SENTINET

Sentinet for Windows Azure

VERSION 2.2

Nevatech

Contents

Introduction

Microsoft Windows Azure is an open and flexible cloud platform that enables organizations to quickly build, deploy and manage applications across a global network of Microsoft-managed datacenters.

Nevatech Sentinet™ platform, a comprehensive SOA Management Infrastructure and services virtualization middleware software solution, helps organizations to govern and manage their SOA and API cloud-based solutions during their entire life-cycle. Sentinet is a unique SOA and API Management Infrastructure because it provides a unified approach for governing and managing organizations' APIs for on-premises, cloud and hybrid environments. Sentinet provides particular benefits, native integration, deployment options and extensibility features, for the Microsoft Windows Azure cloud platform. Sentinet is certified with ***Works for Windows 2008 R2 Server***, ***Certified for Windows Server 2012*** and ***Powered by Windows Azure***.

All enterprise service applications face the same common infrastructural challenges – services' availability and accessibility, discovery, security, monitoring, auditing, service agreements and service level objectives management, alerting, and many others. These common infrastructural challenges are particularly important for organizations that deploy their APIs in the cloud where organizations might have limited control over operational environments compared with on-premises deployments. Common infrastructural challenges are typically not part of an organization's core business and can be addressed by middleware infrastructure tools and products that save time and 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 and predictable environment.

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

Customer Benefits

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

- Integration with Windows Azure security infrastructure and technology stacks.
- Integration with Windows Azure-specific communication transports and protocols.
- Mediation between interoperable and Windows Azure-specific protocols and security models.
- APIs' and services' enablement with Windows Azure communication protocols and security models.
- Native integration with and extensibility of the Windows Azure Access Control Service capabilities.

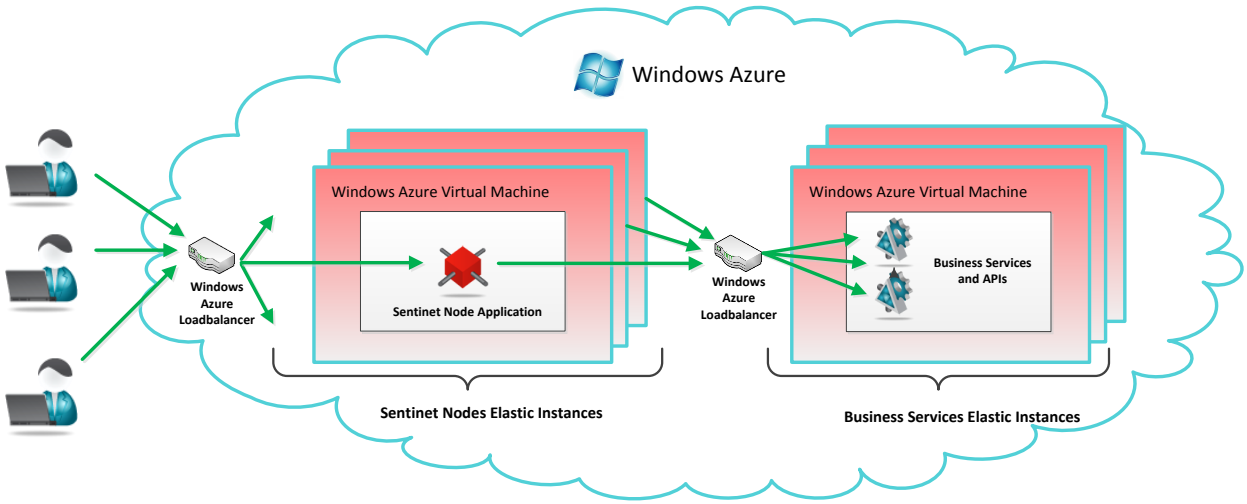
- Native integration with, and extensibility of, the Windows Azure Service Bus relaying capabilities.
- Native integration with, and extensibility of, the Windows Azure Service Bus Queues, Topics, Subscriptions and asynchronous messaging capabilities.
- Native Windows Azure deployment models and topologies.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

Deployment Topologies

Sentinet supports variety of flexible Windows Azure deployment topologies. Sentinet's components-based 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. **Sentinet Overview** whitepaper describes Sentinet architecture Customers' API services managed by the Sentinet Nodes can also be located all in the cloud or spread through cloud and private networks. In general, Sentinet deployment topologies can be categorized by the Sentinet Nodes' locations relative to managed cloud or on-premises services and include **Isolated**, **Collocated** and **Hybrid** deployment models.

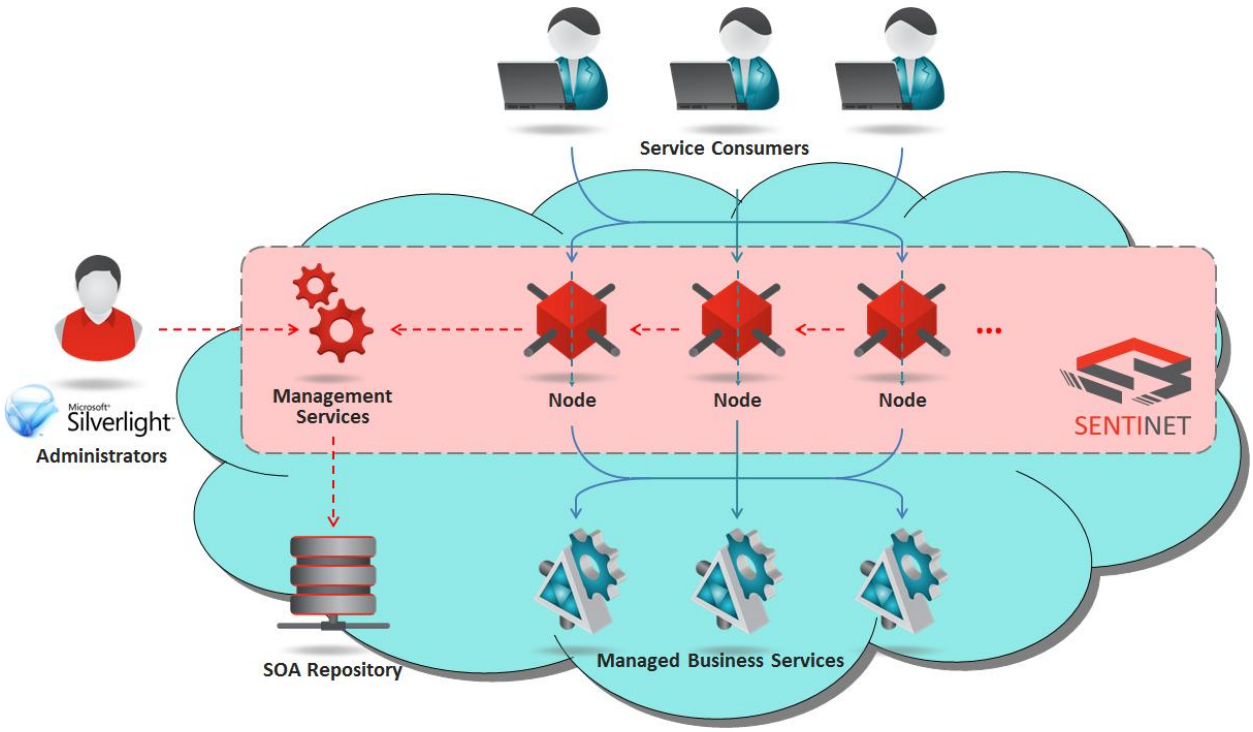
Isolated Deployment Model

In this deployment model, Sentinet software infrastructure is hosted as native Windows Azure applications, isolated from the customer's business services and applications.

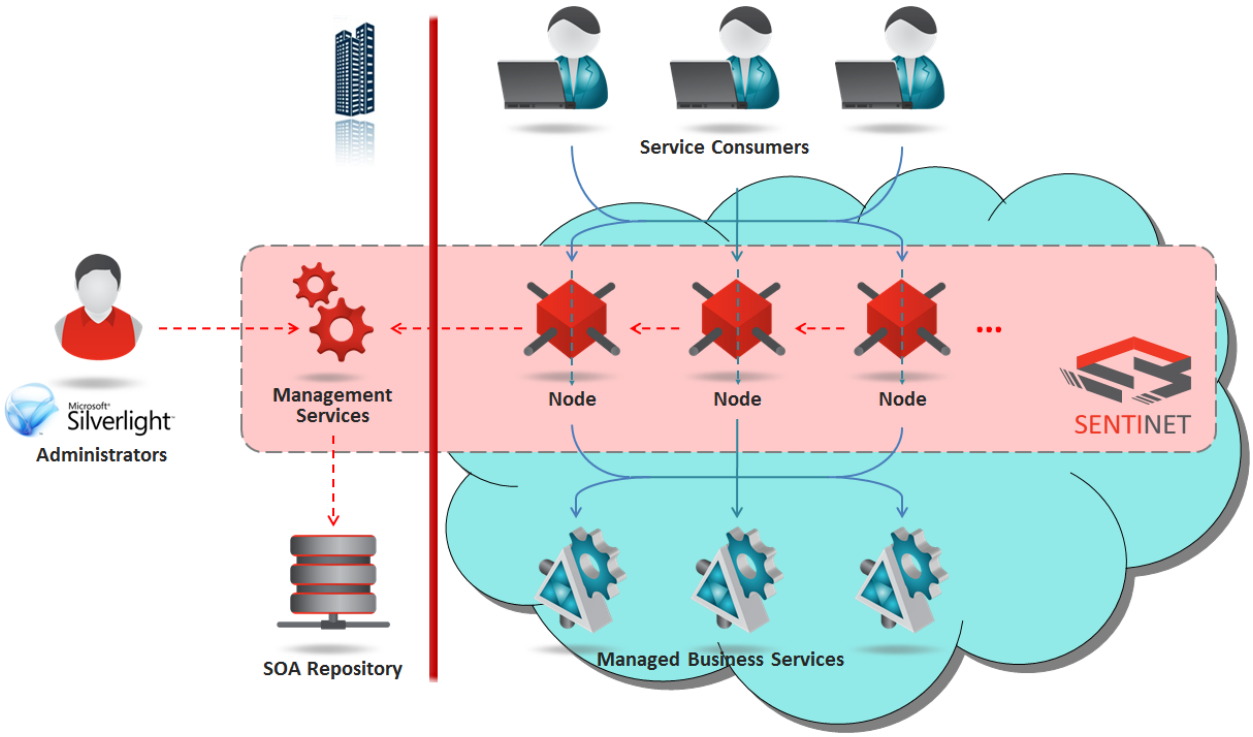


Sentinet Nodes can be deployed as native Windows Azure Cloud Services Web Roles or Virtual Machines, http://www.windowsazure.com/en-us/develop/net/fundamentals/intro-to-windows-azure/#models.

Sentinet Management Services application can also be deployed in the Windows Azure cloud along with the Sentinet Repository SQL Database, so that the entire business solution and its management infrastructure are cloud-based.

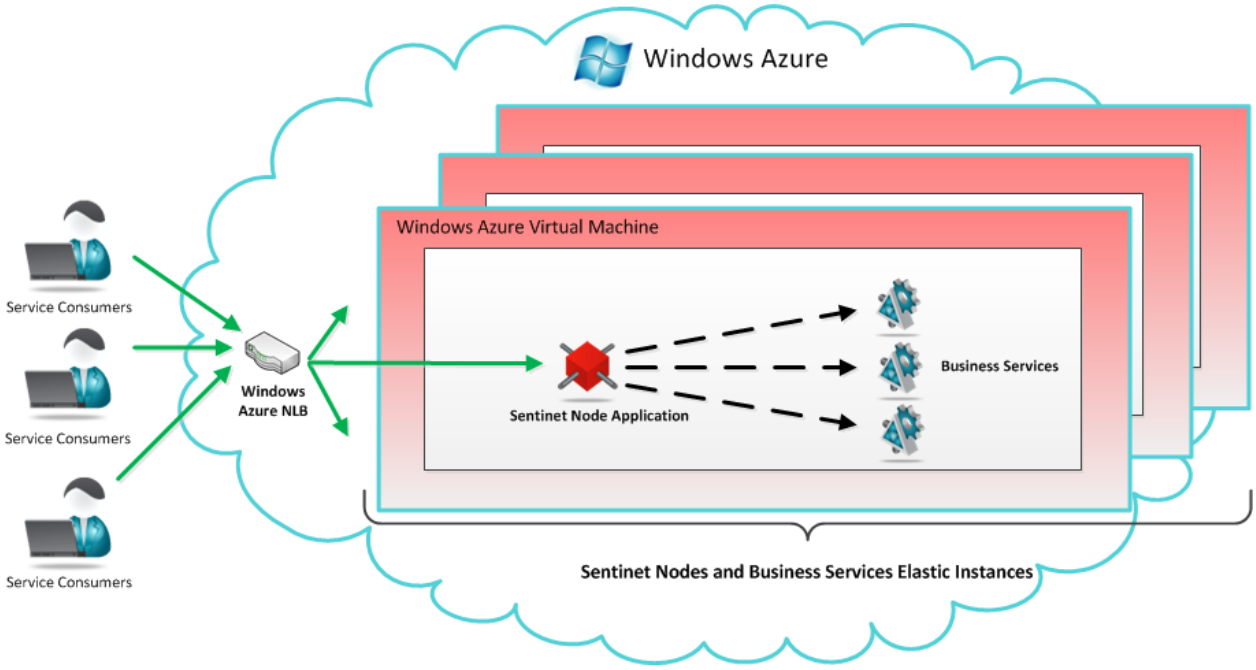


Another deployment option is when Sentinet Management Services application and Sentinet Repository SQL Database are deployed inside the corporate network while Sentinet Nodes and business services remain cloud-based.



Collocated Deployment Model

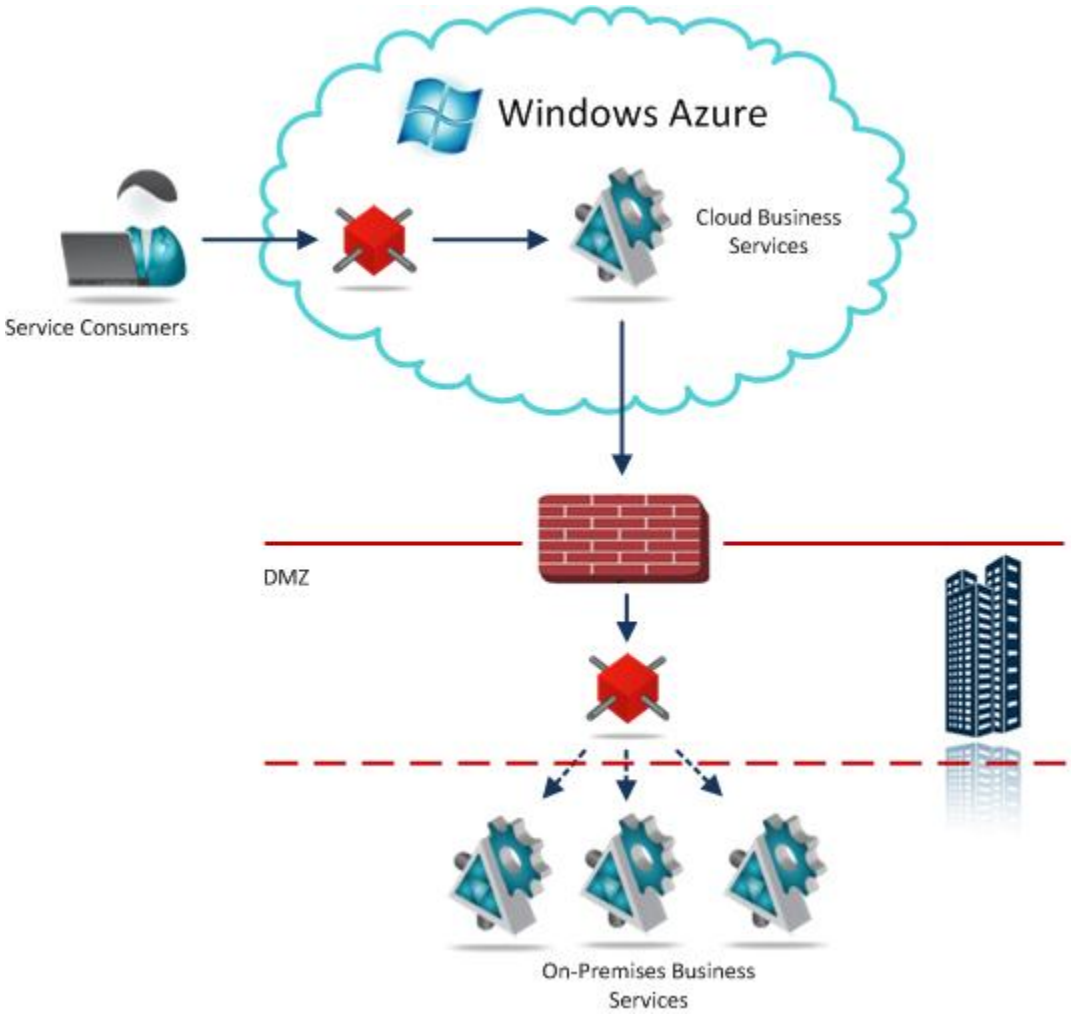
In this deployment model, Sentinet Nodes are deployed as applications packaged (or collocated) with the business service applications, effectively running on the same Windows Azure virtual machines.



Sentinet Node applications can now communicate with business services using local machine, high-performance, and inherently secure communication protocols such as *net.pipe* protocol. By using collocated deployment model business services and customers' APIs are guaranteed to be secure (services cannot be accessed from other computers, unless they are accessed through a Sentinet Node), and there are no additional network latencies because *net.pipe* transport is the most effective local cross-process communication. Sentinet administrators remotely configure Sentinet Node's dynamic endpoints and provide business services with required accessibility, security, monitoring, access control, SLAs management, and other automated design-time and run-time management capabilities.

Hybrid Deployment Model

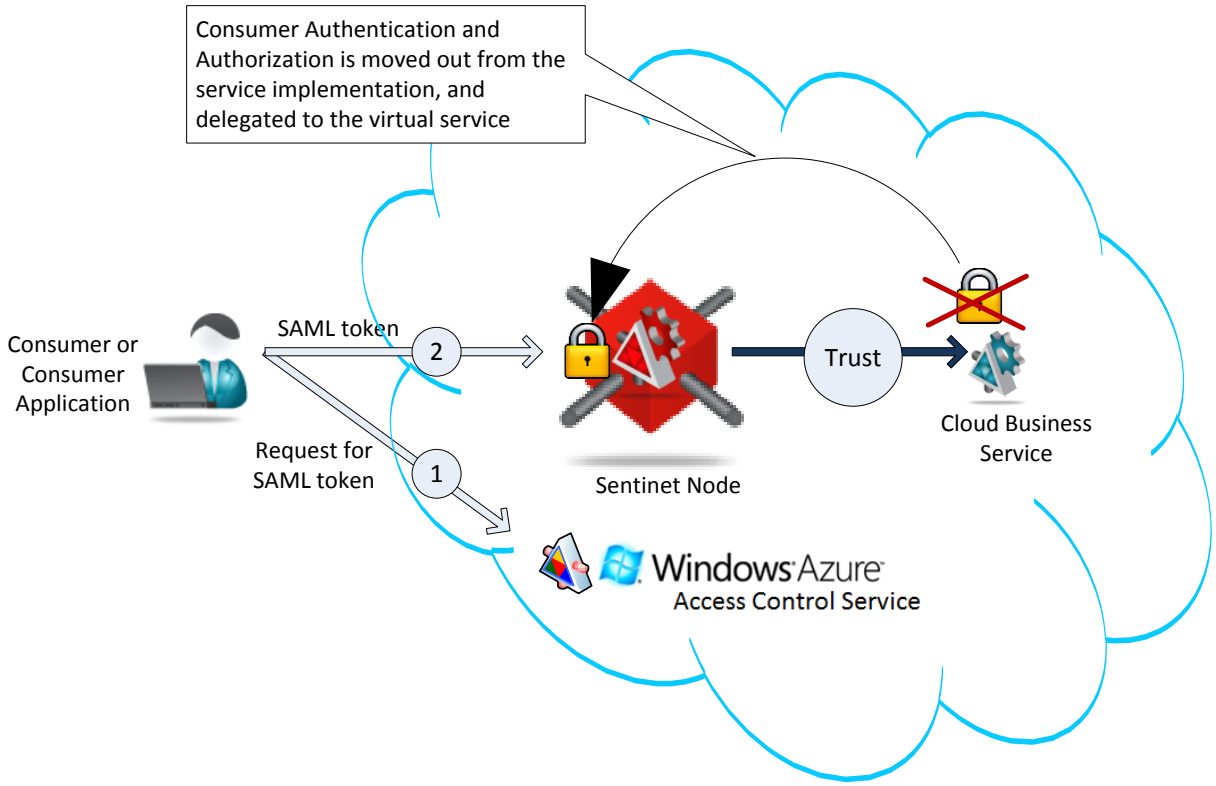
In this deployment model, Sentinet Nodes are spread through the cloud and on-premises environments while being managed and controlled centrally by the Sentinet administrators through the same SOA Repository application. The hybrid deployment model targets SOA architectures where business services are also spread through multiple environments, or when Sentinet Nodes are meant to mediate communication between consumer and service applications providing full transparency of the underlying Windows Azure transport and security protocols.



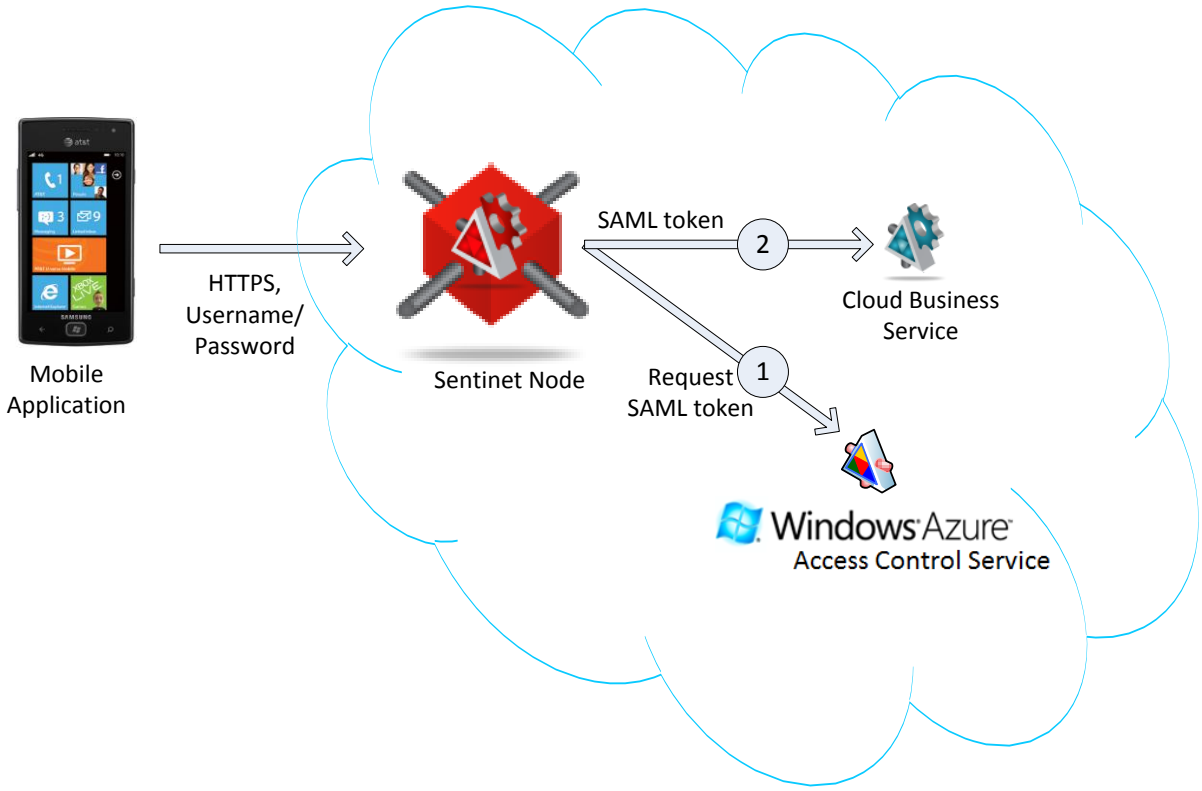
Integration with Windows Azure Access Control Service

Modern security models and cloud platforms promote Federated Security and Single-Sign-On architectures. Windows Azure cloud platform is no exception. Not only does Windows Azure facilitate Federated Security, it also requires it in many cases and scenarios. Sentinet platform fully supports Windows Azure Federated Security architectures and extends their capabilities by enhanced integration with Windows Azure Access Control Service (ACS).

Business services and APIs deployed in the cloud can be remotely configured with Federated Security and integration with Windows Azure ACS through Sentinet Node's dynamic virtual endpoints. By leveraging Sentinet, business services can be non-invasively enabled to understand and process SAML claims issued by Windows Azure ACS. Moreover, Sentinet Node can act as an active ACS claims processor by enforcing dynamic authorization rules that Sentinet administrators create and apply remotely to their virtual services.



Additionally, Sentinet can help consumer applications to integrate with Windows Azure ACS by mediating traditional security and ACS-integrated security. Imagine an application that runs on a mobile device that cannot be enabled with complex SAML-based security and is using traditional https protocol with username/password credentials. Sentinet Node can accept messages sent by a mobile application and exchange provided credentials for SAML tokens issued by Windows Azure ACS on behalf of a mobile application. Administrators will have to configure credentials mapping only with Windows Azure ACS (just as if it had to be configured without Sentinet Node).



Integration with Windows Azure Service Bus Relay

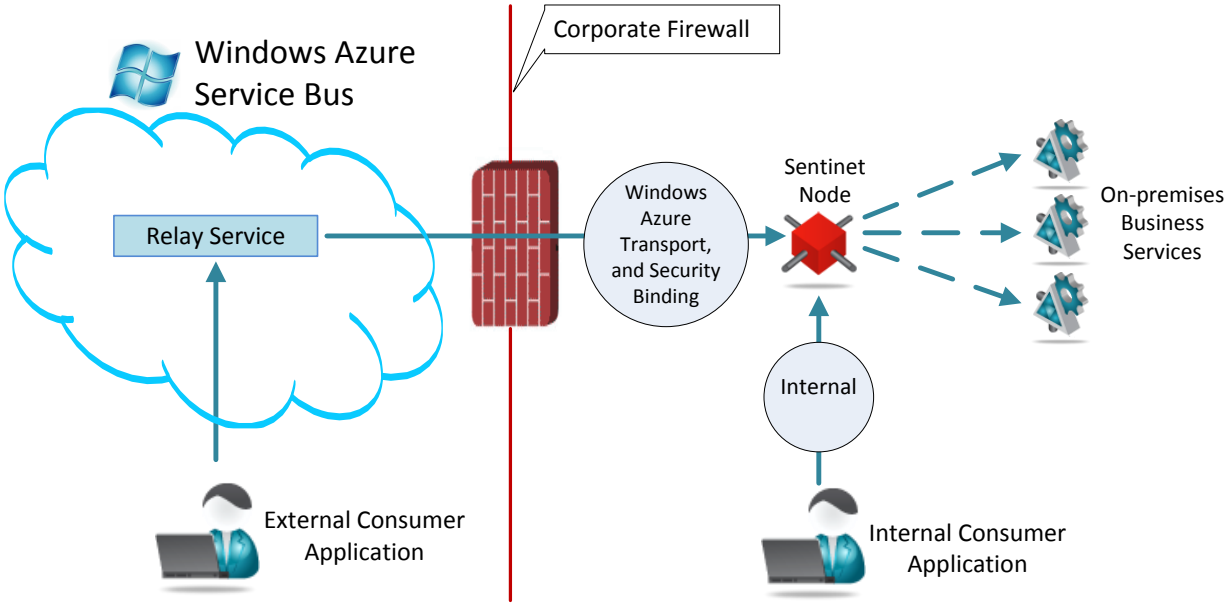
Sentinet provides on-premises SOA services and APIs with easy interactions to external parties with whom integration is desired, without needing complex firewall and security infrastructure. Sentinet Nodes are designed to natively integrate with Windows Azure Service Bus and Windows Azure Access Control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

In order to join Windows Azure Service Bus infrastructure, on-premises business services have to be reconfigured to use special WCF bindings, and configured with Windows Azure subscription's security keys, which is neither a scalable deployment model nor secure enough (all business services have to be given knowledge of subscription security keys).

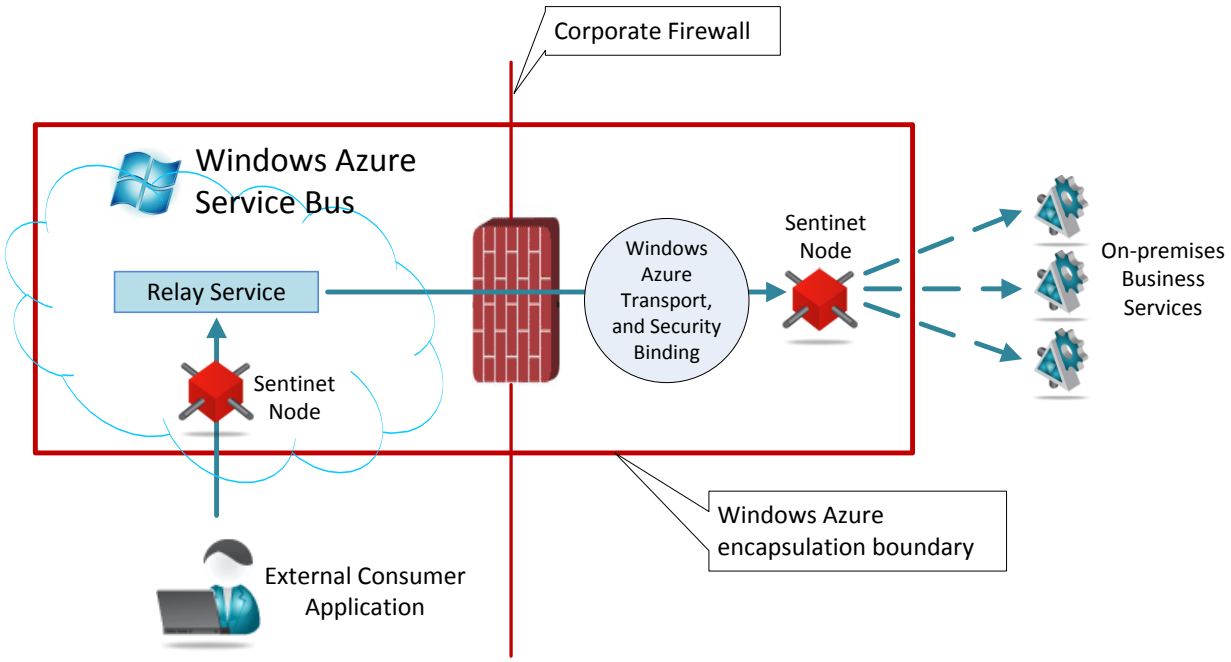
For example, as stated by Microsoft Customer Advisory team (http://windowsazurecat.com/2010/08/leveraging-wcf-extensibility-to-simplify-secure-integration-of-biztalk-server-with-windows-azure-service-bus/), the challenge is that "in a complex composite application that involves both a BizTalk and a Cloud element of the solution architecture, the number of friction points that define how these solution elements interoperate with each other can be substantial. For example, there may well be a large number of Receive Ports configured in the BizTalk environment, each servicing different needs and exposing distinct service contracts. In addition, the on-premise BizTalk solution may be communicating through the Service Bus with a number of services each

requiring a dedicated Send Port configured with WCF-Custom adapter and appropriate Service Bus WCF binding".

By using Sentinet software platform, any service (even a non-Microsoft service), can be on-boarded onto Windows Azure Service Bus infrastructure without any reconfigurations, redeployments or potential security keys compromises. Sentinet administrators can remotely configure Sentinet Nodes to dynamically open and manage Windows Azure Service Bus endpoints and authenticate virtual services with the Windows Azure ACS service. Service Bus security keys are stored in the central Sentinet SOA Repository and securely delivered to the Sentinet Nodes when they have to open Windows 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 Windows Azure Service Bus, and can remotely and dynamically take Service Bus endpoints offline or reconfigure them with new or additional security, access rules, monitoring and SLAs.



Sentinet Nodes can also be deployed in the hybrid deployment scenarious, where some Nodes are deployed on-premises while others are in the cloud. Both consumer and service applications can be fully decoupled (encapsulated) from Windows Azure Service Bus specific APIs and security configurations.



Integration with Windows Azure Asynchronous Messaging

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