Identity and Access Management and the Extended Enterprise

Managing enterprise IT assets such as applications and data, devices, and user identities has radically changed in recent years and led to a phenomenon referred to as the “extended enterprise.” The traditional paradigm wherein IT assets were operated from a single physical location on a homogenous platform and accessed primarily by enterprise employees no longer provides businesses with the agility and connectivity required to remain competitive. In the new “extended enterprise” paradigm, on-premise applications have been replaced with cloud-based applications; the use of desktop computers has been superseded by smartphones, tablets and laptops; and perhaps most importantly, internal employees are no longer the only users of enterprise IT assets. Business partners, customers and contractors are all routinely granted access to enterprise IT assets.

On one hand, identity and access management (IDAM) technologies enable the extended enterprise. For example, techniques such as identity federation enable employees to seamlessly access cloud-based mail or sales applications using their smartphones from any location. This not only enables a level of productivity impossible under the static traditional IT paradigm but also allows the enterprise access to best-of-breed technology while freeing enterprise IT to focus on other tasks. However, when improperly implemented, identity federation can expose the enterprise to significant risks such as data breach and data loss. This poses a challenge for businesses: protecting access to sensitive data regardless of the means used to access it.

Organizations must enter this brave new world with care. As IDAM decisions and controls are extended further from the core of the enterprise, organizations must implement a rigorous governance regimen to mitigate security and privacy risks. Furthermore, organizations should adopt a strategic approach to IDAM deployments, and avoid a series of uncoordinated point solutions. In this way, organizations can establish a strong basis for trust among the participants in the extended enterprise.
In order to be successful, organizations interested in extending their enterprise should consider the following:

- **IDAM for external user populations** – In the extended enterprise, the population of users that interact with enterprise systems and data has grown to include contractors, business partners, customers and social media users. Managing identities for such a diverse user population is a significant cost and operational burden, as well as a major security risk. Solutions for sharing and/or outsourcing this burden include identity federations (e.g., Kantara and InCommon), identity-as-a-service (IDaaS) solutions and identity providers (IdP). However, these solutions come with certain requirements. IDaaS and IdP solutions require contracts and/or service-level agreements (SLAs) with the providers, while joining a federation requires the enterprise to have a common set of policies, practices and protocols in place to establish trust in identities between federation member organizations.

- **IDAM in the cloud applications** – By utilizing cloud applications, organizations can take advantage of best-of-breed software at lower cost with less operational overhead. However, cloud-based computing extends the enterprise security perimeter to include the provider’s computing resources and personnel. This significantly impacts the enterprise’s security posture and risk profile. Organizations often must adopt security controls inherited from the cloud provider, whether they like it or not. Likewise, sharing employee and customer identity data with third parties poses privacy risks, and may complicate monitoring, help desk and audit activities. Enterprise IDAM policies and procedures must be extended to incorporate the access control capabilities of cloud service providers and may necessitate the implementation of compensating controls.

- **IDAM and mobile devices** – The diversity of Internet-connected mobile devices has exploded since the advent of the iPhone. Smartphones, tablets and other mobile devices have become common entry points to enterprise networks, applications and data. Organizations are struggling to find ways to ensure that mobile devices are secure, being used by the right person, and connecting to enterprise assets via a secure connection. To address these concerns, organizations should employ IDAM mechanisms such as adaptive authentication and location-based policies.

**Benefits and Opportunities**

Cloud applications, mobile devices and diversified user populations provide the extended enterprise with opportunities to take advantage of new services previously unavailable. Benefits include:

- **Reduced capital costs** – By utilizing the resources of a cloud computing services provider, an organization can grow its IT capabilities and services without the need to buy expensive hardware, software or software licenses.

- **Improved accessibility** – The cloud, as well as mobile device computing, can enhance the accessibility and availability of enterprise services for customers and employees.
• **Easier introduction of new services** – Cloud applications and services can be deployed quickly in a cost-efficient manner.

• **Reducing user support costs** – Enabling applications to accept external users’ existing identity credentials reduces the cost burden to an organization’s IT resources.

However, existing enterprise IDAM techniques do not readily transfer to the extended enterprise, and there is no “silver bullet” that will eliminate the risks to the extended enterprise. Therefore, it is essential to understand these risks and identify appropriate mitigation strategies before taking action. Organizations should be asking questions such as:

- What customer and employee data can we safely share with business partners and third parties?
- What external identities and credentials should we accept, and what are the risks?
- Who should have access to our systems and data and what privileges should be allowed?

**Our Point of View**

Organizations should conduct a thorough risk assessment of all systems and/or data they plan to share in the cloud or expose to mobile devices. They should give special consideration to the impact of user authentication errors when planning and evaluating remediation strategies. In extending their IDAM capabilities, organizations should consider the following actions:

- **Determine levels of identity assurance** – Not all transactions will require the same level of identity authentication (i.e., affirmation of a person’s unique identity). Give consideration to developing several levels of identity assurance and, ultimately, trust. Criteria for determining trust may include “the degree of confidence in the vetting process used to establish the identity of the individual to whom the [identity] credential was issued, and the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.”

- **Map identified risks** – For each transaction that requires user authentication, map the identified risks to the appropriate controls required to remediate the risk of unauthorized access to the affected systems or data.

- **Select security controls** – It is unlikely that an organization will be able to address all potential risks without investing in some tools and technology. Conduct thorough research when evaluating which IDAM technologies and techniques provide the best solution. This may require obtaining evaluation copies, implementing them in the organization’s test environment and assessing their true capabilities versus those advertised.

- **Develop processes and procedures** – Tools cannot solve the IDAM issues alone. Be sure to make the required changes to organizational policies, processes and procedures.

---

• **Conduct validation** – To ensure that the target system/solution will achieve the desired results as intended, the organization should conduct a comprehensive review of all security controls. Consider engaging the services of an independent third-party auditor.

For enterprise employees and customers, organizations should identify which user data stores are authoritative, and understand how to both provision and de-provision users from cloud applications. Organizations are encouraged to rely on standards-based interfaces with cloud service providers, and to avoid proprietary protocols. Finally, organizations should perform testing and monitoring to validate the deployments’ conformance, performance, usage and uptime.

**How We Help Companies Succeed**

Protiviti works closely with private industry and government agencies, providing comprehensive support and advice for establishing, operating and improving critical aspects of identity and access management (IDAM) initiatives. We provide subject-matter expertise and services for IDAM governance, policy, technology, testing, risk assessment, integration and operations.

Protiviti has experience with numerous IDAM tools and techniques. We help organizations assess and select the most appropriate solution based on their specific risk profile. Protiviti also helps clients implement and manage their IDAM plans to ensure their business objectives are met in the most secure manner possible.

**About Protiviti**

Protiviti ([www.protiviti.com](http://www.protiviti.com)) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 35 percent of FORTUNE 1000® and FORTUNE Global 500® companies. Protiviti and its independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

**Contacts**

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone Number</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chris Louden</td>
<td>+1.703.299.4703</td>
<td><a href="mailto:chris.louden@protiviti.com">chris.louden@protiviti.com</a></td>
</tr>
<tr>
<td>Kevin Hawkins</td>
<td>+1.703.299.4701</td>
<td><a href="mailto:kevin.hawkins@protiviti.com">kevin.hawkins@protiviti.com</a></td>
</tr>
<tr>
<td>Cal Slemp</td>
<td>+1.203.905.2926</td>
<td><a href="mailto:cal.slemp@protiviti.com">cal.slemp@protiviti.com</a></td>
</tr>
</tbody>
</table>

© 2014 Protiviti Inc. An Equal Opportunity Employer M/F/D/V. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.