API Management and API Governance with Sentinet

Overview

Nevatech

Contents

Introduction

Nevatech Sentinet is the **only** enterprise class API Management and API Governance platform **written in .NET** that is available for On-Premise, Cloud and Hybrid environments. It connects, mediates and manages interactions between services across the enterprise or in the cloud. Sentinet supports all industry-standard REST and SOAP communication protocols and security models, as well as Microsoft-specific. Sentinet provides integration architectures with **design-time API Governance** and **automated run-time API Management**.

All enterprise service applications face the same common infrastructural challenges – services and APIs availability and accessibility, discovery, security, monitoring, auditing, alerting, service agreements and service level objectives management and many others. These common infrastructural challenges are typically not part of an organization's core business and can be addressed by software platforms that save time, resources and already provide the necessary solution for day-to-day operations. By using API Management products, development teams are enabled with faster time-to-market delivery of their business solutions, while operations teams are equipped with tools and procedures to manage and maintain production systems in a consistent, predictable and agile environment.

The most effective and popular means of addressing common API Management challenges is based on the concept of virtualization of services and APIs. Services virtualization introduces the notion of software-based agents now commonly referred to as API Gateways, that mediate communication between API consumer and API provider applications and implement dynamic, remote and non-invasive management of common development, test and operational tasks with the real agility to adapt to continuous change.

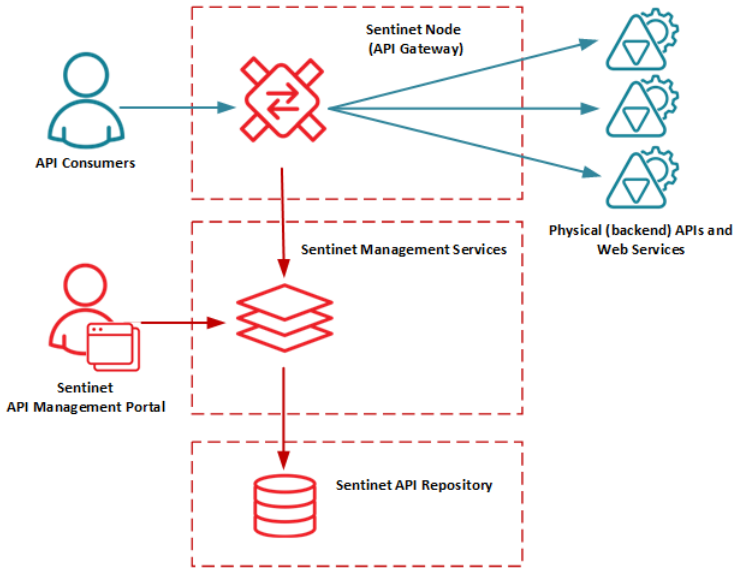
Sentinet is particularly beneficial to both organizations that leverage Microsoft as their strategic platform to develop and operate API and SOA solutions and those organizations that need to integrate and mediate Microsoft and non-Microsoft technologies as part of their API architectures.

Sentinet is a highly scalable and reliable API Management software solution, that can operate in a variety of diverse network configurations within on-premises, cloud or hybrid environments. Sentinet fully and natively integrates with, and **augments** the capabilities of the Microsoft Azure cloud platform.

Sentinet Components

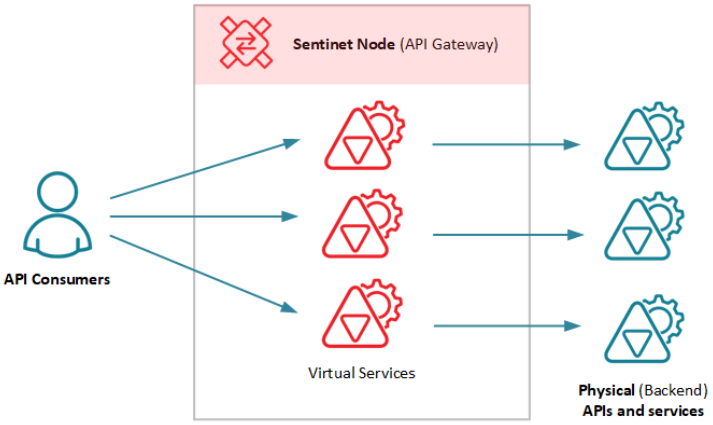
The Sentinet API Management platform consists of four major components:

Sentinet Repository, an on-premises or cloud-based MS SQL server database that provides centralized, hierarchical and secure storage for all API and SOA managed software assets, such as services, microservices, virtual services, metadata and documentation, security policies, authentication & authorization with access control rules, service agreements, identities and identity systems configurations, monitoring data and auditing trails. Sentinet Repository is enabled with a multi-tenancy that allows partitioning of its content, visibility and accessibility per specific Sentinet users and user groups.



Sentinet Management Services is a secure and scalable web application consisting of Sentinet Management RESTful APIs and SOAP services. Sentinet Management services are connected to **Sentinet Repository**, which stores all the Sentinet configuration data along with registered APIs, their artifacts and collected monitoring data.

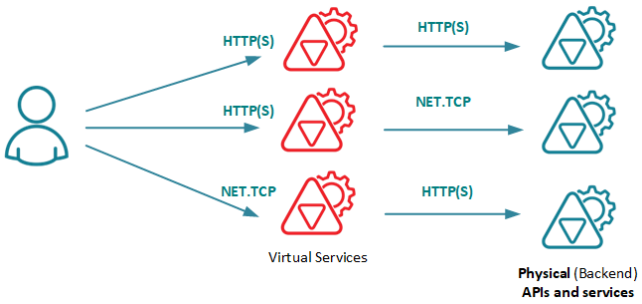
Sentinet Node (API Gateway) is a high-performance, scalable software intermediary that hosts remotely configurable and dynamic virtual APIs (façade APIs). The Sentinet Node mediates communication between API consumers and physical (backend) APIs, microservices and services, and through that brokerage empowers API solutions with diverse run-time management capabilities such as security, monitoring, message transformation, operational and business analytics.

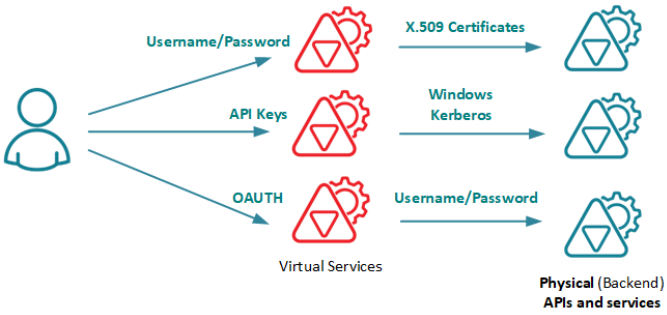


Sentinet API Management Portal (Administrative Console) is a browser-based web application that enables Sentinet users and administrators with highly interactive, intuitive, secure and remote control of all the aspects of their integration solutions' API Management and API Governance.

API Management

Communication Mediation. Sentinet can mediate communication protocols between HTTP and HTTPS for RESTful APIs, and non-HTTP(S) communication protocols, such as Microsoft-specific NET.TCP, NET.PIPE, MSMQ, Azure Service Bus binary.

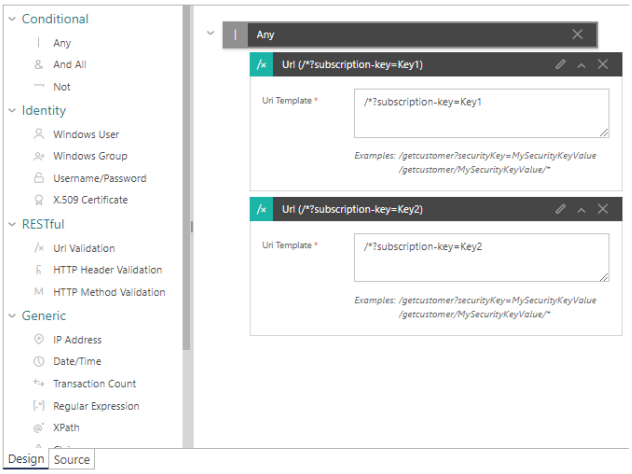




Security Mediation (Authentication Schemes mediation). Sentinet supports pass-through and mediated security models when different authentication schemes are implemented for the virtual services and the physical (backend) services. Sentinet supports all industry standard interoperable and all Microsoft-specific, non-interoperable security models on either side of the virtual services including:

- Username/Password (Basic Authentication and XML message-level for SOAP)
- X.509 Certificates including mutual SSL (SSL certificates and XML message-level for SOAP)
- OAuth and OpenID Connect
- API Security Keys
- WS-* for SOAP including advanced WS-Federation
- SAML 1.1, 2.0
- Windows Kerberos and NTLM
- Windows Active Directory Group membership
- Microsoft Azure Active Directory
- Microsoft Azure ADFS for on-premises and hybrid integrations
- Industry-standard and custom authentication schemes
- Industry-standard and custom security tokens
- Claims based authentication/authorization and claims aware applications

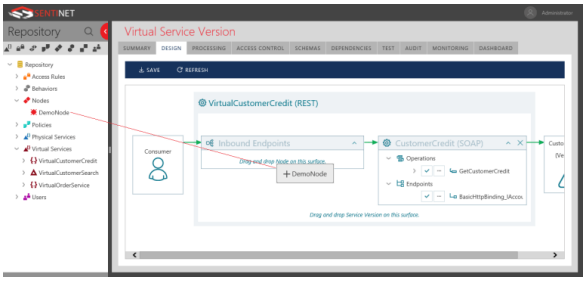
Authorization and Access Control. Service authorization logic is often hardcoded in the business service implementation making it difficult to scale through services and to promote them through different life cycles and environments. Sentinet provides a highly flexible run-time Authorization Engine and an interactive design-time Access Rules Designer. The authorization Engine executes in the Sentinet Node (API Gateway), where it enforces custom authorizations rules designed by the Sentinet users. Business services can now delegate ultimate authentication and authorization decisions to the Sentinet virtual services, while authenticating and authorizing only trusted Sentinet Nodes.



Sentinet Authorization and Access Control rules are managed declaratively using a rich graphical user interface and an Access Control Designer. Administrators can control authorized identities, access time schedules, allowed rate limits and content-based access rules. Developers can enhance the Sentinet Authorization Engine with custom Access Control rules and integrate them easily using the Sentinet API Management Portal (Administrative Console) application.

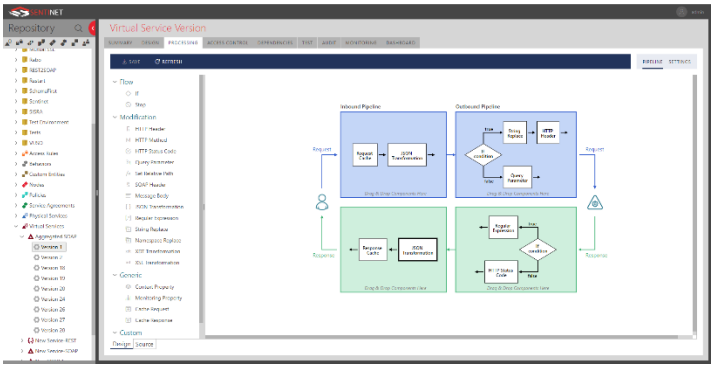
Access Rules are reusable components stored in the API Repository. They can be assigned to more than one REST API or SOAP service via a simple drag-and-drop. Sentinet Authorization Engine supports and extends any industry-standard OAuth provider and Security Token Service (STS), including native support and integration with the cloud-based Microsoft Azure Active Directory (AAD) and the on-premises Active Directory Federation Services (ADFS).

Virtual APIs Designer. Sentinet provides a very intuitive and easy to use graphical Virtual API Designer. Using a simple drag-and-drop User Experience, Sentinet users can design complex RESTful APIs and SOAP services that virtualize physical RESTful APIs and SOAP services. A single physical service can be virtualized by many different virtual services, while a single virtual service can virtualize many aggregated physical services (for example microservices).



Sentinet supports the design and transformation of legacy SOAP services into lightweight RESTful APIs through a configurable graphical User Interface Mapper. Automatic and configurable transformations between XML and JSON help to ease the access to RESTful APIs by web and mobile applications.

Messages Transformation. Physical (backend) APIs are often required to implement agility to adapt to API Consumer applications and their capabilities. Sentinet users can delegate that responsibility to the virtual services, removing the need for changes to the physical (backend) APIs or services.

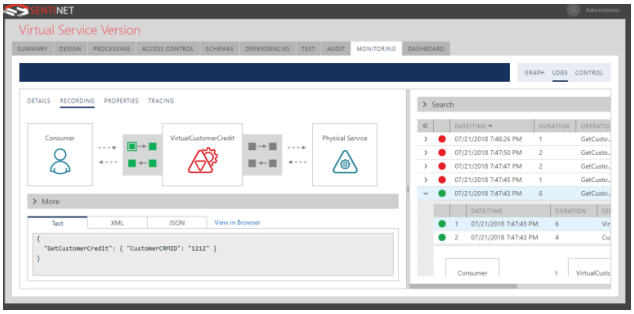


The Sentinet graphical Pipeline Designer and the virtual service processing settings provide User Interface to control the configuration of required message transformations, behaviors and workflows. A pipeline configuration process is implemented through simple drag-and-drop for its components.

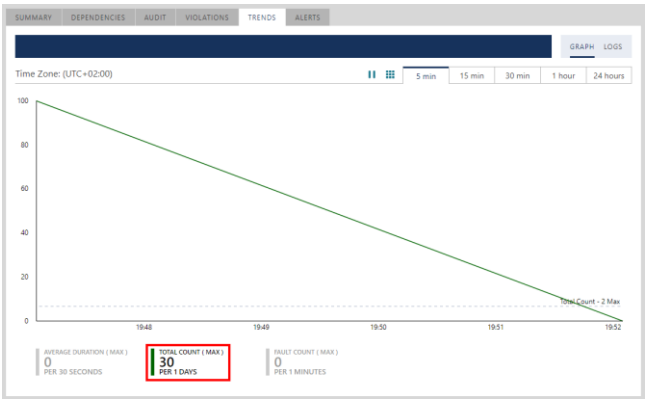
Pipeline processing components can operate on both **request** and **response** message content by adding, removing or modifying existing content. Any part of the message content or its context (for example API client identity) can be extracted and used for further processing and for custom monitoring, auditing and analytics. Sentinet Pipeline components include:

- HTTP headers processing
- HTTP methods processing
- HTTP status codes processing
- Query Parameters processing
- Request URL processing
- Message Body replacement
- String replacement
- Regular Expression replacement
- Support for conversions between XML and JSON formats
- Responses caching
- SOAP header processing
- XSL and XDT transformations
- Injection of the custom Monitoring Content and Context for real-time monitoring, auditing and analytics
- Support for Cross-Origin Resource Sharing (CORS)
- Conditional pipeline execution
- Stop processing and return custom response
- Support for custom message processing components

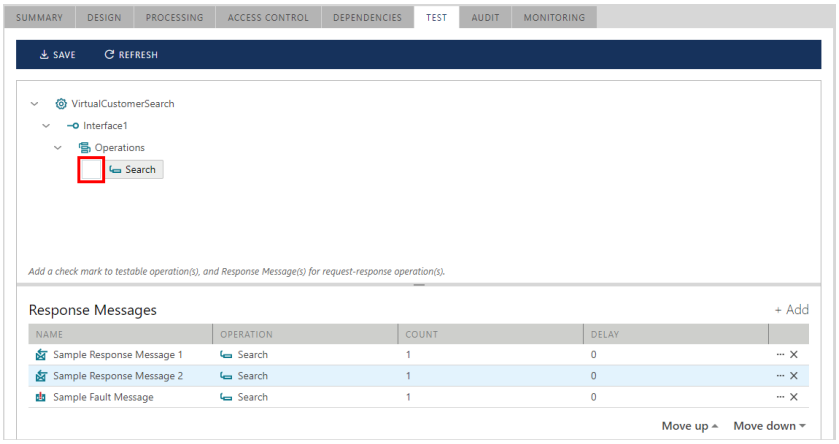
Monitoring and Auditing. Sentinet provides a robust, real-time and historical monitoring capability for all or selected messages sent to and received from the virtual or physical services. Using the real-time charts, Sentinet users can see and analyze real-time traffic, while configurable messages logs provide detailed search and analysis of the messages content, statuses, durations, message sizes, API client identities and many other operational and business metrics.



Service Level Agreements (SLA) management. API operational metrics can be monitored against a set of thresholds providing Sentinet users with immediate access to an API's health and consumption metrics. Service Agreements define these metrics and their thresholds and automatically alert upon SLA violations. Sentinet users can monitor in real-time and analyze historically the state of SLA violations with predictive trends analysis.

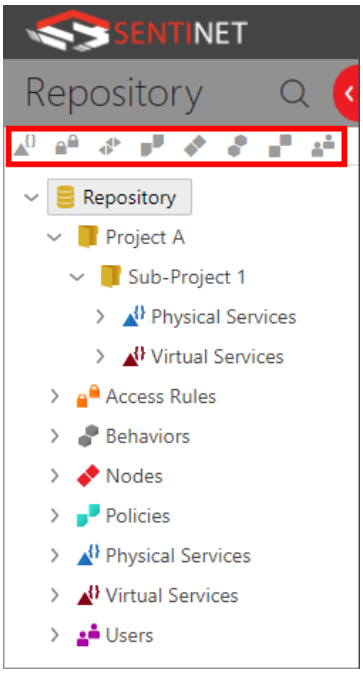


Testing. Sentinet provides non-intrusive automated testing and service-mockup capabilities, that make developers more productive by enabling them to concurrently develop and test consumer and service applications by delivering functional, performance and security testing without any custom code development.



Virtual services can be configured to return test response messages on all or some of its operations instead of forwarding requests to the business services. If a business service's metadata and contracts are registered, services can be immediately tested without concrete implementation or even actual hosting. Developers of consumer applications can test their applications against mock-up virtual services hosted in Sentinet Nodes and against virtual request-reply or even one-way operations. Additionally, they can simulate and test security models and performance implications. Consumer applications can be functionally tested against test response messages; test response messages can be organized in test sets.

API Governance



Sentinet offers comprehensive Governance for API solutions. RESTful APIs, SOAP web service and their artifacts are treated as first-class citizens of the Sentinet Repository. Virtual services designed by the Sentinet users, and physical services registered in the Repository, are independent entities that have their own description, metadata and supplementary documentation. API Management assets are organized by user-created hierarchical folders to offer fine-grained structures for API assets grouping and implicit relationships. A Repository folder may represent an API product, an API project, an API solution, an organization's department, a partner organization or any other logical grouping of API assets. A Sentinet user that is given access to a specific Repository folder will automatically be given the same level of access to all of its subfolders. Each folder can store API assets of different types. The Sentinet Administrative Console automatically organizes them in logical subgroups, such as Physical Services, Virtual Services, Access Rules and Service Agreements. The Repository is not branded. This structure enables multi-tenancy out-of-the-box. Physical APIs and services can be registered using existing metadata documents such as Swagger / OpenAPI for REST and WSDL for SOAP or they can be registered by manually entering registration information in the Sentinet Administrative Console. Regardless how APIs are registered, Sentinet will always provide access to their metadata based on the current state of the physical services description and virtual services design.

Some of the most notable Sentinet's API Governance features are:

- Support for APIs versioning
- Life-cycle management
- Access to API metadata
- Access to documentation in a variety of formats
- Access to message schemas
- Access to message samples
- Auditing of any Repository items and their changes
- API assets change notifications
- Auditing of Sentinet user sessions
- API assets dependencies and change impact analysis
- Repository search capabilities
- Export and import of API assets from and to different API environments, including automated procedures.
- Access to the Sentinet Repository via the Sentinet Management API

Conclusion

Sentinet enables development teams with faster time-to-market delivery of their API solutions in a continuously managed and governed environment. Sentinet benefits span across all stages of customers' API solutions' life-cycle and include information for better decision making, increased internal agility, a consistent, measurable, secure and standardized approach to API Management and Governance regardless of the backend platform. Customers can immediately begin with modernization and transformation utilizing the virtualization techniques without investing extra cost for programming or impacting the physical backend services.