Enabling and Protecting the Open Enterprise

ca technologies

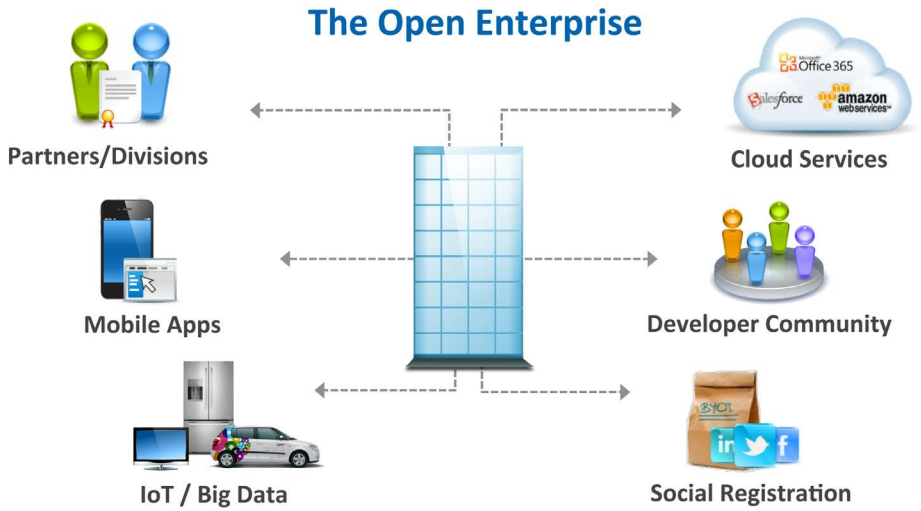
The Changing Role of Security

A decade or so ago, security wasn't nearly as challenging as it is today. Users, data and applications were all centralized in data centers that, in effect, kept them contained within a network perimeter. And whatever or whomever wasn't confined within these boundaries could be authenticated via a virtual private network (VPN).

Those were the "good old days." The days when security was predictable and easier to control. But those days are gone forever.

The consumerization of IT and the march toward cloud, mobility and social media have fundamentally changed how organizations innovate and interact. As a result, business applications and data now exist far beyond the boundaries of corporate firewalls. Indeed, they are often distributed off-premise and across wide geographical areas. What's more, users can access this data via multiple identities and devices.

Thus, the traditional notion of a "network perimeter" no longer exists. The new open enterprise must be able to capitalize on innovation and efficiency enablers, like cloud and mobile. But securing the proliferation of identities dispersed across a new environment is easier said than done.



John Hawley, Senior Director of CA Security Strategy, explains the implications of identity as the new network perimeter.

Watch the video. Click here.

The Challenges of Securing the Open Enterprise

The increasing "inconvenience" of security

The consumerization of IT. Bring your own device (BYOD). The mobility explosion. The relentless speed of the market. All these trends have contributed to the perceived nuisance of end-user security processes. For customers who are accustomed to accessing information quickly, cumbersome registration and authentication processes that vary according to each channel they use (such as web, mobile and API), can turn them away. What customers really want is security that requires less disruption.

Enterprise employees and partners also demand a similar level of user convenience. They, too, want simple security models that enable policies to be enforced across channels—to streamline app deployment times and costs—and to make the process of accessing corporate data more efficient.

The rise of "shadow IT"

While improving enterprise innovation, scalability and efficiencies, the cloud has also complicated the role of security. For one, informal infrastructures of servers, applications and data continue to spring up, as employees easily acquire cloud services online. And oftentimes, IT isn't even aware they exist. Securing these "shadow IT" environments, which reside outside the control of centralized IT and often have their own identities for cloud-based apps, is a significant challenge.

The ever-persistent threat landscape

If the above challenges weren't enough to keep a Chief Security Officer (CSO) up at night, many IT departments are also burdened with trying to protect their organizations from a variety of threats. These include the disclosure or loss of sensitive data by employees and external attacks that are motivated by financial gain. After all, the cost of a successful external breach is approximately $5.4 million on average,[1] not to mention the lingering business impact of reputational harm.

A comprehensive identity and access management (IAM) solution can help you meet these critical challenges. Let's see how.

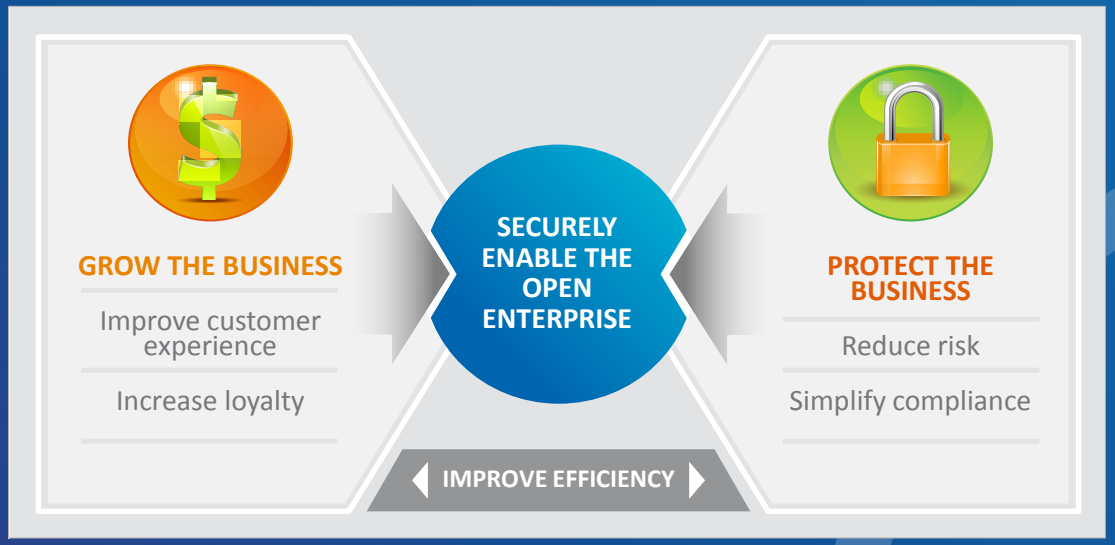
[1]Ponemon Institute, 2013, *Cost of Data Breach Study*: United States.

The New Role of Security: Enable and Protect the Enterprise

In the past, securing and enabling the operations and growth of the enterprise entailed striking a delicate balance. That's because increased security meant less business enablement. The more security you added, the more difficult it became to conveniently do business with you. Conversely, increased business enablement signaled decreased security. But today, security should no longer be a straight balancing act. IT *must* enable the business for growth, and protect it from risks and attacks. It can do that by:

- ☑ Deploying new online services quickly
- ☑ Protecting customer transactions
- ☑ Safeguarding access to corporate resources across channels
- ☑ Improving the user experience

At the same time, enabling the enterprise won't do much good if it is left vulnerable to security threats that can bring business—and profits—to a grinding halt. So IT must also be equally vigilant about protecting systems and data from internal threats and external attacks.



Securely Enabling the Open Enterprise: The Path Forward

The roadmap to enabling and protecting the open enterprise can be viewed in the context of three critical imperatives. Click on each imperative to learn more.

Deliver secure new business services >>	Secure the mobile, cloud-connected enterprise >>	Protect against insider threats and targeted attacks >>

Industry-leading identity and access management (IAM) solutions can help companies achieve all the above goals.

Securely Enabling the Open Enterprise: The Path Forward

The roadmap to enabling and protecting the open enterprise can be viewed in the context of three critical imperatives. Click on each imperative to learn more.

Deliver secure new business services >>	Secure the mobile, cloud-connected enterprise >>	Protect against insider threats and targeted attacks >>

Deliver secure new business services

For organizations to maintain their competitive edge and keep pace with market demands, they must embrace various technologies that support innovation. Equally important is the need to deploy applications securely, seamlessly and at the speed of business. And in doing so, IT must ensure a user-friendly security experience that does not require separate models across web and mobile channels.

Industry-leading identity and access management (IAM) solutions can help companies achieve all the above goals.

Securely Enabling the Open Enterprise: The Path Forward

The roadmap to enabling and protecting the open enterprise can be viewed in the context of three critical imperatives. Click on each imperative to learn more.

Deliver secure new business services >>	Secure the mobile, cloud-connected enterprise >>	Protect against insider threats and targeted attacks >>

Secure access to the mobile, cloud-connected enterprise

IT must ensure that employees, partners and customers around the globe can all access organizational resources securely—whether they're on-premise or in the cloud. In addition, automated processes must exist to ensure that each user has the proper access rights, based on their user type and role.

Industry-leading identity and access management (IAM) solutions can help companies achieve all the above goals.

Securely Enabling the Open Enterprise: The Path Forward

The roadmap to enabling and protecting the open enterprise can be viewed in the context of three critical imperatives. Click on each imperative to learn more.

Deliver secure new business services >>

Secure the mobile, cloud-connected enterprise >>

Protect against insider threats and targeted attacks >>

Protect the enterprise from internal and external threats

While there is no silver bullet that can prevent all threats, organizations can significantly reduce their security exposures by understanding the total threat environment and executing proactive measures to defend the enterprise from exposures and attacks. This includes identity controls at each level of the infrastructure in order to deploy a “defense in depth” strategy.

Industry-leading identity and access management (IAM) solutions can help companies achieve all the above goals.

Deliver Secure New Business Services

The objective: Deploy applications quickly and securely across a range of access models to improve the overall customer/end-user experience while enabling business growth and agility.

The IT initiatives (click on each to learn more):

Improve customer engagement >>	Accelerate service delivery >>	Externalize the business >>

Deliver Secure New Business Services

The objective: Deploy applications quickly and securely across a range of access models to improve the overall customer/end-user experience while enabling business growth and agility.

The IT initiatives (click on each to learn more):

Improve customer engagement >> | Accelerate service delivery >> | Externalize the business >>

Improve customer engagement

Providing a simple, convenient user experience entails more than just offering an attractive GUI. It involves the ability to enable consistent security across all application channels, including web, mobile and API, and to eliminate the inconvenience of different authentication requirements for different apps and access methods. This capability can be enabled through:

- Industry-leading single sign-on (SSO) solutions for Web and mobile apps that allow users to gain access to all applications by logging in once, vs. being prompted to log into each individual application
- Identity federation that links a user's identity across multiple identity management systems
- Social identity registration that enables customers to leverage their existing identities, from sites such as Facebook or Google, for low-risk interactions (such as information gathering)

The benefit: Improve the end-user experience so as to help drive repeat business and increase customer loyalty.

Deliver Secure New Business Services

The objective: Deploy applications quickly and securely across a range of access models to improve the overall customer/end-user experience while enabling business growth and agility.

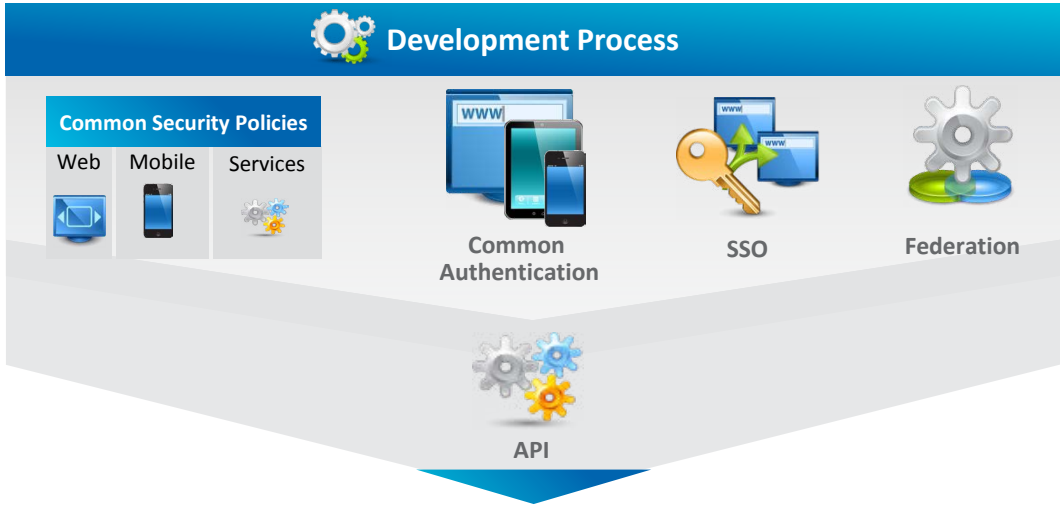
The IT initiatives (click on each to learn more):

Improve customer engagement >> | Accelerate service delivery >> | Externalize the business >>

Accelerate service delivery

These days, the speed at which a company can get apps to market can make or break it. But it's just as critical to release apps across different channels and support numerous access methods. An effective way to facilitate both of these goals is to:

- Centralize identities and access privileges into a single authoritative source that's external from the apps themselves
- Externalize security policy enforcement from the apps, which can simultaneously speed application development while reducing the costs and risks of inconsistent security enforcement
- Implement a strong risk-based authentication solution to deliver consistent and adaptive authentication across all channels



Reduce development time

The benefit: Speed application development while reducing costs and improving the user experience through common security mechanisms across all channels.

Deliver Secure New Business Services

The objective: Deploy applications quickly and securely across a range of access models to improve the overall customer/end-user experience while enabling business growth and agility.

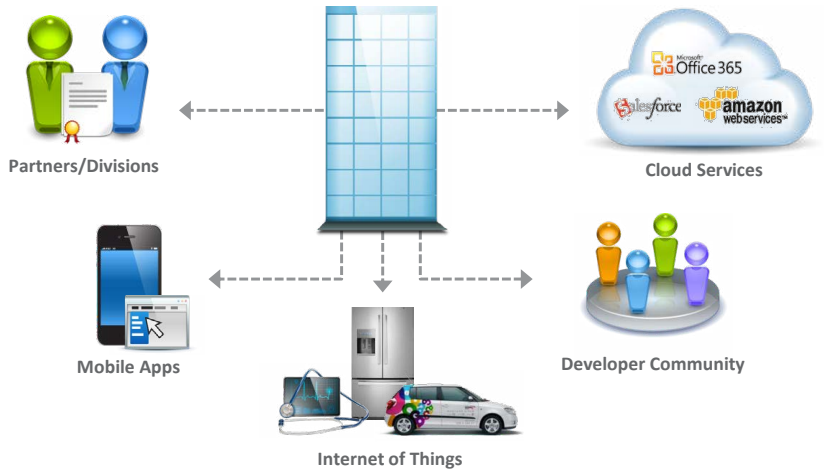
The IT initiatives (click on each to learn more):

Improve customer engagement >> | Accelerate service delivery >> | Externalize the business >>

Externalize the business

The idea here is simple—make data and applications externally available to internal and third-party developers via APIs to capture more distribution channels and potential customers. This will enable an organization's partners to develop complementary solutions, so that the richness of the entire solution environment is increased. This can be achieved through a comprehensive API Security & Management solution that not only controls access to APIs but also enables developers to more easily use them to speed development of these complementary solutions.

The benefit: Develop more market opportunities by securely enabling a partner ecosystem that can develop complementary solutions that can be distributed through new channels.



Develop new channels through API Security & Management

Secure Access to the Mobile, Cloud-connected Enterprise

The objective: Secure business collaboration and access to distributed IT resources across the enterprise for employees and partners, while improving the efficiency of key identity-related processes.

The IT initiatives (click on each to learn more):

Secure access to applications >>	Streamline and govern user access >>	Improve secure collaboration >>

Secure Access to the Mobile, Cloud-connected Enterprise

The objective: Secure business collaboration and access to distributed IT resources across the enterprise for employees and partners, while improving the efficiency of key identity-related processes.

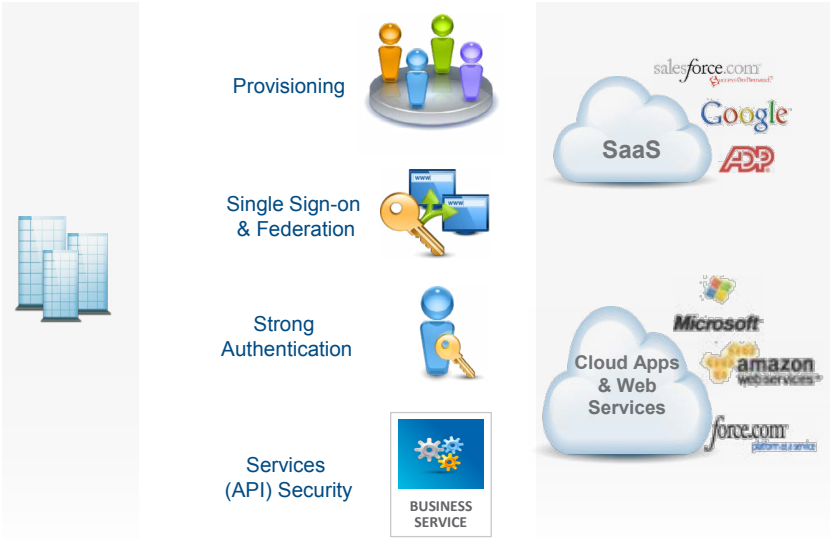
The IT initiatives (click on each to learn more):

Secure access to applications >> | Streamline and govern user access >> | Improve secure collaboration >>

Secure access to applications

Whether applications are based in the cloud, on-premise or a hybrid environment, their level of security should be the same. Organizations need a way to provision and manage access to all apps, and many are deploying identity services in the cloud for the efficiency benefits it can provide. That's why an IAM solution that can be deployed either on-premise or in the cloud is important. This flexibility gives enterprises the increased business agility they need to adopt cloud services as their needs dictate.

The benefit: Enable business collaboration and innovation by securing corporate data.



Secure Access to the Mobile, Cloud-connected Enterprise

The objective: Secure business collaboration and access to distributed IT resources across the enterprise for employees and partners, while improving the efficiency of key identity-related processes.

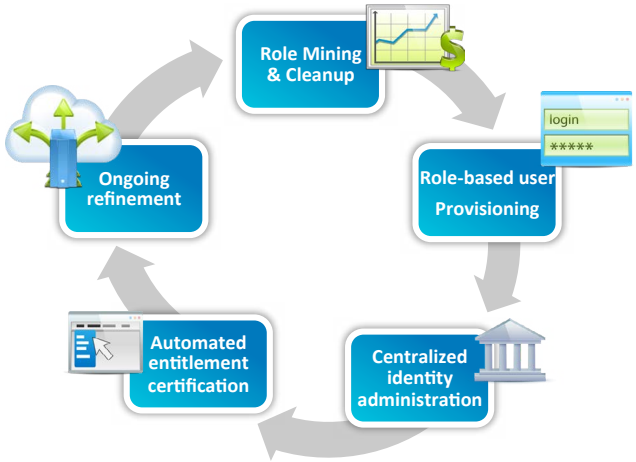
The IT initiatives (click on each to learn more):

Secure access to applications >> | Streamline and govern user access >> | Improve secure collaboration >>

Streamline and govern user access

Many enterprises still rely on manual processes to manage user-access permissions. An identity management and access governance solution can automate, and thus streamline, this entire process. Users can request access rights to applications via forms that are automatically submitted to managers. More importantly, automating the access certification process can improve management productivity, reduce costs and simplify compliance audits.

The benefit: Streamline the process of user access certification while improving security.



Identity lifecycle management and governance

Secure Access to the Mobile, Cloud-connected Enterprise

The objective: Secure business collaboration and access to distributed IT resources across the enterprise for employees and partners, while improving the efficiency of key identity-related processes.

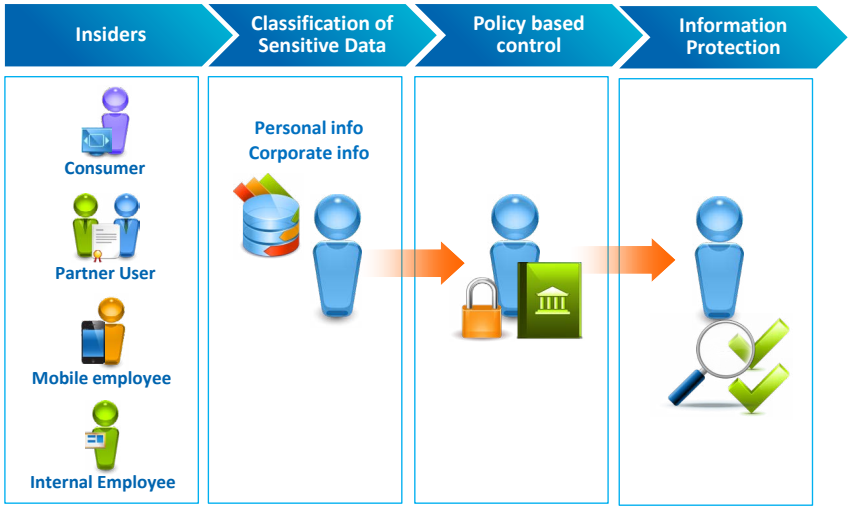
The IT initiatives (click on each to learn more):

Secure access to applications >> | Streamline and govern user access >> | Improve secure collaboration >>

Improve secure collaboration

Employees and partners need to securely share business data so as to facilitate effective business growth. This means they need a strong but non-intrusive method of authenticating themselves to the apps that they share. In addition, it is important to not only control access to data, but also to the use of that data. Improper use of data (such as emailing it outside the company) can have disastrous effects. *Content-aware access management* enables an organization to control access to information based not only on the role of the user, but also on the content of the information.

The benefit: Improved sharing of data and protection against information misuse, theft or disclosure.



Protect the Enterprise from Internal and External Threats

The objective: Prevent data breaches—even from administrators!

The IT initiatives:

Reduce insider exposures

Insiders who commit theft or sabotage can cause significant damage to an enterprise due to their access to sensitive data and critical infrastructure. Privileged administrators are an especially serious threat, as they often have unfettered entry into key systems. Even simple careless acts can have potentially disastrous effects.

Combat external attacks

An advanced persistent threat (APT) is a long-term, sophisticated strike launched against a specific entity. Its targets include the systems and data of a variety of institutions. APTs are often state-sponsored and their objectives usually reach far beyond simple theft; perpetrators are often seeking intellectual property, strategic intelligence, attempting financial extortion or economic or technical sabotage.

Organizations can apply a proactive, holistic approach to security that can help prevent both internal and external attacks by applying a security model that allows or denies actions based on business rules, data sensitivity and specific types of behavior. Capabilities include:

- Controls for data loss prevention
- Privileged identity management

The cases of Edward Snowden and Bradley Manning demonstrate what can happen with a lack of controls for both data and privileged users.

The benefit: Prevent both internal and external security breaches by enforcing controls over privileged users and data.

About the Solutions from CA Technologies

CA IT Security Solutions can help organizations:

Deliver secure new business services

- Deploy secure online business services quicker for improved agility and customer loyalty
- Improve customer engagement through support of social identities
- Develop new business channels through externalization of business APIs

Secure the mobile, cloud-connected enterprise

- Securely adopt cloud services
- Enable secure collaboration with employees and partners
- Streamline and govern user access for increased efficiencies

Protect against inside threats and external attacks

- Control privileged user actions and manage shared accounts for reduced risk
- Combat external attacks
- Protect confidential corporate and customer information from improper use, theft and disclosure

Continue >>

About the Solutions from CA Technologies (continued)

CA IT Security Solutions represent one of the broadest and most comprehensive IAM suites in the industry. Our solutions are highly integrated to simplify and reduce the total cost of IT security management. And, we provide these capabilities across all major environments (cloud/on-premise, virtual/physical, and distributed/mainframe) and access models (Web, mobile and APIs) to significantly increase business agility.

CA Security capabilities

- Identity management and governance
- Secure SSO and access management
- Advanced authentication
- Privileged identity management and virtualization security
- API security and management
- Data protection
- Cloud-based and on-premise identity management services
- Security management for mainframe

CA Security benefits

- Speed the delivery of all apps, including those for mobile devices
- Secure collaboration and data sharing
- Protect data from unauthorized access and use
- Enhance compliance through better control over user access rights
- Grow the business via new distribution and partner channels
- Boost efficiency through identity process automation

For More Information

To learn more about how CA Security solutions can help organizations grow and thrive by reducing risk, improving operational efficiency and increasing business agility, visit ca.com/us/identity-and-access-management.aspx or call 1-800-225-5224.

For additional recommendations on securely enabling the open enterprise, read the following resources:

- Identity-centric Security (whitepaper)
- Identity is the New Perimeter (ebook)
- Defending Against Advanced Persistent Threats (ebook)
- Securely Enable Online Business (whitepaper)
- The Forrester Wave: Identity and Access Management Suites (analyst report)
- Engaging Your Mobile Customers While Protecting Sensitive Data (whitepaper)

CA Technologies (NASDAQ: CA) is an IT management software and solutions company with expertise across all IT environments—from mainframe and distributed, to virtual and cloud. CA Technologies manages and secures IT environments and enables customers to deliver more flexible IT services. CA Technologies' innovative products and services provide the insight and control essential for IT organizations to power business agility. The majority of the Global Fortune 500 relies on CA Technologies to manage evolving IT ecosystems.

ca technologies