SENTINET

Sentinet for BizTalk Server

SENTINET

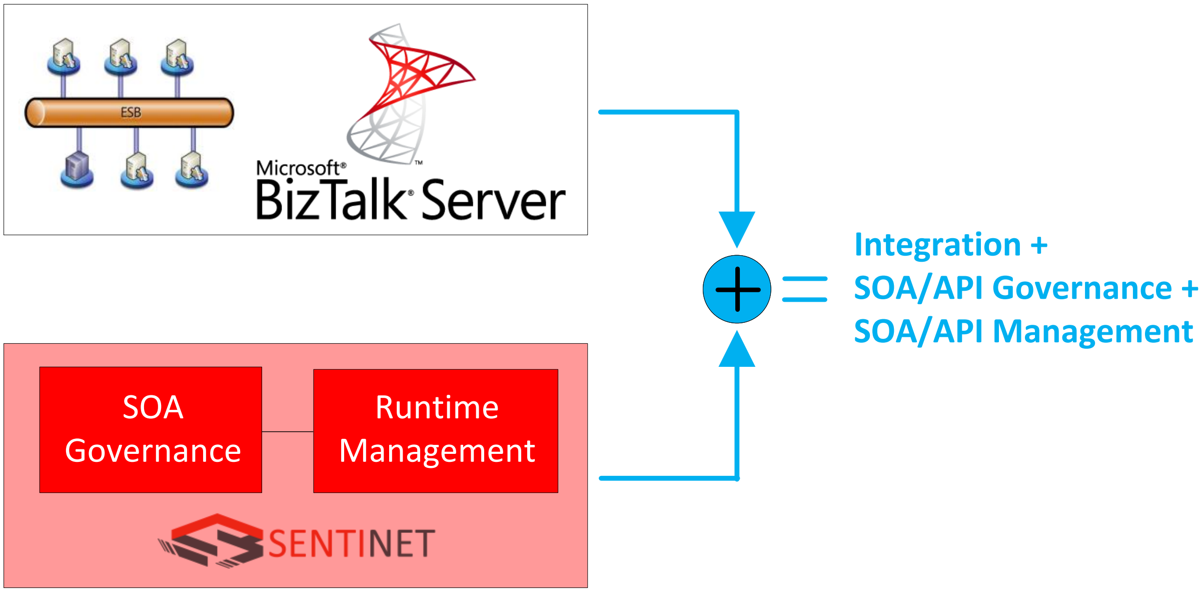
Nevatech

Contents

Introduction

BizTalk Server is Microsoft's integration and connectivity server solution. BizTalk Server provides a solution that allows organizations to more easily connect disparate systems. Including over 25 multi-platform adapters and a robust messaging infrastructure, BizTalk Server provides connectivity between core systems both inside and outside your organization, and for on-premises, cloud and hybrid environments.

Nevatech Sentinet™ is a comprehensive SOA Governance and API Management software infrastructure and services virtualization middleware solution. Sentinet supports industry SOAP and REST standards as well as Microsoft specific technologies and includes an API Repository for API Governance, API versioning, services discovery, description, publishing and Lifecycle Management (for both design-time Governance and runtime Management challenges). Sentinet API Gateway provides APIs with realt-time Monitoring, Security (Authentication and Authorization), Service Agreements Management, Alerting, Analytics and many more features that make it the perfect choice for Microsoft customers, particularly those, whose integration solutions are built on, or integrated with, the Microsoft BizTalk Server platform by extending them with managed governance and runtime agility.



Sentinet is the only SOA Governance and Management Infrastructure that is built entirely on a Microsoft platform and natively integrates with Microsoft technologies and products. It extends SOA solutions' capabilities, speeds up development, and simplifies operational and maintenance processes. Sentinet is Microsoft ***Certified for Windows Server*** environments.

Sentinet Benefits

Developers benefit from using Sentinet by ensuring their BizTalk services are implemented, tested and deployed according to the specified security, performance and any other operational requirements. Sentinet decouples development and deployment efforts from common infrastructural challenges such as security, authentication, authorization and monitoring. Sentinet provides the BizTalk application with agility to adapt to changing deployment requirements without the need to reconfigure or redeploy the actual BizTalk applications or BizTalk application artifacts. Development teams deliver BizTalk integration solutions faster and with less risk and complexity. Key test and development capabilities include:

- Central SOA and APIs Repository with discoverable and reusable services and their metadata.
- Standardized and centralized policy enforcement.
- Project-based policy enforcement.
- Security policy model management.
- Identities management.
- Access Control management.
- Performance testing and impact analysis.
- Monitoring and message exchange capabilities.
- Service transactions recording and auditing.
- Parallel development of consumer and provider applications.
- Automated service and consumer application testing.
- Certificate and PKI key management infrastructure.
- Functional extensibility.
- BizTalk mockup services for easier testing

Operations team benefit from the Sentinet platform by ensuring BizTalk production services and applications are secured, monitored, audited, alerted on, and satisfy performance, consumption and availability metrics defined by existing Service Level Agreements and Service Level Objectives. Sentinet extends BizTalk server capabilities to communicate with interoperable and non-interoperable external and internal systems more effectively, for example providing BizTalk with advanced REST capabilities.

Sentinet ensures that operations teams have the tools they need to manage and maintain production systems in a consistent and predictable manner. Key runtime and operational benefits include:

- Better understanding of system behaviors.
- Provides service high-availability and accessibility.
- Provisions and enforces security policies.
- Policy-based automated performance management.
- Identities management.
- Provides services visibility and control without reconfiguration or redeployment.
- Real-time monitoring that keeps enterprises appraised of applications behavior and their constituent components.
- Performance and impact analysis.
- Performance patterns and trends analysis.
- Service consumption patterns and trends analysis.

- Active and pro-active alerting.
- Root-cause analysis and auditing.
- Service Level Agreements (SLA) and Service Level Objectives (SLO) management.

SOA and API Repository

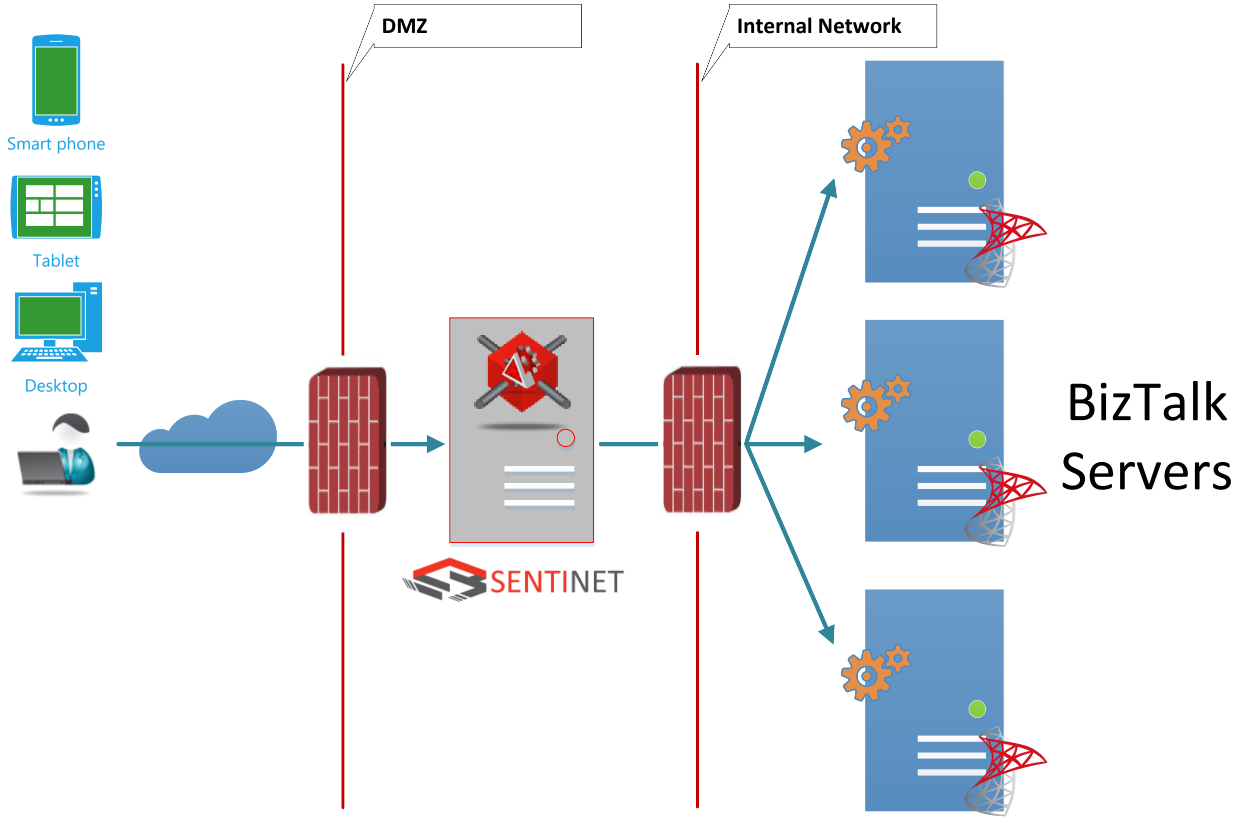
Sentinet extends BizTalk solutions with generic SOA and APIs Repository that provides centralized and secure governance infrastructure for BizTalk SOA software assets. Sentinet Repository stores and manages BizTalk services and their versions, security policies, services metadata and documentation, authentication/authorization and access control rules, service agreements, identities and identity systems configurations, monitoring and auditing trails. Access to the Sentinet Repository is role-based and secured with authentication and authorization control. The Repository is enabled with a multi-tenancy that allows partitioning of its content, its visibility and accessibility per specific Sentinet users or user group. Sentinet users access the Repository by using a browser-based portal, Sentinet Administrative Console to discover and manage BizTalk services and their metadata, BizTalk security and Access Rules, and to monitor the real-time operational environment. BizTalk applications and those that integrate with BizTalk Server can access the Sentinet Repository programmatically by leveraging the interoperable Sentinet Web Services SOAP or REST API.

Security

Sentinet supports a wide range of standards, protocols and message formats, that enhance BizTalk services accessibility, security, monitoring and overall governance and automation:

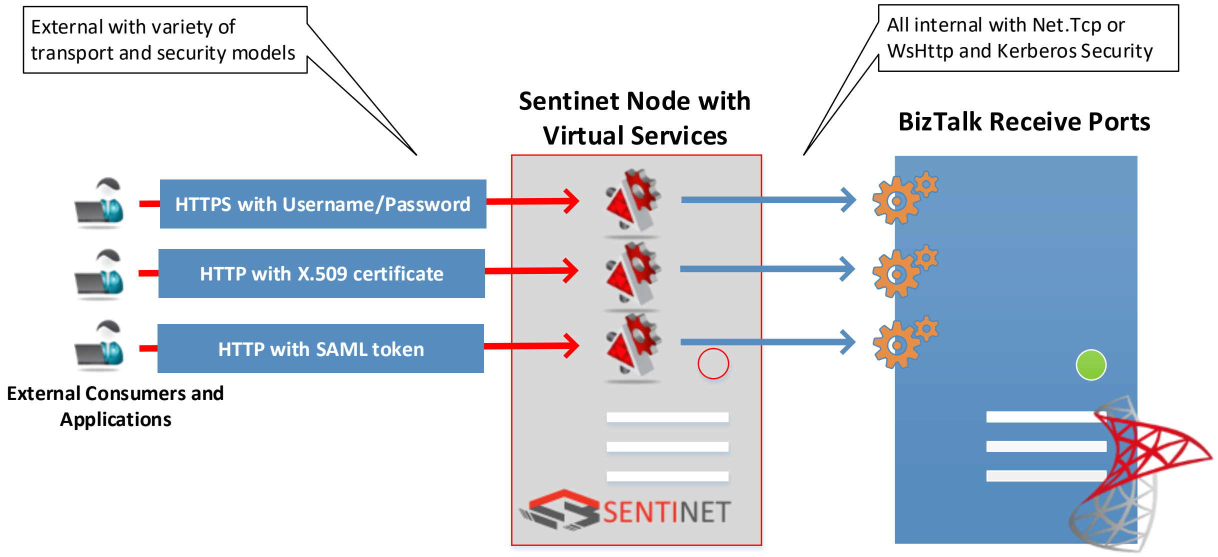
1. SOAP and REST.
2. REST to SOAP mediation.
3. Basic Authentication, X.509 certificates including mutual X.509 security.
4. WS-* security and reliability standards.
5. OAuth, OpenID Connect, API Keys
6. XML, JSON, text, binary.
7. HTTP, HTTPS, NET.TCP, NET.MSMQ, MSMQ.FORMATNAME, NET.PIPE, SB (Microsoft Azure Service Bus binary exchanges).
8. Native integrations with on-premises Active Directories, ADFS servers and cloud Azure Active Directories.
9. Native integrations with industry standard OAuth providers.

Sentinet can be used as an Application Security Gateway to extend internal BizTalk applications with managed access by external applications.

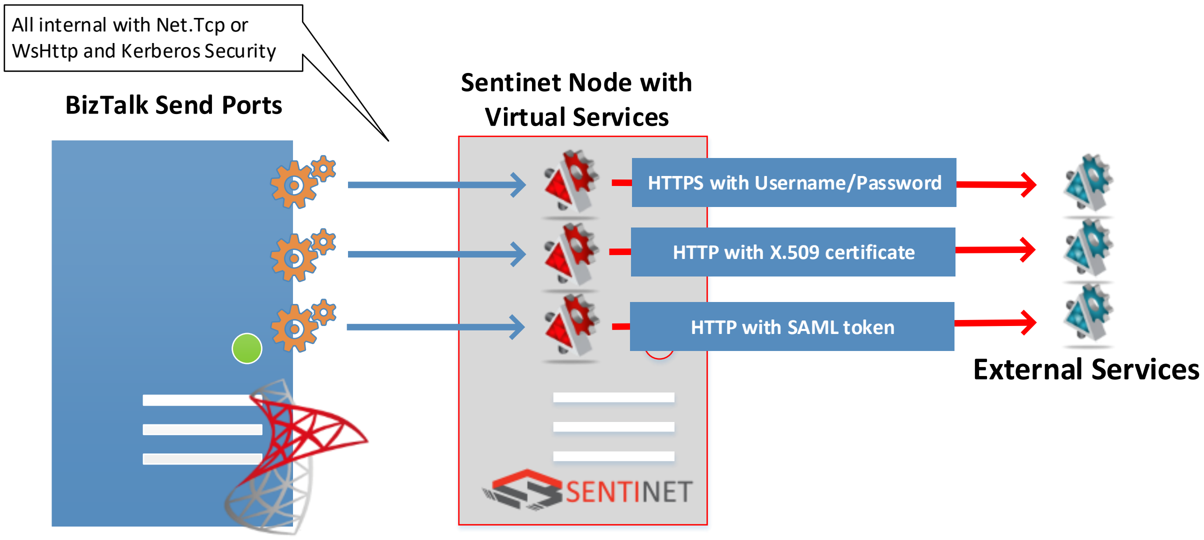


Mediation and Virtualization

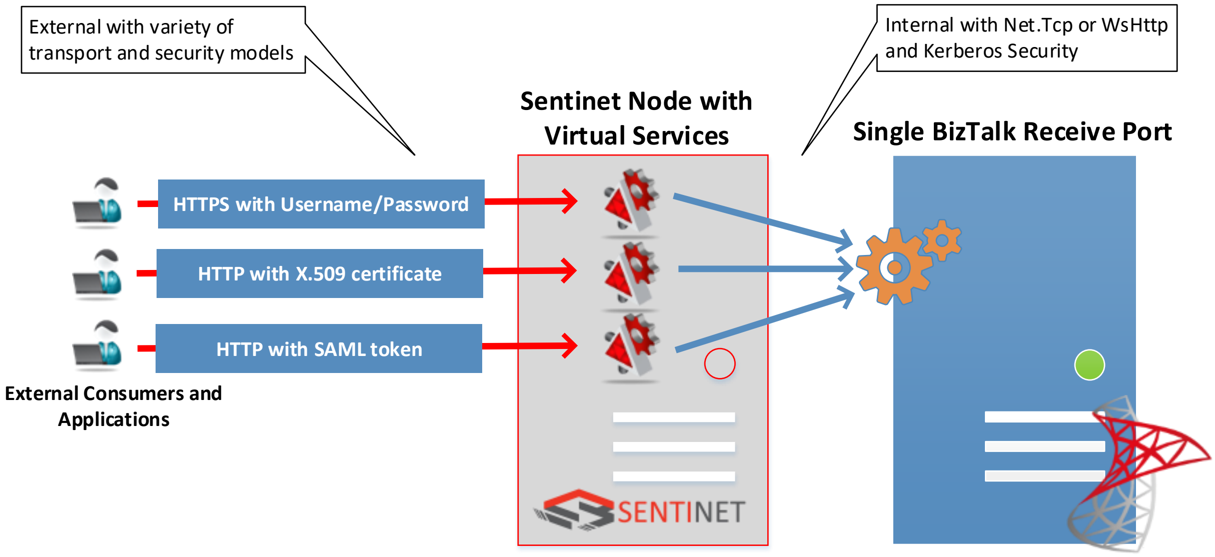
BizTalk services and applications leverage Sentinet to mediate and implement managed security. BizTalk Server Receive Ports can be configured with a unified and standardized WCF adapter configuration, and then exposed to consumer applications as Sentinet dynamic virtual services by using transport and security models that satisfy any security and communication requirements. For example, all BizTalk application's ports can be configured with *WCF-NetTcp* or *WCF-WSHttp* adapter with Windows Integrated ("internal") security. Without changing any BizTalk configurations, Sentinet can expose these ports to consumer applications using a variety of transport and message-level security models that may require a Username/Password, X.509, SAML or OAuth based authentication (or all of the above at the same time). Administrators use Sentinet Administrative Console to create and remotely manage virtual services and virtual endpoints hosted on the Sentinet Nodes. Effectively, BizTalk applications deployed in development, test and production environments are decoupled from the specific knowledge and implementation details of the required communication and security protocols used by consumer applications to call BizTalk services.


External with variety of transport and security models
All internal with Net.Tcp or WsHttp and Kerberos Security
Sentinet Node with Virtual Services
BizTalk Receive Ports
HTTPS with Username/Password
HTTP with X.509 certificate
HTTP with SAML token
External Consumers and Applications
SENTINET

Similar benefits apply to BizTalk applications that consume external services, so that the overall Sentinet benefits are bidirectional. BizTalk Send Ports do not have to be enabled with the knowledge of specific communication and security requirements imposed by the external services, nor they must be configured with specific consumer identities expected by external services. All of these security and communication challenges are fully delegated to the Sentinet Nodes that mediate and route messages to the external services.

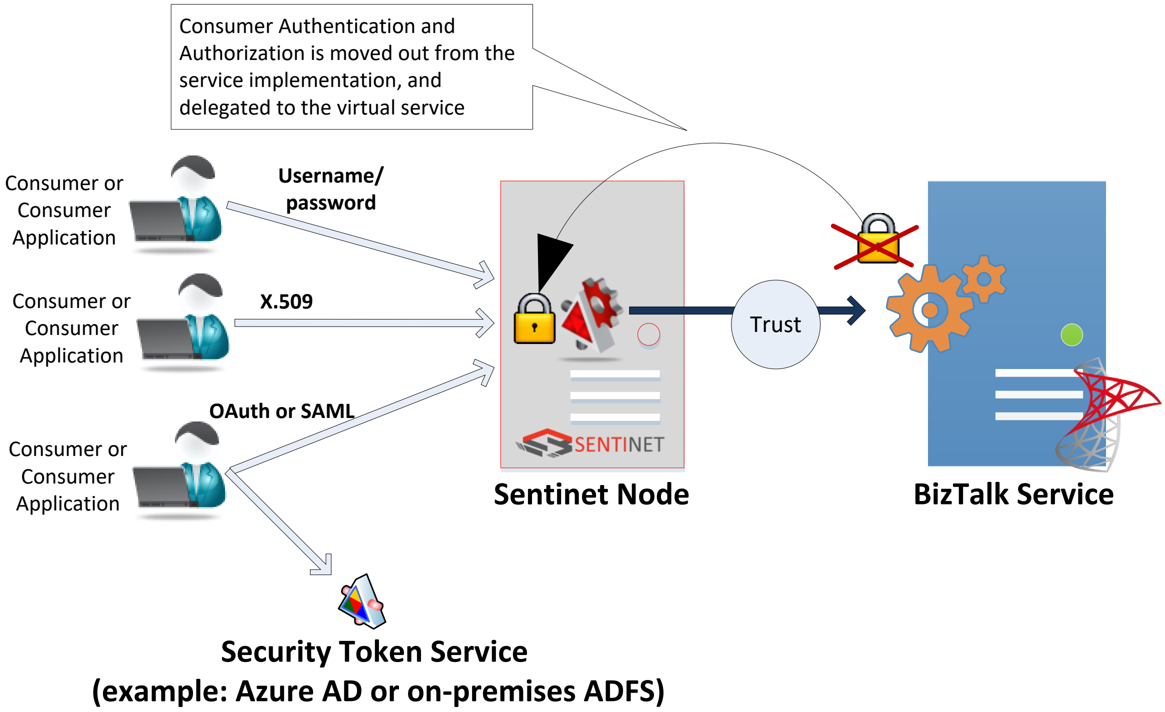

All internal with Net.Tcp or WsHttp and Kerberos Security
BizTalk Send Ports
Sentinet Node with Virtual Services
HTTPS with Username/Password
HTTP with X.509 certificate
HTTP with SAML token
External Services
SENTINET

Sentinet supports both industry standard and all Microsoft-specific communication and security protocols and can mediate between interoperable and Microsoft-specific message exchanges. A single BizTalk Server Receive Port (BizTalk Service) can be exposed through any number of Sentinet virtual services reducing the need for multiple BizTalk Receive Ports with their own BizTalk Adapters and Adapters' configurations.


External with variety of transport and security models
Internal with Net.Tcp or WsHttp and Kerberos Security
Sentinet Node with Virtual Services
Single BizTalk Receive Port
HTTPS with Username/Password
HTTP with X.509 certificate
HTTP with SAML token
External Consumers and Applications
SENTINET

Authentication and Authorization

BizTalk applications can be decoupled from authentication and authorization decisions by delegating these tasks to Sentinet Nodes. An explicit trust relationship can be established between BizTalk Server and Sentinet Nodes. Messages that are pre-authenticated and pre-authorized by a Sentinet Node will be automatically trusted by BizTalk Server applications and services, which can now be deployed with unified security and identity requirements that only authorized and authenticated Sentinet Nodes can satisfy. By leveraging Sentinet, BizTalk services can be enabled to understand and process SAML claims in Federated Security scenarios.


Consumer Authentication and Authorization is moved out from the service implementation, and delegated to the virtual service
Consumer or Consumer Application
Username/ password
Consumer or Consumer Application
X.509
OAuth or SAML
Consumer or Consumer Application
Trust
SENTINET
Sentinet Node
BizTalk Service
Security Token Service
(example: Azure AD or on-premises ADFS)

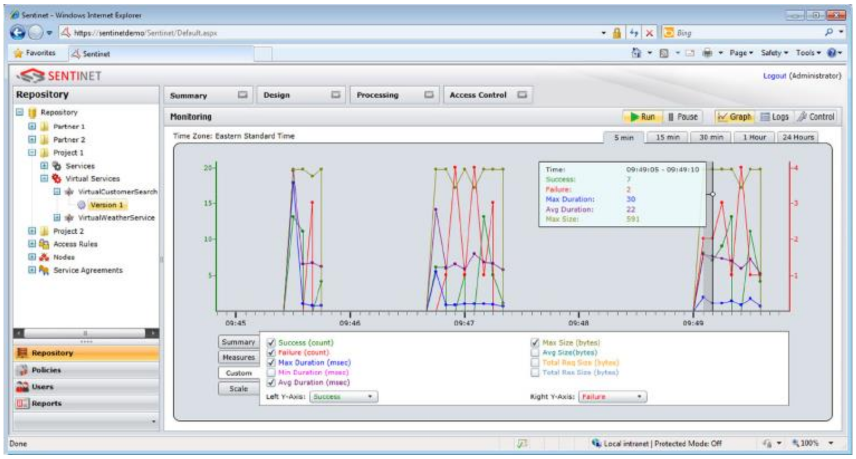
Implementing Authorization rules within BizTalk applications is an exceedingly challenging task, that does not scale well with the growing number of services and applications.

Sentinet addresses these critical authorization challenges.

Administrators can create, modify and apply sophisticated and extendable authorization rules dynamically and remotely, without reconfiguring or redeploying BizTalk Server applications and their artifacts. Sentinet Authorization Engine executes on the Sentinet Nodes, where it enforces custom authorization rules designed by Sentinet administrators.

Monitoring, Recording and Service Agreements Management

In addition to virtualization, Sentinet provides BizTalk applications with a wide array of non-invasive enabling capabilities including monitoring, recording, auditing, dynamic alerts, Service Level Agreements (SLA) management and real-time and historical reporting.

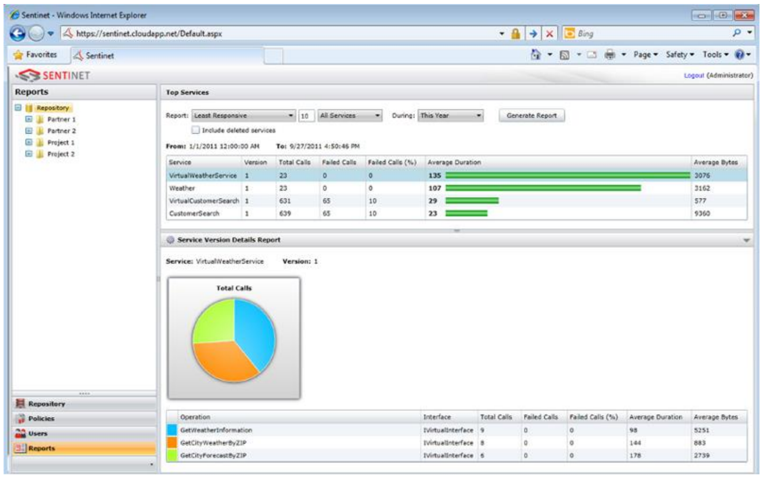


Time Zone: Eastern Standard Time

Time: 09:49:05 - 09:49:10
Success: 7
Failure: 2
Max Duration: 30
Avg Duration: 22
Max Size: 591

☑ Success (count)
☑ Failure (count)
☑ Max Duration (msec)
□ Min Duration (msec)
☑ Avg Duration (msec)
Left Y-Axis: Success

☑ Max Size (bytes)
□ Avg Size(bytes)
□ Total Req Size (bytes)
□ Total Res Size (bytes)
Right Y-Axis: Failure



Top Services

Report: Least Responsive 10 All Services During: This Year

□ Include deleted services

From: 1/1/2011 12:00:00 AM To: 9/27/2011 4:50:46 PM

Service	Version	Total Calls	Failed Calls	Failed Calls (%)	Average Duration	Average Bytes
VirtualWeatherService	1	23	0	0	135	3076
Weather	1	23	0	0	107	3162
VirtualCustomerSearch	1	631	65	10	29	577
CustomerSearch	1	639	65	10	23	9360

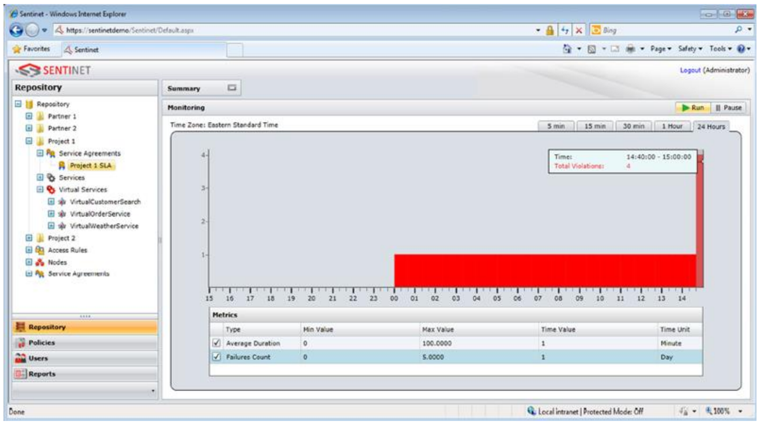
Service Version Details Report

Service: VirtualWeatherService Version: 1

	Operation	Interface	Total Calls	Failed Calls	Failed Calls (%)	Average Duration	Average Bytes
🟦	GetWeatherInformation	IVirtualInterface	9	0	0	98	5251
🟧	GetCityWeatherByZIP	IVirtualInterface	8	0	0	144	883
🟩	GetCityForecastByZIP	IVirtualInterface	6	0	0	178	2739

Sentinet complements BizTalk's Business Activity Monitoring (BAM) by providing development and operations environments with both high-level and detailed service-level monitoring and recording of web-service calls and message exchanges.

Sentinet provides BizTalk solutions with full visibility and analysis of who is using BizTalk services, when, and how. Sentinet SLAs can be created per individual consumer identity or consumer application, and validated against configurable performance, traffic volume and service availability metrics. Multiple services can be covered by a single SLA. Sentinet monitors and alerts on SLA violations, it produces real-time and historical SLA trends before SLAs are violated.



Repository
- Partner 1
- Partner 2
- Project 1
  - Service Agreements
    - Project 1 SLA
  - Services
  - Virtual Services
    - VirtualCustomerSearch
    - VirtualOrderService
    - VirtualWeatherService
- Project 2
- Access Rules
- Nodes
- Service Agreements

Time Zone: Eastern Standard Time

Time: 14:40:00 - 15:00:00
Total Violations: 4

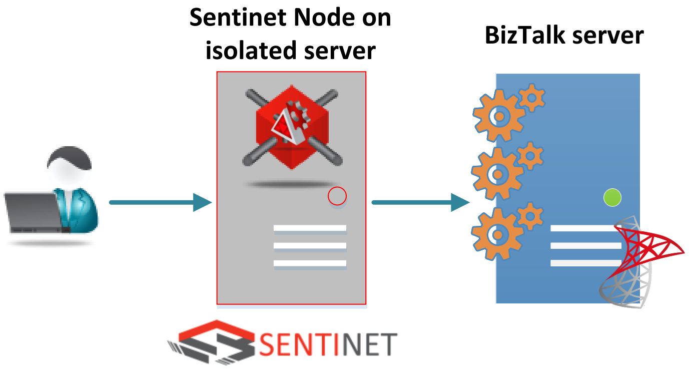
Metrics

	Type	Min Value	Max Value	Time Value	Time Unit
☑	Average Duration	0	100.0000	1	Minute
☑	Failures Count	0	5.0000	1	Day

Deployment Topologies

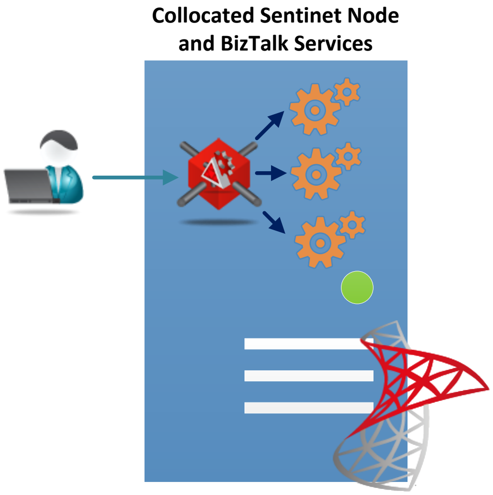
Isolated Deployment

Sentinet Nodes are typically deployed as security gateways (or stand-alone network intermediaries). Additional network latencies introduced by a network intermediary are negligible compared to BizTalk Server's persistent messaging delivery. Gateway latencies can be further minimized by leveraging optimized network communication protocols such as *net.tcp* transport with binary encoder.



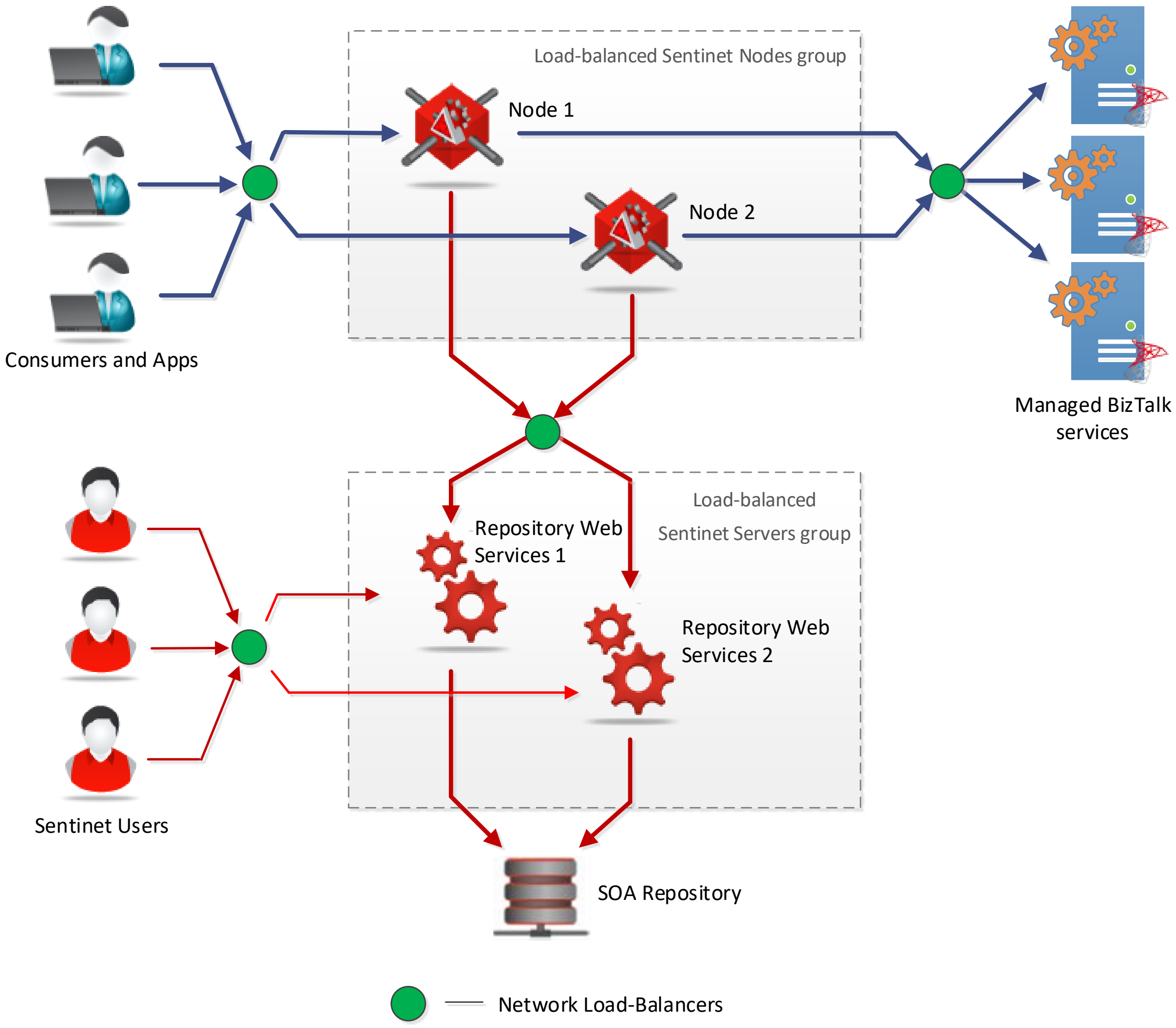
Collocated Deployment

Sentinet Node is particularly performance effective when it is deployed side-by-side with BizTalk Server on the same servers. In this case BizTalk Ports can be configured with inter-process communication via *WCF-NetNamedPipe* adapter, where Sentinet Node routes messages to local BizTalk services via *net.pipe* transport. By using *net.pipe* transport, BizTalk applications 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 protocol.



High-Availability

Sentinet fully supports high-availability, redundant deployment topologies where clustered Sentinet Node and Sentinet Repository Web Services Management Servers are deployed behind the load-balancers for high performance and high availability.


Load-balanced Sentinet Nodes group
Node 1
Node 2
Consumers and Apps
Managed BizTalk services
Load-balanced Sentinet Servers group
Repository Web Services 1
Repository Web Services 2
Sentinet Users
SOA Repository
Network Load-Balancers

In this scenario, Sentinet is fully deployed in high-availability environment. Repository database is subject to standard SQL Server clustering and high-availability models.

Sentinet for Microsoft BizTalk ESB Toolkit

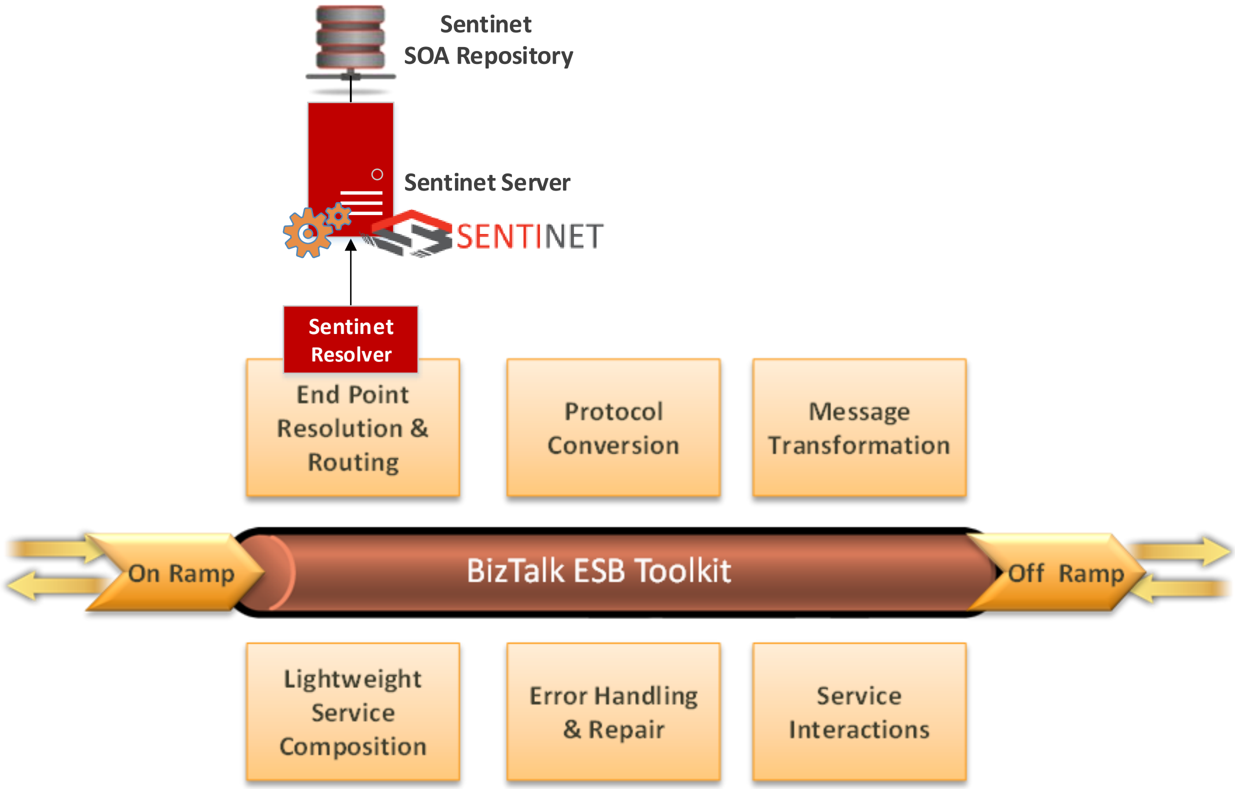
The Microsoft BizTalk ESB Toolkit extends the functionality of BizTalk Server to provide a range of capabilities focused on building connected, service-oriented applications that incorporate itinerary-based service invocation and integration with SOA governance solutions. Sentinet BizTalk Server

Extensions offers an advanced ESB Toolkit **SOA Repository Resolver**, that integrates with BizTalk Server 2013, 2013 R2, BizTalk ESB Toolkit and Microsoft Visual Studio.

Combined with Sentinet SOA/API Repository, Sentinet Repository Resolver provides BizTalk ESB architectures with advanced, and easy to use ESB configurations, dynamic messages routing and message security implementation capabilities.

Sentinet Repository Resolver extends BizTalk ESB Toolkit capabilities by offering:

1. Integration to the robust and comprehensive Sentinet SOA Repository
2. Ease of registering and managing ESB services
3. Comprehensive and yet simple to use Sentinet Administrative Console
4. Management and configuration of the resolved ESB endpoints' custom behaviors
5. Advanced ESB endpoints search and resolution criteria
6. Guarantee of unique resolution results
7. Advanced ESB resolution testing capabilities



BizTalk Server and Microsoft Azure Cloud Platform

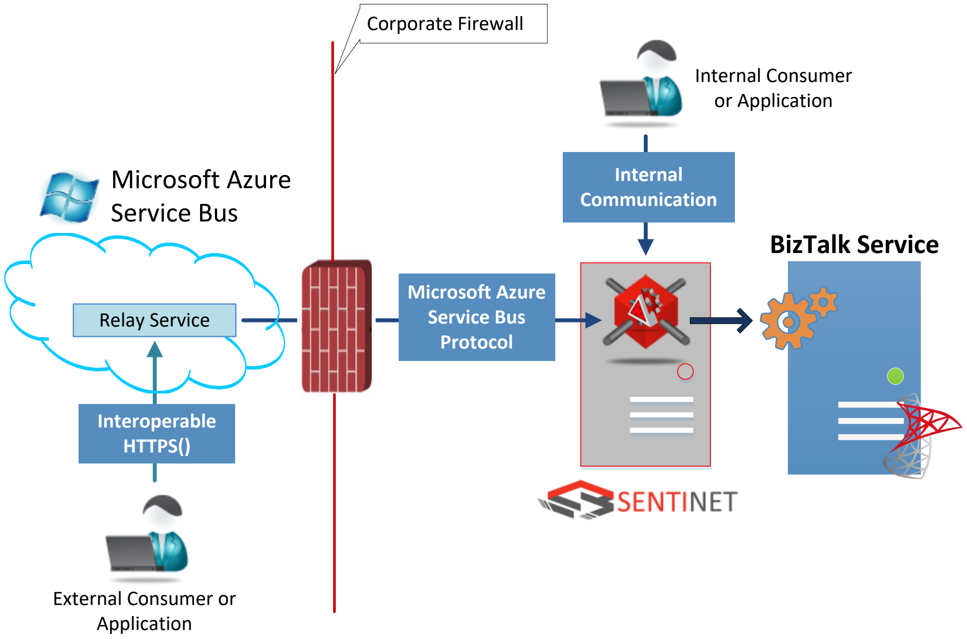
Integration with Microsoft Azure Service Bus Relay

The Sentinet platform, non-intrusively, extends BizTalk Server capabilities to the Microsoft Azure cloud platform. Sentinet provides BizTalk with easy interactions to the external parties to integrate with, without needing complex firewall and security infrastructure. Sentinet Nodes are designed to natively integrate with Microsoft Azure Service Bus and Microsoft Azure Access Control Service. Sentinet Nodes can be dynamically and remotely configured with Azure Service Bus endpoints, encapsulating Service Bus non-interoperable protocols and Microsoft Azure ACS security identities.

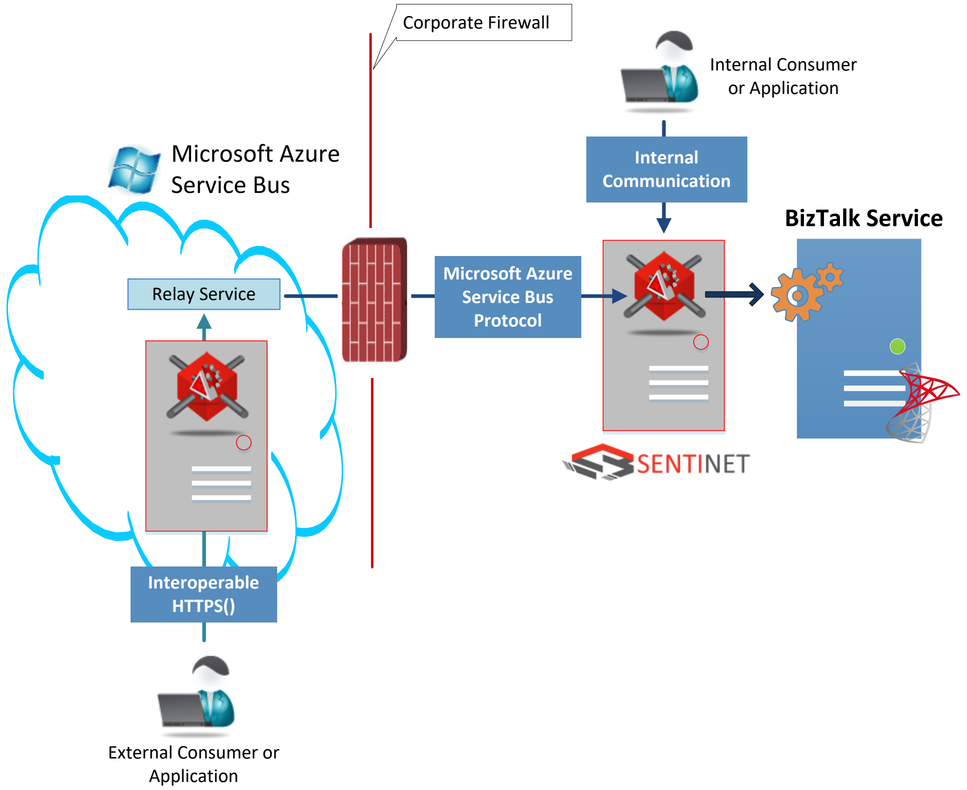
In order to join Microsoft Azure Service Bus infrastructure, BizTalk services have to be reconfigured to use special WCF bindings (via *WCF-BasicHttpRelay, WCF-NetTcpRelay, SB-Messaging*, W*CF-Custom* or *WCF-CustomIsolated* adapters' configurations). Each adapter has to be configured with Microsoft Azure subscription's security keys, which is neither a scalable deployment model nor a secure one (all ports have to be given knowledge of all the subscription security keys).

In a complex composite application that involves both a BizTalk and a Cloud element in 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-premises BizTalk solution may be communicating through the Service Bus with any number of services each requiring a dedicated Receive Location or a Send Port configured with its own adapter, that supports Service Bus WCF binding.

By using Sentinet, any service (including BizTalk service), can be on-boarded onto Microsoft Azure Service Bus infrastructure without reconfigurations, redeployments or potential security keys compromises. 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 ACS service. Service Bus security keys are stored in the central Sentinet SOA/API Repository and securely delivered to the Sentinet Nodes, when opening Microsoft Azure Service Bus endpoints. Moreover, Sentinet Nodes can be configured side-by-side with Microsoft Azure Service Bus endpoints and additional internal endpoints, e.g. for testing and staging. Sentinet Administrators get full visibility and control over endpoints exposed via Microsoft 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.

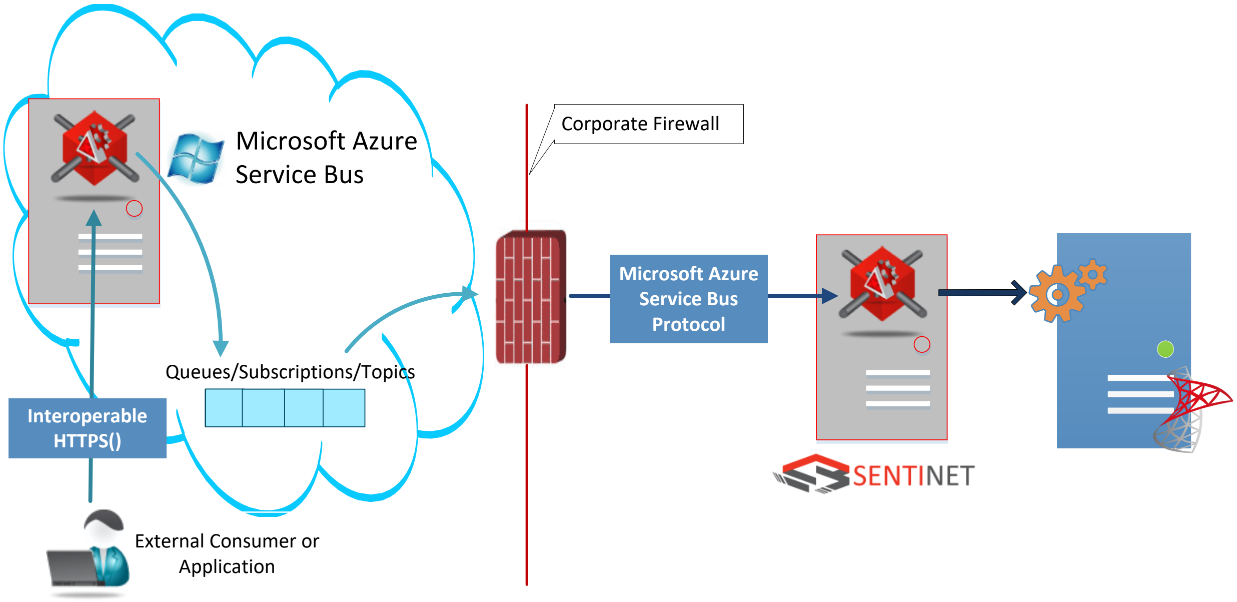

Corporate Firewall
Internal Consumer or Application
Microsoft Azure Service Bus
Internal Communication
BizTalk Service
Relay Service
Microsoft Azure Service Bus Protocol
Interoperable HTTPS()
SENTINET
External Consumer or Application

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


Corporate Firewall
Internal Consumer or Application
Microsoft Azure Service Bus
Internal Communication
BizTalk Service
Relay Service
Microsoft Azure Service Bus Protocol
SENTINET
Interoperable HTTPS()
External Consumer or Application

Integration with Microsoft Azure Asynchronous Queuing

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


Microsoft Azure Service Bus
Corporate Firewall
Microsoft Azure Service Bus Protocol
Queues/Subscriptions/Topics
Interoperable HTTPS()
External Consumer or Application
SENTINET

Summary

Sentinet extends BizTalk by:

- Making BizTalk open and extensible to 3rd Party Best of Breed applications and services
- Extending BizTalk Cloud, SaaS and Hybrid capabilities by providing REST support
- Adding connection to any transports or security models
- Providing Real-Time and Historical Monitoring Data
- Introducing graphical Authorization Access Controls