Securing Your API Layer

NetIQ Secure API Manager extends your access and authentication environment to include secure API delivery for all your secure integration needs. In today's emerging API-based business models, Secure API Manager is an essential core component for your access layer.

NetIQ API Manager at a Glance

- Secure all types of APIs—REST, SOAP, Microservices, IoT
- Traffic management and mediation policies to ensure that APIs and data are protected
- Enable risk-aware access control and gain API usage insights
- Create, secure, and manage REST APIs

Increasingly, companies are looking for new ways to leverage digital assets that expand their business into more efficient models of integration and collaboration. As this trend continues to accelerate, CIOs and IT teams need to adopt new types of security models to protect their digital offerings. Because APIs provide interfaces to core sets of software modules and resources, they need more protection than simply being hardened. Instead, they merit the same level of security offered by an access management platform. NetIQ API Manager gives organizations that level of protection and flexibility.

Microservices Imposes a New Approach to Security

Microservices use an architecture approach where applications are separated into a series of smaller and more specialized set of services. Because these services need to communicate with one another, they do so using standard interfaces such as APIs and REST. Each microservice tends to have its own distinct data stores and method for generating its logs, as well as a unique approach to authentication. It is also common for these services to be grouped as a container of services, where they are managed with a specialized set of tools.

The antithesis of microservices is the traditional monolithic model of building applications as a single entity on a server, underpinned by a single relational database. As you evaluate how traditional security practices for these monolithic systems are typically applied to microservices, you will see that a key difference is the modularized nature of this new type of architecture and the lack of mature administration and security solutions that will work in that environment. And beyond the lack of robust enterprise tools, the complex web of dependencies created by microservices configurations further complicates corporate administration and security challenges.

Gain a Competitive Edge with the Right Type of Security

As organizations pursue their API strategies, a critical component of a successful implementation and delivery of their library of microservices is to employ a security strategy that serves as a business enabler, not an inhibitor. Taking a full access management approach to securing your microservices allows you to enforce process verification and access control in ways that aren't possible with traditional API hardening approaches and in ways that are far less expensive than private networks. Moreover, as you expand and change your API-centric business models, you will appreciate the high level of protection, variety of supported configurations, and business payoff of being able to handle such a wide range of access control requirements made possible through an access management platform. So, as the role of APIs in B2C and B2B interactions continues to explode, having a security platform that can grow and adapt with it becomes paramount.

Why NetIQ Secure API Manager

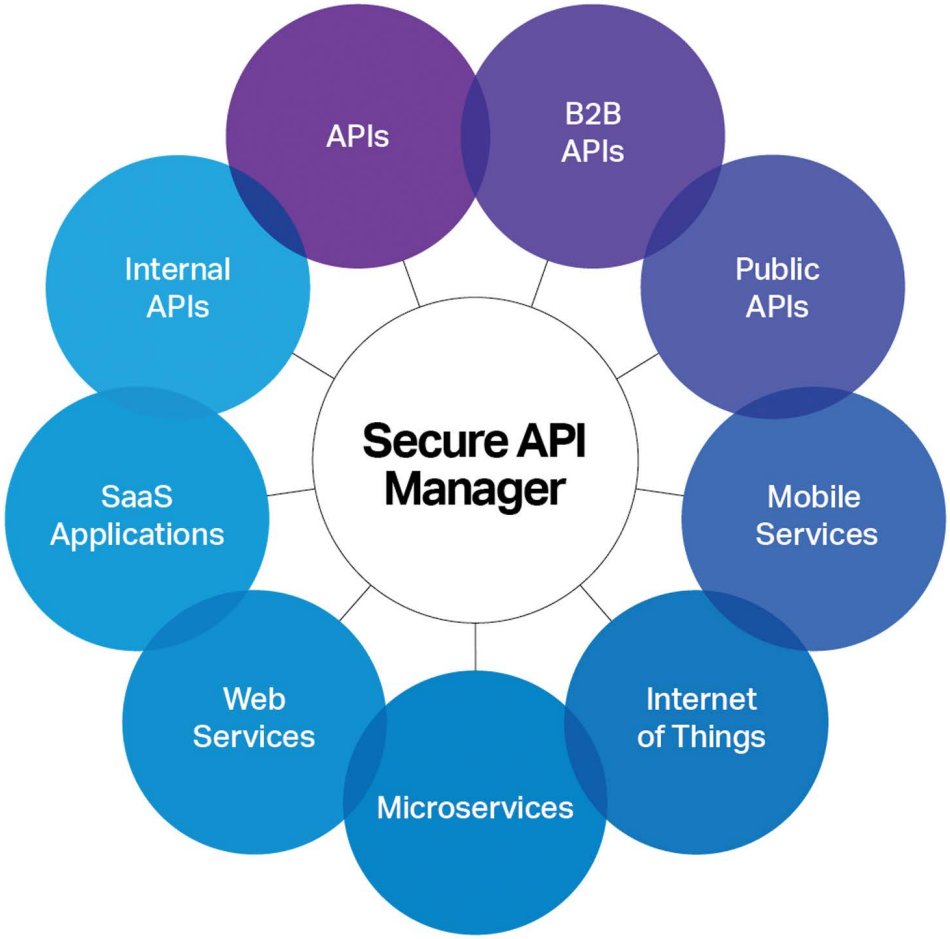
A survey* of experts conducted by DZone confirms, "API security is just as critical as application security." Thus, it shouldn't be implemented as an afterthought. They also agree, "API gateways are the most commonly

used solution, and with good reason—they provide many great out-of-the-box management services in addition to security." This is where NetIQ Secure API Manager comes in. It extends NetIQ's experience in delivering a best-of-breed access gateway out to API access. As API access emerges as a significant piece of the digital transformation puzzle, offering simple and secure access is a must. If an API gateway isn't yet a core component of your access security layer, it should be—and NetIQ Secure API Manager has just what it takes.

Enterprise-Grade Protection and Control
NetIQ Secure API Manager provides a specialized layer of security for public-facing APIs that are frequently used as an interface to valuable and often sensitive information. Built to plug into your existing infrastructure, Secure API Manager integrates with enterprise identity systems through an LDAP interface. This integration enables you to implement role-based access control for managing users to specific privilege levels. Serving as an API protection layer, the gateway is designed to be deployed in your DMZ, while the authentication and access control components are kept safe behind the firewall.

Developer Services
Because the developer portal provides full authentication and access control, you can use it as a collaboration center for joint publication across internal and partner development teams. To provide ubiquitous access, the portal can be placed in the DMZ, while its management components reside behind the firewall. The portal includes an interactive API test console, where notifications are sent out to subscribers about results and updates. Just like the administration component, the actual publication engine deploys from behind the protection of the corporate firewall.

At the highest level, the Secure API Manager provides API lifecycle management from inception to end of life: create, publish, block, deprecate, and retire. Within API Manager, you can model APIs to enable collaboration with others as they are refined and updated.



Access Control and Security
Once you are finished with your API design and prototyping phase, you can securely manage visibility and access to get early feedback. Secure API Manager provides management of both sandbox and production keys to test for security. This level of control can be applied for internal users, collaborating partners, and even specific external API consumers. It enables you to secure, deliver, and customize the API lifecycle. When you're ready, Secure API Manager offers one-click deployment to the preconfigured gateway(s) for immediate publishing. Access control isn't limited to the pre-release phases; it can also be applied to consumers who authenticate using OAuth2, OpenID Connect, or SAML protocols. These options provide secure access across a broad range of platforms, including existing web apps.

Manage and Scale Traffic
NetIQ Secure API Manager enables you to segment production traffic from sandbox sessions, ensuring a higher level of security as well as protection against unexpected performance degradation. Secure API

Contact us at **CyberRes.com**
Like what you read? Share it.

Manager is also designed to control access beyond just user privilege: it can be configured by timeframe or frequency of use. By managing access beyond just limiting who can access a specific set of APIs, you can set up trial periods as well as exclude access by country, consumption, digital type, prioritization, and even throttling.

The Whole Is Greater Than the Sum of its Parts

Adding Secure API Manager to your existing Access Manager and Advanced Authentication infrastructure provides one of the most comprehensive access management platforms on the market. With its robust gateway and authentication services, Access Manager offers a leading mobile and web single sign-on solution for your internal users, customers, partners, etc. It is especially well suited for mixed environments that require a user experience beyond what is possible with simple federation alone. NetIQ Access Manager is also ideal for situations where you need to integrate multiple applications into a single user experience or integrate several backend processes into a single mobile experience. Adding Secure API Manager to that configuration further expands your ability to leverage your set of access policies and configurations.

Learn More

To learn more about NetIQ Secure API Manager, or to start a trial, go to: **www.microfocus.com/en-us/cyberres/identity-access-management/api-manager**

CyberRes
A Micro Focus line of business