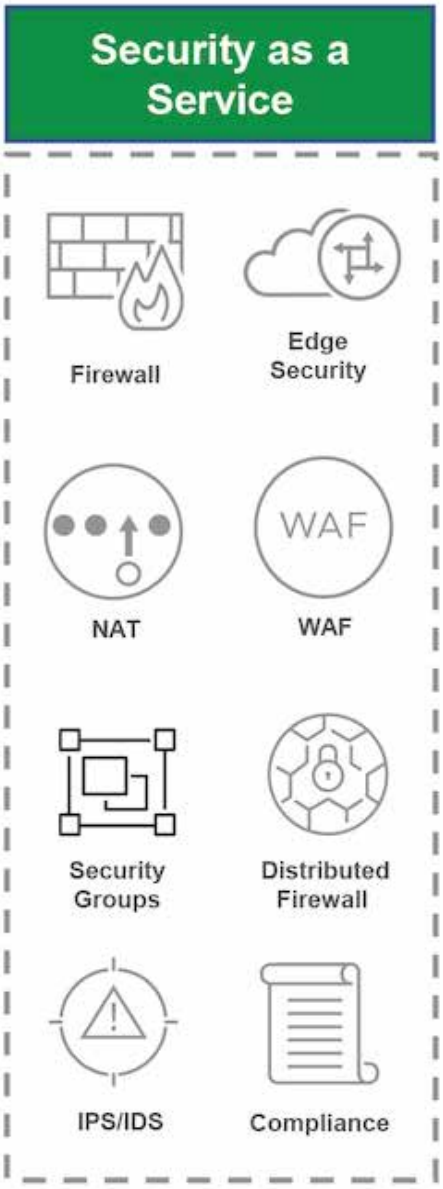
Security as a Service



Cloud security is a critical element in ensuring that the iBridge Cloud computing environments are protected against various cyber threats. Here are some technical details of cloud security that are implemented in our custom designed, managed secure cloud environments:

- **Identity and Access Management (IAM)**
  An essential aspect of cloud security that ensures that only authorized users can access cloud resources.

- **Encryption**
  The process of converting data into a form that cannot be understood without the correct decryption key.

- **Network Security**
  The process of protecting the cloud network from cyber threats such as Distributed Denial of Service (DDoS) attacks, man-in-the-middle attacks, and other types of network-based attacks.

- **Application Security**
  The process of protecting cloud applications from cyber threats such as SQL injection attacks, cross-site scripting (XSS) attacks, and other types of application-based attacks.

- **Data Protection**
  The process of protecting sensitive data in the cloud environment from unauthorized access, modification, or destruction.

- **Compliance**
  An essential aspect of cloud security that ensures that cloud environments comply with various regulatory standards such as PCI-DSS, HIPAA, and SOC 2.

It is essential iBridge understands, implements, and monitors these technical elements of cloud security in their design, implementation, and managed secure cloud environments. By leveraging these technical elements, clients can be assured that cloud environments remain secure, available, and resilient against various cyber threats.

iBRIDGE
1-866-790-7391
sales@iBridgeCloud.com
2851 Gold Tailings Court,
Rancho Cordova, CA 95670
iBridgeCloud.com

Firewall A virtual firewall from Palo Alto Networks is a software-based security solution that provides network protection for virtualized environments. Virtual firewalls are designed to protect virtual machines (VMs) and other virtualized resources, providing network security for multi-tenant cloud environments and other virtualized infrastructures. Uses include multi-tenant security, application visibility and controls and threat prevention.'

Edge Security Edge security in IaaS (Infrastructure as a Service) refers to the security measures and protocols that are implemented at the edge of a network, where the network interfaces with the outside world. Edge security is paramount in a hosted environment because it helps to protect against cyber threats and other security risks that can compromise the security and integrity of the network. Features are firewall protection, intrusion detection and prevention, web application firewalls, secure gateways and DDoS protection.

NAT (Network Address Translation) and WAF (Web Application Firewall) are two important components of network security in IaaS (Infrastructure as a Service) environments.
NAT is a protocol used to translate private IP addresses into public IP addresses, allowing devices on a private network to communicate with devices on a public network, such as the internet. WAF is a type of firewall designed specifically to protect web applications from attacks such as cross-site scripting (XSS), SQL injection, and other types of web-based attacks.

Security Groups are utilized in Security as a Service by MSPs (Managed Service Providers) as a way to control access to resources and applications within a network. Security groups are essentially collections of network rules that dictate which traffic is allowed and which traffic is blocked. These rules are based on a variety of factors, such as IP address, protocol, and port number. Uses are network segmentation, control access to resources, simplify network management and improve network performance.

Distributed Firewall is a network security solution that is designed to protect distributed computing environments, such as cloud computing or virtualized environments. Unlike traditional firewalls, which are typically located at the network perimeter, distributed firewalls are distributed throughout the network, allowing them to provide protection at multiple points in the network.

IPS and IDS in Cloud are two critical components of cloud security, designed to identify and prevent malicious traffic on the network. IDS is a system that monitors network traffic for suspicious activity, such as traffic patterns that are characteristic of a particular attack or malware. While the IPS systems typically use signatures and heuristics to identify and block threats, and can be configured to automatically respond to threats in real-time.

Compliance is a hot topic in cloud computing in 2023 due to the increasing importance of data privacy and security, as well as the significant risks associated with non-compliance. As cloud computing continues to grow in popularity, compliance will likely remain a key consideration for organizations and cloud service providers alike. Reasons for the importance include increase in regulatory requirements, security concerns, reputation risks and competitive advantages.