identity as the new perimeter: securely embracing cloud, mobile and social media
IT transformation and evolving identities

A number of technology trends, including cloud, mobility, social media and the consumerization of IT, have transformed not only IT, but also the way employees, partners and customers interact with an organization. And as software as a service (SaaS) and cloud applications have grown in popularity, IT environments have become more distributed, fragmented and nebulous – with many components existing outside of the traditional security perimeter of firewalls and virtual private networks (VPNs).

As a result, protecting today’s cloud-based, mobile enterprise requires a new approach. Because our applications and data are protected by many different cloud providers, authenticating users into those environments is the one central point of control we can maintain. In other words, identity must become the new “perimeter” security control for the distributed IT environment.

According to a recent CA commissioned Ponemon Institute survey, 64% of IT and IT Security professionals now look to hybrid identity and access management solutions, which can support both on-premise and cloud-based applications.¹

the disappearance of the traditional network perimeter

Historical network with single outer shell

In the past, the network perimeter would provide a hard outer shell around all of its data and applications. This kept everything contained, and security and IT teams could easily manage employee identities internally. Then, as the number of remote employees grew, VPNs became part of the perimeter and took over the job of authenticating employees when they were off-premise.

Today’s reality with activity outside of the security perimeter

However, as the popularity of cloud, infrastructure as a service (IaaS), platform as a service (PaaS) and SaaS offerings has grown in recent years, more and more applications have moved outside of the firewall. What’s more, external partner and customer users are now accessing both on-premise and cloud applications – some behind a firewall and some not – creating additional identity management challenges outside of the traditional perimeter.
the rise of “shadow IT”

With the traditional perimeter disappearing and the increased use of cloud applications, business managers can now purchase cloud services on the spot – all they need is a credit card. In some cases, organizations have informal infrastructures of servers, applications and data that have been acquired in this manner. When this happens, the central IT group usually has little control over the service, which creates significant security challenges for the content in the cloud.

cloud-based “shadow IT” leads to “shadow identities”

When shadow IT components become part of the infrastructure, users create new identities to access them, possibly using the same username and password as they do on the enterprise systems, which multiplies security risks. Or, users will generate new usernames and passwords for each service, collecting a variety of “shadow identities” that must be managed alongside their enterprise credentials.

The challenge for IT security is that the more fragmented these shadow components are, the more difficult it becomes to manage identities and access. For example, if identities are not being centrally managed, it can become impossible to remove access when an employee changes job roles or leaves the organization.
the rise of identity as the new network perimeter

The concepts of “inside the network” and “outside the network” have no meaning anymore. The traditional perimeter is gone, so organizations have to change how they manage security and user identities if they want to keep their data and applications secure. In this new landscape, identity must become the security perimeter.
a new approach to identity management

Traditionally, organizations have approached security from a technology-stack perspective, infusing identity and access management directly into the servers (physical and virtual), databases, applications, operating systems and networks that comprise their IT infrastructures.

However, with the traditional perimeter disappearing and organizations consuming more business services via the as-a-service model, it’s time to start thinking about security from a brokerage perspective. In this model, an organization will broker security between itself and all of the application instances where its data resides:

The cloud provider: handles the infrastructure and application security as part of its service-level agreements (SLAs). Authentication of enterprise customers should be left to the enterprise.

The enterprise security team: can limit proliferation of shadow identities if it manages all user authentications to cloud services. The enterprise can control password policy and implement multi-factor authentication as necessary for access to cloud services, including prohibiting access for terminated employees.
the need for centralized user authentication

In order to have success with this business service brokerage model, security teams must find a way to eliminate shadow identities and authenticate all users via their identity services before the users access the applications they need. This approach can simplify access management for all user types, including:

Employees
While employees can still be authenticated against the corporate directory, contextual, multi-factor authentication should be available for high-value transactions or access to sensitive applications. For example, if a user normally logs in from the office or his/her home in the U.S. during normal business hours, but a log-in attempt is made from Europe in the middle of the night, the service should refuse the authentication or demand additional credentials.

Privileged Administrators
Privileged administrators can be a challenge, because they often have more access entitlements than they need, and they share the use of a common account (e.g., root). To combat this, a central authentication service should act much like it does for employees, but when a privileged user logs in, he/she will be given a single-use password for that individual session – eliminating the lack of accountability that is endemic to shared account use.
The common thread in each of these user scenarios is a centralized identity service that controls access to all enterprise applications, whether on-premise or in the cloud.
defining a path forward

While a centralized identity and access management service can help organizations create a new identity perimeter that secures today’s fragmented data centers, the question of how to implement such a service remains. Below are some recommendations for how to best define a path forward:

Step 1: Establish a cloud broker architecture

Because of its ease of use and integration with cloud services, many organizations are choosing to implement identity and access management as a service. In fact according to Gartner, cloud delivery of identity as a service is expected to grow to 30% by 2016.2 But why should you consider IAM as a service?

For starters, it enables you to augment the security you have in place today, rather than resort to a full “rip and replace.” You can begin with cloud-based applications – many of which will be pre-integrated – and add on-premise applications over time. Eventually, this cloud broker architecture will transform into a single, centralized identity perimeter.

Step 2: Create a checklist and evaluate cloud providers

Prior to evaluating IAM as-a-service solutions, it is imperative that you develop a must-have security checklist, so you can evaluate cloud providers against it. What should the checklist include? Look for capabilities that will help you control identities in cloud-based applications, such as:

- SAML-based authentication with the ability to turn off local authentication
- Automated provisioning and de-provisioning
- A query for current users
- Usage log access
- Ability to externalize authorization
- Standards-based practices

Step 3: Build out a catalog

Finally, meet with business managers about their upcoming projects, so you can build out a catalog of services prioritized by the latest IT and business initiatives. For example, if you know what new SaaS application types the organization is considering, you can proactively seek out ones that align with the checklist you developed in the previous step. By figuring this out ahead of time, you can help the organization choose applications that will not only meet core functionality requirements, but also support a fast and seamless implementation – accelerating the development of new services.
sell this to the organization with a business discussion, not technology

When an organization pursues a centralized identity and access management approach, it sees immediate security benefits in the following areas:

- Access to IT assets on premise and in the cloud
- Visibility of privileged-user actions
- Assurance of users’ identities
- Protection of customer information
- Improved governance of all users’ access rights (i.e., Who has access to what?)

Another, less obvious benefit is increased business agility. When identities are managed centrally, new business services can be deployed more easily and quickly than if each one required manual security integration. As a result, organizations can react faster to changing market conditions, accelerate the creation of new business services and create competitive advantage.

What’s more, security executives can show value to the entire executive suite, helping them secure a spot at the executive table:

- **Business Managers** benefit from easier audits, quicker SaaS deployments and improved experience for their customers (e.g., reduced sign-on)
- **CIOs** benefit from reduced operational and helpdesk costs and increased reliability
- **Compliance Officers** benefit from automated reporting and improved visibility
- **IT Security** achieves its security goals while enabling better, faster adoption of new business services
about the solutions from CA Technologies

CA Security solutions can help you not only protect your business, but empower your business to grow, while enabling you to securely leverage the benefits of cloud, mobility, virtualization and Big Data. With our solutions you can:

- Speed the delivery of new, secure business services to your customers
- Secure access to data across your extended enterprise
- Leverage new channels – securely – to help grow your customer base and increase loyalty
- Protect against insider threats and external attacks
- Improve efficiencies through automation of key, identity-related processes
- Protect confidential information from theft or disclosure

We provide these benefits through the following capabilities:

- Identity management and access governance
- Web access management and SSO
- Advanced authentication and fraud prevention
- Shared (admin) account management
- Mobile security
- Information classification and control
- Cloud-based identity services

For more information about CA Security solutions, visit www.ca.com/security.
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. For additional information, visit CA Technologies at ca.com.