iboss™
CYBERSECURITY

A **New Kind** of Cloud

UNDERSTANDING NODE-BASED CONTAINER ARCHITECTURE

iboss CYBERSECURITY

A **New Kind** of Cloud

UNDERSTANDING NODE-BASED CONTAINER ARCHITECTURE

The cloud isn't news anymore. The majority of enterprises have at least some pieces of their computing environment running in a cloud, whether public, private, or hybrid. The benefits of cost and scalability are simply too compelling to ignore, despite ongoing concerns about security and compliance.

In the past, access to business-critical applications such as payroll, help desk, and data repositories was easier to monitor. The services were local, so traditional signature-based data loss prevention was a workable approach.

However, today's enterprise faces far greater challenges in monitoring access to their assets. Applications that send service requests directly to the cloud, the growth of distributed organizations and mobile users, and encrypted communications between users and systems make it harder to manage who is doing what and when.

One Breach, Many Victims

Most clouds run on virtual machines (VM). A VM is a software environment that contains an operating system and applications. Multiple VMs can be installed on a single server, enabling the box to run many self-contained systems simultaneously, with each behaving like a dedicated server. This is how resources are shared on most clouds.

Orchestrating the use of the resources is a piece of software called a hypervisor. A hypervisor controls a host's processor, allocating resources to each VM as needed and preventing any single VM from disrupting the operation of another.

Complexities Create Vulnerabilities

Clouds are high-value targets for hackers because an attacker who gains access to a hypervisor potentially has access to the VMs — and the data — of every cloud customer.

If a cloud is penetrated through one customer's weak password or badly-written PHP, it's possible that the more secure customers could be attacked through the hypervisor, which is an unexpected — and therefore unprotected — direction for an attack to originate.

Hypervisors are vulnerable because they have large attack surfaces with many entry points. Also, they are based on complicated code that is hard to design, test, and manage simply because there is so much of it. Despite these concerns, there are no best practices for managing hypervisor security.

Cloud customers have no control or even knowledge of the other businesses sharing their hypervisor; an enterprise handling highly-sensitive data could be in the same virtual environment as a novice developer who is programming web servers with gaping security holes. It only takes one successful breach to result in the loss of data, intellectual property, and company secrets from all the companies sharing the cloud, so VMs running on the same hypervisor are only as secure as the least secure neighbor.

HYPERVISOR VULNERABILITIES

- **VM Escape:** An attacker runs code that allows an operating system running in the VM to break out and interact directly with the hypervisor.
- **Patch Deficiencies:** Virtualization happens on network devices as well as servers, creating a large surface to patch each time a new exploit emerges.
- **Open SSL Vulnerabilities:** If the OpenSSL server shares a hypervisor with other customers in the same cloud, attacks could allow data to be injected into other sessions or allow denial of service attacks.
- **APT Vulnerabilities:** RAM scraping attacks may allow attackers to view CPU states.

Shared Proxies, Shared Pains

Most cloud providers scan customer data through a shared proxy in the cloud. A proxy acts as a middleman between endpoints outside the cloud and applications inside the cloud. Because a compromised proxy can provide a path from one customer network to another, proxies can be a source of risk. The use of proxies also increases latency, which is the time it takes data to move from one point to another. As more traffic goes through the proxy, latency increases. In cloud computing, that means that when one customer experiences an increase in traffic, other customers may experience delays in their own.

Containing Risk in the Global Organization

A node-based cloud architecture eliminates the problems of scalability and flexibility while delivering a more secure cloud.

Node-based architecture allows organizations to adopt the public cloud when it makes sense, such as for remote sites or mobile users, while hosting other elements, such as sensitive data repositories, in private clouds. This lets organizations take a traditional “appliance at headquarters” approach to service the data from corporate headquarters, while simultaneously serving their mobile users and remote offices with greater speed and security through a geographically distributed cloud.

The Crowded Cloud

Web security has traditionally been browser-based, focusing on ports 80 and 443; that legacy approach creates blind spots because it only sees two ports. Today, web security has evolved into “internet” security that detects evasive attack protocols that don’t use web ports. Data anomaly detection, containment, and advanced cyber analytics can help identify a breach even if none of the perimeter sensors have been triggered. This is critical because most data is stolen with minutes of a breach, so continuous monitoring for infections inside a network is critical.

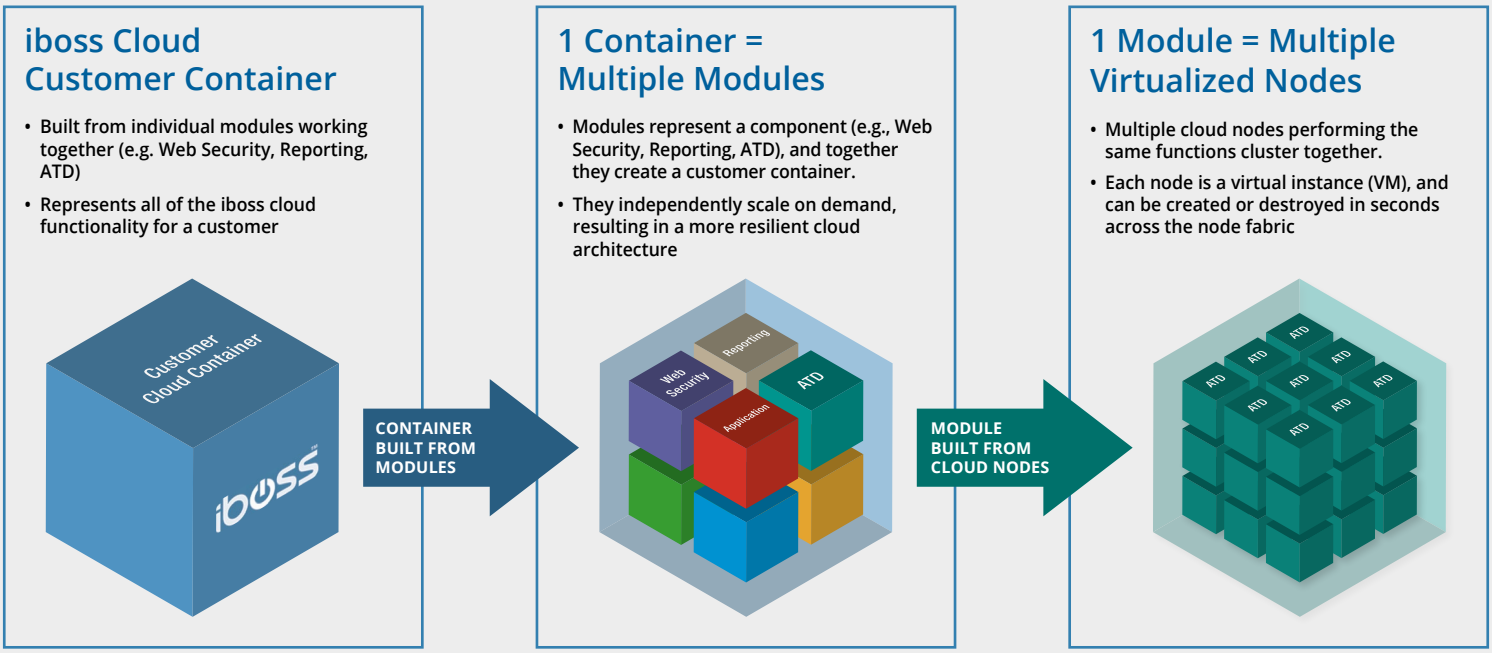
The ways in which web security is delivered have also evolved. In the past, enterprises had to choose between on-premises hardware and cloud security. Some organizations lacked the skill and resources to feel confident about their on-premises security, while some organizations were unwilling or unable to offload any part of their security to a third party.

Organizations that are cloud-averse have had good reason to hold that position. Typical peer-to-peer cloud providers take a monolithic approach to their architecture. Their clouds are one big system, so sensors that deal with security, scalability, latency, and regional requirements are shared – and all of their users’ data is potentially shared as well. A monolithic architecture does not enable location-awareness, and with no way to know if data is in the US or the EU, customers have concerns about meeting in-country regulatory requirements.

To address these issues, enterprises should consider moving away from the monolithic cloud to a node-based containerized approach.

Unpacking the Container

A **container** is a collection of modules. A **module** is a collection of clusters. A **cluster** is a collection of nodes.



NODES

Nodes are the building blocks of the iboss Cloud Container. Each node performs specific module functions such as:

- Web Security
- Advanced Threat Defense
- Behavioral Sandboxing
- Behavioral DLP
- Reporting and Logging

Multiple cloud nodes performing the same functions are clustered together. For example, a cluster may be composed of a collection of Advanced Threat Defense nodes or a collection of Web Security nodes, but it won't be composed of a mix of the two. Any one node can be eliminated from a module because its functions are replicated in the nodes that remain. The risk of data loss is minimized because the nodes completely isolate customer databases.

Cloud nodes are allocated globally on the iboss Cloud, close to the mobile users and remote sites that demand their services. The cloud nodes are virtualized so they can be created or destroyed in seconds to deliver the right level of capacity, redundancy, and availability as user loads and customer counts change.

Even cloud-averse organizations can benefit by using the nodes to better manage their mobile users and remote sites while avoiding the difficulties of backhauling data. iboss Cloud nodes can be hosted on-site, allowing customers to perform any function of the iboss Cloud within their own perimeters.

Since the iboss Cloud does not treat nodes hosted on-site differently from any other node, they can be removed at any time without any loss of functionality. And because nodes can be placed inside an organization's network, compliance with Privacy Shield requirements can be met.

CLUSTERS

Nodes of the same type form clusters. Every cluster has *one master cloud node* that interacts with master cloud nodes in other clusters. Any node can become the master of its cluster at any time, ensuring maximum availability and interface responsiveness. Because every customer has its own container, heavy loads from multiple customers do not result in a slow or non-responsive interface. Clustering prevents downtime, and in no case will one issue affect all customers in the cloud.

MODULES

Modules are collections of clusters designed to reduce complexity; each one is responsible for a specific function that works in concert with other modules in the iboss Cloud. While the modules on a customer's platform work together, they are isolated from those on the platforms of other customers, so they can scale on demand and deliver their functionalities independently. The result is a more resilient architecture that facilitates ease of use and time to market on new functionalities.

CONTAINERS

Containers provision all of the iboss Cloud functionality. Containers are elastic, dynamically spanning multiple data centers to provide web security for mobile employees and branch offices. Data can be retained wherever an organization chooses, so in-country regulatory requirements can be fulfilled. Containerized data in transit and at rest is encrypted, and containers are separated by OS boundaries so there is no possibility of overlap between organizations. Redundancy is completely performed in the cloud, so tape backups are not necessary.

CONNECTING THE CONTAINERS WITH THE IBOSS CLOUD CORE

Tying the containers together is an underlying fabric that routes traffic to nearby nodes by utilizing DNS record clustering to provide load balancing and user geolocation. Multi-factor authentication is natively included through SSO authentication for administrators using the management console. Administrators are brokered to the appropriate containers by the iboss Cloud Core.

Scalable, secure, and sensible

As organizations grow, they need more bandwidth and more endpoints, As companies rack and stack repeatedly, an increasingly expensive and complicated appliance-based architecture forms, resulting in a mishmash of new systems and legacy systems that potentially hide security gaps and definitely absorb operating capital.

The architecture of the iboss Cloud Elastic Container is fundamentally different from conventional cloud security architectures. iboss' seamless node-based solution allows organizations to add users or field offices without having to negotiate an intensive planning process.

Nodes can be added almost instantly, either inside the customer's datacenter, on the iboss Cloud Core, or both. Because nodes automatically cluster with each other, expandability is almost infinite.

Policy and reporting is consistent across all users and managed through one central management console in a secure isolated environment. Location-awareness is enabled, so organizations subject to in-country regulations can meet compliance.

Iboss' proprietary container-based virtualized architecture delivers an infinitely scalable, dynamic, and elastic cloud that makes sense for organizations that need to respond to changing business needs while locking down the security of their assets.

About iboss Cybersecurity

iboss Cybersecurity defends today's large, distributed organizations against targeted cyber threats which lead to data loss, with the next-gen iboss Cloud Secure Web Gateway Platform, leveraging patented advanced threat defense technologies delivered 100% direct-to-cloud. iboss' unique cloud architecture provides each organization with its own container, so that a customer's data is never mixed with any other's in the public cloud. Our advanced security solutions deliver unparalleled visibility across all inbound/outbound data channels, and include security weapons that reveal blind spots, detect breaches and minimize the consequences of data exfiltration. With leading threat protection and unsurpassed usability, iboss is trusted by thousands of organizations and millions of users worldwide.

iboss, Inc. · 877.742.6832 · sales@iboss.com · U.S. HQ 4110 Campus Point Court · San Diego, CA 92121