

Azure Security Accelerator: 3-Week Implementation



Week 1

Assessment

We review your security, compliance, and governance requirements and assess your Azure environment for potential costs of a new Azure Policy and Defender implementation.



Week 2

Implementation

We implement Azure Policy by defining and assigning custom or built-in policies, then activate and configure Azure Defender plans and settings.

```
1 {
2   "properties": {
3     "displayName": "Enforce Virtual Network Filtering on Cosmos DB accounts",
4     "policyType": "Custom",
5     "description": "This policy ensures Virtual Network Filtering is enabled on all Cosmos DB accounts",
6     "mode": "Indexed",
7     "metadata": {
8       "category": "Cosmos DB"
9     }
10    "parameters": {},
11    "policyRule": {
12      "if": {
13        "allOf": [
14          {
15            "field": "type",
16            "equals": "Microsoft.DocumentDB/databaseAccounts"
17          },
18          {
19            "field": "Microsoft.DocumentDB/databaseAccounts/isVirtualNetworkFilteringEnabled",
20            "exists": "false"
21          }
22        ]
23      }
24      "then": {
25        "effect": "deny"
26      }
27    }
28  }
29 }
30
31 {
32   "if": {
33     "allOf": [
34       {
35         "field": "type",
36         "equals": "Microsoft.DocumentDB/databaseAccounts"
37       },
38       {
39         "field": "Microsoft.DocumentDB/databaseAccounts/isVirtualNetworkFilteringEnabled",
40         "exists": "false"
41       }
42     ]
43   }
44   "then": {
45     "effect": "deny"
46   }
47 }
48
49 {
50   "resourceGroup": {
51     "type": "String",
52     "metadata": {
53       "displayName": "Resource Group",
54       "strongType": "Existing"
55     }
56   }
57 }
```

Week 3

Management

We set up monitoring, reporting and alerts, then define a continuous security improvement plan together with detailed documentation of your new Azure Policy and Defender configurations.

