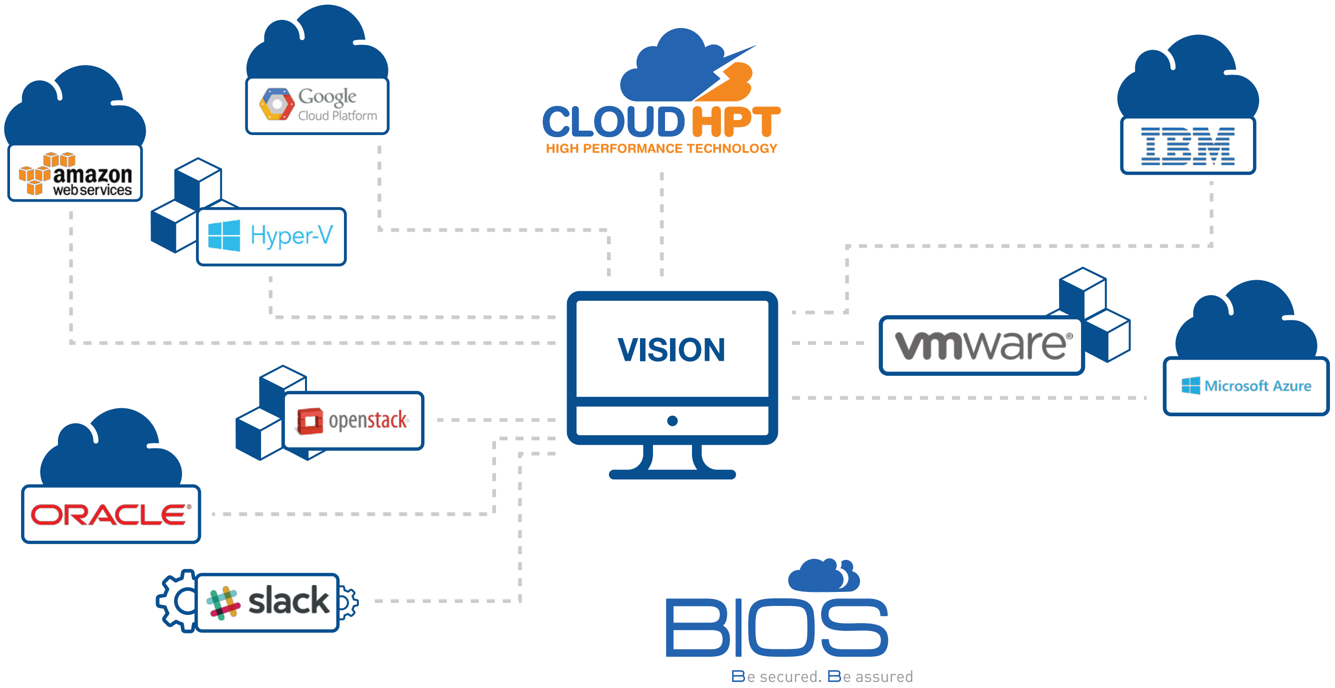
We understand that the benefits of cloud for our customers will be most felt most when they leverage a managed and secured multi-cloud offering. That is why we are launching 'Vision'.

Vision

Vision is a single pane of glass that allows us and our customers to see and manage multiple cloud environments. Vision also includes BIOS Assured (our managed Service) and BIOS Secured (our security as a service) across a customer's entire cloud footprint. Whether it be on CloudHPT, AWS, Azure or other clouds, these services come with dashboards that will show the customer's environment health and security posture in real time and are backed by a 24x7 NOC and SOC.

Vision will be the core of our managed cloud offering and provides a simplified cloud management engine that allows customers complete control to create, provision and manage all of their separate cloud services. This single pane offering provides access to all public cloud providers, as well as our own cloud platform CloudHPT. Our public cloud provider partners include AWS, Azure and many others.

Vision controls multiple cloud providers:

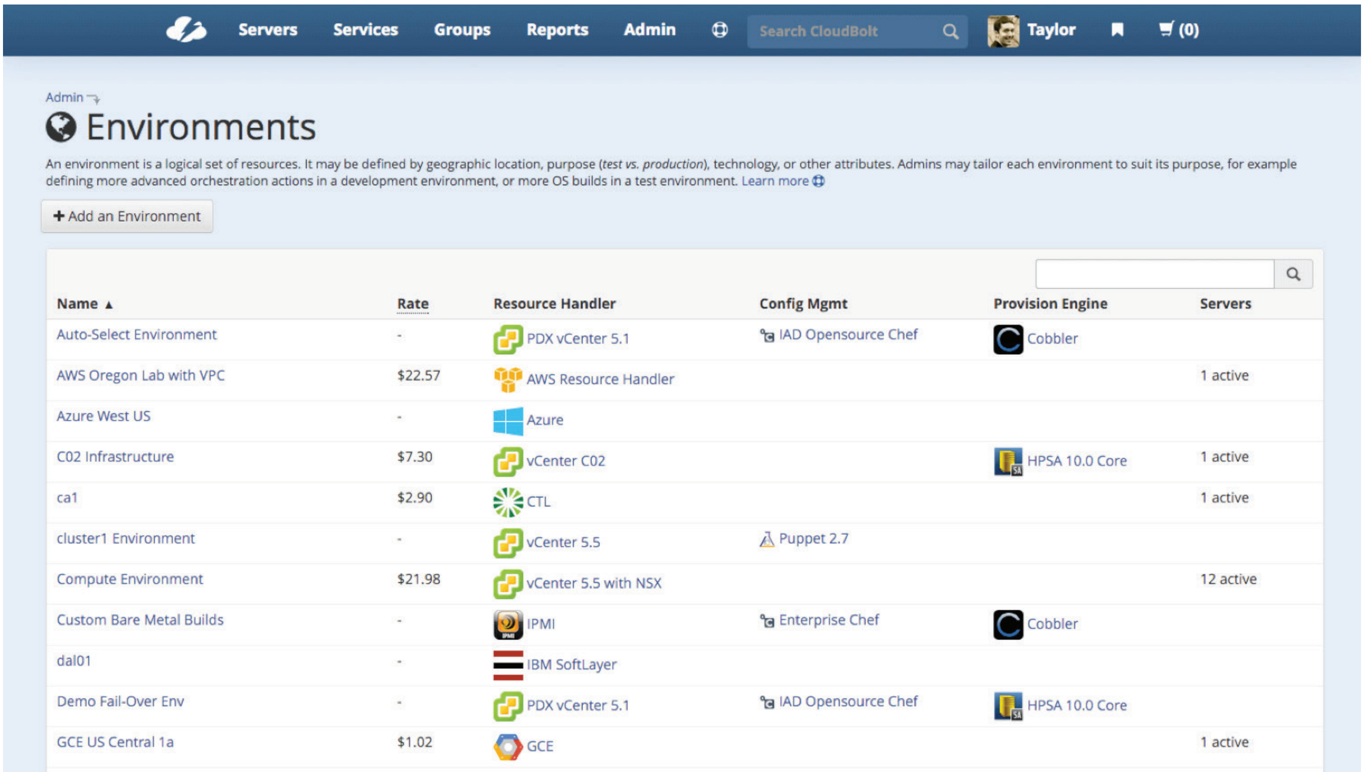


The Benefits of Vision:

- A multi-cloud strategy is now a reality. Access the full range of public cloud services in one central place while eliminating complexity.
- Gain full control using a single cloud services dashboard that guarantees the end of Shadow IT in your organization.
- Take charge of costs with simplified billing.
- Ensure that data residency and compliance issues are no longer a worry with a comprehensive cloud brokerage model.

Self-service with work flow for approval

Vision, which comes as a fully managed and secure multi-cloud platform will also provide companies with the ability to self-service provision and provide costing across multiple cloud platforms. Credits can be pre-defined and workflows for approval can be custom built during onboarding.



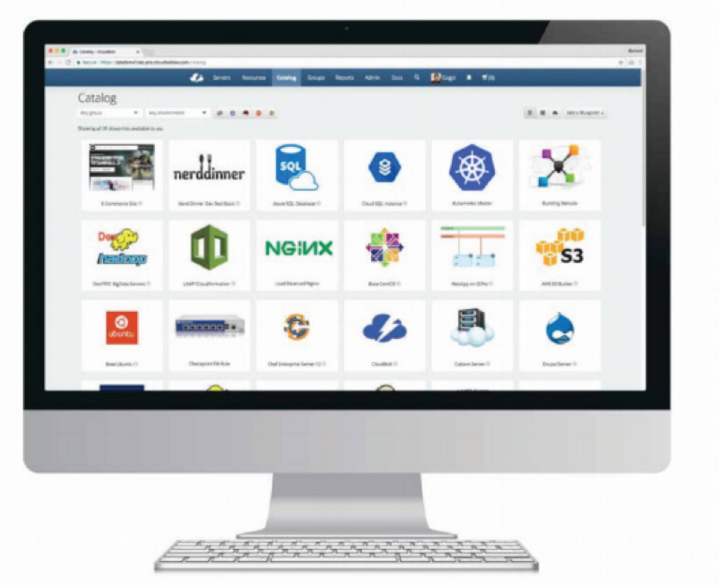
Environments

An environment is a logical set of resources. It may be defined by geographic location, purpose (*test vs. production*), technology, or other attributes. Admins may tailor each environment to suit its purpose, for example defining more advanced orchestration actions in a development environment, or more OS builds in a test environment. Learn more

Name ▲	Rate	Resource Handler	Config Mgmt	Provision Engine	Servers
Auto-Select Environment	-	PDX vCenter 5.1	IAD Opensource Chef	Cobbler	
AWS Oregon Lab with VPC	$22.57	AWS Resource Handler			1 active
Azure West US	-	Azure			
C02 Infrastructure	$7.30	vCenter C02		HPSA 10.0 Core	1 active
ca1	$2.90	CTL			1 active
cluster1 Environment	-	vCenter 5.5	Puppet 2.7		
Compute Environment	$21.98	vCenter 5.5 with NSX			12 active
Custom Bare Metal Builds	-	IPMI	Enterprise Chef	Cobbler	
dal01	-	IBM SoftLayer			
Demo Fail-Over Env	-	PDX vCenter 5.1	IAD Opensource Chef	HPSA 10.0 Core	
GCE US Central 1a	$1.02	GCE			1 active

Predefined workloads:

Pre-defined workloads cross multiple clouds are ready to be deployed in minutes providing scale and agility to customers.



Managing a Multi-Cloud enviroment with BIOS Assured

BIOS Assured is a 24x7 ITIL based monitoring, support and managed service offering focused on cloud and datacenter. With Network Operating Centers (NOCs) in Dubai, UAE and Bangalore, India, plus more than 100 cloud focused engineers, BIOS Assured has become the corner stone of our business. The Service is offered on our Cloud, CloudHPT, Azure Stack, Azure and AWS and includes:

- 24x7 Monitoring & Optimization
- Centralized Ticketing with measurable SLA's
- Scheduled daily, weekly, monthly checks
- Patch management services
- Configuration management service
- ISO standard incident management
- Detailed monthly reports

Below: Our Dubai based NOC at Boulevard Plaza 1, Downtown Dubai.

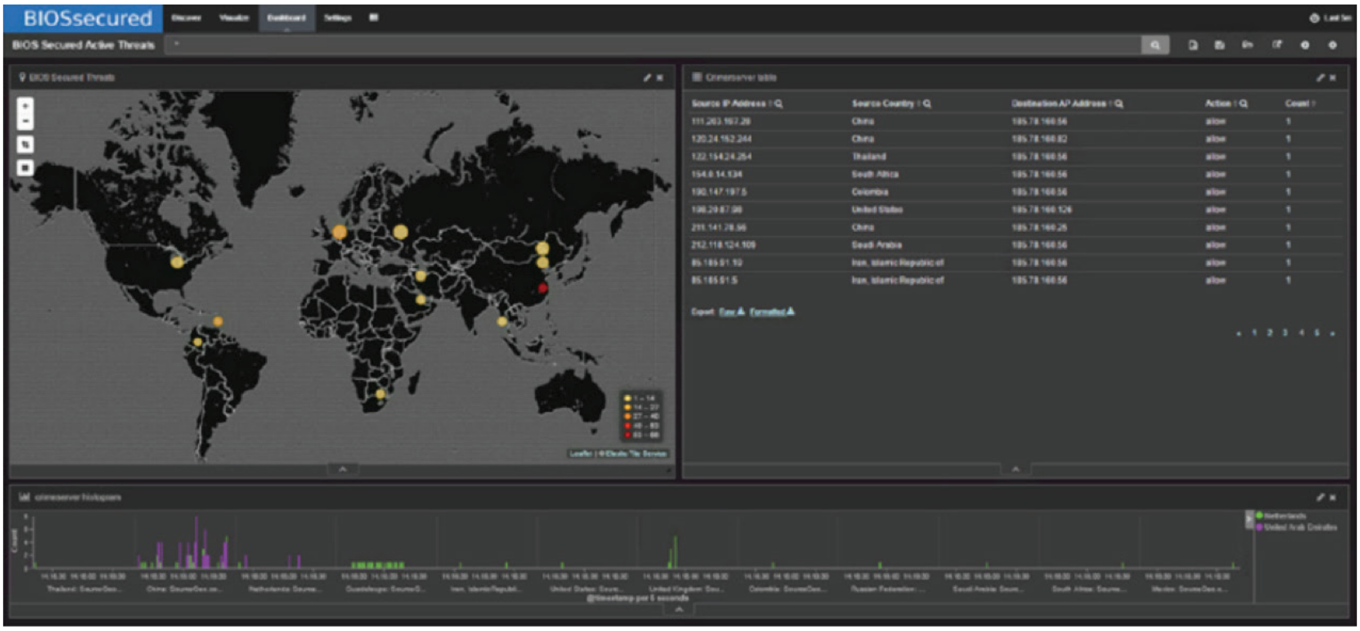
Securing a Multi Cloud enviroment with BIOS Secured

BIOS Secured is a Security-as-a-Service that combines security engineers, tools and process to provide a robust and compressive battled hardened approach to Cloud Security. BIOS Secured was developed to protect our cloud and our client's private cloud, but has now been developed as an overlay on other clouds. Combining BIOS Assured and BIOS Secured provides customers with an excellent way to manage and secure their business critical data and applications regardless of which cloud they reside on. BIOS Secured chiefly consist of these elements:

- 24x7 Security Operation Center (SOC)
- Security Information and Event management tool (SIEM)
- Cyber Threat Intelligence Platform (CTIP)
- Security analytics and dashboards
- Continuous Vulnerability assessments
- An ISO 27001 compliant response and incident management framework
- Logging events for forensic analysis
- Reporting

The BIOS Secured Operations Centre provides around the clock supervision of our customers' cloud environments. In addition to a 24x7 SOC and continuous vulnerability scanning of cloud environments, BIOS Secured comes with its own SIEM platform. The SIEM Platform is built on highly distributed technology which includes a Cyber Threat Collectors which will be placed within the various cloud environments. The Cyber Threat Collectors aggregates enterprise-wide security events from virtual routers, firewalls, intrusion detection systems, servers and more. The Cyber Threat Collector then normalizes this data and sends it to our Secured Big Data platform which then compares events to known malicious activity and known normal activity. Malicious and unknown events are correlated and alerts are presented to our SOC for remediation in real time.

Below, every connection into and out of your multi cloud environment is tagged for reputation, analyzed and if malicious blocked.



Source IP Address	Source Country	Destination IP Address	Action	Count
111.203.167.28	China	185.78.160.56	allow	1
120.24.162.244	China	185.78.160.82	allow	1
122.154.24.254	Thailand	185.78.160.56	allow	1
154.0.14.134	South Africa	185.78.160.56	allow	1
190.147.197.5	Colombia	185.78.160.56	allow	1
198.20.67.98	United States	185.78.160.126	allow	1
211.141.28.56	China	185.78.160.25	allow	1
212.118.124.108	Saudi Arabia	185.78.160.56	allow	1
85.185.81.10	Iran, Islamic Republic of	185.78.160.56	allow	1
85.185.81.5	Iran, Islamic Republic of	185.78.160.56	allow	1

Export: Raw Formatted

Conclusion

The average business is said to use around four to six types of cloud. Managing those cloud computing resources can be a challenge which is why we have developed Vision as a single pane of glass to build, provision and manage workloads. To further reduce complexity we have incorporated our 24x7 BIOS Assured managed service and our BIOS Secured offering across multiple clouds as well as our on-premise managed services.

The end goal is to provide our customers with a cloud that best suits their business needs while keeping everything as simple as possible.