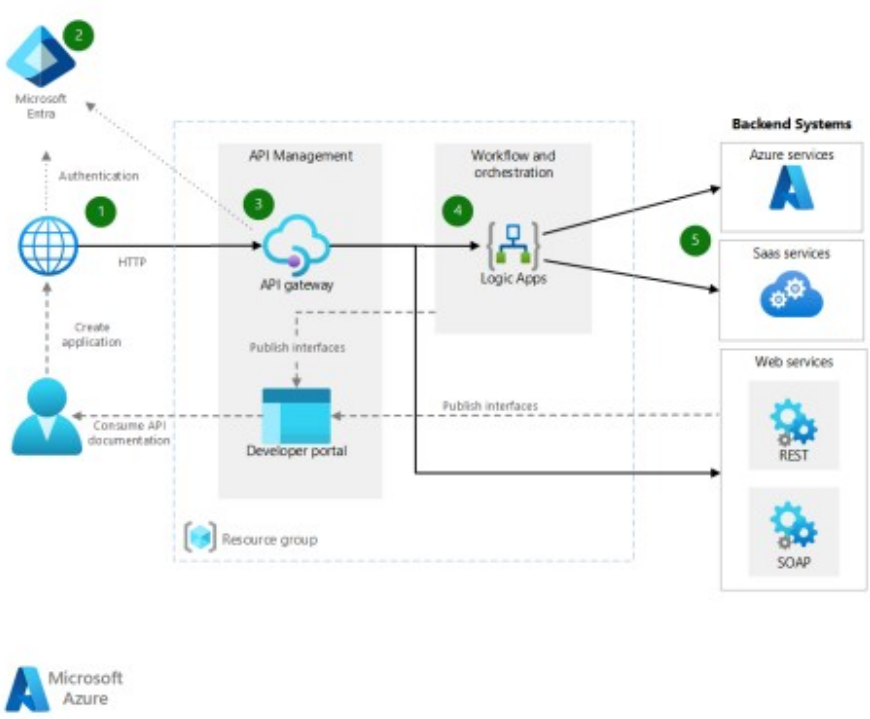
Evaluation Only. Created with Aspose.PDF. Copyright 2002-2025 Aspose Pty Ltd.

Relatório de análise da solução: tmpcv6msfte



Análise completa da solução atual

Modelo de cloud:
- Microsoft Azure

Lista com os componentes:
- Consumidor/Cliente de API (aplicativo/usuário externo)
- Microsoft Entra ID (antigo Azure AD) – autenticação, registro de aplicativos e emissão de tokens
- Azure API Management (APIM)
  - API Gateway
  - Developer Portal
  - Políticas (validação JWT, rate limit, transformação)
  - Publicação de interfaces
- Azure Logic Apps – Workflow and orchestration
- Backend Systems
  - Azure services (ex.: Functions, App Service, Service Bus, Storage, SQL/Cosmos DB) – genérico no diagrama
  - SaaS services (ex.: Office 365, Dynamics, Salesforce) – genérico no diagrama
  - Web services (REST e SOAP)
- Resource Group (contenção e governança de recursos)
- Internet/HTTP(s) como meio de acesso

Interação entre os componentes:
1) O consumidor acessa o Developer Portal do APIM para descobrir APIs e obter/subscrever credenciais (chaves) e integra o cliente para usar OAuth2/OIDC via Microsoft Entra ID.
2) O cliente autentica no Microsoft Entra ID, obtendo tokens (JWT) para chamar a API.
3) O cliente chama a API via HTTPS no API Gateway do APIM. O APIM valida o JWT, aplica políticas (throttling, quotas, CORS, transformação, schema validation, cache) e roteia a chamada.
4) O APIM invoca Logic Apps quando é necessário orquestrar fluxos/integrações multi-etapas e/ou conectores de terceiros.
5) A Logic App e/ou o próprio APIM consome sistemas de backend: Azure services, SaaS services e Web services (REST/SOAP). As respostas retornam pelo mesmo caminho até o cliente.

O que esse sistema faz:
- Provê uma camada de gestão e exposição de APIs (façade) com segurança, observabilidade e governança.
- Orquestra integrações entre clientes externos e múltiplos backends (Azure, SaaS e serviços web), agregando e transformando dados/serviços por meio de Logic Apps.

Evaluation Only. Created with Aspose.PDF. Copyright 2002-2025 Aspose Pty Ltd.

- Oferece onboarding de desenvolvedores via Developer Portal e operacionaliza políticas de segurança, versionamento e limitação de uso.

Vulnerabilidades e Solução para cada vulnerabilidade:
- Identidade e autenticação (Microsoft Entra)
  - Risco: configuração fraca de aplicativos (sem PKCE, confidenciais sem segredo rotacionado, consentimentos amplos), tokens com vida longa, falta de MFA/CA.
  - Mitigações: OAuth2/OIDC com PKCE, tokens de curta duração + refresh controlado; Conditional Access e MFA; revisão de consentimentos; Managed Identities para chamadas entre serviços; rotação de credenciais e uso de certificados armazenados no Key Vault.

- API Management (Gateway e Políticas)
  - Risco: ausência de validação JWT/escopos, TLS fraco, CORS permissivo, falta de rate limiting/quotas; exposição de detalhes internos em erros; secrets em políticas.
  - Mitigações: políticas validate-jwt, validação de escopos/roles; TLS 1.2+/HSTS; CORS restritivo por origem; rate limit/quotas por assinatura/IP; mascaramento de erros; extrair segredos para Azure Key Vault; usar gateway privado/VNet + Private Link sempre que possível.

- Developer Portal
  - Risco: vazamento de chaves de subscrição, enumeração de APIs, conteúdo injetável.
  - Mitigações: exigir login/role para visualizar APIs; aprovação manual/automática com política; mascarar chaves; rate limit no portal; varredura de conteúdo e CSP estrito.

- Logic Apps (orquestração)
  - Risco: triggers HTTP expostos publicamente sem auth robusta; conectores com credenciais estáticas; identidades com privilégio excessivo; injeção via payloads mal validados; segredo em texto claro.
  - Mitigações: autenticação mTLS/OAuth e assinatura HMAC em triggers; uso de Managed Identity e Key Vault; princípio de menor privilégio nas conexões (RBAC, scopes mínimos); schema validation e sanitização; IP restrictions/Private Endpoints; masking de dados sensíveis nos logs.

- Backends (Azure/SaaS/Web services)
  - Risco: endpoints públicos sem WAF; ausência de mTLS; dados em repouso sem criptografia; falta de validação de entrada; dependência de versões inseguras de APIs SOAP/REST.
  - Mitigações: Application Gateway/WAF, mTLS, Private Endpoints, TLS up-to-date; criptografia at-rest (TDE/Storage encryption) e em trânsito; validação de entrada/contract-first (OpenAPI/XSD); pinagem de certificado onde aplicável; revisão de versões/patching.

- Rede e perímetro
  - Risco: tráfego Internet → backend sem isolamento; falta de DDoS proteção; ausência de NSGs/ASGs.
  - Mitigações: VNet integration para APIM/Logic Apps, Private Link, NSGs/ASGs, Azure Firewall; Azure DDoS Protection Standard; Segregar por sub-redes e RGs.

- Observabilidade e resposta a incidentes
  - Risco: logs insuficientes, sem trilha de auditoria nem correlação; retenção curta; alertas inexistentes.
  - Mitigações: Log Analytics/Monitor, diagnostics no APIM/Logic Apps/backends; trilhas imutáveis (WORM) para auditoria; alertas, dashboards e integração com SIEM/SOAR; time sync (NTP).

- Governança/configuração
  - Risco: mudanças não rastreadas (config drift), IaC insegura, permissões amplas de operadores.
  - Mitigações: Infra as Code (Bicep/Terraform) com revisão/PRs; RBAC + PIM; Azure Policy/Blueprints; varreduras estáticas (tfsec/checkov) e posture management (Defender for Cloud).

Relatório de Modelagem de Ameaças (STRIDE):
- Escopo
  - Exposição de APIs via Azure API Management e orquestração por Logic Apps, autenticando com Microsoft Entra e consumindo backends Azure/SaaS/Web.

- Ativos principais
  - APIs e contratos (OpenAPI/XSD), tokens/jwt e chaves de subscrição, dados de negócio/PII, configurações de APIM/Logic Apps, segredos (conexões, certificados), logs/auditoria.

- Atores
  - Consumidores externos (apps/usuários), operadores DevOps, identidade de serviço (Managed Identities), provedores SaaS/serviços web.

- Fronteiras de confiança
  - Internet → APIM (gateway)

Evaluation Only. Created with Aspose.PDF. Copyright 2002-2025 Aspose Pty Ltd.

  - APIM → Logic Apps (intra-cloud)
  - APIM/Logic Apps → Backends Azure (privado) e SaaS/Web (externo)
  - Portal do desenvolvedor (usuários → plataforma)

- Principais fluxos de dados
  - DF1: Cliente ↔ APIM (HTTPS + JWT)
  - DF2: APIM ↔ Entra (validação/metadata, jwks)
  - DF3: APIM ↔ Logic Apps (HTTPS/mTLS; identidade gerenciada)
  - DF4: Logic Apps ↔ Backends Azure (Private Link/RBAC)
  - DF5: Logic Apps/APIM ↔ SaaS/Web (conectores OAuth2/mTLS)
  - DF6: Telemetria/Logs → Log Analytics/SIEM

- STRIDE
  - S – Spoofing (falsificação de identidade)
    - Ameaças: JWT forjado/replay; cliente se passando por serviço; conector SaaS com token comprometido.
    - Mitigações: validate-jwt com emissor/audiência/assinatura; clock skew curto; CA/MFA/Conditional Access; mTLS entre serviços; Managed Identity; proteção de segredos no Key Vault; certificado cliente para triggers.

  - T – Tampering (violação/integridade)
    - Ameaças: payloads alterados; políticas APIM/Logic Apps adulteradas; manipulação de contratos.
    - Mitigações: TLS 1.2/1.3; assinatura/verificação (JWS); schema validation (OpenAPI/XSD); CI/CD com revisão e assinaturas de release; RBAC/PIM; bloqueio de alteração direta em produção.

  - R – Repudiation (repúdio)
    - Ameaças: ações sem trilha (ex.: exclusões/execuções sem log correlacionável).
    - Mitigações: logs imutáveis com correlação (x-correlation-id), carimbo NTP, auditoria do Entra/APIM/Logic Apps; retenção adequada; acesso de somente leitura a logs operacionais.

  - I – Information Disclosure (exposição de informação)
    - Ameaças: dados sensíveis em erros/logs; chaves no portal; endpoints públicos expondo metadados; conexão SaaS vazando tokens.
    - Mitigações: data masking/redaction em logs; políticas de resposta genéricas no APIM; segredo no Key Vault; Private Endpoints; classificação/rotulagem e DLP; segredo por identidade gerenciada.

  - D – Denial of Service (negação de serviço)
    - Ameaças: bursts de tráfego e abuse de quotas; DDoS na borda; long-running workflows exaurindo conexões.
    - Mitigações: quotas/rate limit/burst control no APIM; Azure DDoS Protection Standard; autoscaling e políticas de timeout/retry/circuit breaker; filas assíncronas (Service Bus) para suavizar picos; cache quando aplicável.

  - E – Elevation of Privilege (elevação de privilégio)
    - Ameaças: operadores/identidades com permissões excessivas; execução de conectores com escopos amplos; exploração de má configuração para acesso lateral.
    - Mitigações: RBAC mínimo necessário; PIM para elevar sob demanda; segmentação por RG/VNet; políticas de acesso condicional e bloqueio por localização; revisões periódicas de acesso; verificações de postura (Defender for Cloud).

- Riscos prioritários (alto impacto/provável)
  - Endpoints públicos sem validação de identidade forte → aplique validate-jwt, mTLS e Private Endpoints.
  - Ausência de rate limiting → habilite quotas/throttling no APIM imediatamente.
  - Segredos em configuração/políticas → migre para Key Vault e Managed Identity.
  - Conexões Logic Apps com privilégio excessivo → reescopar permissões e ativar PIM.

- Plano de tratamento resumido
  - Curto prazo: reforçar políticas APIM (JWT, quotas, CORS), ativar logs/telemetria e mascaramento, mover segredos para Key Vault, bloquear triggers HTTP públicos.
  - Médio prazo: VNet/Private Link, DDoS Standard, WAF, CI/CD com validações de segurança, revisão de RBAC/PIM, schema validation em todas as APIs.
  - Contínuo: monitoramento/alertas SIEM, pentests e API security testing (OWASP API Top 10), gestão de vulnerabilidades e patching.

Additional resourcing needs:
- Project Manager (leads STRIDE sessions, scope, scheduling)
- Network Administrator (VNet/Private Link, NSG/Firewall, DDoS/WAF design)
- Security Officer/Architect (policies, standards, risk acceptance, compliance)

Evaluation Only. Created with Aspose.PDF. Copyright 2002-2025 Aspose Pty Ltd.

- Cloud/DevOps Engineers (APIM/Logic Apps/IaC, CI/CD, observability)
- Software Developers (API design, OpenAPI contracts, input validation, secure coding)
- IAM Specialist (Microsoft Entra, Conditional Access, PIM, RBAC, Managed Identity)
- Data/Integration Engineer (Logic Apps connectors, data mapping, PII handling)
- Privacy/Legal (data classification, retention, DPIA)
- Supplier representatives (SaaS/web services owners for integration constraints)
- Optional: Hardware Developer (only if there is device/edge component storing credentials)

Notas finais:
- Este desenho segue o padrão de integração API-led na Azure, com APIM como fachada de segurança/governança e Logic Apps para orquestração. Priorize a criação de fronteiras de confiança claras (Internet ↔ Gateway ↔ Orquestração ↔ Backends) e aplique controles técnicos alinhados ao STRIDE em cada fronteira.

Sugestões de melhorias

A seguir estão:
1) um diagrama Mermaid que mostra a arquitetura proposta, os relacionamentos e os principais controles de mitigação de vulnerabilidades;
2) um script Terraform de referência para criar os principais recursos no Azure com boas práticas de segurança (VNet, APIM, Logic Apps Standard com VNet integration, Key Vault com Private Endpoint, Log Analytics, diagnósticos e políticas básicas no APIM).

Diagrama Mermaid (arquitetura e mitigações)
```mermaid
flowchart LR
  %% Fronteiras
  subgraph Internet[Internet / HTTPS]
    Client[Consumidor/Cliente de API]
  end

  subgraph RG[Azure Resource Group]
    subgraph Identity[Identidade]
      Entra[Microsoft Entra ID (OIDC/OAuth2)\n- CA/MFA\n- Tokens curtos\n- App Reg com PKCE\n- Consentimentos mínimos]
    end

    subgraph Net[VNet + Sub-redes + Segurança]
      APIMSN[(Subnet APIM + NSG)]
      LASN[(Subnet Logic Apps + NSG)]
      PESN[(Subnet Private Endpoints + NSG)]
      DDoS[Azure DDoS Protection Standard]
      FW[Azure Firewall / WAF (opcional)]
    end

    subgraph Sec[Segurança e Governança]
      KV[Azure Key Vault\n- Segredos/Certs\n- RBAC/Access Policy\n- Private Endpoint\n- Soft Delete + Purge Protection]
      LAWS[Log Analytics / Azure Monitor\n- Diagnósticos e Auditoria\n- Dashboards/Alertas]
      Policy[Azure Policy / PIM / RBAC]
    end

    subgraph APIM[Azure API Management]
      GW[API Gateway]
      Portal[Developer Portal\n- Acesso autenticado\n- Chaves mascaradas\n- Rate limit]
      Policies[Políticas:\n- validate-jwt (issuer/audience/escopos)\n- TLS >= 1.2 / HSTS\n- Rate limit + Quotas\n- CORS restritivo\n- Cache / Transform / Schema Validation\n- Mask de erros\n- Segredos via Key Vault]
    end

    subgraph Orq[Logic Apps Standard (VNet Integration)]
      LA[Workflows\n- Managed Identity\n- IP Restriction\n- Schema validation\n- Sanitização de payloads\n- Data masking em logs]
    end

    subgraph Backends[Backends]
      AZ[Serviços Azure (Functions, App Service, Service Bus, Storage, SQL/Cosmos)\n- Private Link / RBAC\n- Criptografia at-rest/in-transit]
```

Evaluation Only. Created with Aspose.PDF. Copyright 2002-2025 Aspose Pty Ltd.

```
    SAAS[SaaS (O365, Dynamics, Salesforce)\n- Conectores OAuth2\n- Escopos mínimos]
    WS[Web Services REST/SOAP\n- mTLS/TLS atual\n- Contract-first (OpenAPI/XSD)]
  end
end

%% Fluxos e Controles
Client -- "DF1: HTTPS + JWT(OIDC)\nMitigações: TLS1.2+, validate-jwt, CORS restritivo,\nRate limit/Quotas, HSTS, masking erros" --> GW
Portal -. "Onboarding devs\nPolicies de aprovação, chaves mascaradas" .- Client

GW -- "DF2: JWKS/metadata\nissuer/audience" --- Entra

GW -- "DF3: HTTPS (mTLS/OAuth)\nManaged Identity\nSchema validation" --> LA

LA -- "DF4: Private Link/RBAC\nIdentidade gerenciada\nIP Restrictions" --> AZ
LA -. "DF5: OAuth2/mTLS\nEscopos mínimos" .- SAAS
LA -. "DF5: TLS atual, validação de entrada,\nPinagem de certificado onde aplicável" .- WS

GW -. "Secrets/Certs\n(Key Vault via reference)" .- KV
LA -. "Secrets/Creds\n(Key Vault via MI/Policy)" .- KV

GW == "DF6: Diagnostics/Logs/Metrics" ==> LAWS
LA == "DF6: Diagnostics/Logs/Metrics" ==> LAWS
AZ == "DF6: Logs/Auditoria" ==> LAWS

DDoS -. Proteção de borda .- Net
FW -. NSG/ASG/Segregação .- Net
Policy -. "IaC, RBAC+PIM, Azure Policy, Postura" .- RG
```

Script Terraform (referência)
Observações:
- Escolha Developer SKU para ambiente de teste; para produção, prefira Premium e redes privadas end-to-end.
- Logic Apps Standard exige um App Service Plan “Workflow Standard” (WS1/WS2/WS3) e uma Storage Account.
- O Key Vault usa Private Endpoint e bloqueio de rede pública. APIM e Logic Apps acessam KV pela VNet.
- O exemplo cria uma API no APIM com políticas de segurança (validate-jwt, CORS, rate/quotas, HSTS e mascaramento de erros). Ajuste audience/escopos conforme seu App Registration no Entra.
- Habilita diagnósticos para APIM, Logic Apps e Key Vault no Log Analytics.

Copie o conteúdo abaixo em um arquivo main.tf. Ajuste variáveis marcadas com TODO.

```hcl
terraform {
  required_version = ">= 1.5.0"
  required_providers {
    azurerm = {
      source  = "hashicorp/azurerm"
      version = "~> 3.113"
    }
    azuread = {
      source  = "hashicorp/azuread"
      version = "~> 2.48"
    }
    random = {
      source  = "hashicorp/random"
      version = "~> 3.6"
    }
  }
}

provider "azurerm" {
  features {}
}

provider "azuread" {}
```

Evaluation Only. Created with Aspose.PDF. Copyright 2002-2025 Aspose Pty Ltd.

```
data "azurerm_client_config" "current" {}

#####################
# Variáveis
#####################
variable "location" {
  description = "Região do Azure"
  type        = string
  default     = "brazilsouth"
}

variable "rg_name" {
  description = "Nome do Resource Group"
  type        = string
  default     = "rg-apim-logicapps-sec"
}

variable "project_name" {
  description = "Prefixo de nomes"
  type        = string
  default     = "apimla"
}

# TODO: ajuste as origens permitidas no CORS
variable "cors_allowed_origins" {
  type    = list(string)
  default = ["https://example.com"]
}

# TODO: ajuste o audience da sua API registrada no Entra ID (ex.: api://<app-id-uri>)
variable "oidc_audience" {
  type        = string
  description = "Audience esperado no JWT"
  default     = "api://CHANGE-ME-APP-ID-URI"
}

# Limites de uso
variable "rate_limit_per_minute" {
  type    = number
  default = 60
}
variable "quota_calls_per_hour" {
  type    = number
  default = 1000
}

#####################
# Utilidades
#####################
resource "random_string" "suffix" {
  length  = 4
  upper   = false
  lower   = true
  numeric = true
  special = false
}

#####################
# Resource Group
#####################
resource "azurerm_resource_group" "rg" {
  name     = var.rg_name
  location = var.location
}

#####################
# Log Analytics / Monitor
#####################
resource "azurerm_log_analytics_workspace" "law" {
```

Evaluation Only. Created with Aspose.PDF. Copyright 2002-2025 Aspose Pty Ltd.

```
  name                = "${var.project_name}-law-${random_string.suffix.result}"
  location            = azurerm_resource_group.rg.location
  resource_group_name = azurerm_resource_group.rg.name
  sku                 = "PerGB2018"
  retention_in_days   = 30
}

#####################
# Rede (VNet + Subnets + DDoS)
#####################
resource "azurerm_network_ddos_protection_plan" "ddos" {
  name                = "${var.project_name}-ddos-${random_string.suffix.result}"
  resource_group_name = azurerm_resource_group.rg.name
  location            = azurerm_resource_group.rg.location
}

resource "azurerm_virtual_network" "vnet" {
  name                = "${var.project_name}-vnet"
  address_space       = ["10.20.0.0/16"]
  location            = azurerm_resource_group.rg.location
  resource_group_name = azurerm_resource_group.rg.name
  ddos_protection_plan {
    id     = azurerm_network_ddos_protection_plan.ddos.id
    enable = true
  }
}

resource "azurerm_subnet" "snet_apim" {
  name                 = "snet-apim"
  resource_group_name  = azurerm_resource_group.rg.name
  virtual_network_name = azurerm_virtual_network.vnet.name
  address_prefixes     = ["10.20.1.0/24"]
}

resource "azurerm_subnet" "snet_logicapps" {
  name                 = "snet-logicapps"
  resource_group_name  = azurerm_resource_group.rg.name
  virtual_network_name = azurerm_virtual_network.vnet.name
  address_prefixes     = ["10.20.2.0/24"]
  delegation {
    name = "delegation-appsvc"
    service_delegation {
      name = "Microsoft.Web/serverFarms"
      actions = [
        "Microsoft.Network/virtualNetworks/subnets/action"
      ]
    }
  }
}

resource "azurerm_subnet" "snet_private_endpoints" {
  name                 = "snet-priv-endpoints"
  resource_group_name  = azurerm_resource_group.rg.name
  virtual_network_name = azurerm_virtual_network.vnet.name
  address_prefixes     = ["10.20.10.0/24"]
  private_endpoint_network_policies_enabled = true
}

#####################
# Key Vault com Private Endpoint
#####################
resource "azurerm_key_vault" "kv" {
  name                        = "${var.project_name}-kv-${random_string.suffix.result}"
  location                    = azurerm_resource_group.rg.location
  resource_group_name         = azurerm_resource_group.rg.name
  tenant_id                   = data.azurerm_client_config.current.tenant_id
  sku_name                    = "standard"
  soft_delete_enabled         = true
  purge_protection_enabled    = true
```

Evaluation Only. Created with Aspose.PDF. Copyright 2002-2025 Aspose Pty Ltd.

```
  enable_rbac_authorization   = false
  public_network_access_enabled = false
}

# Acesso do operador atual (ajuste conforme necessidade)
resource "azurerm_key_vault_access_policy" "ap_me" {
  key_vault_id = azurerm_key_vault.kv.id
  tenant_id    = data.azurerm_client_config.current.tenant_id
  object_id    = data.azurerm_client_config.current.object_id

  secret_permissions = ["Get", "List", "Set", "Delete", "Purge", "Recover"]
}

# Segredo de exemplo para uso em políticas do APIM (HMAC, por ex.)
resource "azurerm_key_vault_secret" "apim_hmac" {
  name         = "apim-hmac-key"
  value        = "CHANGE-ME-STRONG-RANDOM"
  key_vault_id = azurerm_key_vault.kv.id
}

# Private DNS para Key Vault
resource "azurerm_private_dns_zone" "pdz_kv" {
  name                = "privatelink.vaultcore.azure.net"
  resource_group_name = azurerm_resource_group.rg.name
}

resource "azurerm_private_dns_zone_virtual_network_link" "pdz_kv_link" {
  name                  = "kv-dnslink"
  private_dns_zone_name = azurerm_private_dns_zone.pdz_kv.name
  resource_group_name   = azurerm_resource_group.rg.name
  virtual_network_id    = azurerm_virtual_network.vnet.id
}

# Private Endpoint para KV
resource "azurerm_private_endpoint" "pe_kv" {
  name                = "${var.project_name}-pe-kv"
  location            = azurerm_resource_group.rg.location
  resource_group_name = azurerm_resource_group.rg.name
  subnet_id           = azurerm_subnet.snet_private_endpoints.id

  private_service_connection {
    name                           = "kv-priv-conn"
    private_connection_resource_id = azurerm_key_vault.kv.id
    subresource_names              = ["vault"]
    is_manual_connection           = false
  }
}

resource "azurerm_private_dns_zone_group" "pdzg_kv" {
  name                 = "kv-dnszone-group"
  private_endpoint_id  = azurerm_private_endpoint.pe_kv.id
  private_dns_zone_ids = [azurerm_private_dns_zone.pdz_kv.id]
}

######################
# App Service Plan (Logic Apps Standard)
######################
resource "azurerm_app_service_plan" "plan" {
  name                = "${var.project_name}-plan-${random_string.suffix.result}"
  location            = azurerm_resource_group.rg.location
  resource_group_name = azurerm_resource_group.rg.name
  kind                = "elastic"

  sku {
    tier = "WorkflowStandard"
    size = "WS1"
  }
}
```

Evaluation Only. Created with Aspose.PDF. Copyright 2002-2025 Aspose Pty Ltd.

```
# Storage Account para Logic Apps Standard
resource "azurerm_storage_account" "st_la" {
  name                     = "st${var.project_name}${random_string.suffix.result}"
  resource_group_name      = azurerm_resource_group.rg.name
  location                 = azurerm_resource_group.rg.location
  account_tier             = "Standard"
  account_replication_type = "LRS"
  min_tls_version          = "TLS1_2"
  enable_https_traffic_only = true
  allow_nested_items_to_be_public = false
}

# Logic App Standard com Managed Identity
resource "azurerm_logic_app_standard" "la" {
  name                = "${var.project_name}-la-${random_string.suffix.result}"
  location            = azurerm_resource_group.rg.location
  resource_group_name = azurerm_resource_group.rg.name
  app_service_plan_id = azurerm_app_service_plan.plan.id
  storage_account_name = azurerm_storage_account.st_la.name
  storage_account_access_key = azurerm_storage_account.st_la.primary_access_key

  identity {
    type = "SystemAssigned"
  }

  site_config {
    minimum_tls_version = "1.2"
    # Restrições de IP (exemplo - ajuste conforme necessário)
    ip_restriction {
      name       = "DenyAllByDefault"
      priority   = 65000
      action     = "Deny"
      ip_address = "0.0.0.0/0"
    }
  }

  app_settings = {
    WEBSITE_RUN_FROM_PACKAGE = "0"
    FUNCTIONS_EXTENSION_VERSION = "~4"
    # Boas práticas de logs
    APPINSIGHTS_INSTRUMENTATIONKEY = ""
    WEBSITE_CONTENTAZUREFILECONNECTIONSTRING =
azurerm_storage_account.st_la.primary_connection_string
    WEBSITE_CONTENTSHARE = "${var.project_name}-share-${random_string.suffix.result}"
  }
}

# Integração VNet (Swift) para Logic App Standard
resource "azurerm_app_service_virtual_network_swift_connection" "la_vnet" {
  app_service_id = azurerm_logic_app_standard.la.id
  subnet_id      = azurerm_subnet.snet_logicapps.id
}

# Acesso do MI da Logic App ao Key Vault (Get/List)
resource "azurerm_key_vault_access_policy" "ap_la" {
  key_vault_id = azurerm_key_vault.kv.id
  tenant_id    = data.azurerm_client_config.current.tenant_id
  object_id    = azurerm_logic_app_standard.la.identity[0].principal_id
  secret_permissions = ["Get", "List"]
}

#####################
# API Management (APIM) com VNet (External) + MI
#####################
resource "azurerm_api_management" "apim" {
  name                = "${var.project_name}-apim-${random_string.suffix.result}"
  location            = azurerm_resource_group.rg.location
  resource_group_name = azurerm_resource_group.rg.name
```

Evaluation Only. Created with Aspose.PDF. Copyright 2002-2025 Aspose Pty Ltd.

```
  publisher_name  = "API Platform"
  publisher_email = "admin@example.com"

  sku_name = "Developer_1" # Produção: Premium_1

  virtual_network_type = "External"
  virtual_network_configuration {
    subnet_id = azurerm_subnet.snet_apim.id
  }

  identity {
    type = "SystemAssigned"
  }

  protocols {
    enable_http2 = true
  }

  # Habilitar o portal do desenvolvedor (novo portal é habilitado por padrão)
}

# Acesso do MI do APIM ao Key Vault (Get/List)
resource "azurerm_key_vault_access_policy" "ap_apim" {
  key_vault_id = azurerm_key_vault.kv.id
  tenant_id    = data.azurerm_client_config.current.tenant_id
  object_id    = azurerm_api_management.apim.identity[0].principal_id
  secret_permissions = ["Get", "List"]
}

# Named Value no APIM referenciando segredo no KV (boa prática: não embedar secrets nas policies)
resource "azurerm_api_management_named_value" "nv_hmac" {
  name                = "hmac-key"
  api_management_name = azurerm_api_management.apim.name
  resource_group_name = azurerm_resource_group.rg.name
  display_name        = "HMAC Key"
  secret              = true
  key_vault_secret_id = azurerm_key_vault_secret.apim_hmac.id
}

# API de exemplo no APIM que roteia para Logic Apps (ajuste o backend/rota conforme seu
workflow)
resource "azurerm_api_management_api" "api_orchestrations" {
  name                = "orchestrations"
  resource_group_name = azurerm_resource_group.rg.name
  api_management_name = azurerm_api_management.apim.name

  revision   = "1"
  display_name = "Orchestrations"
  path         = "orchestrations"
  protocols    = ["https"]

  # Base URL do backend: Logic App Standard (exponha um endpoint seguro no workflow)
  service_url = "https://${azurerm_logic_app_standard.la.default_hostname}"

  subscription_required = true
}

# Políticas da API: validate-jwt, CORS, rate/quotas, HSTS, mascaramento de erro
resource "azurerm_api_management_api_policy" "api_policy" {
  api_name            = azurerm_api_management_api.api_orchestrations.name
  api_management_name = azurerm_api_management.apim.name
  resource_group_name = azurerm_resource_group.rg.name

  xml_content = <<POLICY
<policies>
  <inbound>
    <base />
    <cors allow-credentials="false">
      <allowed-origins>
```

Evaluation Only. Created with Aspose.PDF. Copyright 2002-2025 Aspose Pty Ltd.

```
        ${join("\n", [for o in var.cors_allowed_origins : "<origin>${o}</origin>"])}
      </allowed-origins>
      <allowed-methods>
        <method>GET</method>
        <method>POST</method>
        <method>PUT</method>
        <method>DELETE</method>
      </allowed-methods>
      <allowed-headers>
        <header>content-type</header>
        <header>authorization</header>
        <header>x-correlation-id</header>
      </allowed-headers>
      <expose-headers>
        <header>x-correlation-id</header>
      </expose-headers>
    </cors>

    <validate-jwt header-name="Authorization" require-scheme="Bearer"
failed-validation-httpcode="401">
      <openid-config
url="https://login.microsoftonline.com/${data.azurerm_client_config.current.tenant_id}/v2.0/.well-kno
wn/openid-configuration" />
      <audiences>
        <audience>${var.oidc_audience}</audience>
      </audiences>
      <!-- Opcional: valide escopos/roles -->
      <!--
      <required-claims>
        <claim name="scp">
          <value>api.read</value>
        </claim>
      </required-claims>
      -->
      <clock-skew>PT60S</clock-skew>
    </validate-jwt>

    <rate-limit calls="${var.rate_limit_per_minute}" renewal-period="60" />
    <quota calls="${var.quota_calls_per_hour}" renewal-period="3600" />

    <set-header name="Strict-Transport-Security" exists-action="override">
      <value>max-age=31536000; includeSubDomains</value>
    </set-header>

    <set-header name="x-correlation-id" exists-action="override">
      <value>@(context.RequestId)</value>
    </set-header>
  </inbound>

  <backend>
    <base />
  </backend>

  <outbound>
    <base />
    <!-- Remover detalhes internos de cabeçalhos -->
    <set-header name="Server" exists-action="delete" />
    <set-header name="X-Powered-By" exists-action="delete" />
  </outbound>

  <on-error>
    <base />
    <return-response>
      <set-status code="500" reason="Internal Server Error" />
      <set-header name="Content-Type" exists-action="override">
        <value>application/json</value>
      </set-header>
      <set-body>@("{""error"":""Unexpected error"",""id"":""" + context.RequestId +
"""}")</set-body>
```

Evaluation Only. Created with Aspose.PDF. Copyright 2002-2025 Aspose Pty Ltd.

```
    </return-response>
  </on-error>
</policies>
POLICY
}

#####################
# Diagnósticos → Log Analytics
#####################
resource "azurerm_monitor_diagnostic_setting" "diag_apim" {
  name                       = "diag-apim"
  target_resource_id         = azurerm_api_management.apim.id
  log_analytics_workspace_id = azurerm_log_analytics_workspace.law.id

  enabled_log {
    category = "GatewayLogs"
  }
  enabled_log {
    category = "WebSocketConnectionLogs"
  }
  enabled_log {
    category = "AuditLogs"
  }
  metric {
    category = "AllMetrics"
  }
}

resource "azurerm_monitor_diagnostic_setting" "diag_la" {
  name                       = "diag-logicapps"
  target_resource_id         = azurerm_logic_app_standard.la.id
  log_analytics_workspace_id = azurerm_log_analytics_workspace.law.id

  enabled_log { category = "AppServiceHTTPLogs" }
  enabled_log { category = "AppServiceConsoleLogs" }
  enabled_log { category = "AppServiceAppLogs" }
  metric { category = "AllMetrics" }
}

resource "azurerm_monitor_diagnostic_setting" "diag_kv" {
  name                       = "diag-keyvault"
  target_resource_id         = azurerm_key_vault.kv.id
  log_analytics_workspace_id = azurerm_log_analytics_workspace.law.id

  enabled_log { category = "AuditEvent" }
  metric { category = "AllMetrics" }
}

#####################
# Saídas
#####################
output "apim_gateway_hostname" {
  value = azurerm_api_management.apim.gateway_regional_url
}

output "developer_portal_url" {
  value = azurerm_api_management.apim.developer_portal_url
}

output "logic_app_hostname" {
  value = azurerm_logic_app_standard.la.default_hostname
}

output "key_vault_name" {
  value = azurerm_key_vault.kv.name
}
```

Pontos importantes e próximos passos

Evaluation Only. Created with Aspose.PDF. Copyright 2002-2025 Aspose Pty Ltd.

- Entra ID:
  - Crie/ajuste as App Registrations (cliente e recurso) com PKCE, escopos mínimos e tokens curtos. Atualize var.oidc_audience com o App ID URI da API.
  - Habilite Conditional Access + MFA para contas humanas. Use Managed Identity para chamadas entre serviços.
- Logic Apps:
  - Defina workflows com triggers HTTP seguros (mTLS/OAuth/HMAC). Bloqueie triggers públicos. Faça schema validation e sanitização de entrada.
  - Se o workflow precisar acessar outros serviços privados (ex.: SQL/Cosmos), crie os Private Endpoints e Private DNS correspondentes.
- APIM:
  - Ajuste CORS para origens específicas e reduza métodos/headers ao mínimo.
  - Considere usar gateways privados/VNet-internal + Front Door/AppGW WAF na borda para ambientes de produção.
  - Publique APIs com contratos OpenAPI; aplique validação de schema.
- Observabilidade:
  - Construa consultas KQL, alertas e dashboards. Integre com SIEM/SOAR.
- Governança:
  - Use PRs/CI para aplicar Terraform com validações (tfsec/checkov). Aplique Azure Policy para reforçar TLS, Private Endpoints e criptografia.
- Segurança de rede:
  - Segregue sub-redes, aplique NSGs/ASGs. Considere Azure Firewall/WAF e DDoS Standard (já incluso).
- Dados e segredos:
  - Centralize segredos no Key Vault (já incluso) e rotacione certificados/chaves. Ative purge protection (já incluso).

Este material serve como base segura e extensível. Em produção, substitua o SKU do APIM para Premium, torne o gateway privado, finalize fluxos de Private Link aos backends e reforce autenticação dos triggers/operadores conforme compliance do seu ambiente.