# IGA Buyers Guide

## Selecting the Right Identity Governance & Administration Solution

Guide

www.netiq.com

**Buyers Guide**

Identity Governance and Administration

NetIQ

# What Is IGA?

Organizations have been trying to manage identities for many years. It originally began as a necessity to simply provision new employees into the system. The administrative duties of IT staff having to manage the requests and provision an employee's identity and their access entitlements into each of the systems and applications they need in order to do their job became quite labor intensive. Adding to this was the fact that when an employee left the company, it was then up to IT again to go back and remove all of the employee's access from each of these disparate systems and applications.

Great effort was put in to automate as much of these tasks as possible, but doing so across so many different applications was difficult. At the same time, as awareness of security incidents involving abuse of access began to rise, more and more compliance regulations were written and access review and recertification became necessary for proving to auditors that your organization was properly governing access entitlements. In recent years, analysts declared that the markets for both provisioning and governance have essentially converged into what is now commonly referred to as "Identity Governance and Administration" or "Identity Management and Governance."

## Market Forces

It is an exciting—and challenging—time in the identity management space. Digital disruptors such as IoT, the Cloud, Hybrid, Blockchain, Shadow IT, DevOps, and others suggest a big change in identity management. Now more than ever, it's critical to ensure that the IT infrastructure is working to protect business requirements. As we move into the future of identity management, identity governance and administration will be the critical element to secure the business of the future.

It's no secret that an organization's most valuable asset is its data. But access to that data is determined based on an individual's (or entity's) identity within that organization. It doesn't matter whether those identities are internal or external to the organization or if they are user devices or things. Ensuring those assets are properly managed and secured will require an IGA solution.

Some key facets to the decision making process of what IGA solution an organization chooses are:

- Is it future proof, can we apply what we know to future technologies?
- Should we start over, or can we evolve leveraging some of our existing investments?
- What about new drivers—does it address some of the disruptors mentioned above (i.e. Shadow IT)?
- Do our current identity management practices fit the purpose we originally intended, or have things changed?

## Do I Need IGA?

IT managers are under extreme pressure to protect business critical assets, even while they have too few resources to defend an attack on a surface area that is expanding exponentially.

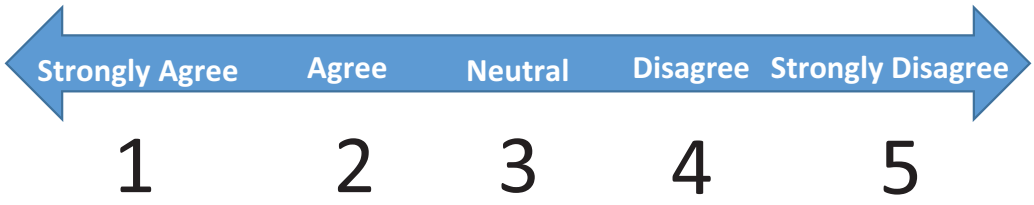
New service delivery models, mobile applications, and IT technologies are overloading our IT staff. On top of that, there is an expanding set of new identities to keep an eye on and manage. Contractors, partners, and customers now require easy, yet secure, access to our most sensitive information. There are new types of identities that don't represent "a person" as we have historically viewed them, but can be "things" like a service for example (consider the Internet of Things). All of this interaction between identities and critical assets must be accomplished, not only on legacy platforms but also in the cloud.

The effect of all this interaction is a growing attack surface. Cybercriminals are evolving their data breach approaches to exploit the weakest link, which in this scenario are the identities that access our sensitive assets. Today, almost 65% of all data breaches involved the use of stolen credentials.[1]

How vulnerable is your organization? Take this brief quiz to understand your risk of compromise.

1 *Verizon (2017, Apr 27) 2017 Data Breach Investigations Report. Retrieved from* **www.verizonenterprise.com**

## Are You Safe? Rate Your Readiness




| In My Organization… | Rating |
|---|---|
| 1. I have the data to prove, and certify, that I know who has access to what. | |
| 2. I maintain accurate historical records of when individuals access applications. | |
| 3. I maintain accountability for access and use of machine and service accounts. | |
| 4. I have controls in place to enforce segregation of duty (SoD) and mitigate access abuse by the approver. | |
| 5. My access fulfillment is "closed loop." I can prove that we fulfill and revoke access consistently. | |
| 6. I can easily define and enforce policy for who should have access to what and when approval is necessary and have involved my line of business managers. | |
| 7. Getting the right people the right access is a fast process that doesn't consume too much staff time. | |
| 8. I am confident that my managers and application owners do a thorough and complete job when performing the required scheduled access certification reviews. | |
| 9. It's simple for users to request access and for managers to approve access requests. | |
| 10. Our managers have enough information about an access request to approve or certify access in a timely and secure manner. | |
| Totals | |

| | |
|---|---|
| **10-19** | Congratulations! You likely have a solid IGA solution in place. Consider a review of your tools and processes to ensure that your implementation is future-proof. |
| **20-29** | You've done a good job at putting some key identity and access controls in place, but there is still some work to do to reduce organizational inefficiencies and reduce your risks from access misuse. |
| **30-39** | You may have a few identity and access management solutions in place, but demonstrating access control and ensuring users get access when they need it is hard if the solutions aren't integrated. |
| **40-50** | Your organization could be at risk from outside attack or misuse of access by employees, with a high potential for audit findings. Consider an IGA solution from a trusted vendor. |

If you scored 20 or above, an IGA solution can help you to reduce your overall attack surface by minimizing access rights to only those essential for the business. It can also help you to streamline access fulfillment, so it's easy for the business to manage, while users get easy and fast access to the assets and applications they need, when they need them.

## Getting Started

Every organization is different and is going to have unique pressing issues it needs to address first. Here are some common challenges that can help you understand what you need to work on first:

- **Regulatory Compliance:** 45% of people who work in information security admitted they knowingly circumvented their own security policies[2]
- **Cloud Adoption:** 59% of technology decision makers are adopting a hybrid cloud model[3]
- **Digital Transformation:** 98% of Fortune 100 companies use Office 365[4], which didn't even exist five years ago
- **Cyber Crime:** 63% of breaches featured hacking and 25% of breaches involved internal actors[5]
- **Consumerization and Shadow IT:** 77% of decision makers have used a third-party cloud application without the approval or knowledge of their IT departments[6]

Let's look more in detail at the business drivers for IGA—the goals organizations most frequently hope to achieve with their implementation.

2 *Dipietro, B. (2016, Feb 19). Survey Roundup: Enforcing But Not Following IT Security Rules. Wall Street Journal Retrieved from* **www.wsj.com**
3 *Boulton, C. (2017, Jun 19) 6 trends shaping IT cloud strategies today. CIO Retrieved from* **www.cio.com**
4 *Wilson, D. (2016, Feb 3) Office 365: Why 98% of the Fortune 100 have adopted this tech. Slideshare 3 Retrieved from* **www.slideshare.net**
5 *Verizon (2017, Apr 27) 2017 Data Breach Investigations Report. Retrieved from* **www.verizonenterprise.com**
6 *NTT Communications (2016, March) Shadow IT—Cloud Usage a Growing Challenge for CIOs. Retrieved from* **www.eu.ntt.com/en/Shadow_IT.html**

### 1. Lower Risk of Excessive Access or Fraud with Better Controls

#### "I don't know who has access to what!"

It's impossible for the organization to demonstrate compliance with data access regulations if teams cannot pinpoint who has access to what and whether that access is appropriate. Some key aspects of this challenge are:

i) Difficulty acquiring the necessary data to show who has access to what. Manual entitlement collection is time-consuming and error-prone, with a high potential for audit findings.
ii) Maintaining historical references of when individuals had access to applications. Missing information makes it difficult to research incidents and put in place compensating controls.
iii) Maintaining accountability for non-human accounts, such as service accounts, and identifying who is ultimately responsible for these accounts. Once created, machine or service accounts are often forgotten, leaving them vulnerable to attackers. These orphan/unmanaged accounts can be compliance violations.

To achieve an effective, efficient and value generating IGA implementation, ensure the solution has:

i. Collection of entitlements across enterprise applications regardless if they are on-prem, cloud or hybrid
ii. Automation of access certification processes
iii. Business-friendly access certifications
iv. Compliance reporting
v. Separation of duties enforcement
vi. Closed-loop verification

The benefits to achieving the above elements of IGA are the reduction of audit findings and stress, reduction of the risk of malicious insider abuse and finally—greater confidence in knowing who has access to what, who approved that access, when and if necessary, why.

## 2. Reduce the Cost of Compliance

### "How do I maintain compliance without spending my whole budget on it?"

Compliance with mandates that govern secure access to data can be costly in term of tools, SME resources, and auditor time spent. Solutions are needed that automate and streamline this process, and provide a feedback loop. Some key aspects of this challenge are:

i) Preparing for an audit can take many hours

ii) Producing reports to prove compliance can be difficult as you likely need to pull information from many disparate programs and systems

iii) You still have a day job, the rest of your team's responsibilities don't simply disappear when you are responding to audit requests

To achieve an effective, efficient and value generating IGA implementation, ensure the solution has:

i. A constant state of preparation so that you aren't starting from scratch

ii. Reporting functionality that is able to draw the necessary information from the various locations that your users have access to

iii. The ability to adapt to changing business needs to improve the efficiency for role based access, request/approvals, etc.

iv. Minimal interference in your IT team's routine efforts so that an audit doesn't affect other areas of your business

Compliance doesn't have to be a nuisance. In fact, it was designed to be the opposite. Preparation for future compliance audits should be done on a regular basis, so when a request comes in, you already have a large portion of your work done. The benefit is that you will also be more likely to spot problems as they arise.

## 3. Efficient Delivery of Access to the Right People

### "How can I automate security and provide self-service to reduce the IT workload?"

IT infrastructure and operations teams are tasked with fulfilling access requests in an efficient manner. But they can be suspicious of heavy identity management projects that don't deliver results. Some key aspects of this challenge are:

i) Making sure the right people have access to the right applications in an efficient manner. When users do not have what they need in a timely fashion, they either find another non-compliant solution or become very vocal, distracting IT from more productive activities. It is equally import to remove access that is no longer needed or appropriate.

ii) Administrative interfaces can require proprietary scripting languages that are difficult to learn, needing difficult-to-find talent to maintain policies and workflows. If it is too difficult to build or maintain custom processes, most processes will remain manual or require expensive consultants to provide maintenance.

To achieve IGA, ensure the solution has:

i. Adaptable roles-rules-workflow engine

ii. Automated provisioning via connectors to applications

iii. User self-service password reset

vi. Identity self service portal including access, request and approval

If you automate and offer self-service options, you benefit by reducing the time involved in manual provisioning while reducing the risks associated with inaccurately provisioning a user becuase the line of business is involved in determining whether the user should have that access. Additionally, when you off-board a team member, managers can revoke their access immediately. These benefits also remove a great deal of burden on the IT team.

### 4. Increase Business User Productivity

**"How can I be more responsive and avoid 'Shadow IT'?"**

Consumer technologies have advanced a great deal but have unfortunately conditioned users with an expectation of self-service App Store-like request and instant fulfilment. This expectation creates the following challenges for many IT teams:

i) Struggle to minimize or eliminate calls to the help desk for routine access requests and password resets. It's expensive to maintain helpdesk staff 24 hours a day, 7 days a week. More calls mean more staff.

ii) Cumbersome processes to request and approve access to applications, while managers can't see what their employees have access to. Users can't access what they need or don't use what they have, wasting resources (e.g., employee time or app licenses) and reducing organizational efficiency. Users having more access than they need adds unnecessary risk to the organization, as an infiltrator could take advantage of this access.

iii) Idle time for employees waiting an extensive period of time for necessary application access to complete their job. Employees remain unproductive while waiting for access, wasting money.

To achieve IGA, ensure the chosen solution provides:

i. A user-friendly self-service access request and approval system, backed by automated fulfillment for the most commonly used applications

ii. Identity lifecycle management, including onboarding, role changes, and deprovisioning

By addressing these needs, it ensures that the business users not only obtain their needed access faster but also provides business users with the necessary visibility to understand and approve or deny access requests. The IT team will experience a reduction in workload and the approvals will be more accurate as it involves the line of business. An IGA system also provides feedback to IT so that they can continue to "tune" access based upon historical analysis, significantly improving the end-user experience. Ultimately, both the IT department and the end users waste less time and are more efficient.

### 5. Reduce the Administrative Overhead of Access Requests

**"How can I get business approvers the information they need to respond to access requests?"**

It's the ultimate goal to have the line of business owners approve access requests, but if they lack context when approving or certifying access, this often results in the following challenges for both the business and IT teams:

i) Time delays: Lack of context requires them to ask for additional information to support their decision.

ii) Frustration: It also often leaves them with no choice but to clone access of another user, "can you just give them the same access as John?"

iii) Rubber-stamp approvals: Even though they aren't totally sure if the level of access is accurate, they approve because the task is now done and work can continue.

To achieve IGA, ensure the chosen solution provides:

i. Visibility for the approvers to see contextual information and risk scoring for decision support

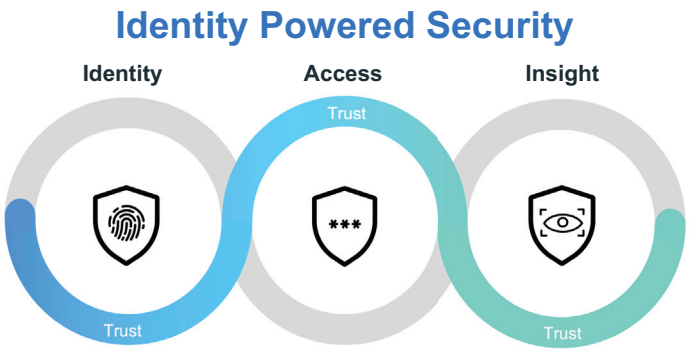
ii. Highlight of certifications that require special attention or access approval warnings

iii. Reduced risk of employees having more access than they require

By addressing these needs, you can ensure that business users have all the information they need in order to make an appropriate decision. This also removes a burden on the IT team for having to manually track down additional information at the request of the business owner as the solution has already provided it.

## Choosing the Right IGA Solution

There are many IGA solutions available from a host of trusted vendors. Which one is right for your organization?




In the not-so-distant past, organizations focused their IGA efforts on the provisioning of identity and access and on satisfying auditors as part of a compliance effort. This is a good start; however, the rapid pace with which threats are evolving, regulations are increasing, and business-enabling technologies are emerging has changed the game. Today's hyper-connected, always-on business environment has created the following potential trouble spots:

**Business Apathy:** In addition to their "day jobs," business managers are tasked with certifying access. In effect, they become risk managers without the information and education they need to make informed decisions about access. The result is rubber-stamped approvals that leave an expanded attack surface of excessive access.

**"Carl says he needs this access to get metrics for the presentation he's working on for the CEO's keynote. I don't really understand why, but I don't want to be the reason why he's not able to get that info for the CEO."**

**Tunnel Vision on Compliance:** Compliance should be the result of a well-managed IGA program and good security, not the goal. Many a breach has been perpetrated by legitimate users who misused or mistakenly exposed their privileges or by a cyberattacker who obtained legitimate credentials through a phishing attack. Don't let a passed audit fool you into a false sense of security.

**"The auditor said there were no issues with that group on our last audit, and our next audit isn't for another six to eight months. I'm not going to run this now if I don't need to."**

**Blind Spots Created by Point-in-Time Access Certifications:** If access reviews are performed every 6 to 12 months, as is common in most organizations, what happens between the reviews? People change roles or leave the organization. Projects end. Yet those privileges remain longer than is necessary, even if good certifications result in accurate revocations. The result is large windows of time for an attacker to exploit a compromised account.

**"We just checked that team's access privileges last quarter. I doubt much has changed since then."**

### Be a Part of the Digital Transformation

Think back just five years ago. Office 365 had not yet been released, and no one would have thought that within a few years, the majority of the world's Fortune 500 companies would migrate their email and data to the cloud. IGA has a critical role to play in supporting digital business transformation, including interactions with the Internet of Things (IoT).

- Consumer and IoT-level scalability: NetIQ has proven implementations involving hundreds of millions of identities. One of our customers is leveraging our Identity Manager solution to manage 55 million active identities.
- Strong federation and identity capabilities: Many vendors do not have strengths in both areas.
- A strong attribute authority model: It isn't enough to just store an identity. For Customer Identity Access Management (CIAM), you need to have an authoritative source of attributes as well—such as where that identity is located, what machine it uses for access, what preferences it has for services, and so on—in order to comply with different global regulations.
- Maintaining the relationship of an identity to devices and things is a critical component of the identity relationship model.

A strategic approach to IGA must close the loopholes that expose organizations to risk while satisfying the diverse needs of users—from employees to customers. If your business is undertaking efforts in digital

business transformation, then you must consider an IGA solution that positions you for the future.

### Balancing Risk and Business Need

A strategic approach to IGA must balance risk and business needs. IGA must become more adaptive, fulfilling the access needs of dynamic organizations while still protecting its most sensitive assets. Implementation of a strategic IGA solution can be driven by one of four requirements:

- Risk and compliance
- Security
- Operational efficiency
- Business demands

IGA has a role to play in supporting each. You should prioritize the implementation to fit your most pressing needs first becuase every organization has different priorities and challenges. Whichever area you focus on first, you must take into account critical shifts as you formulate your IGA strategy. Consider trends such as BYOD, which is really more of a reality than a trend at this point. Does your strategy account for the proliferation of devices? Will your efforts enable you to reduce the attack surface, and is it set up to adapt to future needs from the next digital transformation?

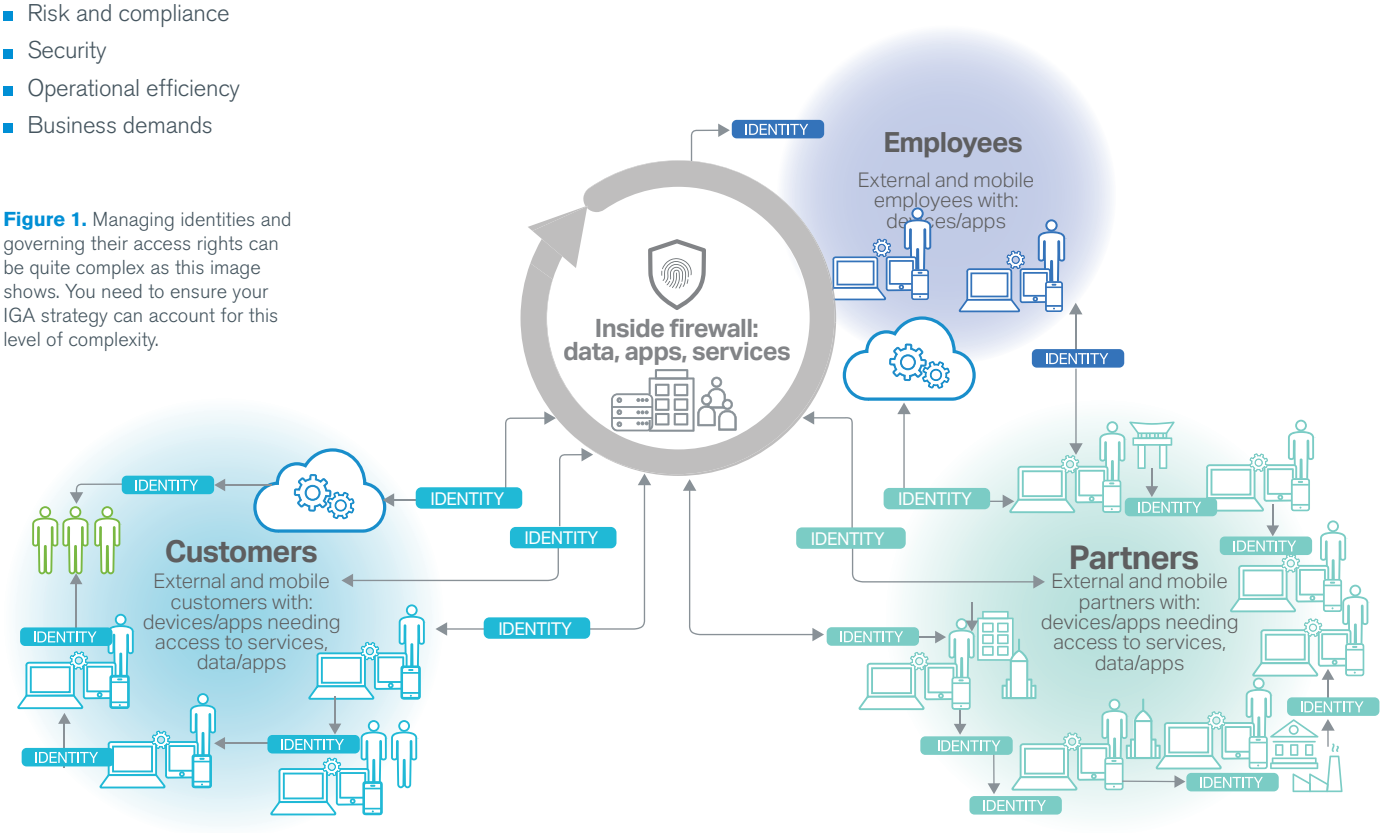



**Figure 1.** Managing identities and governing their access rights can be quite complex as this image shows. You need to ensure your IGA strategy can account for this level of complexity.

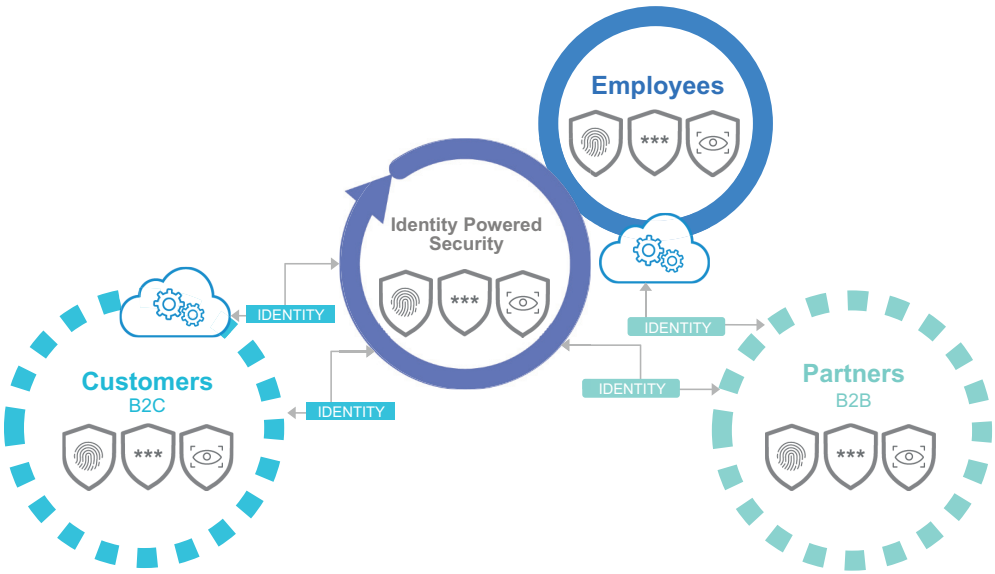
As you evaluate and ultimately make your choice of which solution you will leverage for achieving IGA, your final outcome should both improve your productivity and enable your line of business staff to be further involved in the process through approvals and self-service options. These improvements will in turn free up your IT staff to spend more time on other important facets of your business.

## Blueprint to Success

Our IGA solution helps you to efficiently provide appropriate access permissions so your users can do their job. The governance capabilities help you run effective access certification campaigns and implement identity governance controls to meet compliance mandates while proactively mitigating risk. It replaces error-prone, time-consuming manual methods that can expose your organization to compliance violations and risk from excessive access. The administration capabilities of our solution power the entire identity management lifecycle by managing identities and their associated attributes. It helps you ensure that users have the right amount of access for their roles. These capabilties enable your organization to reduce the costs of manual account management while reducing the risk of unauthorized access.

NetIQ works as a partner with our customers on an approach that incorporates governance into the identity management and access request process. Your organization can leverage this approach to simplify, secure, and remove a lot of the burden on your staff. With more than 5,300 customers worldwide, we have worked with organizations of numerous industries and sizes and have modelled an approach method on how to tackle IGA.

# An Identity-Centric Approach




**A Desired State**

- Scale
- Centrally managed identities providing a single view
- Multiple delivery models (on-prem, SaaS, hybrid)
- Clear roles and relationships modelled
- Risk based adaptive security
- Business benefit - solution architecture
- Clear consistent governance, privacy controls and privilege management implementations
- Experience embedded at the beginning

## Why Us, How Are We Different?

While there are many solutions on the market that tackle either identity administration or governance, the NetIQ solution set is different. We take an integrated approach to Identity Governance, which leverages common components for a unified experience for both your users and your IT staff. This approach and our experience offer several benefits to your organization.

### Less Complexity and Services

Through integration, we're able to reduce the amount of custom services you would normally have to purchase from other vendors to make their governance and identity solutions talk to each other. In terms of importing and interpreting data from your various applications, our IGA solution is able to read it as is in most cases, again saving you conversion and rewrite services.

### Single Point of Contact

If you rely on two (or more) vendors and you have a technical support issue, you will need to make several calls. Additionally, you may encounter the blame game, where one vendor tells you it's the other vendor's software that is causing the issue and vice versa. When you leverage the same vendor for both identity administration and governance, you have one company to call, and we have no concern with blame. We concern ourselves only with finding the solution.

### Scalability

We have more than 5,300 identity customers, which means we're managing more than 436 million users combined. About 33% of our customers are larger than 10,000 users, with the largest account managing 55 million active identities. All that to say, our solution can scale.

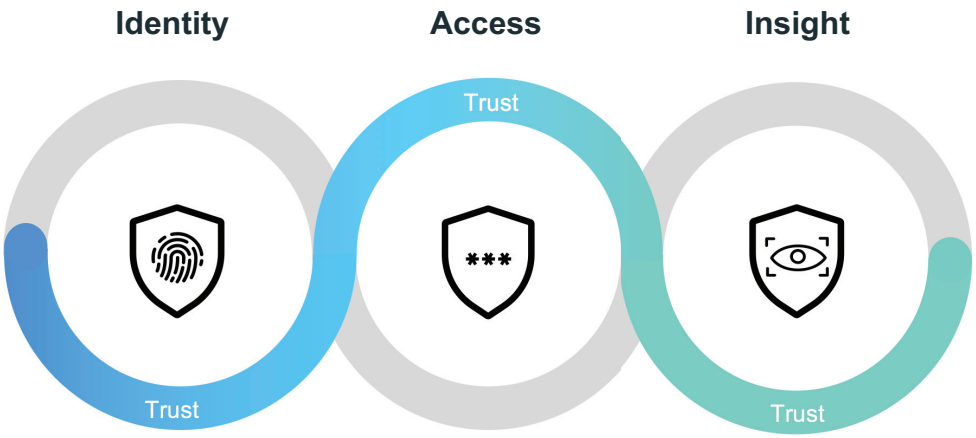
### Adaptive Governance

Identity Governance needs actionable insight to stay current and provide context for good decision-making. It is the missing ingredient in many of today's approaches to IGA. To meet the demands of dynamic environments, we offer Adaptive Identity Governance. Event driven changes that cause real-time responses along with analytics that provide context drive down risk, going above and beyond satisfying auditors.

## IGA Is One Part of an Integrated Approach to Identity Access and Security

Identity and access management is disconnected from security management in many IT organizations. But both want the same thing—to protect sensitive information from misuse or theft, using a method that is transparent and convenient for users. And both teams have capabilities that would be useful for the other. NetIQ helps organizations address risk and complexity, from both privileged and regular users, with an integrated set of solutions that manage the identity and access lifecycle, authentication, identity governance, and security monitoring. We call this approach Identity-Powered Security.

# Identity Powered Security




Consisting of three complementary disciplines, Identity-Powered Security also includes specialized Privileged Identity Management solutions that help organizations meet compliance regulations and prevent data breaches associated with the misuse of privileged user accounts.

To learn more about NetIQ's IGA solutions, please visit: **www.netiq.com/solutions/identity-access-management/**

**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

**www.netiq.com**