SENTINET

Sentinet for Microsoft Azure

SENTINET

Nevatech

Contents

Introduction

Microsoft Azure is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through a global network of Microsoft-managed data centers.

Sentinet™ is a comprehensive API Management and API Governance platform created by Nevatech for helping organizations govern and manage their SOA and API solutions during their entire life-cycle.

Sentinet is a unique API and SOA Management Infrastructure, as it is the only enterprise class solution in the market written in .NET and it provides a unified approach for securing, governing and managing organizations' APIs and services for on-premises, cloud and hybrid environments. Sentinet provides unique benefits, native integration, deployment options and extensibility features for the Microsoft Azure cloud platform. Sentinet is certified with ***Powered by Microsoft Azure, Certified for Windows Server 2016, Windows 2012*** and ***Works for Windows 2008 R2 Server***.

All enterprise service applications face the same common infrastructural challenges – services availability and accessibility, discovery, description, security, monitoring, auditing, service agreements and service level objectives management, alerting, and many more. These common infrastructural challenges are particularly important for organizations which deploy their APIs in the cloud in which they have limited control over operational environments in comparison to on-premises deployments. Common infrastructural challenges are typically not a part of an organization's core business and can be addressed by middleware infrastructure products. These products will save time, resources, and provide organizations with the confidence of their APIs' accessibility, security, visibility and control. Development teams are enabled with faster time-to-market delivery of their cloud-based solutions, while operations teams are equipped with tools and procedures to manage and maintain cloud-based production systems in a consistent, reliable and predictable environment.

Sentinet is particularly beneficial for cloud-based services and applications in that they can be easily be placed under comprehensive management using Sentinet's non-invasive services virtualization capabilities.

Customer Benefits

Sentinet provides an array of benefits and management capabilities to a customers' cloud APIs and SOA services. These are the same benefits described in the **Sentinet Overview** whitepaper with the additional benefits specific to cloud environments in general, and to the Microsoft Azure cloud platform specifically, such as:

- Integration with Microsoft Azure security infrastructure and technology stacks.
- Integration with Microsoft Azure-specific communication transports and protocols.
- Mediation between interoperable and Microsoft Azure-specific protocols and security models.
- Enablement of APIs and services with Microsoft Azure communication protocols and security models.

- Native Microsoft Azure deployment models and topologies.
- Native integration with and extensibility of the:
    - Microsoft Azure Active Directory (AAD) service capabilities.
    - Microsoft Azure Service Bus relaying capabilities.
    - Microsoft Azure Service Bus Queues, Topics, Subscriptions and asynchronous messaging capabilities.
- Native packaging option for Sentinet management infrastructure components with the customer's APIs and SOA services.

Deployment Topologies

Sentinet infrastructure consists of the following components:

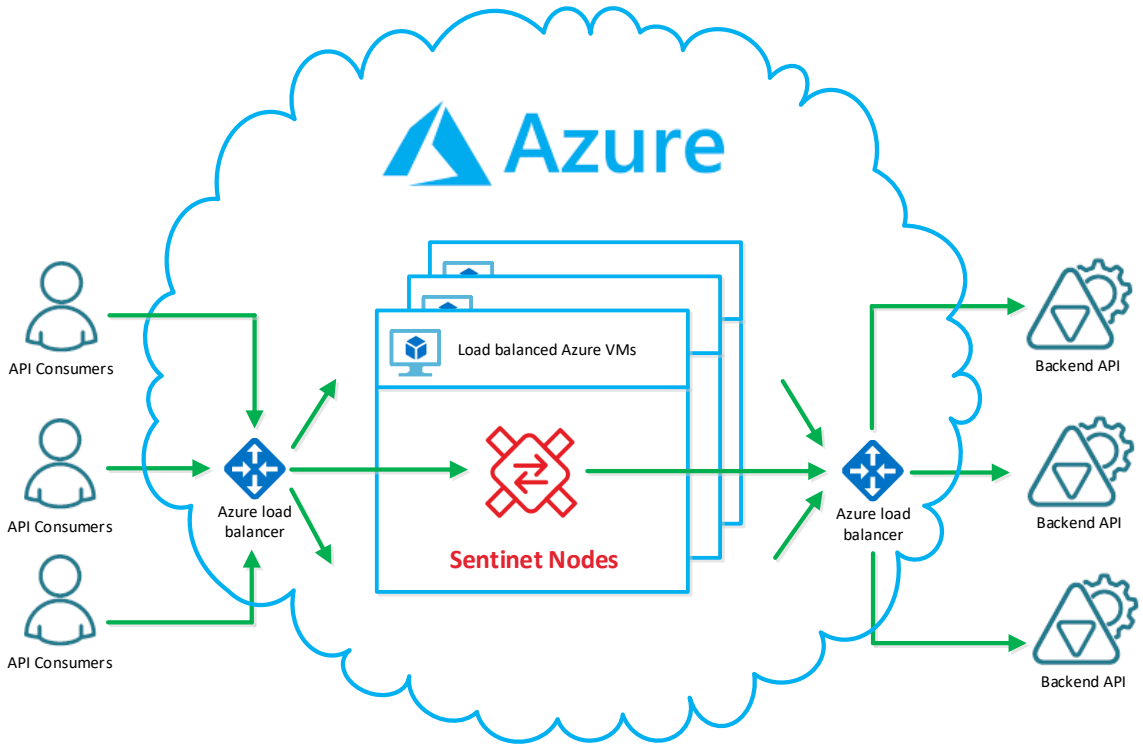
- **Sentinet Nodes** (API Gateways)
- **Sentinet Repository Web Services Application** (Sentinet Management Services)
- **Sentinet Repository database**

Sentinet natively supports Microsoft Azure deployment topologies and execution models. Sentinet's distributed architecture allows any, or all of its components to be deployed in the cloud, on-premises, or to be spread through multiple diverse network environments. At the same time, customers' APIs and services managed by the Sentinet Nodes can also be located in the cloud or spread throughout different cloud and private networks. In general, Sentinet deployment topologies can be categorized by the Sentinet Nodes' locations relative to the managed backend cloud or on-premises APIs. These topologies are described as **Cloud** and **Hybrid** deployment models.

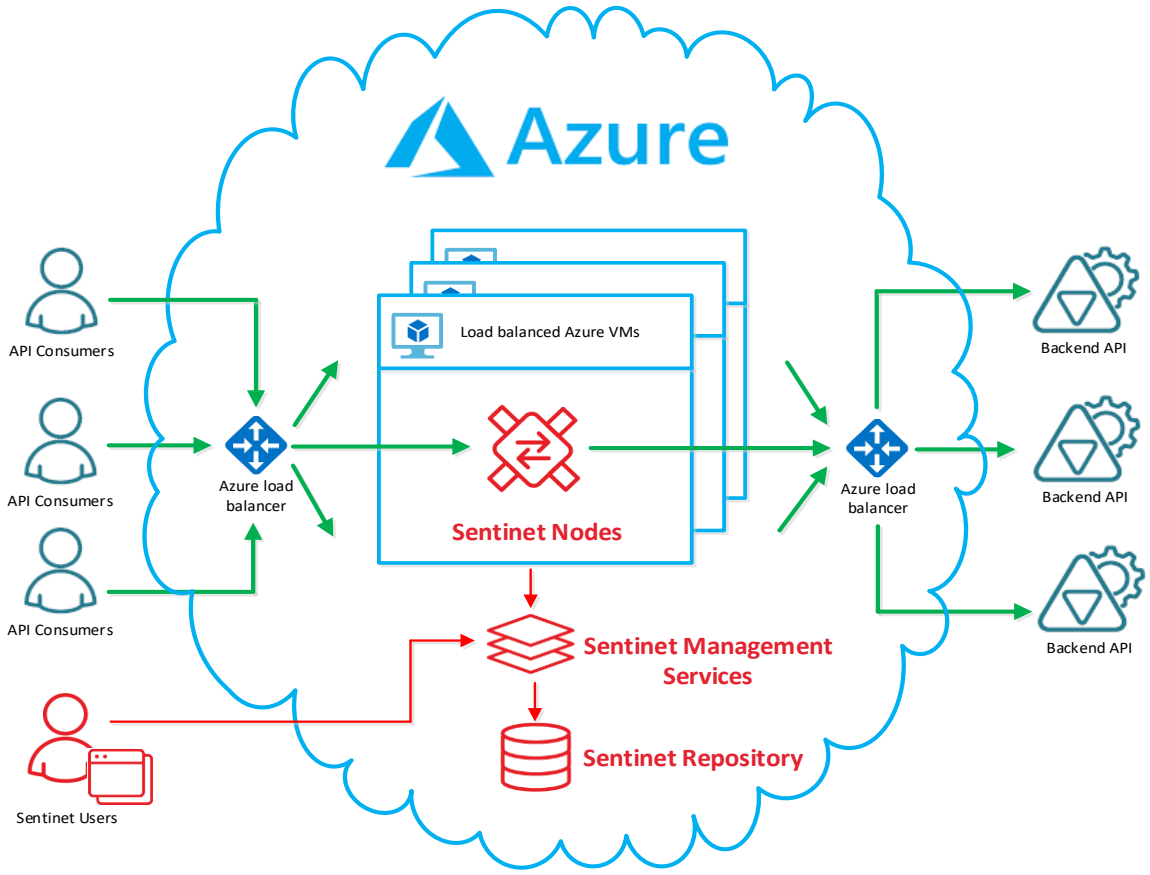
Cloud Deployment Model

In this deployment model, the Sentinet software components are hosted as native Microsoft Azure applications entirely deployed in the cloud.

The diagram below shows Sentinet Nodes (Sentinet API Gateways) deployed in the Microsoft Azure cloud, where they can be scaled using Azure's built-in scalability services. The API Consumer applications and the Backend APIs may also run in Azure, or in any other cloud, public or private network.



If all Sentinet components are deployed in the cloud, Sentinet is called to be in a **Cloud Model**. The diagram below shows extended version of the previous diagram.



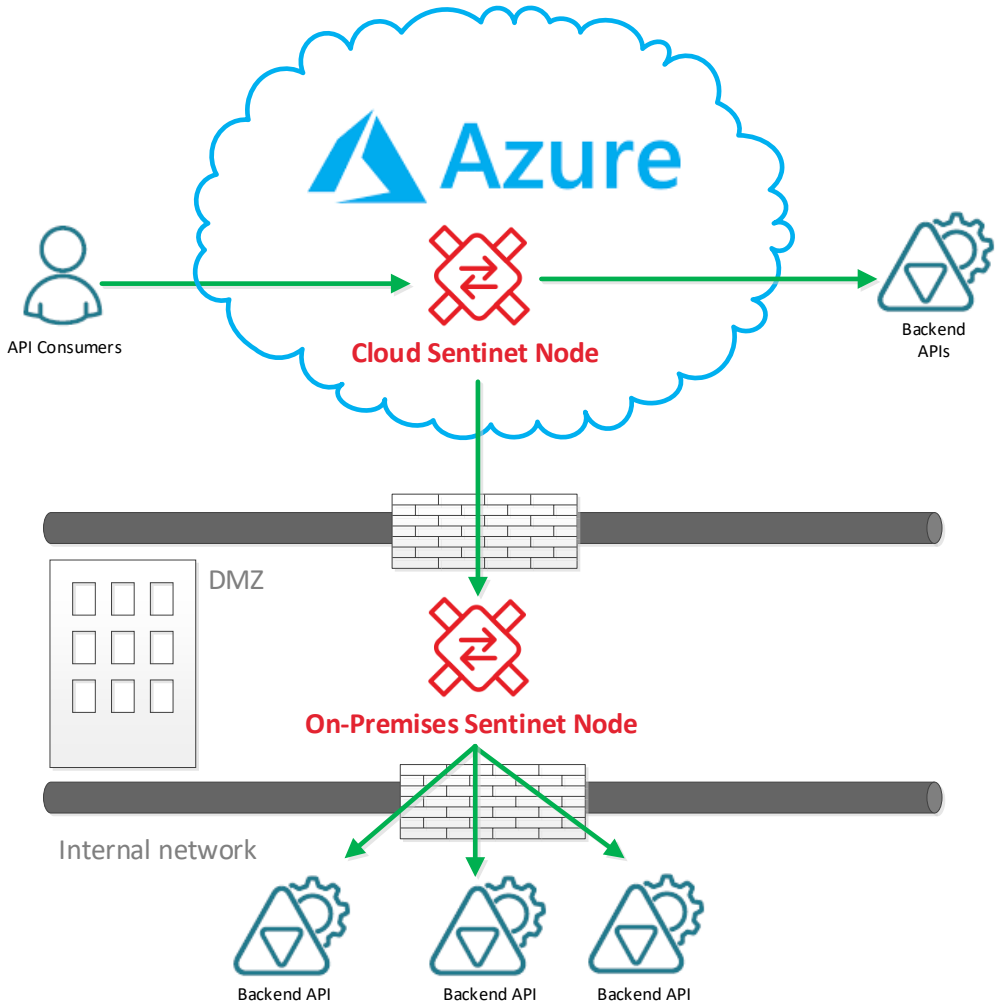
The Sentinet Repository can be a dedicated Azure SQL Server or an Azure SQL Database.

Sentinet Administrators and Sentinet Users control the entire infrastructure using a highly secure Web Interface, which is also provided by the Sentinet Management Services. A Rich Web User Interface application, the Sentinet Administrative Console leverages modern JavaScript and HTML5 technologies to ensure a "desktop-like" level of interactivity.

Hybrid Deployment Model

In this deployment model, Sentinet components can be spread throughout the cloud and on-premises environments, while being managed and controlled centrally by Sentinet administrators through the same Sentinet Administrative Console application. For example, Sentinet Nodes may remain in the cloud, while both Sentinet Management Services and the Sentinet Repository remain in the private network.

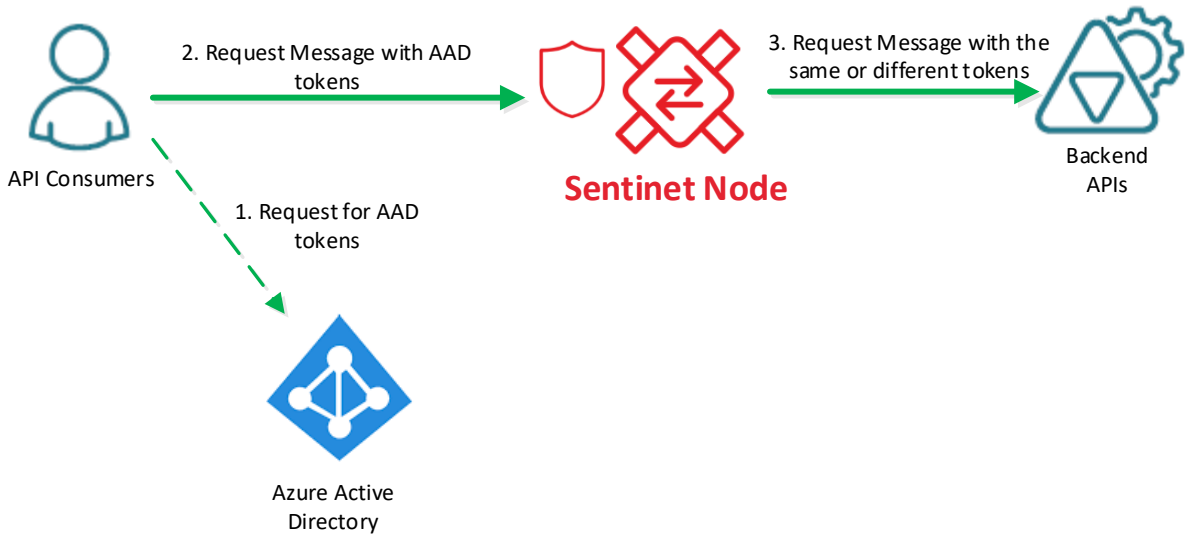
The hybrid deployment model often targets API and SOA architectures with business services and APIs spread over multiple environments, or when the Sentinet Nodes are meant to mediate communication between consumer and service applications providing full transparency of the underlying Microsoft Azure transport and security protocols. Internal corporate services can be safely protected by an internal On-Premises Sentinet Node.



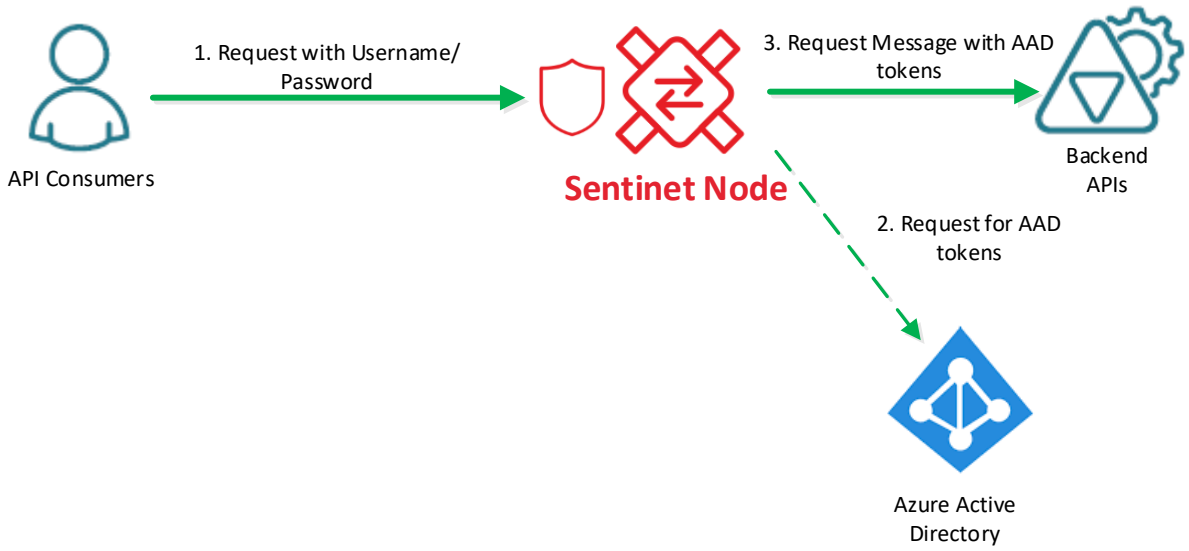
Integration with Microsoft Azure Active Directory

Modern security models and cloud platforms promote Federated Security and Single-Sign-On architectures. Microsoft Azure is no exception as it not only facilitates Federated Security, it also requires it in many cases and scenarios. Sentinet fully supports Microsoft Azure Federated Security architectures and extends their capabilities by enhanced integration with Microsoft Azure Active Directory (AAD).

Business services and APIs deployed in the cloud can be remotely configured with Federated Security and integration with Microsoft Azure Active Directory through the Sentinet Node's dynamic virtual endpoints. By leveraging Sentinet, business services can be non-invasively enabled to understand and process security tokens and claims issued by a Microsoft Azure Active Directory. Moreover, a Sentinet Node can act as an active Access Control Claims Processor by enforcing dynamic authorization rules that Sentinet administrators create and apply remotely to services and APIs. Backend services and APIs do not have to have any capability or knowledge to understand and integrate with Azure Active Directory, Sentinet will assume this responsivity on their behalf, providing Backend APIs with any other required security model.



Additionally, Sentinet can help consumer applications to integrate with Microsoft Azure Active Directory by mediating traditional security and AAD-integrated security. Imagine an application that runs on a mobile device that cannot be enabled with complex OAuth-based security and is using the traditional https protocol with username/password credentials. The Sentinet Node can accept messages sent by a mobile application and exchange the provided credentials with OAuth tokens issued by Microsoft Azure Active Directory on behalf of the mobile application. Administrators only have to configure credentials mapping with Microsoft Azure Active Directory (the same way it has to be configured without Sentinet Node).

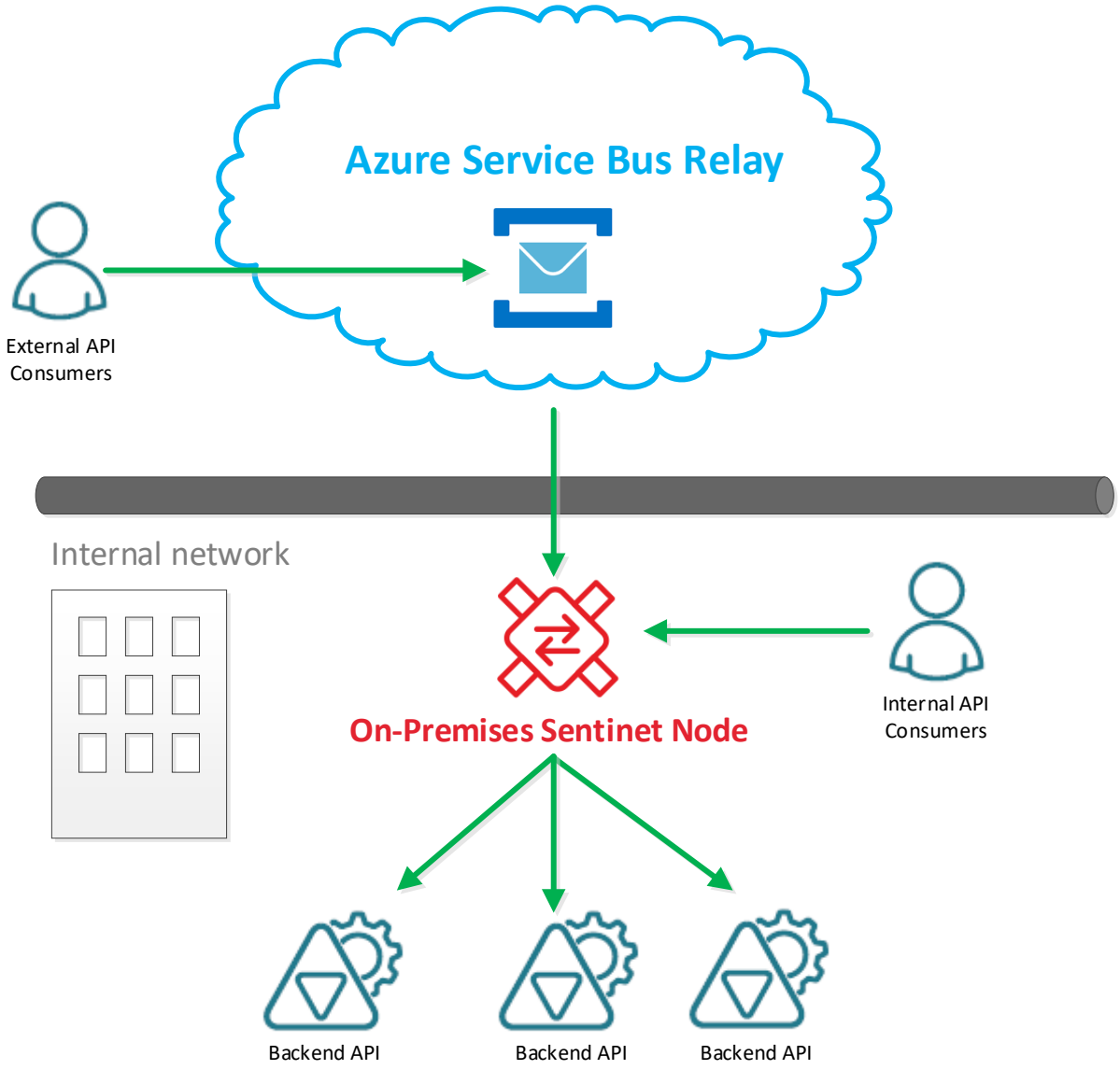


Integration with Microsoft Azure Service Bus Relay

Sentinet provides on-premises services and APIs with easy interactions to external parties with whom integration is desired, without needing complex firewall and security infrastructure. Sentinet Nodes are designed to natively integrate with Microsoft Azure Service Bus. They can be dynamically and remotely configured with Azure Service Bus endpoints encapsulating Service Bus non-interoperable protocols and Microsoft Azure Active Directory security identities.

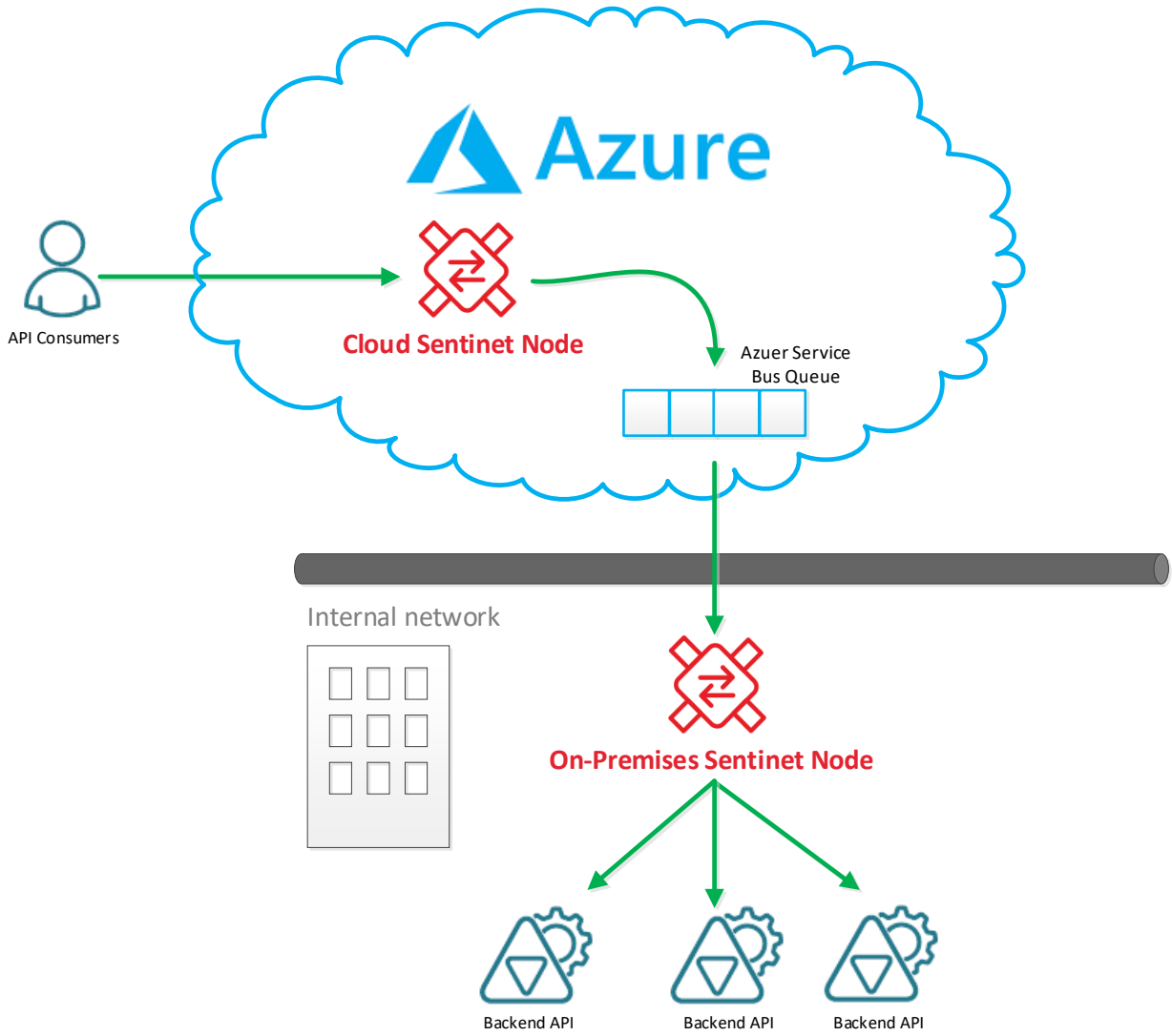
Without Sentinet, and in order to join Microsoft Azure Service Bus infrastructure, on-premises business services and APIs must be configured to use special WCF bindings, and with Microsoft Azure subscription's security keys, which is neither a scalable deployment model nor secure enough (all business services have to be given knowledge of the subscription security keys).

By using Sentinet, any SOAP service or a RESTful API (even a non-Microsoft service), can be on-boarded onto the Microsoft Azure Service Bus infrastructure without reconfiguration, redeployment or potentially compromising security keys. Sentinet administrators can remotely configure Sentinet Nodes to dynamically open and manage Microsoft Azure Service Bus endpoints and authenticate virtual services with the Microsoft Azure Active Directory. Service Bus security keys are stored in the central Sentinet Repository and securely delivered to the Sentinet Nodes when they have to open Microsoft Azure Service Bus endpoints. Moreover, Sentinet Nodes can be configured side-by-side with Service Bus endpoints and additional internal endpoints for testing and staging. Sentinet Administrators get full visibility and control over endpoints exposed via Microsoft Azure Service Bus, and they can remotely and dynamically take Service Bus endpoints offline or reconfigure them with new or additional security, access rules, monitoring and Service Level Agreements.


Azure Service Bus Relay
External API Consumers
Internal network
On-Premises Sentinet Node
Internal API Consumers
Backend API
Backend API
Backend API

Integration with Microsoft Azure Asynchronous Messaging

Sentinet provides SOA services and APIs with asynchronous messaging with automatic load-leveling by tightly integrating with Microsoft Azure Service Bus Queues, Topics and Subscriptions. Consumer applications and service applications can be completely decoupled from any knowledge and mechanics of Microsoft Azure queuing while staying enabled to handle load-leveling with asynchronous messages delivery.



Summary

Sentinet makes it easy to secure and manage services and APIs, whether on-premises or in the cloud. The seamless and native integration to Microsoft's (sometimes non-interoperable) technology stack makes Sentinet the first choice when implementing an API Management platform for companies with a predominant Microsoft IT strategy.