Enabling and Securing Digital Transformation

The Promise of Digital Transformation

Several recent trends are combining to dramatically reshape the business landscape for all forward-leaning organizations. Cloud, mobile, the Internet of Things (IoT) and the demand for always-on access are forcing dramatic changes in business and technology strategies. The new application economy requires that organizations embark on a large-scale digital transformation. They're becoming highly distributed digital enterprises that house web and mobile apps on-premises, in the cloud or in hybrid environments, and grant user access from a variety of locations and devices. Gone are the days of the network perimeter providing a control mechanism for this access. Now, people and things are the new perimeter, and their identities are the single unifying control point across all of the devices, apps and data that drive the business.

This transformation demands new methods of customer engagement, new channels and new approaches to security. Traditional security practices must adapt to this new open enterprise. The move is on—from traditional security that puts up obstacles that protect but inhibit business to an enablement-focused approach that first and foremost protects the business, but also enables it for growth. Identity-centric security is essential for a successful digital transformation.

"The network perimeter is all but gone and identity is the new perimeter. With network and organizational boundaries disappearing and people working from hotel rooms and cafes, IAM has become the primary factor for ensuring that only authorized people from authorized locations access authorized resources."[4]

50%
of business applications are SaaS[2]

94%
of executives face increased pressure to release apps more quickly[3]

6.4 billion
connected "things" will be in use in 2016, up 30% from 2015[4]

[1] TechRadar(trademark): Identity And Access Management, Q1 2016.
[2] A commissioned study conducted by Forrester Consulting on behalf of CA Technologies, September 2015.
[3] Vance-Bourne Study, 2015.
[4] Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015, Gartner Press Release, November 10, 2015, http://www.gartner.com/newsroom/id/3165317.

But, the New Digital Enterprise Also Brings Challenges

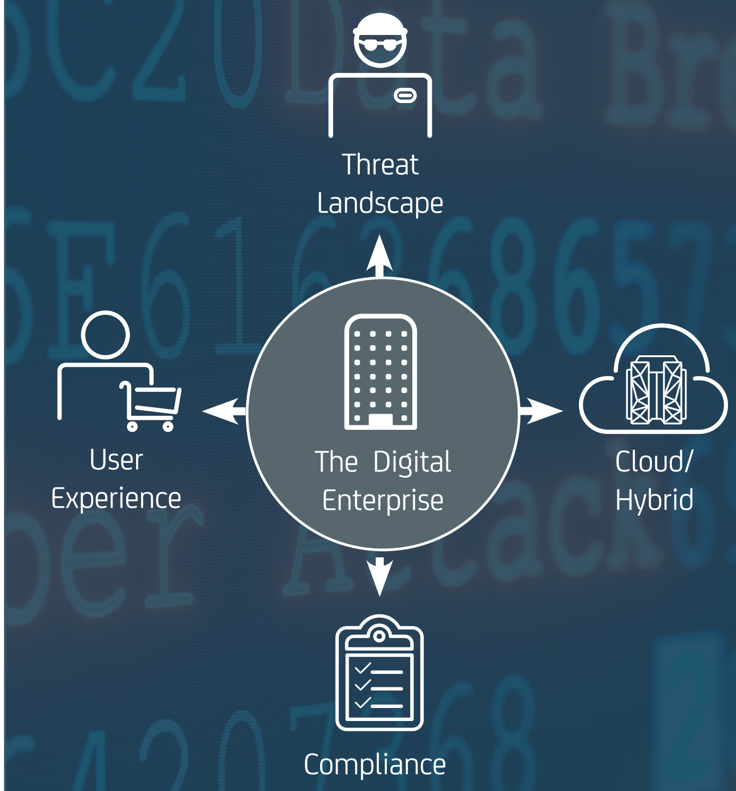
Thriving—and not just surviving—in this new norm requires you to face pressing security challenges head on. Some of the most difficult ones include:

An increasing threat landscape
Most IT departments are struggling to protect their organizations from a variety of threats, such as the disclosure or loss of sensitive data by employees and external attacks that are motivated by financial gain. After all, a successful external breach can cost millions of dollars, not to mention the lingering business impact of reputational damage.

A positive user experience
As identity services are used more and more by business users and consumers, the importance of a simple, intuitive user experience becomes critical and can determine whether a business grows or stagnates. In short, the quality and convenience of the user experience has emerged as a critical element in driving the increased adoption of identity services across the enterprise, and the growth of its customer base.

Compliance is *still* hard
The new threat landscape and increasing regulatory requirements for data privacy and control of privileged users has increased the challenge of achieving and maintaining compliance. Strong, risk-based controls, governance of all user access (especially privileged users) and user behavioral analytics are important capabilities to help create a strong compliance platform.

Growing cloud/hybrid adoption
The increasing use of cloud applications complicates security across the entire environment. There is a strong need for an identity platform that can transparently control access to these apps (no matter where they reside), and govern access entitlements across the entire hybrid environment.



Who Are Your Security Stakeholders?

Almost all groups within your organization need a seat at the "security table." Everyone is concerned and has a stake in protecting key apps and data. But, equally important are the business enablement benefits that effective security can provide. The benefits of security and enablement cut across many groups in the organization. Two of the most important stakeholders include the security team and the IT organization.

Security—stakeholder

Protect critical apps, systems and data.

Titles: Chief (Information)

Security Officer, VP IT Security

These executives set the information security agenda for the organization by identifying, developing, implementing and maintaining security-related processes, policies and architecture that reduce the organization's risks. They often oversee (or at least monitor) regulatory compliance and data privacy efforts.

IT—stakeholder

Meet efficiency and security needs of the business.

Titles: VP/Director IT

These technology executives manage 24/7/365 operation of computer technology: systems, applications, databases and infrastructure. They also support the growth and development of the company, including new technologies, emerging markets and serving the existing customer base. They must do this while managing IT costs and resources.

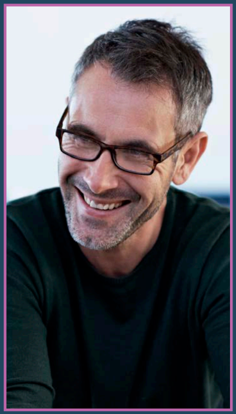
Who are Your Security Stakeholders?

Increasingly, the line of business is becoming a key security stakeholder because effective security is what enables the business to grow securely, take advantage of new business opportunities and improve customer satisfaction and loyalty. The enterprise architect is also a very strong influencer for security technologies because they are responsible for ensuring that the entire identity infrastructure is consistent, secure and meets both the security and enablement needs of the entire enterprise.

Line of business—stakeholder

Leverage new business opportunities. Ensure customer loyalty and retention.

Titles: General Manager, Chief Digital Officer, VP Digital



These executives are responsible for P&L and the overall direction and performance of products, solutions and services of the specific business unit. They are measured on identifying business opportunities and driving growth, as well as managing resource allocation, capex and opex budgets. Their critical concerns include customer engagement, retention, growth, increasing competitiveness and market dynamics because they take a holistic view of the business.

Enterprise architect—influencer

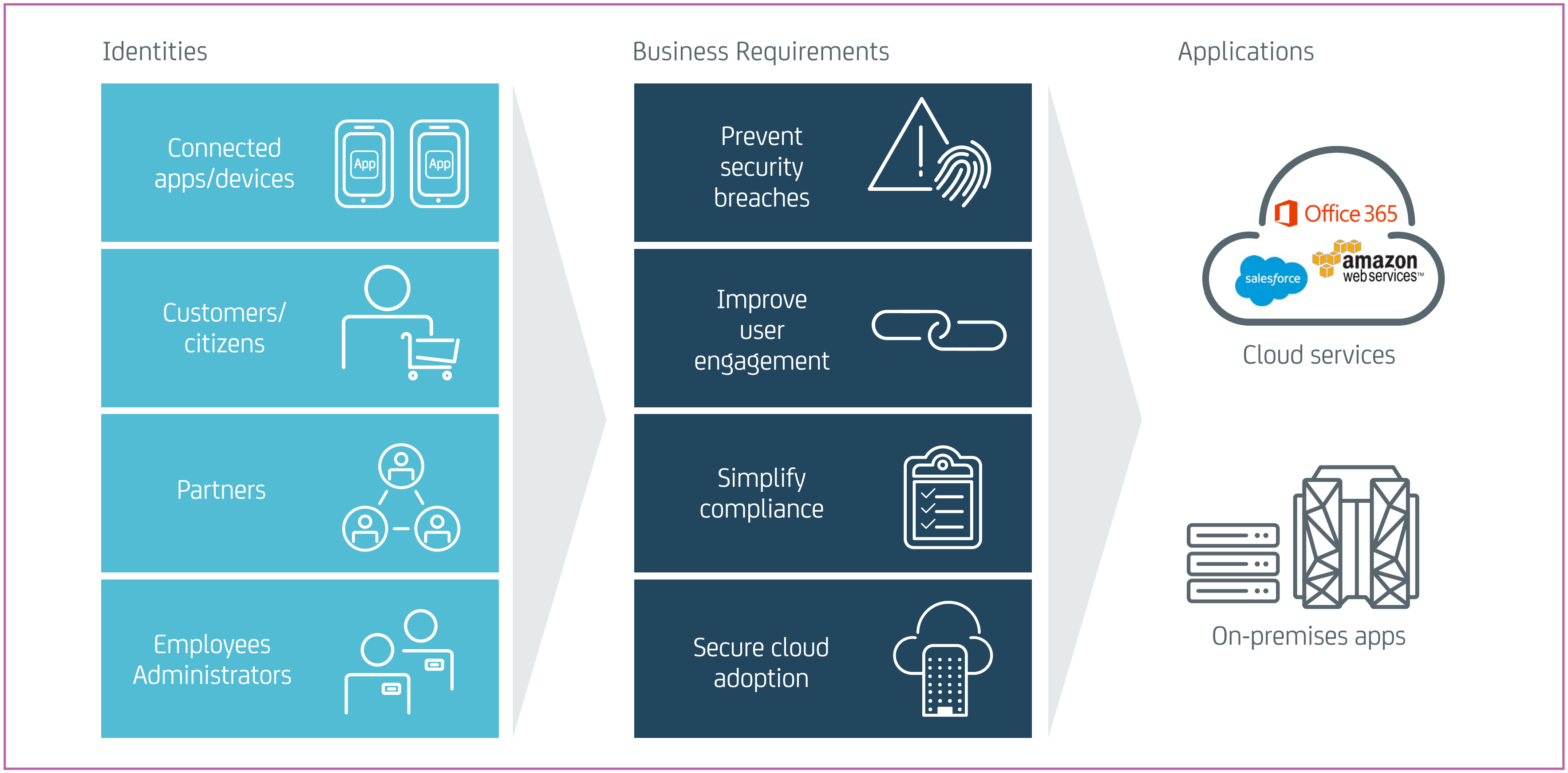
Ensure consistency, scalability and security across the identity infrastructure.

Titles: Chief Architect, Director Identity Management, VP Integration

These technology experts manage the enterprise architecture across all domains, including information, data, technology, business, security, and application environments. They strive to gather and synthesize information about each domain and provide clear, consistent architectural direction, ensuring that technology solutions meet corporate strategic direction and the enablement and security needs of their business units.

Requirements for Success

Security deployments cut across the entire organization and attempt to meet the critical business and technology drivers of each group. But there are four key ***business requirements*** that can serve to capture the needs of each major stakeholder. Let's look at each of these requirements in order to understand how they can impact your security strategy.



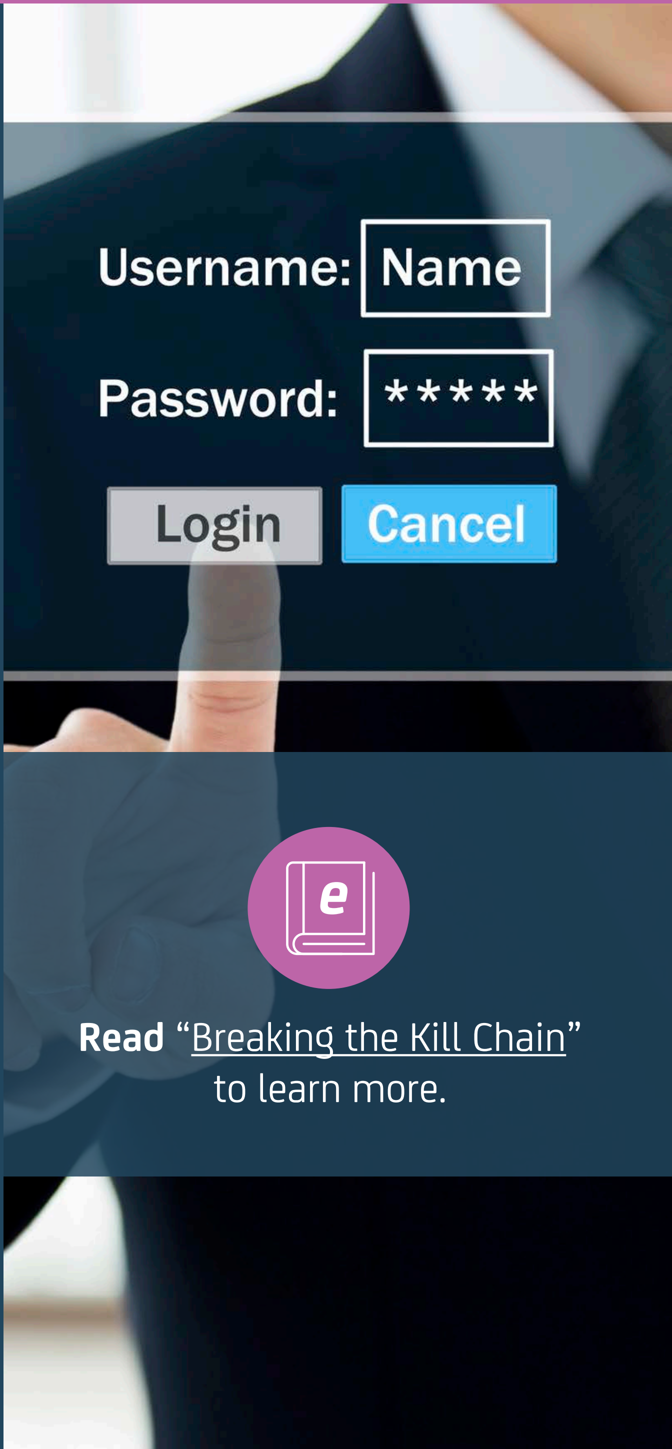
Prevent Breaches

Key players: security

Breaches and attacks continue to escalate in frequency, severity and impact—and so organizations are at greater risk of financial and reputational damages. With compromised privileged credentials serving as a primary attack vector in virtually every security breach, organizations are looking to privileged access management to secure and manage their system admins and neutralize the surge of breaches. The right solution will help organizations:

Prevent unauthorized access by implementing strong authentication and enabling proactive enforcement of policies.
Privileged access management provides key capabilities to safeguard privileged credentials. Employing multifactor authentication, enforcing policies associated with login restrictions and keeping credentials vaulted and secured enables stronger authentication. And employing command and socket filters, as well as limiting access rights, provides precise controls over what users can and cannot do on a system.

Stay ahead of the curve by facilitating privileged user activity monitoring and auditing.
Privileged access management monitors, records and audits all privileged user activity, making it even more difficult for threat actors to successfully execute an attack. Session recordings help determine what actions occurred, while playbacks speed investigations, troubleshooting and recovery. Alerts and events provide immediate warnings of policy violations and attempted breaches.



Read "Breaking the Kill Chain" to learn more.

Improve User Engagement

Key players: Line of business, IT and enterprise architect

A business can succeed or fail based on the level of engagement with its users. Employees, partners and customers all have a relationship with the organization, and that relationship must be nurtured. Easy, frictionless access to information and applications is what they need to conduct their business. So, the two key requirements for effective user engagement include:

Provide a simple, frictionless customer experience. Online customers are notoriously impatient and fickle—give them a few minutes of an inconvenient user experience and they are gone. They want a simple and convenient way to make business transactions with as little friction in the experience as possible. Capabilities, such as single sign-on and a secure, transparent, risk-based authentication experience are essential for your customer engagement strategy.

Improve workforce productivity. Employees have similar needs for easy access to the resources required to do their job. They want to manage their own profile information and their entitlements must always be appropriate for their roles. Capabilities, such as access requests/approvals and certification campaigns must be simple, intuitive and business-oriented.

Read "Managing and Governing Identities in the New Open Enterprise" to learn more.

Read "Keep the Door Open" to learn more.

Simplify Compliance

Key players: security

Organizations face increasing pressure to comply with a growing number of regulatory requirements. They look to privileged access management to address specific mandates around the audit, control and monitoring of privileged user access to sensitive data and systems. This helps them comply with standards and thwart adverse audit findings, as well as costly penalties and fines. The right solution will help organizations:

Prevent compliance violations by establishing critical automated controls.
Privileged access management provides privileged user and credential controls, encompassing tasks like authentication and robust access controls mandated by the Payment Card Industry Data Security Standard, Health Insurance Portability and Accountability Act (HIPAA), North American Electric Reliability Corporation critical infrastructure protection (NERC-CIP), Federal Information Security Management Act (FISMA) and other industry standards and governmental regulations.

Demonstrate ongoing compliance by facilitating privileged user activity auditing and monitoring.
Privileged access management enables a single point of control, implementing all critical privileged access management functions. This allows organizations to gain complete visibility into all privileged user activities, accelerating compliance assessments, speeding up investigations of policy violations and facilitating information archiving necessary to satisfy audit and compliance demands.

Read "Addressing PCI Compliance Through Privileged Access Management" to learn more.

Read "Preparing for EU Payment Security Directive (PSD2) and How CA Can Help" to learn more.

Secure Cloud Adoption

Key players: security

Cloud adoption is on the rise for many good reasons—improved end-user productivity and collaboration, faster and simpler implementations and attractive pay-as-you-go/pay-as-you-use pricing models. However, the pace at which cloud and services are being adopted in enterprises today is outpacing security. This is driving the need for security solutions that can support hybrid environments with agility, and without compromising security. Two key requirements for enabling secure cloud adoption are:

Secure access to hybrid cloud environments.
The large number and dynamic nature of resources that are typically deployed in cloud and hybrid environments, and the presence of powerful management consoles and APIs, can expand the available attack surface. Therefore, it is imperative to establish dynamic protections and controls to address new security risks, comply with regulations and govern who has access to what in cloud environments, especially privileged access to cloud platforms, management consoles, APIs and applications.

Enable end users with convenient access to cloud applications.
The proliferation of cloud applications that employees use on a regular basis has increased the volume of credentials users need to remember, and also the potential for those credentials to be compromised. Without the right security solutions in place, users are likely to recycle weak, easily memorable passwords. Capabilities, such as single sign-on and two-factor authentication, provide a frictionless way to enable user productivity, while managing risk.

Read "How Can I Defend my Hybrid Enterprise From Data Breaches and Insider Threats?" to learn more.

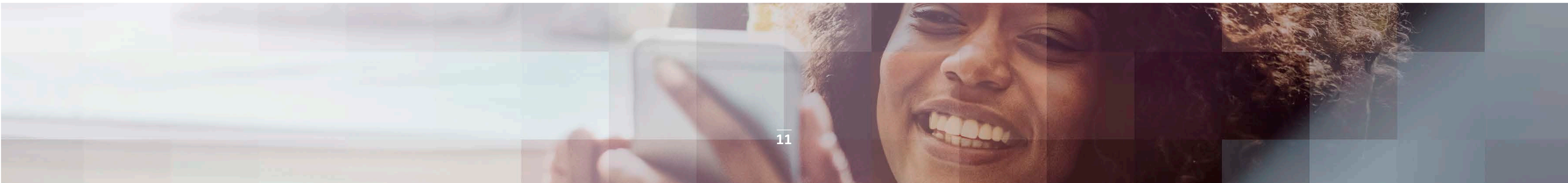
Requirements for an Effective Security Solution

In this ebook, we have seen that in the new application economy, every business is now a digital business. Customers expect always-connected convenience and security, putting tremendous demands on the business to be faster and more agile. Identity-centric security is essential to enable businesses to move to the cloud, deliver a strong customer experience and ensure secure access to enterprise applications and data for employees, customers and partners.

These profound changes in the business landscape call for new ways of protecting and enabling the business through strong but flexible security. Current solutions often cannot support the evolving requirements created by the emergence of cloud, mobility and the IoT. But, what are the attributes of an effective security platform that can meet your current needs while providing for flexible growth? Some of the most important things to demand include:

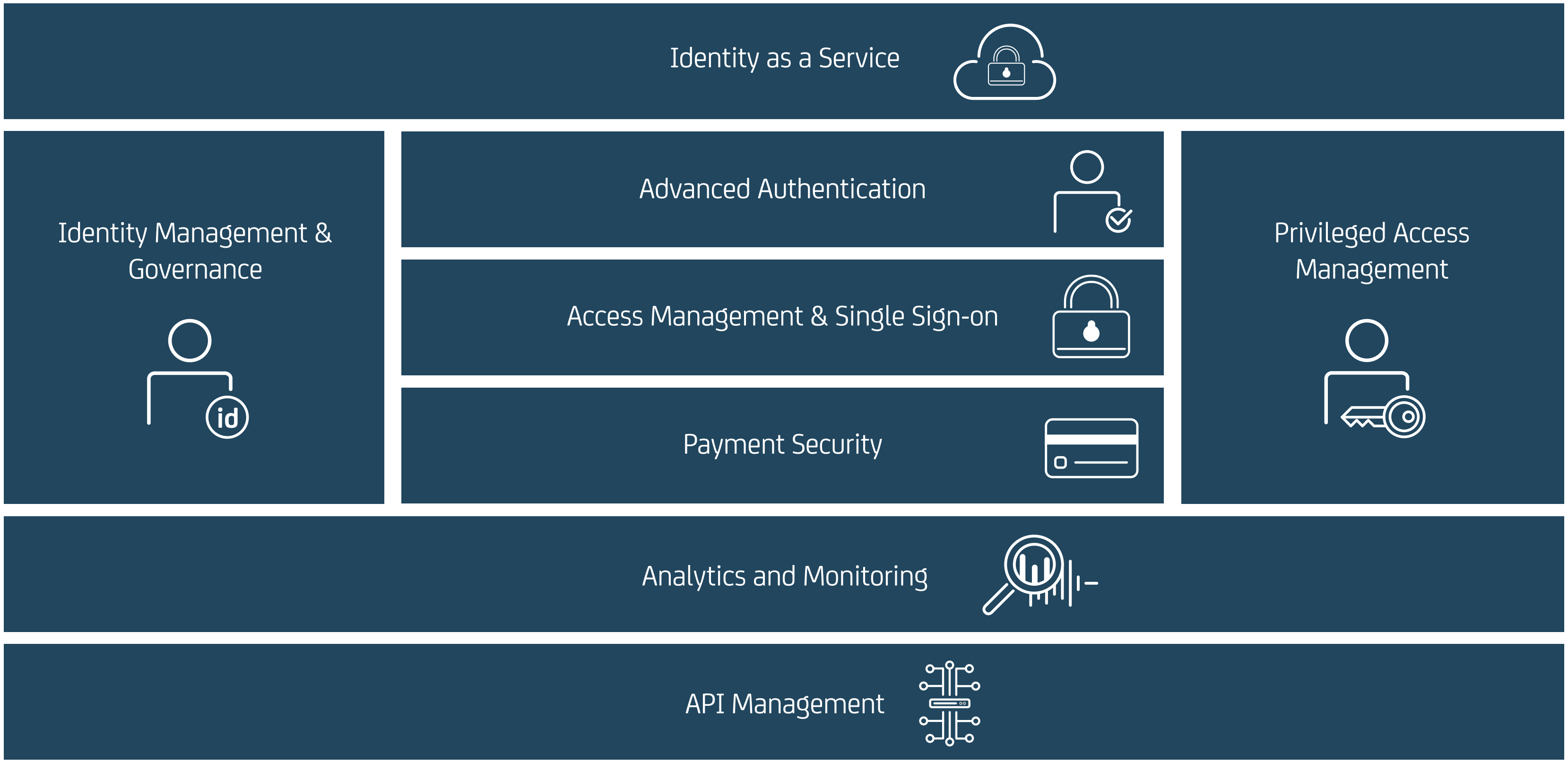
- **Breadth of capability**—Point solutions generally do not provide the comprehensive solution that is required today, and they often pose integration challenges with other technologies.
- **Multi channel support**—Look for consistent and comprehensive security capabilities across web, mobile and APIs. Your customers and partners will use the channel of their choice, so you must be able to provide the security and user experience that they expect across all channels.
- **Business-oriented user experience**—The experience that you present to your users (of all types) will drive their satisfaction and loyalty (or lack thereof). An outstanding user experience is the foundation of customer retention and employee productivity.
- **Internet-level scalability**—The number of users and the number of applications and systems are expanding rapidly—often exponentially. To support this growth, any solution must support both small and very large numbers of identities (>100M in some cases).
- **Vendor commitment and viability**—The identity management landscape is littered with the bodies of companies that came and went. Make sure that your vendor not only provides a broad and deep identity platform, but also is committed to continuing to expand its capabilities in the future.

The next section will highlight the breadth and capabilities of the CA Security portfolio.



The Identity-Centric Security Portfolio From CA

The identity-centric security portfolio from CA is an integrated, comprehensive set of solutions that can enable organizations of all sizes to protect their critical assets from threat and attack, as well as support new business opportunities and growth. Beyond these capabilities, the portfolio also helps to reduce IT management costs, simplify compliance and provide an outstanding, business-oriented user experience.



Identity as a Service

Identity Management & Governance

Advanced Authentication

Access Management & Single Sign-on

Payment Security

Privileged Access Management

Analytics and Monitoring

API Management

CA Identity Suite

Today's digital enterprise demands new, more-effective ways of managing identities and entitlements for the increasing number of workforce and consumer users. CA Identity Suite enables organizations to more easily manage user identity information and ensure that all users always have the correct entitlements. The solution also provides an intuitive user experience that can dramatically simplify processes, such as user access requests and access certifications, resulting in improved productivity and user satisfaction. In addition, Identity Suite performs risk analysis and enables remediation actions in real time during the access provisioning steps, thereby improving audit performance and risk posture with preventive policy enforcement.

CA Identity Suite also delivers core identity management and governance capabilities, including broad provisioning support for on-premises and cloud apps, as well as extensibility and flexibility to integrate with other identity management/security solutions and consumer-grade scale. Today, CA Identity Suite manages millions of user identities in some of the largest, most complex IT environments across the globe.

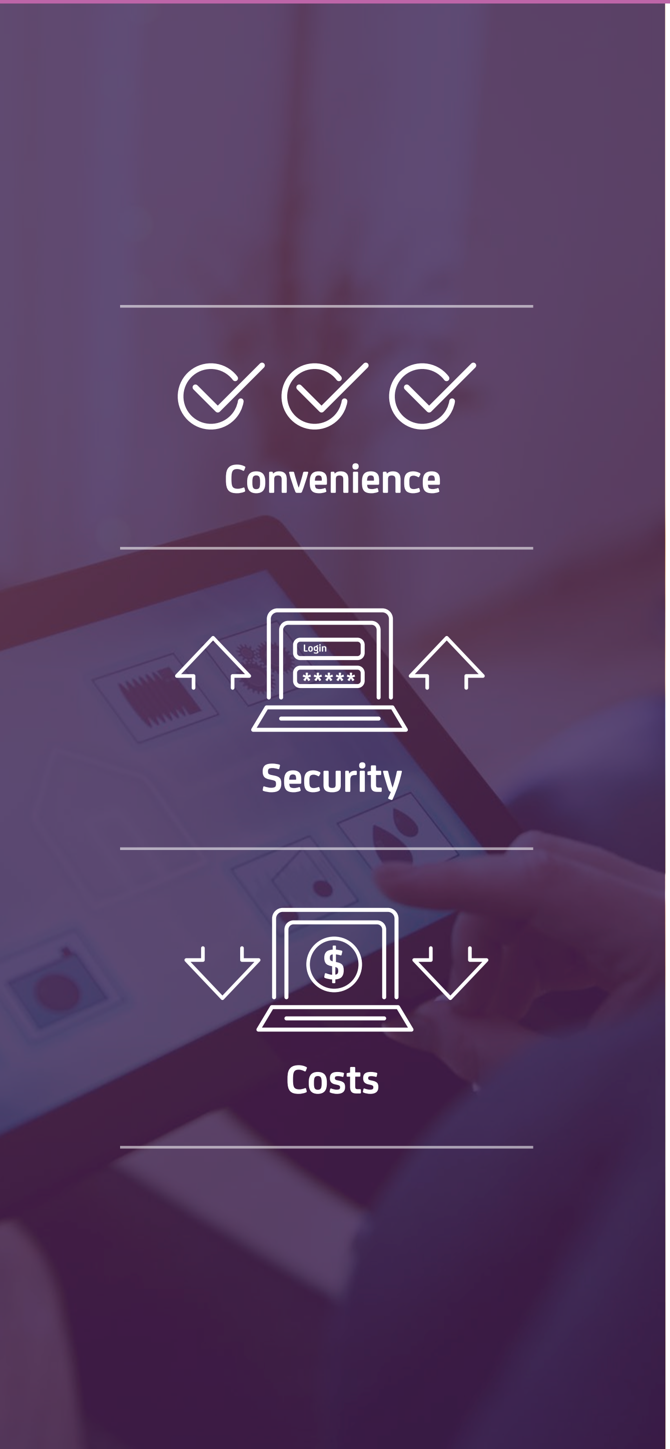
Why CA?

- An outstanding, business-oriented user experience to increase employee productivity and customer loyalty
- Risk analysis and simulation to quickly identify and correct high-risk access
- Extensive support for mobile users to ensure a consistent experience across the web and mobile devices
- Reduced TCO through deployment and configuration tools designed to decrease time-to-value
- Enterprise level scalability to meet your growing needs

Improve user experience

Reduce risk of improper access

Improve operational efficiency



CA Advanced Authentication

Passwords are the most common way for users to authenticate to web and mobile applications, but they are also a critical, weak link in an online security system. The enterprise needs to provide a more secure way to protect user identities and ensure data privacy without undue burden for the user.

CA Advanced Authentication provides greater assurance that the user is whom they claim to be through transparent risk analysis and user behavioral profiling, as well as automatic step-up authentication when risk is deemed too high. The solution also provides several two-factor credentials to help organizations address regulatory compliance requirements.

Why CA?

- Convenience provides transparent risk analysis and two-factor credentials that do not change the user's login experience
- Visibility offers default reports and analytics that give full visibility into why users are challenged
- Flexibility allows administrators to create/modify risk rules to balance user convenience with threat mitigation
- Faster time-to-value with a self-learning behavior model that assesses risk based on each individual user's behavior patterns
- Trust that credentials are protected with a patented key concealment process against brute force and dictionary attacks

CA Privileged Access Manager

Stolen and compromised privileged credentials serve as a crucial attack vector in many breaches and security incidents. Failure to prevent these attacks can lead to data loss, reputational damage, service interruptions, audit and compliance penalties and other costly consequences.

CA Privileged Access Manager defends and controls privileged users and the credentials they use to access, manage and control your digital infrastructure. Quickly deployable and delivering fast time-to-protection, CA Privileged Access Manager helps prevent breaches, demonstrate compliance and boost operational efficiency. Offered as either a hardened hardware or virtual appliance, CA Privileged Access Manager protects sensitive administrative credentials, enforces role-based limits on privileged user access and proactively enforces security policies—all while monitoring and recording privileged user activity across virtual, cloud and physical environments.

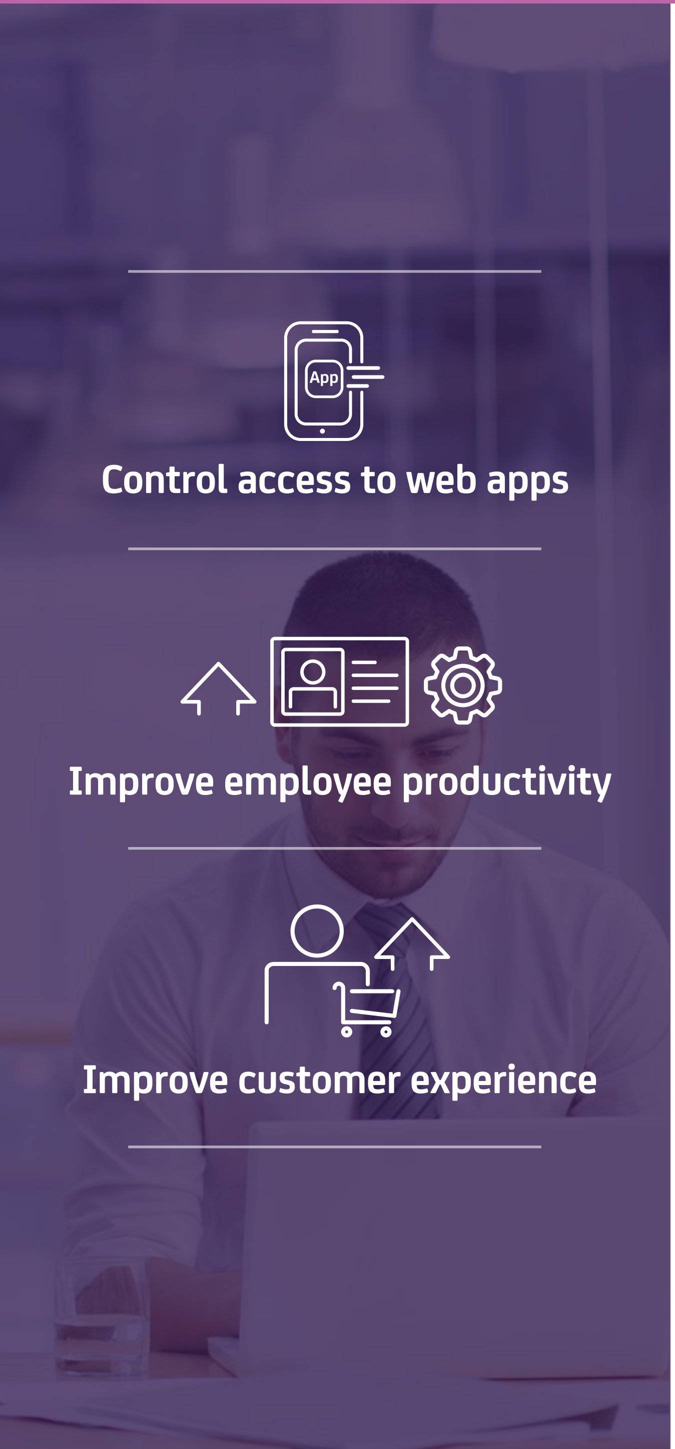
Why CA?

- Enterprise-ready to deploy in hours—not the weeks needed for other solutions—and secures the largest and most complex environments and networks
- Reduces TCO by simplifying the cost of protection with intuitive pricing and packaging, and cutting deployment and maintenance costs with an appliance form factor
- Comprehensive protection to defend and control privileged across the entire hybrid enterprise
- Extensive certification: the industry's most highly certified solution

Stop targeted attacks

Mitigate insider threats

Achieve compliance



Control access to web apps

Improve employee productivity

Improve customer experience

CA Single Sign-On (SSO)

Digital transformation means that organizations must give employees, customers, partners and suppliers secure access to essential information and applications, whether on-premises, in the cloud, from a mobile device or at a partner's site. As web applications increase, so does the need for users to sign on once and gain access to everything they require—all while protecting the organization from breaches and threats. With CA Single Sign-On (SSO), you get flexible and secure identity access management. It accelerates application availability by offering an unparalleled range of options for managing access to applications. CA SSO enhances security by providing a common policy layer that reduces the possibility of access policy gaps. And CA SSO reduces cost of ownership by supporting traditional web applications, identity federation standards and web service standards, all from a single, integrated, high-performance platform.

Why CA?

- An outstanding user experience for employees, customers and partners because CA SSO is designed to work with a wide variety of third-party platforms, operating systems, web applications and authentication solutions
- Increased application availability with unparalleled access management options
- Session security for both the SSO session and the application sessions
- Reduced TCO through deployment of federation and access management in a single solution

Additional CA Security Capabilities

We have explored the core capabilities in the CA Security solution that enable you to both protect and enable your organization. But, unlike point solution providers, the CA portfolio includes a full suite of components that provide a comprehensive cybersecurity solution—one that can meet the needs of enterprises competing to succeed in the application economy. These capabilities include:

Identity as a Service

Many enterprises are choosing to adopt identity services in the cloud, taking advantage of the simpler initial setup and the reduced manpower costs that it provides. Basic identity capabilities such as provisioning, governance, single sign-on and authentication have proven to be increasingly successful in either pure cloud or hybrid cloud/on-premises deployments of identity services.

API Management

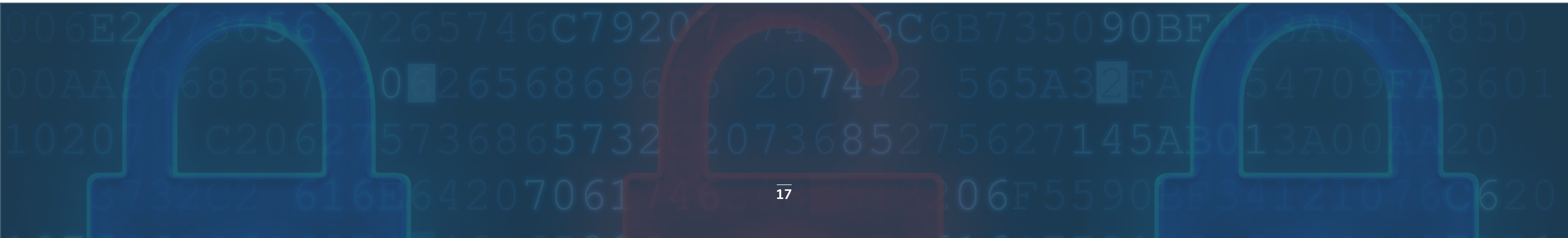
The ability to easily manage and secure APIs is often what separates industry leaders from technology laggards. CA API Management is a flagship solution that addresses and streamlines the entire API lifecycle and digital value chain. The functionality it provides allows organizations to rapidly integrate and create APIs, secure the open enterprise, accelerate mobile development and unlock the value of data.

Analytics and monitoring

CA Security includes comprehensive user behavioral analytics in order to reduce the risk of improper user actions, especially among privileged users. It also provides real-time service performance analytics to provide increased insight into the efficiency and effectiveness of your identity services, and to help you meet service level goals.

Payment security

CA Technologies is a leader in securing 3D Secure card-not-present transactions, protecting over 250 million cards worldwide. Our Payment Security solutions provide zero-touch authentication, helping card issuers minimize online fraud while providing a frictionless checkout experience for cardholders. Sophisticated risk analytics and dynamic, granular bank-defined rules help to identify emerging fraud patterns and take action on potentially fraudulent transactions in real time.



Next Steps

The application economy requires new and more creative ways of managing security. External attacks are more dangerous than ever, and internal threats remain a major challenge. Protecting critical information and apps is the top priority. Effective identity and access management can help you accomplish this and improve workforce productivity, reduce IT costs and strengthen customer engagement.

The Identity-Centric Security portfolio from CA is a comprehensive, integrated identity solution that provides capabilities to support consistent security across web, mobile and API channels. It can help you protect your business from being the victim of the latest breach attack, but it offers far more than just breach protection. By providing an outstanding user experience as well as security across hybrid and cloud environments, the portfolio can enable you to leverage new business opportunities, extend your partner ecosystem securely and improve your overall customer experience and loyalty. The CA Security portfolio not only protects your business, it enables it so that it can grow … securely.

To determine your next step, ask yourself the following questions about your own environment:

- Do you know who all your privileged users are and can you easily control their actions on your systems?
- Are you convinced that your breach prevention strategy is completely effective?
- Are you providing an outstanding user experience to your users of all types, especially business users?
- Is it easy for you to demonstrate compliance?
- Can you easily control access to all your critical applications, both on-premises and cloud, for your entire user population?

If your answer to any of these questions is “No,” talk to us about the CA Security Portfolio.

For more information, visit:

Identity Management and Governance

Advanced Authentication

Privileged Access Management

Single Sign-On

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate—across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.