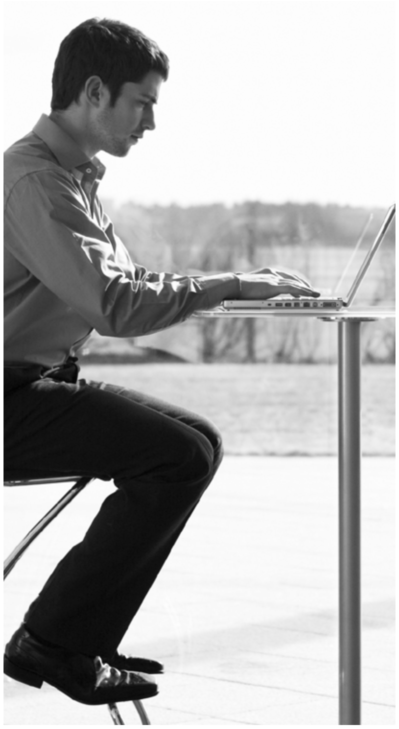
DXC.technology

White Paper

Thriving safely in the age of digital identity management

Security

April 2018



The traditional enterprise network perimeter, memorialized in countless slide decks with the image of a medieval castle surrounded by a moat, is dead. Today, applications and data live in the cloud, employees work from home, and customers want frictionless transactions from wherever they are, on whatever devices they happen to be using.

Organizations engaged in digital transformation understand that a new approach is required if they are going to thrive in this new world. The bedrock principle for enterprise security is no longer about the "where." It's about the "who" — identity of the person, system or service that is making a request to access information or services.

In other words, thriving safely in this economy requires a comprehensive focus on digital identity management. Identity and access management (IAM) allows companies to effectively establish a logical perimeter that enables digital transformation.

Many factors have led to the demise of the traditional security perimeter, from inherent weaknesses in passwords to emerging technologies. But by deploying the right IAM technologies, organizations can protect the perimeter, improve customer service and increase revenue.

The porous perimeter

Digital transformation and business transformation to the cloud are bringing decentralization and the use of multiple on-premises and cloud-based services. According to RightScale's 2017 State of the Cloud Report, 85 percent of enterprises are using multiple clouds, and 75 percent of enterprise workloads are running in either a public or a private cloud.[1]

Companies must change their focus to protect data and business processes running in the cloud. What's needed is an information-centric approach to security and risk management.

Mobility has also driven gaping holes in the perimeter. To compete in the market, attract the best skills and retain the best people, companies are enabling more agile ways of working. Employees expect to be able to work wherever they are, on the device of their choosing.

This has serious implications, because security must now extend to every corner of the boundaryless enterprise. Security must protect data and business processes whether they are running in the cloud or in a coffee shop.

[1] RightScale 2017 State of the Cloud Report
https://www.rightscale.com/lp/2017-state-of-the-cloud-report?campaign=70170000000vFyc

Traditional approaches to authentication are no longer good enough. The trusty password can no longer be trusted, when the majority of breaches can be traced back to weak or stolen passwords

The typical user has multiple logins. And the horror stories of users writing out passwords on sticky notes attached to their monitors or using "12345" as a password for all their logins are legion. There has to be a better way.

To further complicate the issue, the internet of things (IoT) is introducing new device types, such as sensors, that might be located outside of the network boundary and need to have a digital identity. Also, items such as wearables and machine-to-machine interactions need to be accounted for. And, let's not forget regulatory requirements focused on data protection, such as the European Union's General Data Protection Regulations (GDPR).

Identity is at the heart of every digital transaction. As companies escalate their digital transformations, much of the focus is on customer interactions. Companies want to give customers a more personalized, streamlined experience — all of which is driven by identity. IAM becomes even more critical as we move into an era where digital assistants can execute transactions — such as booking a flight or finding a hotel room — on behalf of the customer.

While the basic concepts of authentication (who you are) and authorization (what you're allowed to do) are relatively simple to understand, putting IAM into practice is not easy.

DXC Technology has strong views on the need for companies to transition from a traditional perimeter defense posture to an identity-driven model that protects data wherever it is located. And DXC has a clear vision for how companies can successfully implement user identity, device identity, identity management and identity federation as foundations for digital transformation and the hybrid enterprise.

Bedrock for digital transformation

As the new perimeter, identity allows companies to adopt more agile and cost-effective ways of working. IAM is a foundational element of digital transformation and a key enabler for information-centric security and risk management. IAM can help companies cut costs as they shift the focus of their budgets from CAPEX to OPEX and increase revenue by extending their reach to their customers.

Effective identity management and identity federation enable an enterprise to establish a web of trust across all of the services it uses to support its business and effectively protect its data. Built on open standards such as Security Assertion Markup Language (SAML) for exchanging authentication and authorization data between parties, OAuth for delegating access, and object identifiers (OIDs) — which work as identifying mechanisms — this web of trust allows one entity to safely and securely accept authentication that has been approved by another entity. And it allows companies to eliminate the need for multiple identities.

Companies should move quickly to select an enterprise identity provider (IDP) as a single point of control and management for enterprise user and device identities. They should support federation efforts — business-to-business and consumer-to-business.

DXC has developed an IAM blueprint within its Cyber Reference Architecture (CRA) that it uses with customers to help them define their IAM solution architectures. DXC also has a range of consulting and managed services to deliver the blueprint to customers.

Implications of an identity-based perimeter

One of the first steps an organization needs to take on the journey to identity-based security is to address the password issue. Clearly, passwords aren't sufficient, but they probably aren't totally going away, either.

Companies need to move to some form of two-factor or multifactor authentication that can blend a variety of methods, depending on the user, the device, the context and the action the user is trying to accomplish.

An identity management system needs to be built with levels of trust. Maybe a trusted employee can log into the corporate network with just a password, which would enable the employee to access specific applications or datasets. If the employee wanted to access more-protected data or business processes, a second form of authentication would be required. Perhaps a customer on a mobile phone would be asked to provide authentication through some form of biometrics, such as facial recognition, voice recognition or a fingerprint, rather than being asked to type in a long, complex set of letters and numbers.

Organizations that can achieve a high level of personalization, recognize and understand their customers, and provide a streamlined experience will be able to leverage IAM to increase customer satisfaction and drive revenue.

A federation broker can help manage trust relationships that are fundamental to digital transformation. Digital relationships between a company and its suppliers and partners, between a company and its customers, and between a company and its employees, demand a level of trust that can only be achieved through federation.

Access control is another key component in any IAM deployment. To help achieve effective access control, companies should look into cloud access security brokers (CASBs), which mediates between cloud service consumers and cloud service providers to enforce security, compliance and governance policies. CASBs help organizations extend the security controls of their on-premises infrastructure to the cloud.

Companies should also consider context-based authentication, which analyzes a variety of factors in combination to verify the identity of an employee or customer and to throw up a red flag when something doesn't look right. These factors can include everything from the signature of the device to geolocation data to biometrics that can identify someone by the way they are holding the device. With context-based or conditional access control, the system makes a determination as to what risk level to apply.

Other technologies that factor into access control include data loss prevention (DLP), digital rights management (DRM) and encryption.

Recommendations for the CISO

Fortunately, chief information security officers (CISOs) have many options for managing digital identities, but to be successful every organization needs a sound identity management strategy. Here are some key recommendations for CISOs:

1. **Invest in identity and access management (IAM).** The traditional network security perimeter is no longer providing effective protection for company data in today's world of cloud, mobile and social.
2. **Implement an enterprise identity provider (IDP) and single sign-on access management** to address the issue of employees needing to log into multiple systems with different passwords. This can be either in-house or cloud-based.
3. **Deploy an identity federation broker**, either in-house or in the cloud, to streamline and simplify the federation process.
4. **Enable end-to-end visibility across the entire enterprise.** IAM is that enabler because it delivers consistent identity across all of a company's services.

The cloud, mobility and IoT have rendered obsolete a security strategy based on defending the perimeter. Companies must recognize that to thrive safely in this environment, they must build a new set of defenses based on identity and access management.

About the author

Mark Evans is chief security architect of Security Advisory Services for the United Kingdom and Ireland region at DXC Technology. He has a background in enterprise security architecture and cloud security. Previously, Mark was chief security architect for HP/HPE's UK Government Cloud Program (formerly known as Helion-G and now known as DXC UK Restricted Cloud Delivery), designing and delivering secure cloud services for the UK government. Connect with Mark on Twitter or on LinkedIn.

Learn more at www.dxc.technology/iam.

March 2018