Managed Services

Customer: India’s AI Tech company

Problem Statement

Worxogo is a pioneer in AI and sales have extended the services across the globe. They require to have security in terms of data and as well in the Network level infra running in Azure systems.

Proposed Solution

PUC recommended the following for the client to enhance the security aspects.

1. Azure Security Centre:

Azure Security Center is a unified infrastructure security management system that strengthens the security posture of the data centers, and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as well as on-premises.

In the Security Center, we can set our policies to run on management groups, across subscriptions, and even for a whole tenant.

The advanced monitoring capabilities in the Security Center also let us track and manage compliance and governance over time. The overall compliance provides you with a measure of how much your subscriptions are compliant with policies associated with your workload.

2. Continuous Assessments

Security Center continuously discovers new resources that are being deployed across your workloads and assess whether they are configured according to security best practices if not, they’re flagged and you get a prioritized list of recommendations for what you need to fix to protect your machines.
As our client add up new resources to the environment, this feature helps in the validation of the resources and fix the security issues based on the recommendations.

3. Network Map

Enables us to see the topology of the workloads, so we can see if each node is properly configured. We can see how the nodes are connected, which helps you block unwanted connections that could potentially make it easier for an attacker to creep along with your network.

Security Center makes mitigating your security alerts one step easier, by adding a Secure Score. The Secure Scores are now associated with each recommendation you receive to help you understand how important each recommendation is to your overall security posture.

**Azure Security center protects the following**

- Protect against threats
- Integration with Microsoft Defender Advanced threat protection
- Protect PaaS
- Brute force attack
- Protect IoT and hybrid cloud workloads

Hence Azure Security Center speaks to the growing need for an enterprise-grade security management platform that encompasses both cloud and onsite resources with a unified, analytics-rich, actionable interface that helps you take control of the security of your resources on all fronts.

**Disk Encryption**

Azure managed disks automatically encrypt your data by default when persisting it to the cloud. Server-side encryption (SSE) protects your data and helps you meet your organizational security and compliance commitments.
Data in Azure managed disks is encrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant.

Note: Encryption does not impact the performance of managed disks and there is no additional cost for the encryption.

If Azure Security Center is used, it notifies an alert if you have VMs that aren't encrypted. The alerts show High Severity and the recommendation is to encrypt these VMs.

**Accessing Azure resources Using Secure VPN Connection**

As the organizational members access the VM resources for deployment and coding purposes daily and there is a need for secure communication between the Azure resources and the PC’s of the organizational members.

A Point-to-Site (P2S) VPN gateway connection lets to create a secure connection to your virtual network from an individual client computer. A P2S connection is established by starting it from the client computer. Users use the native VPN clients on Windows and Mac devices for P2S. Azure provides a VPN client configuration zip file that contains settings required by these native clients to connect to Azure.

- For Windows devices, the VPN client configuration consists of an installer package that users install on their devices.
- For Mac devices, it consists of the mobileconfig file that users install on their devices.

The zip file also provides the values of some of the important settings on the Azure side that you can use to create your profile for these devices. Some of the values include the VPN gateway address, configured tunnel types, routes, and the root certificate for gateway validation.
Fortigate Firewall-Azure:

Add a layer of security, Fortigate firewalls have been configured to monitor the incoming/outgoing traffic.

The FortiGate-VM on Microsoft Azure delivers next-generation firewall capabilities for organizations of all sizes, with the flexibility to be deployed as a next-generation firewall and/or VPN gateway. It protects against cyber threats with high performance, security efficacy, and deep visibility.

Cloud platform

Azure.