# Cloud Based Internet Security Designed for GDPR

As applications move to the cloud and the traditional network perimeter erodes, the need for cloud-based Internet security increases. The iboss cloud delivers Internet security in the cloud while supporting GDPR compliance.

# GDPR and iboss cloud Overview

GDPR and other regional regulations make SaaS cloud migrations difficult. As applications continue to move to the cloud and mobility increases, using traditional approaches to Internet security become unsustainable due to increases in bandwidth and strategies that include less network infrastructure and management. The iboss cloud runs in the cloud and can secure user Internet access regardless of location, but has the unique ability to do so while aligning to regulations such as GDPR. The containerized architecture allows the iboss cloud to deliver the following benefits:

- Containerized cloud gateway capacity ensures data is inspected within regulated countries
- Containerized cloud reporting capacity ensures data is stored within regulated countries
- Admin defined and controlled zones allow clear visibility to how data will flow through cloud-based Internet security when users are within regulated regions
- Admin controlled reporting logging flow ensures reporting data remains within regulated regions
- Log and reporting encryption for user personal data such as username, source IP and group membership
- Private cloud can meet the needs that demand private capacity while still leveraging the global iboss cloud presence for users globally

# Challenges Related to Cloud-Based Internet Security and GDPR

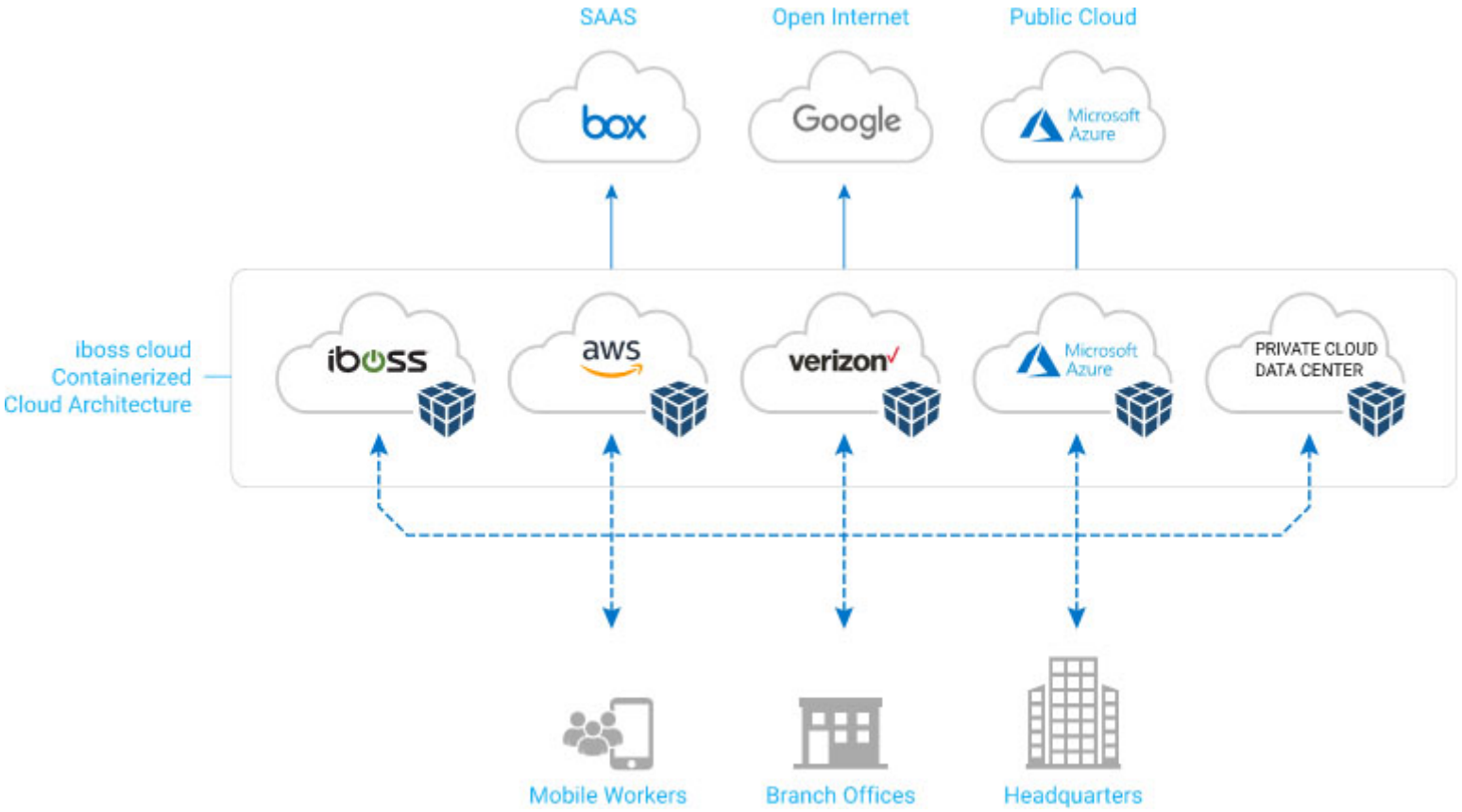
GDPR and other regional regulations make cloud application use challenging. This is especially true of cloud-based Internet security that is scanning user data as it is traversing to cloud applications and the public Internet. To make things even more challenging, Internet security platforms must store user Internet activity event logs that may contain information that falls under GDPR constraints. Typical challenges include:

- When users are accessing the Internet within regionally regulated countries, data may be required to be inspected/stored in specific geographic regions
- User Internet activity that contains user personal data may be required to be obscured from view by administrative users by role or jurisdiction
- HTTPS data decryption may not be permitted, by regulation or policy, to be transmitted to particular destinations in particular regions and must traverse the Internet uninspected
- The need to adapt what happens with data as it is scanned and secured may vary depending on user location to meet regulations for that particular country or region

Regulations may even conflict from region to region or jurisdiction to jurisdiction making things more challenging for organizations with a global footprint.

The iboss cloud easily solves the challenges involved with meeting regulatory compliance while delivering the value of a SaaS cloud delivered Internet security platform. The containerized architecture is the foundation for supporting these regulations which is not found in any other Internet security platform.

# iboss cloud Supports GDPR Compliance



## Containerized Cloud Gateway Capacity Within Regions Ensures Data is Scanned Within Regions

The concept of containerization allows for containerized work units, such as gateway, to exist in iboss cloud specifically within a defined region. Users are always connected to iboss cloud through the containerized gateway work units for Internet security including compliance, malware defense and data loss prevention. Since these cloud gateway units are what scan user data for security, the scanning of the data occurs within the regulated regions in which the gateways exist. Containerized gateway capacity can exist in tightly controlled regions to ensure user data is scanned by specific containerized gateways depending on user location. This helps support GDPR compliance for the processing of the data as it is scanned for Internet security.

## Containerized Cloud Reporting Capacity Within Regions Ensures Data is Stored Within Regions

Like the containerized gateway work units that scan end user data for security, reporting databases are also containerized. These containerized reporting units can store event log and drill down reports within the specific regions in which they exist. Depending on where a user is located, the gateways can send reporting log events to the appropriate containerized reporting work unit that exists within the regulated region to ensure reporting data stays within that region. This helps support GDPR compliance for reporting and log storage.

## Admin Defined Zones Provide Explicit Visibility and Control

With some cloud security platforms, supporting GDPR and other regional compliance is difficult to do and many times very vague. The iboss cloud allows administrators to define zones within the iboss cloud admin console to control how data flows from end users and where reporting events are stored. The iboss cloud uses the end user's source IP to determine the user's location and maps the user to a zone defined by the iboss cloud administrator. The administrator can create as many zones as necessary including country-based zones. As users are mapped to the zone, the zone instructs the endpoint on how and where to send data to the iboss cloud to ensure data is scanned and stored within a region. This also provides clear visibility to the administrator to help support GDPR compliance.

## Reporting and Log Data Can Flow To Different Reporting Databases Depending on User Location

As users move from place to place, the iboss cloud allows administrators to configure where the Internet activity log data is stored. This includes sending data to reporting databases specifically within a region or country when a user is in that region and a completely different reporting database when the user moves to a different region.

## Log and Reporting Encryption

Regulations may require or recommend that personal data is encrypted. The iboss cloud can be configured to encrypt personal data in logs and reports such as username, source IP and group membership. Administrators with appropriate customer-defined roles and permissions can decrypt data when necessary to reveal the true source of the data. Delegated administrators will only see encrypted information in the Internet activity reports.

## Selective Decryption to Prevent Decryption When Needed

The iboss cloud has extensive HTTPS decryption controls to gain visibility into encrypted traffic, which may be necessary under certain laws. Making this more powerful is that it can be selectively applied using an extensive number of criteria including domain, category and user group membership. This allows traffic to remain uninspected when needed due to regulations within a particular region, while decrypting when other regulations or the organization require or allow it.

## Extending Into Private Cloud

The containerized architecture of iboss cloud allows cloud gateway capacity to run anywhere, including within a private cloud datacenter. The private cloud capacity will run in parallel to the other iboss cloud capacity providing the global reach and infinite capacity needed by global organizations. The private cloud capacity is turnkey and completely provided by iboss.

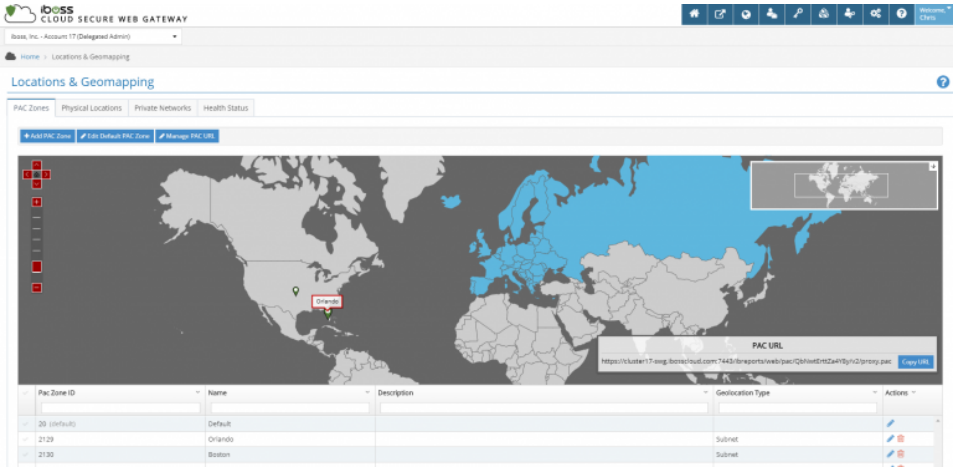
# How It Works

## Taking advantage of iboss cloud for GDPR is easy. To get started:

1. Get an active iboss cloud account
2. Connect users to iboss cloud using the iboss cloud connectors or branch office tunnels
3. Create zones within the iboss cloud admin console to define how data flows when users are within regions

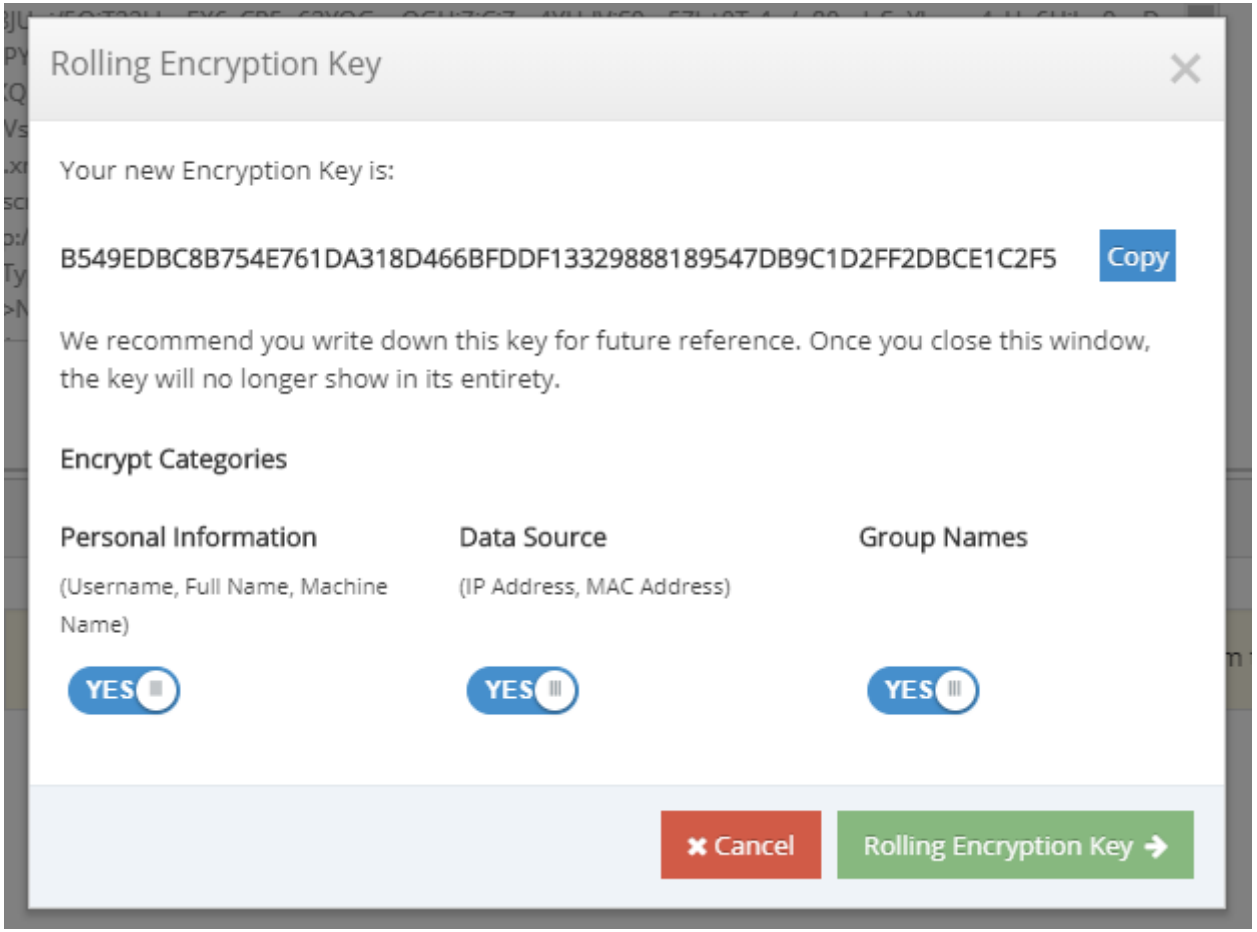
# Feature Highlights

## Admin Controlled Zones


The Locations and Geomapping features within iboss cloud allow for the creation of admin defined zones. These zones are mapped to users by using the source IP of the user and geolocating the IP Address to an admin defined Geo-Zone. The Zone contains the routing data for the end user while the user is in that zone. Administrators can also create zones based on public IP subnets to map users when they are in specific offices to iboss cloud gateway capacity in a particular region.

# Log and Reporting Encryption




The log encryption feature uses symmetric AES encryption to protect user personal data within logs and reports. The encryption key can be used to decrypt the data only by administrators with appropriate customer-defined roles and permissions. When encrypted, the data is stored within the reporting database in encrypted format as well as displayed in encrypted form to administrators viewing reports.

# Pricing

| GDPR Zoning Features, Encryption and In-Region Cloud Capacity | Contact Us |
| --- | --- |
| GDPR capabilities are included with all iboss cloud subscriptions at no additional cost. | |

# Learn More About GDPR and iboss cloud

To learn more about GDPR and iboss cloud, visit https://www.iboss.com/business/ensure-gdpr-compliance.

# About iboss

iboss is a cloud security company that provides organizations and their employees secure access to the Internet on any device, from any location, in the cloud. This eliminates the need for traditional security appliances which are ineffective at protecting a cloud-first and mobile world. Leveraging a purpose-built cloud architecture, iboss is designed to make transitioning from security appliances to cloud security a seamless process. iboss is trusted by more than 4000 organizations worldwide, spans over 100 points of presence globally and is backed by over 110 patents.

To learn more, visit https://www.iboss.com