White Paper
Access Manager

Architect's Guide: Making Enterprise Products Cloud-Ready

Cloud computing is fueling the digital transformation of enterprises of all sizes. It has permeated the enterprise landscape and is revamping how companies consume services, innovate and grow. Every statistic and prediction is pointing to Cloud adoption growing at breakneck speed.

Architects of enterprise products have to keep pace with this revolution, in order to stay relevant for their customers. This whitepaper is intended for Enterprise Architects, who are looking to revamp their enterprise products to be cloud-ready.

This whitepaper covers:

- Essential Characteristics of a Cloud Application
- Paths to Cloud
- Migration Roadmap
- Case Study: NetIQ Access Manager's Journey to Cloud

by Harippriya Sivapatham,
Micro Focus® Engineering

Enterprise Cloud Strategy

Cloud computing has gone well beyond being a buzzword and is altering the fundamental way of running a business. Enterprises of all sizes are looking at cloud as a means to grow in an easy but cost effective manner.

81% of enterprises have multi-cloud strategy and 44% already have central cloud team.

Right Scale 2018 State of the Cloud Survey

Enterprises have enjoyed the benefits of cloud services like Office 365 and are looking to expand more on cloud. Hence they are assessing the cloud-readiness of all other applications in their environment.

In order to retain existing customers and to gain new customers, it is crucial to make the on premise enterprise applications to be cloud-ready. This whitepaper covers the pragmatic approaches for transforming existing products to be cloud-ready while also catering to the existing customer base.

Cloud Application Characteristics

Some vendors freshen up their legacy products by adding "Cloud" to it in some way, in order to claim cloud support – a practice known as "cloud washing". Hence the National Institute of Standards and Technology (NIST) has published the following ***Essential characteristics of Cloud Computing*** [1]

To support these characteristics, the enterprise application should be transformed to:

- Be stateless and multi-tenant
- Support API based loose coupling
- Support rapid provisioning
- Support distributed storage for logs/data
- Micro services and containers to help scale up/down and be resilient.

In reality, transforming a traditional application into a cloud application having the characteristics listed above would most likely require a major revamp. Customers, on the other hand, are looking for a cloud-ready solution in a short span of time. Hence it is a matter of striking a balance between technical needs and business needs.

Paths to Cloud

The transformation of an on premise application to cloud is typically a journey, wherein the application matures gradually and takes on the cloud native characteristics in stages. Gartner specifies three stages of cloud application maturity:

Gartner: Stages of Cloud Maturity [2]

Cloud Migration Strategies

AWS and Gartner's 6 R Migration Strategies [3] specify the path to the various stages of cloud maturity.

Re-host / "Lift-and-shift" ⟹ Cloud-Hosted

- ✓ Application is deployed as-is on Cloud VMs.
- ✓ Fastest path to meet business needs. GE Oil & Gas realized 52% cost savings through lift and shift.
- ✓ Does not leverage cloud native services.

Re-platform / "Lift-tinker-and-shift" ⟹ Cloud-Optimized

- ✓ Application is enhanced to leverage cloud services, while the core architecture remains the same.
- ✓ Can support cloud attributes like auto scaling, backup and restore, disaster recovery, secure stores.
- ✓ Middle ground between "move as-is" and "complete rewrite"
- ✓ **Sweet spot for enterprise applications.**

Refactor ⟹ Cloud-Native

- ✓ Fully designed for cloud.
- ✓ Maximizes cloud attributes directly – elasticity, infrastructure services, pay for usage, etc.
- ✓ Significant effort in revamping application to have the NIST essential characteristics.

Retain

- ✓ Choose to not move to cloud and remain on premise.
- ✓ This could be decided for various reasons like security, compliance, latency or complexity.

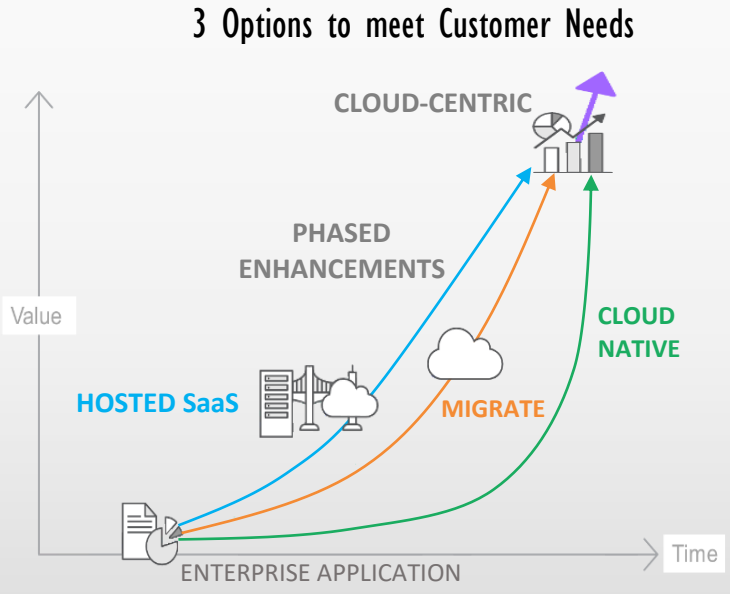
Re-purchase and Retire

- ✓ Not applicable for product architects.

Hosted SaaS: A Cloud Alternative

Hosted Software as a Service concept started during late 1990s to solve the specific problems that are currently addressed by Cloud. It allows customers to use the application without the overhead of installing and managing it.

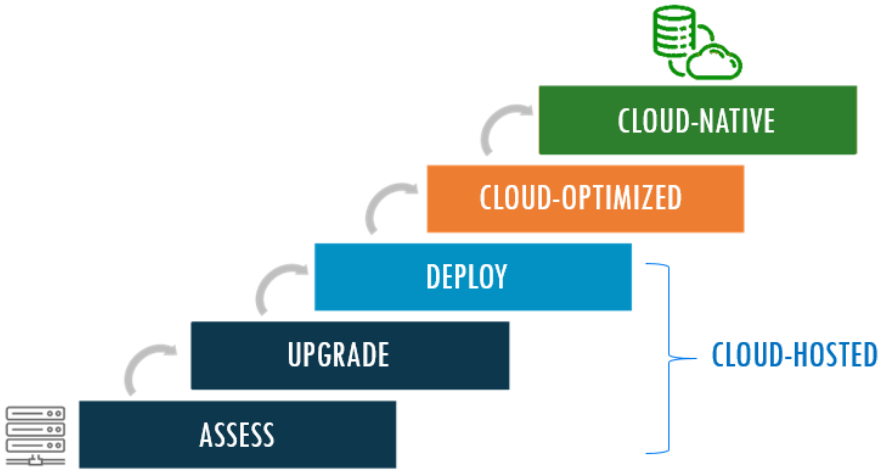
When a customer purchases the license, a team of engineers at the product company (Micro Focus in our case) will install the software in their own data center, monitor and manage it. Customer gets to use the software without the maintenance headaches. Micro Focus' Control Tower product is used to manage such hosted applications.



Any product could be offered as a Hosted SaaS with minor enhancements. This is arguably the quickest way to meet business needs, especially if the application cannot be easily moved to cloud.

Migration Roadmap

The pragmatic steps for transforming on premise application to a cloud application are:

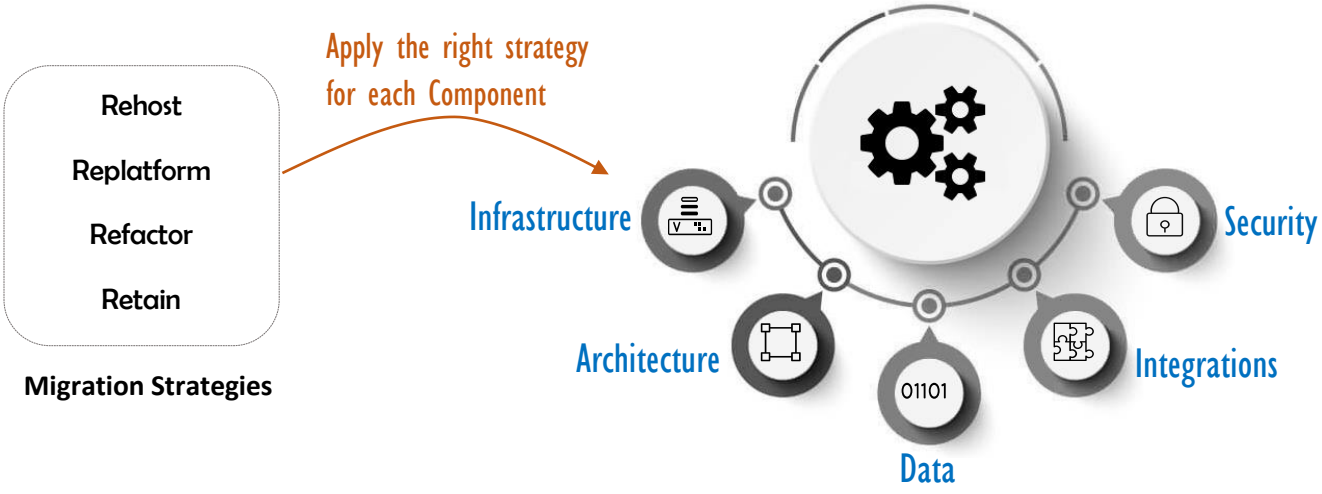


The primary focus of this whitepaper is the first three steps, which would make the application cloud-ready. Once the application is running on cloud, the next steps of optimizing and finally becoming cloud-native can be done iteratively on an as needed basis.

1. Assess and Upgrade

The first step in migration is to assess the state of the application.

- Decompose the application into components (like UI, server processes, data store, etc.)
- Assess the following 5 focus areas for each component and for the application as a whole.
- Choose the right strategy for each component. Some components may be ready to run on cloud while others cannot.



Migration Strategies

Cloud-Readiness Assessment Focus Areas [4]

Note: Public cloud is rapidly evolving with new capabilities being added by cloud providers at a staggering pace. Hence it helps to revisit the assessment periodically to see if more components could be moved to the cloud.

a) Infrastructure Considerations

Identify the hardware, OS and other network elements needed to run the application. Re-hosting Virtualized servers or x86-based Windows and Linux applications is typically straightforward.

Assess Infrastructure:

- Is the application virtualized or does it require bare metal/physical servers?
- Does it require any specific hardware?
- What are the Operating systems supported?
- Does it require specific network switches, routers, load balancers, firewalls, etc.?

Action:

- Upgrade if using legacy or un-supported hardware or OS.
- Move to Virtualized servers if possible.
- Choose the service model (IaaS or PaaS or both) and suitable cloud service provider.

IaaS vs PaaS: Which model is right for you?

Infrastructure as a Service (IaaS) provides Virtual machines and takes care of networking. You can install the OS, software, database tools, etc. You can also implement your own security, which is useful for companies in highly regulated fields.

Platform as a Service (PaaS) includes OS, databases on top of the IaaS offerings. It allows you to focus on your software and not worry about building and managing databases, security, servers, and networks. This is suitable if you have typical OS and database needs. Also note that your data will be stored in shared databases, though precautions like encryptions are done to ensure data safety. Cloud providers like Amazon AWS and Microsoft Azure support both IaaS and PaaS.

b) Application Architecture Considerations

A monolithic application can be moved as-is as the first step. However to get to the cloud optimized stage, evaluate and enhance as needed.

Assess Architecture:

- Is the application monolithic?
- What is the effort required to separate into tiers or create micro services?
- Does it expose or consume APIs?
- How does it scale? How it is made fault tolerant?
- How does it support monitoring, backups and disaster recovery?

Action:

- None may be required for stage 1. Monolithic applications can be re-hosted as-is.
- Helps to create logical grouping of components, if all cannot be moved to cloud.
- Plan for cloud-optimized stage based on this assessment.
- Ensure existing monitoring and backup approach works on cloud.

c) Data Considerations

Data is a business asset beyond imagination. Determining where the data resides, how it's secured and how it's accessed is immensely important. Data confidentiality and integrity must be preserved by the migration.

Myth: Data is not safe in the Cloud

With the enforcement of regulations like GDPR, data security is a top priority for IT directors. Hence there is a natural fear that data outside the confines of enterprise network is vulnerable. We could in fact make a case that cloud is more secure than enterprise because:

- Cloud security is designed and managed by highly trained security professionals. This is the same principle behind renting a safe deposit box at a bank rather than keeping their valuables at home.
- Even if an attacker penetrates the network, he won't know which one of the thousands of unnamed VMs is holding the data.
- Cloud providers typically use encrypted disks and also keep at least 3 copies of the data for redundancy.

Assess Application Data:

- Are there any regulations about the physical location of data?
- Are there any regulations about the movement of data across geographies?
- Are there any privacy or compliance requirements to be satisfied?
- What are the kinds of data handled and the regulations / sensitivity of those data?
- Security concerns with data handling and data exchange in the application?
- Size and frequency of data transfer that might impact the cost or performance?

Action:

- Ensure that the data compliance, security and privacy are maintained on cloud.
- Determine which data can be migrated and which data should stay on premise.
- Design the deployment to meet the data residency regulations.
- Ensure user data, configuration, logs and audit are segregated in multi-tenant setup.
- Encrypt data!

Data Protection Best Practices

Typically data must be protected in three states: at rest, in use and in motion. Migration to cloud adds one more state of vulnerability. Each state has its unique set of challenges.

i. "**Data at rest**" is the data stored on cloud hard disks while "**Data in motion**" is the data exchanged between components.
   a. Encrypt the data and to use SSL for communication.
   b. Keep and manage your own encryption keys, and do it off the cloud provider's premises.
   c. Configure strict data access control and data usage policies.
   d. Monitor who, what, where and when data was accessed.
   e. Back up the data to on premises or another cloud provider.

ii. "**Data in use**," is when the data is actually read into memory by the application process. These are harder to exploit but are also harder to handle correctly. Minimize handling clear text data.

iii. **Bulk migration of data** from the on-premises system to the cloud service is an especially vulnerable point. Ensure that data is not cached in some intermediate hop and that data is encrypted during transfer. Explore the data migration tools offered by the Cloud service providers.

d) Integrations

Applications may rely on common facilities such as user directory for single sign on or they may depend on each other through control integration (they invoke each other), data integration (they read or write the same databases or files), or presentation integration (they are mashed up on the same window or Web page). Two integrations to consider are:

i. Cloud to Cloud: Fundamental to SaaS services where multiple services interact to provide a functionality.
ii. Cloud to Enterprise: Hybrid integration is the common scenario where only select services are moved to cloud.

Assess Integrations:

- Network Integration:
  - Is Cloud to Enterprise interaction mandatory? Any alternatives for now?
  - Is there topology dependent integration?
- Application Integration:
  - Protocol used for communication between applications or components?
  - Are the tightly coupled?
  - Fail gracefully when dependent components are not available?
- Data Integration:
  - Is there a common data store to be shared across applications?
  - Are there process intensive data processing or transfer?
- Identity Integration:
  - Will corporate identities be used to access cloud applications?
  - Can corporate identities be saved on cloud or re-use enterprise user store?
  - Is single sign on required across on premise and cloud applications?
  - What is the de-provisioning process?

Action:

- Explore VPN or DirectConnect features for Cloud to Enterprise interactions, if there are no other alternatives available.
- Gradually make the applications loosely coupled by using API based integration or asynchronous messaging.
- Staging databases, replication, offline data transfers etc. could be considered with data security, performance and latency in mind.
- Authentication protocols like SAML2, WS-Trust or simple proxy services can be used to achieve SSO while keeping corporate identities on premise.
- Implement central process to terminate user access (de-provision) very quickly.
- Use Standards!

Integration Patterns:

Select the integration pattern based on the complexity and effort of the integration:

- "Bite the bullet" and modify each integration point individually. May be the approach if all else fails.
- Migrate *more* systems than initially planned – that is, move the entire "spaghetti" of integrated applications to the cloud. Focus is on keeping the integration simple and secure.
- Use caches and processes to improve performance, reduce bandwidth needs.
- Refactor the application to use APIs, asynchronous message bus or micro services

e) Security and Compliance

Cloud being less secure is mostly just a perception and not the reality. In an enterprise, the boundaries are clear and we believe that it can be easily locked down. However in a cloud, the boundaries are vanishing, responsibility is shared with the cloud provider and the attack surface is more. This leads to anxiety about cloud security. Australian web security expert Troy Hunt says that cloud security is not a binary, but that it is just "differently secure". We trade in physical control but gain experts and advanced tools that would better manage the security.

Security concepts are the same for cloud and on premise. Essentially, whatever IT teams traditionally do inside the perimeter must be extended to the cloud, but enhanced for extra measure. For example, traditional authentication should be replaced by two factor auth. The critical aspect with cloud security is that administrators need to educate themselves about the cloud provider tools and design the security elements. Poor configuration is the cause of the major security breaches in recent times.

Assess Security and Compliance:

- What are the Infrastructure level security controls already in place in your enterprise?
- What are the application level security already in place?
- Are the current security settings up to industry standards?
- Any additional security needed for the integrations?
- What are the security and compliance certifications of the cloud provider?

Action:

- Ensure that application level security will continue on cloud as well.
- Understand and configure the cloud security tools correctly.
- See the next section for details.

Cloud vendors have hundreds of different services and tools that could be put together to create your deployment. Hence there is no single tried and tested recipe for cloud security. The security elements must be customized according to your use case.

2. Build Deployment Topology

Design the deployment based on the assessments done and the action items listed above.

1. Choose the service model (IaaS or Paas) and the service provider. Ideal to choose multiple vendors to prevent vendor lock in.
2. Design the virtual network – where each component runs, how many instances and the integrations.
3. Setup VPN or Direct Connect if necessary.
4. Select the savailability zone based on data residency requirements and other security.
5. Design the disaster recovery setup.
6. Design the security elements.
    - Know what you are responsible for -- understand the Shared Responsibility Model.
    - Understand the security features and tools provided by the cloud vendor.
    - Understand the SLA and contracts provided by cloud provider.
    - Understand if there is isolation to protect your systems from malware introduced by another customer in a multi-tenant environment.
    - Understand who owns the data and if the cloud provider is obligated to deliver it to any law enforcement agency if requested.
    - Design the deployment to ensure infrastructure level security.

- Use cloud perimeters, cloud DMZs and trust zones.
- Defense in Depth - Web Application Firewalls, Multi-Factor Authentication.
- Enable two factor authentication
- Control who has access to what
- Protect the data. Encryption is the obvious choice.
- Use cloud vendor provided options like end to end encryption or Hardware Security Module (HSM) that allows to store encryption keys on premise.

7. Explore and configure vendor provided monitoring tools to watch for unusual activity.
8. Store backup on another cloud provider or on premise.

3. Deploy and Test

- Create individual virtual machines and attach them to their respective storage units. Reconfigure the domain name service (DNS) by updating the name servers to resolve the newly created VMs through the network gateways.
- Provision security devices including firewalls and VPN routers.
- Configure directory services access by implementing and testing the connections between the cloud service and the organization's directory server (LDAP, Active Directory, etc.) or, if specified by the architecture, the federation between the cloud service provider's authentication system and the customer's.
- All monitoring solutions should be implemented and tested, including any add-on monitoring tools.
- If the cloud application servers are to manage and monitor licenses, apply the activation kits and keys. If the existing monitoring and key services are to be reused, make and test the connections from the application servers to these resources.
- Harden the production environment.
- Execute a mock migration.
- Validate the deployment.
    - Ensure the core use cases are met
    - Test the security, performance, scalability.
    - Ensure that the SLAs are met.
- Document the steps!

4. Optimize

Areas to consider for optimization – disaster recovery, scalability, certify, etc.

Multi-Cloud. In order to build highly scalable and reliable applications, a *multi-cloud de-ployment* is appropriate. A multi-cloud environment is capable of distributing work to resources deployed across multiple clouds without vendor lock in.

Technical professionals must be wary of locking their applications into a particular cloud provider's service. Application architects must weigh the costs and benefits of portability on an application-by-application basis. The trend in application architecture toward radical distribution of loosely coupled, highly cohesive components is a natural fit with multicloud deployment. (Such components include APIs, miniservices and microservices.)

5. Enhance

Enhance continually towards cloud-native architecture – Microservices, 12 Factor App, etc.

To effectively leverage the full range of cloud capabilities, developers must adopt an application architecture designed with the cloud in mind, taking into consideration essential cloud characteristics:

Infrastructure Independent - Many multi-tier applications, for example, are coupled to specific infrastructure locations by incorporating server names, IP addresses, or particular web server configurations. This approach makes it impossible to use automation to scale out to multiple VMs or burst instances among private and public clouds.

Elasticity -- Elasticity provides the means for optimizing resource usage in case of fluctuating and/or unknown application workloads. Different elasticity strategies can be implemented depending on the decisions to be made on a) what part of the application to scale, b) how much it is necessary to scale taking also into account issues related to licensing costs for multiple VMs, c) which scaling type to use and, d) when and how fast is it necessary to scale, considering the observed effect of scaling latency (Brebner, 2012) for starting new images in the Cloud.

Resilience - Failures in cloud infrastructure must be handled fluidly without interruption of service

Multi-tenancy -- The multi-tenant model of serving multiple consumers from a common pool of computing resources, including storage, processing, memory and network bandwidth, is one of the essential characteristics of Cloud computing

Cost and resource consumption aware -- Application architecture is designed to minimize costs due to bandwidth, CPU, storage consumption, and I/O requests.
For more details: OPEN DATA CENTER ALLIANCE Best Practices: Architecting Cloud-Aware Applications Rev. 1.0

IBM DeveloperWorks lists Top 9 rules for cloud applications. If you follow some simple rules in your application design, you can usually make your existing applications cloud-ready without having to go through an entire reimplementation.

1. **Don't code your application directly to a specific topology**
2. **Don't assume the local file system is permanent**
3. **Don't keep session state in your application**
4. **Don't log to the file system**
5. **Don't assume any specific infrastructure dependency**

6. **Don't use infrastructure APIs from within your application**

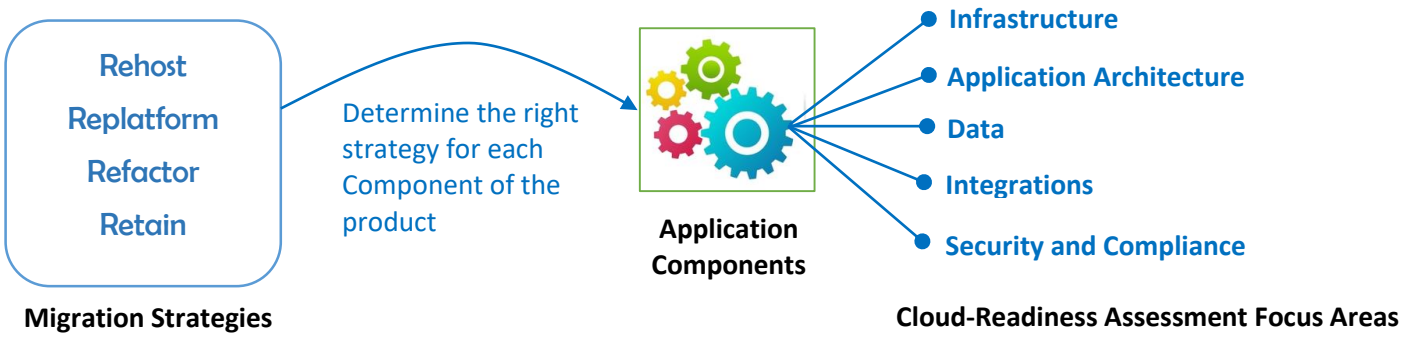
7. **Don't use obscure protocols**

8. **Don't rely on OS-specific features**

9. **Don't manually install your application**
10.

Case Study: NetIQ Access Manager's Journey to Cloud

The first step is to assess the state of the application. Decompose the application into components (like UI, server processes, data store, etc.) and evaluate the right strategy for these individual components.



Bibliography

Works Cited

[1] National Institute of Standards and Technology: "The NIST Definition of Cloud Computing". Special Publication 800-145. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

[2] Driver, Mark. "How Cloud is Revolutionizing Modern Application Development". Gartner Webinar. May 18, 2016. https://www.gartner.com/webinar/3274118

[3] Orban, Stephan. "6 Strategies for Migrating Applications to the Cloud". AWS Cloud Enterprise Strategy Blog. https://aws.amazon.com/blogs/enterprise-strategy/6-strategies-for-migrating-applications-to-the-cloud/

[4] Cloud Standards Customer Council: Migrating Applications to Public Cloud Services - Roadmap for Success. Version 2.0. http://www.cloud-council.org/deliverables/CSCC-Migrating-Applications-to-Public-Cloud-Services-Roadmap-for-Success.pdf

Next Steps

Learn more about OAuth 2.0 support and view the sample code at [OAuth 2.0 Reference for NetIQ Access Manager].

NetIQ Access Manager provides a comprehensive solution for securing your enterprise APIs, mobile, SaaS and PaaS offerings, federated applications and legacy systems. To learn more about NetIQ Access Manager, go to:

www.netiq.com/accessmanager

Worldwide Headquarters
515 Post Oak Blvd., Suite 1200
Houston, Texas 77027 USA
+1 713 548 1700
888 323 6768
info@netiq.com
www.netiq.com
www.netiq.com/communities/

For a complete list of our offices
In North America, Europe, the Middle East, Africa, Asia-Pacific and Latin America, please visit: www.netiq.com/contacts