The Challenges and Benefits of Identity and Access Management

Identity and access management (IAM) solutions today must balance streamlined authentication with increasingly complex security concerns.

White Paper

by F5

Overview

The need for a robust identity and access management (IAM) strategy has become an integral part of enterprise IT. Strong IAM solutions can enable enterprises to boost employee productivity and bolster their overall security postures. However, the growth of cloud computing and an increasingly distributed mobile workforce make IAM more complex every day.

Organizational teams in charge of authenticating user identities and managing access to corporate resources must walk a fine line, ensuring that the enterprise has robust security controls in place while streamlining authentication procedures to increase user productivity. In the end, business is about delivering value to customers, and IAM is an essential part of ensuring that employees are both empowered to deliver that value and prevented from damaging the business's reputation, security, or bottom line.

When considering adopting or changing an IAM strategy, enterprises must be aware of some of the most important trends in authenticating identity and managing access to corporate applications. The general IAM landscape is becoming increasingly complex and must continue to evolve with advancing security threats, posing specific challenges for both users and administrators. The most important elements of a holistic IAM solution—including centralized access management, automation, reporting, and contextual application of security policies—can help enterprises meet those challenges while accommodating dynamic growth.

Identity and Access Management Today

Businesses rely on agile systems to adapt to continually evolving challenges and pivot to take advantage of new opportunities. Speed is of the essence, with pressure on IT staff to provision information resources quickly and seamlessly when required by users. However, in counterpoint to this desire for on-demand access are the very real security issues that keep IT managers up at night. Facing attacks on critical applications both inside and outside the traditional security perimeter, enterprises must make sure that access is tightly regulated to keep data secure.

IAM strategies often live in silos housed in various departments, including information security, application development, and regulatory compliance. Because each department often customizes access privileges to best suit its business goals, corporate IT requirements are often left unenforced. This patchwork IAM strategy can lead to awkward provisioning and de-provisioning of access, lost productivity, and even security breaches.

While implementing a comprehensive IAM strategy can be much more complex than simple technology deployment, when done correctly, enterprises can realize tangible business value, including increased operational efficiency, simplified regulatory compliance, and enhanced employee satisfaction. However, to successfully deploy a robust IAM solution, several problems must be overcome.

Challenges and Solutions

Today's enterprise IT departments face the increasingly complex challenge of providing granular access to information resources, using contextual information about users and requests, while successfully restricting unauthorized access to sensitive corporate data.

Challenge: An increasingly distributed workforce

One way organizations can recruit and retain the best talent is to remove the constraints of geographic location and offer a flexible work environment. A remote workforce allows businesses to boost productivity while keeping expenses in check—as well as untethering employees from a traditional office setting. However, with employees scattered all over a country or even the world, enterprise IT teams face a much more daunting challenge: maintaining a consistent experience for employees connecting to corporate resources without sacrificing security. The growth of mobile computing means that IT teams have less visibility into and control over employees' work practices.

Solution

A comprehensive, centrally managed IAM solution returns the visibility and control needed for a distributed workforce to an enterprise IT team.

Challenge: Distributed applications

With the growth of cloud-based and Software as a Service (SaaS) applications, users now have the power to log in to critical business apps like Salesforce, Office365, Concur, and more anytime, from any place, using any device. However, with the increase of distributed applications comes an increase in the complexity of managing user identities for those applications. Without a seamless way to access these applications, users struggle with password management while IT is faced with rising support costs from frustrated users.

Solution

A holistic IAM solution can help administrators consolidate, control, and simplify access privileges, whether the critical applications are hosted in traditional data centers, private clouds, public clouds, or a hybrid combination of all these spaces.

Challenge: Productive provisioning

Without a centralized IAM system, IT staff must provision access manually. The longer it takes for a user to gain access to crucial business applications, the less productive that user will be. On the flip side, failing to revoke the access rights of employees who have left the organization or transferred to different departments can have serious security consequences. To close this window of exposure and risk, IT staff must de-provision access to corporate data as quickly as possible. Unfortunately, in many organizations this means that IT has to go through each user's account to understand what resources they have access to and then to manually revoke that access. Manual provisioning and de-provisioning of access is labor-intensive and prone to human error or oversights. Especially for large organizations, it is not an efficient or sustainable way to manage user identities and access.

Solution

A robust IAM solution can fully automate the provisioning and de-provisioning process, giving IT full power over the access rights of employees, partners, contractors, vendors, and guests. Automated provisioning and de-provisioning speed the enforcement of strong security policies while helping to eliminate human error.

Challenge: Bring your own device (BYOD)

To manage or not to manage—there really is no choice between the two for today's enterprises. Employees, contractors, partners, and others are bringing in personal devices and connecting to the corporate network for professional and personal reasons. The challenge with BYOD is not whether outside devices are brought into the enterprise network, but whether IT can react quickly enough to protect the organization's business assets—without disrupting employee productivity and while offering freedom of choice. Nearly every company has some sort of BYOD policy that allows users to access secure resources from their own devices. However, accessing internal and SaaS applications on a mobile device can be more cumbersome than doing so from a networked laptop or desktop workstation. In addition, IT staff may struggle to manage who has access privileges to corporate data and which devices they're using to access it.

Solution

Enterprises must develop a strategy that makes it quick, easy, and secure to grant—and revoke—access to corporate applications on employee- and corporate-owned mobile devices based on corporate guidelines or regulatory compliance. In addition, technology shifts such as the trend toward an Internet of Things requires corporate IT teams to deploy solutions that can scale to meet the onslaught of devices looking to tax the corporate network.

Challenge: Password problems

The growth of cloud-based applications means that employees must remember an increasing number of passwords for applications that may cross domains and use numerous different authentication and attribute-sharing standards and protocols. User frustration can mount when an employee spends more and more time managing the resulting lists of passwords—which, for some applications, may require changing every 30 days. Plus, when employees have trouble with their passwords, they most often contact IT staff for help, which can quickly and repeatedly drain important resources.

Solution

Enterprises can readily make password issues a thing of the past by federating user identity and extending secure single sign-on (SSO) capabilities to SaaS, cloud-based, web-based, and virtual applications. SSO can integrate password management across multiple domains and various authentication and attribute-sharing standards and protocols.

Challenge: Regulatory compliance

Compliance and corporate governance concerns continue to be major drivers of IAM spending. For example, much of the onus to provide the corporate governance data required by Sarbanes-Oxley regulations falls on the IT department. Ensuring support for processes such as determining access privileges for specific employees, tracking management approvals for expanded access, and documenting who has accessed what data and when they did it can go a long way to easing the burden of regulatory compliance and ensuring a smooth audit process.

Solution

A strong IAM solution can support compliance with regulatory standards such as Sarbanes-Oxley, HIPAA, and the payment card industry data security standards (PCI DSS). In particular, a solution that automates audit reporting can simplify the processes for regulatory conformance and can also help generate the comprehensive reports needed to prove that compliance.

Conclusion

Security. Efficiency. Simplicity. Productivity. Compliance. While the benefits of deploying a robust IAM solution are clear, the cost and complexity of implementation can derail even the most well-intentioned organization. However, when enterprises consider the cost of a potential security breach or study the inefficiencies inherent to the manual provisioning and de-provisioning of access to corporate resources, the imperative is clear: Now is the time to build a centralized IAM team that can build and enforce organization-wide identity and access management policies.

The traditional security perimeter is shrinking. Enterprises searching for IAM solutions must take into account the realities of an increasingly mobile workforce and a highly distributed and complex network of applications. A robust IAM solution can ease management pains, streamline provisioning and de-provisioning, and boost user productivity, while lowering costs, reducing demands on IT, and providing the enterprise with comprehensive data to assist in complying with regulatory standards.

In addition, enterprises can ensure security by deploying solutions with strong multifactor authentication, while eliminating user frustration by delivering seamless access to cloud-based applications through SSO. Furthermore, as identity and access management becomes increasingly complex, the ability to create policies based on granular, contextual information will become more and more important. IAM solutions that can collect and make decisions based on user identity, location, device, and the requested resource will allow enterprises to deliver quick access to bona fide employees, partners, contractors, or guests—and easily revoke or deny privileges to unauthorized users.

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com