opentext™ | Cybersecurity

Data Sheet

NetIQ Secure API Manager

NetIQ Secure API Manager offers a single solution to create, manage, secure and measure the APIs that your company uses. Working together with NetIQ Access Manager, NetIQ Secure API manager provides a comprehensive access and security solution for all your web, mobile and API access requirements.

NetIQ Secure API Manager by OpenText™ allows you to secure API access from your partners and customers, while making it easy for you to combine multiple APIs to create new functionality without exposing your application infrastructure behind it.

Product Highlights

Application programming interfaces (APIs) are sets of definitions, protocols, and tools for building software. Much of the software as well as many other components that make up the Internet of Things (IoT) use APIs to provide functionality that your business requires. The APIs also provide the ability to customize software to solve your business problems.

NetIQ Secure API Manager is a comprehensive solution for development, life-cycle management, security, integration and monitoring of all types of APIs—be it REST, SOAP, IoT or legacy custom APIs.

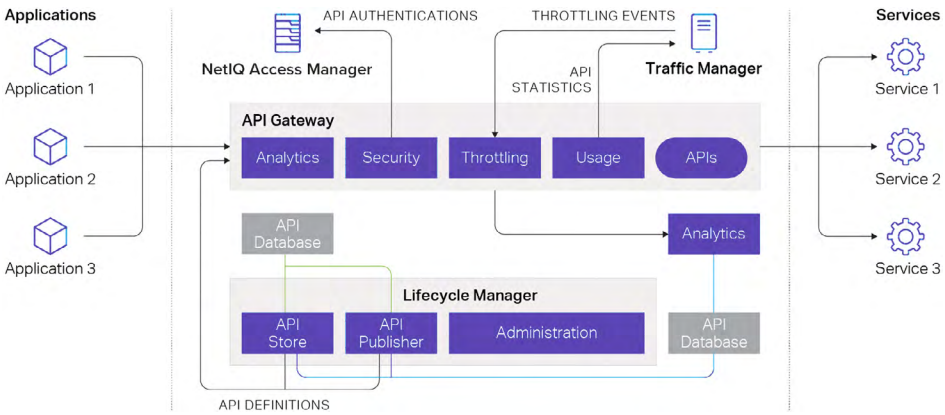

Figure 1. A comprehensive solution for development with Secure API Manager

Key Features

Single Repository to manage all APIs: NetIQ Secure API Manager provides a single repository where you can store and manage all of the APIs you use, allowing you to deploy, control and manage API-driven ecosystems.

API Gateway: NetIQ Secure API Manager includes a highly scalable API Gateway that provides options to secure, control, transform and manage APIs of all types. The API Gateway allows you to control traffic while enabling secure access to the APIs from anywhere

Key Benefits

OpenText solves these issues by providing a system that allows you to manage, create, control, and audit the APIs used in your environment through NetIQ Secure API Manager. It gives you:

- A single repository for all of your APIs—REST, SOAP, legacy or IoT
- A lifecycle management system to create, manage and version your APIs
- An API Gateway to control traffic while enabling secure access to the APIs from anywhere
- Risk-based access control and multifactor authentication for API clients to mitigate authentication and access risk
- Authentication and authorization of API through integration with NetIQ Access Manager
- API security settings to control access, limit traffic and throughput and enable zoning
- Controls to limit potential DoS attacks on APIs
- An analytics system that gives insights on the API usage, traffic patterns and statistics

Authentication & Authorization: Authentication and authorization of API through integration with NetIQ Access Manager by OpenText™

Rate Limiting & traffic control: API security settings to control access, limit traffic and throughput and enable zoning

Risk-based access control: enables dynamic authentication levels based on the criteria that you setup

Multifactor authentication for API clients: offers a rich set of methods that best match your organization's needs

DoS Attack Prevention: Controls to limit potential DoS attacks on APIs

API Analytics: This solution allows to create audit trails and offer deeper APIs analytics to prove compliance with regulation and licensing requirements for the APIs.

System Requirements

Component	Requirements
Virtual system	VMware ESX 6.5 or later **Note:** Your VMware license must be Enterprise or Enterprise Plus if you want to use remote serial connections. For more information, please refer to VMware support. For more information, see the VMware documentation.
Hard disk space	60 GB (per appliance)
Memory	12 GB of RAM (per appliance)
Processors	4 (per appliance)
Browsers	• Google Chrome latest version • Microsoft Edge latest version • Microsoft Internet Explorer 11 with latest patches • Mozilla Firefox latest version
IP Ports	Ensure that the default ports for the NetIQ Secure API Manager are open in your firewall. For more information, see Default Ports for NetIQ Secure API Manager.
Trust root certificate or self-signed certificate	The NetIQ Secure API Manager components communicate securely over SSL. You must have a trusted root certificate or use a self-signed certificate to have the Deployment Manager work.
License	License is required to receive online updates. Obtain the license from the Customer Care Center. You add the license to each appliance after you complete the installation. For more information, see "Performing an Online Update" in the *NetIQ Secure API Manager 1.0 Administration Guide*.
NetIQ Access Manager 4.5 or later	NetIQ Secure API Manager is an add-on product for NetIQ Access Manager 4.5 or later. You must have NetIQ Access Manager deployed and running before deploying Secure API Manager. For more information, see Section 3.0, Integrating NetIQ Secure API Manager with NetIQ Access Manager.
Network File System v3	If you cluster the component for high availability and load balancing, you must have a Networking File System (NFS) server deployed and running in your IT environment that NetIQ Secure API Manager uses. For more information, see Using High Availability and Load Balancing with NetIQ Secure API Manager.

Connect with Us

www.opentext.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

760-000011-003 | O | 10/23 | © 2023 Open Text