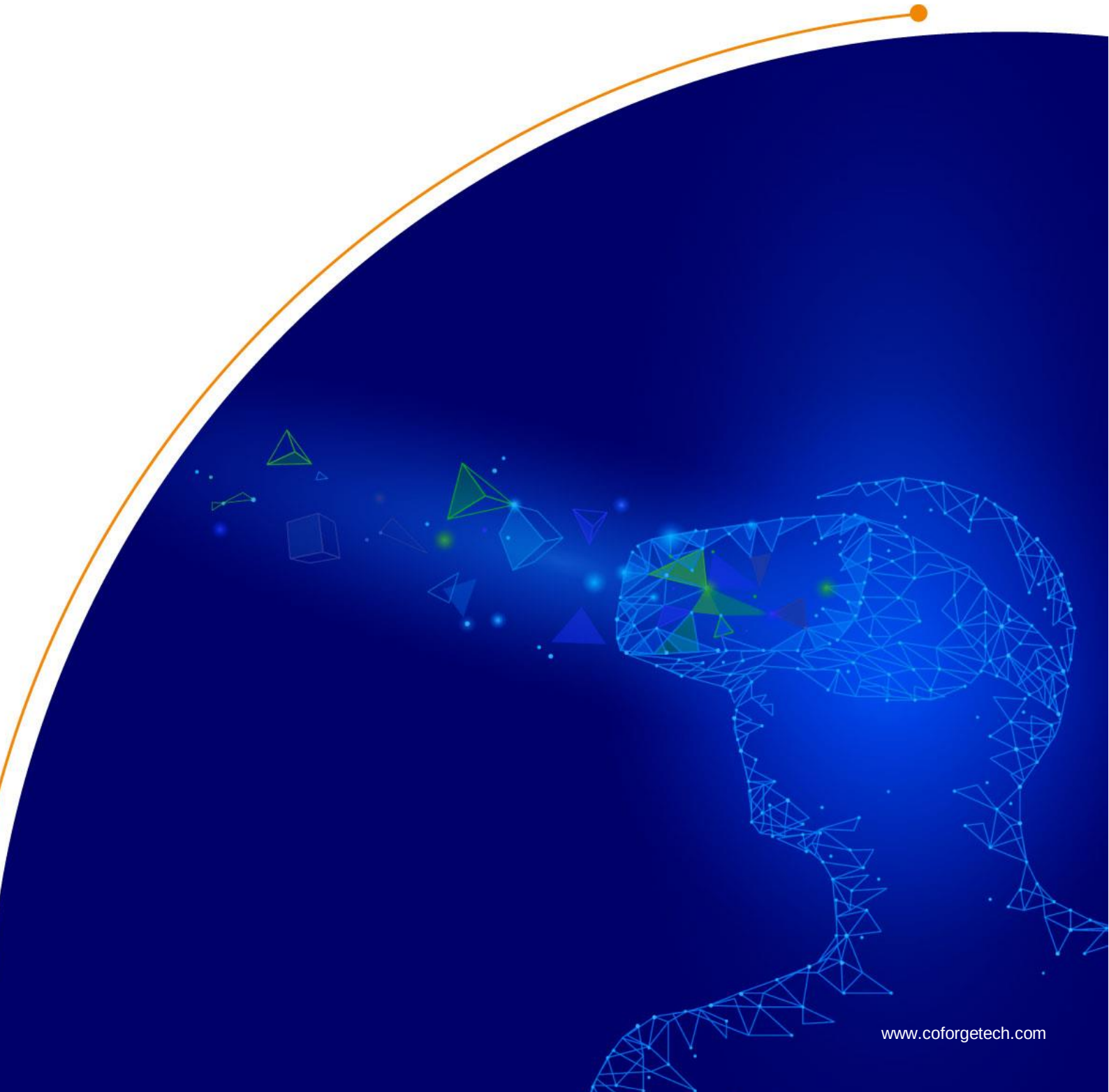
Coforge

Secure Landing Zone Implementation



Summary

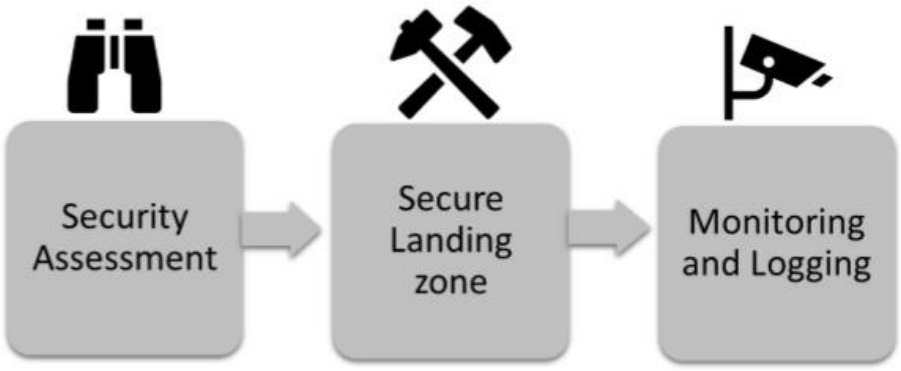
Worried about the Cloud Security! Looking for a solution providing paramount importance to secure Landing Zone to Cloud Journey and commits protection threats and vulnerabilities? Coforge uses azure best practices to deploy Integrated Cloud Security Solution. It makes the IT infrastructure resilient to attacks while safeguarding user access and protecting customer data. Realizing integrated visibility and protection across clouds, Hub and Spoke model ensures organization's efficient management of cloud security with better track and monitor attacks than non-cloud-based security solutions, and real-time firewall and signature updates blocking harmful traffic.

About the Solution

Data breaches occur nearly every day. This urgent need to secure systems and business from threats and attack vectors, "Cloud Security" is one of the major aspects of Cloud solutions with set of guidelines to block any possible form of data loss, breech, or unavailability, and acts as a specialized, add-on cloud service that ensures secure cloud environments and the data stored. As per the popular researches, security is being the main reason for restricting many enterprises to move their highly confidential data to cloud, and limited thoughts to meet necessary regulatory compliances.

Coforge's Solution is embedded by Azure Best Practice to start with a secure foundation. Hub and Spoke network topologies vouch security to the solution, where the spoke vNet(s) that peers with the hubvNet and can be utilized to isolate workloads. Traffic flows between the onpremises data-centre and the hub vNet through a secure Express Route or encrypted VPN connection. It gives your IT department an effective way to enforce security policies by a central location, reducing the potential for miss-configuration and exposure.

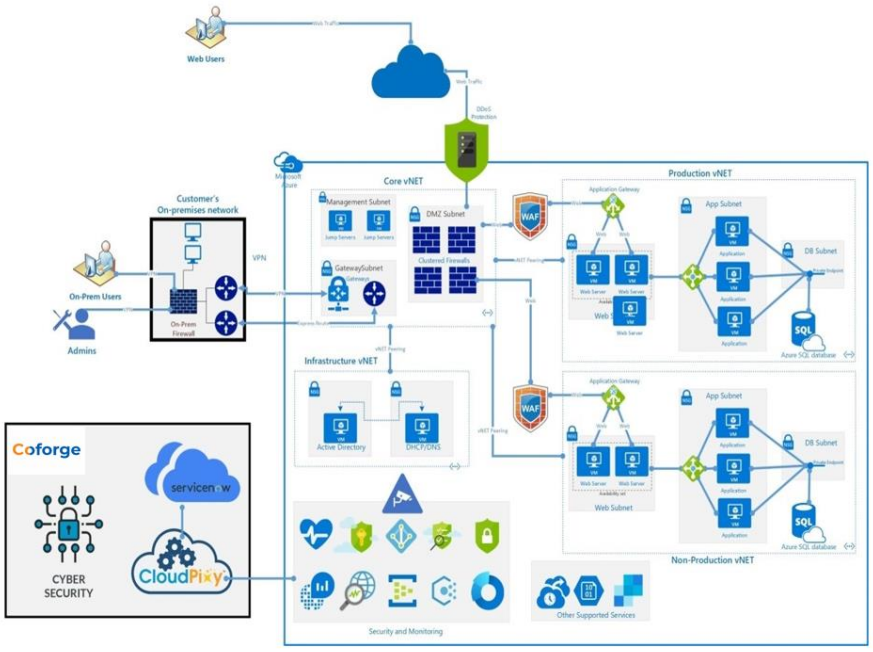
This Security Framework has following components to secure end to end cloud:



Evolving from traditional defence techniques, Coforge proposes Adoption of Zero Trust approach in the solution, eliminate the concept of trust based on network location within a perimeter, thereby validate trust at the time of access and enhance the level of network security. We also utilize Azure native security controls— Azure Firewall and the web application firewall in Application Gateway offer basic security with a fully stateful firewall as a service. Here, Coforge also offers Vulnerability Assessment and Penetration Testing(optional) offers enterprises with a wide range of application/system/network assessment than any single test carried out alone. VAPT allows organization to get a more detailed view of the threat the applications are facing, which aid business to better protect its systems and data from malevolent attacks.

Hence, Coforge offers Proactive Alerts and Troubleshooting approach with Cyber Intelligence Centre to concentrate on mitigating crucial vulnerabilities while enduring to discover and categorize vulnerabilities and make sure organization's critical data is properly protected and compliance requirements are being met.

Coforge built high level reference architecture to implement a fully secure landing zone for cloud. Setting up Network Security Group (NSG) gives enterprises a first level stateful packet filtering firewall and enables to control access based on a 5-tuple, including ability to customize the routing behavior for network traffic by configuring User-Defined Routes, etc in Azure.



This architecture also integrates security monitoring and policy management across Azure subscriptions, and prevent, detect, and respond to threats with increased visibility into and control over the security of resources through Azure Security Centre. Enforcing intelligent azure access policies to the solution, helps cloud environment become compliant with internal policies and external regulations.

Coforge enables strong authentication and MFA options, to protect users from 99.9 percent of identity attacks, along with Azure DDoS Protection for designing resilient solutions. Utilizing Cloud Native Azure Monitor in the solution, help in alerting, and analysing security events, with threat protection suggestions, and forward it to a central repository, which gives the maximum flexibility and control for cloud-based management of infrastructure. Enhancing the data protection and compliance, Solutionincludes a secure key management to monitor and audit the keys stored in hardware security modules (HSMs) and enables Customers to enrol and automatically renew certificates from supported public Certificate Authorities. This Consulting Solution analyse the Cloud's network for any harmful intrusions or vulnerabilities through Network Watcher, and monitor the entire network health of IaaS platforms such as Virtual Machines, Virtual Networks, Application Gateways, Load balancers, etc. Integration of ServiceNow and CloudPixy (CMP) provides the solution for Incident Management and resolution which improves visibility into the operations footprint, manage service health, and record/track all security incident until service is restored or the issue is resolved.

Collaborating with the customer's security team, Coforge will comprehend the functional requirements of business, corresponding to security and compliances. During the period of 5 weeks, we will engage with your architects to plan the infrastructure for the landing zone. Based on the prepared plan we will

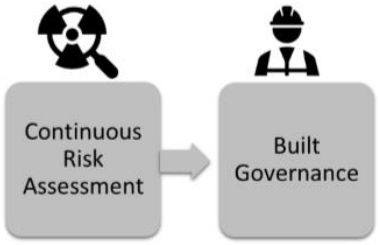
implement the Landing Zone with integrated high security and customized requirements. At the end of the project, the customer will have in hand the high level and low level diagrams, policy documents, SOPs and a secure Landing Zone on azure to migrate their services and have a secure environment during the operations.

Timeline: (5-6 weeks)

Features & Benefits

- Flexibility: Greater flexibility in terms of management and security for cloud environment
- Avoid data loss: Visualize infrastructure instantly and identify misconfigurations and possible data breach points. Reduces the liability of Scale: hub and spoke network come with growing the business and maintaining consistent architecture that scales.
- Stop Unauthorized Access: Ensure that only legitimate traffic is allowed, and security could be defined as the process of protecting resources from unauthorized access or attack by applying controls to network traffic.
- “Reduce complexity and costs (ingress and egress vNet traffic)” by centralizing a bunch of logical network segments or zones to
- Network Security: Isolating customer networks in single shared physical network
- Reduce Time to Breach Detection — and Gain Visibility into Enterprise Traffic, by Zero trust principle of “always verify and never trust.”
- Adopt Zero trust approach: Perimeter-based networks operate on the assumption that all systems within a network can be trusted.
- Rendering a comprehensive outlook of potential threats within the network
- Protects network from both inside/outside threats and safeguard data from malicious attack.

Next Steps: Post this framework implementation and Based on the engagement scopes, Coforge may also help customer to maintain next steps towards cloud security –



These overall 5 Steps of framework will cover the end-to-end Security in Cloud.