Government

Business Challenge

The security architect for this state agency needs to manage access for over 5,500 state employees and 5,000 partner organizations interacting with its systems.

Transformation

The IBM identity management system, supported by several IBM software solutions, gives the access management team a hands-off way to secure systems.

Results

By automating user-provisioning processes, the state agency reduced time demands on administrative staff by over 80 percent

Business benefits

80%

reduction

in administrative staff demands

Reduces

provisioning times

for new employees from weeks to hours

Increases

application security

by automatically de-provisioning employees based on inactivity

A large state agency

Reduces administrative demands by 80 percent with IBM ID Management system

This state agency's security architect characterizes the systems environment to which he controls access and security the "Wild West of IT." Five state agencies — composed of 13 departments, approximately 5,500 employees and over 5,000 outside partner organizations — need access to hundreds of this agency's systems.

> *"Before we had this system, [the process took] days or weeks. Now all requests and approval processes are online, and it takes hours to get users provisioned to the applications they need."*
>
> — security architect, large state agency

Connect with us

Identity management on a massive scale

It’s an immensely complex identity management challenge. Speaking only of the five state agencies, the architect says, “We had to get 13 independent organizations and IT departments to essentially merge so we could develop a security infrastructure that would provide all their users web access to the applications they need while maximizing security and minimizing demand on our administrative resources.”

That security infrastructure must govern user authentication, authorization, password management, provisioning and more for each application. Beyond that, various users also need access to the agency’s network, file shares, active directory distribution lists and group shares.

For many applications and IT systems, manual processes govern requests and authorizations for access. “It could take weeks for users to get access to the systems or the resources they need to do their jobs,” he says, while pointing out that he and his identity and access management team are midstream in a drive to integrate all agency systems into an enterprise identity access management platform. “In addition, several key applications were not meeting our agency’s security policies regarding such things as passwords and automated deprovisioning of user accounts upon termination. So the idea was to deploy a system to provide authentication and authorization and the ability to self-register and request access to different applications, and then once access is granted, have the ability to track and audit the approval process in an electronic way,” he says. With approval processes completed, he wanted users automatically provisioned and able to access the application through one entry point.

Secure, auditable application access

Supporting the agency’s identity management platform are three IBM solutions: IBM Security Access Manager for Web, IBM Security Identity Manager and IBM Security Access Manager for Enterprise Single Sign-On virtual appliances. The Security Access Manager for Web appliance provides runtime authentication and authorization while the Security Identity Manager appliance provides the back-end user provisioning and deprovisioning platform. Used in conjunction with a customer interface that IBM WebSphere Portal software supports, users throughout the agency and its partner organizations request access to previously mainframe-based applications from one URL.

The Security Access Manager for Enterprise Single Sign-On appliance allows users to automatically log in to all of their systems and applications using one ID and password. The appliance is integrated with the agency’s identity management platform so that users enjoy seamless access even as their passwords automatically change every 90 days. “The applications didn’t have to worry about how to implement the security policy or the password complexity or how often,” says the security architects. “And we’re asking our business users to interact with the system, so we want to make their experience a very easy, uninterrupted and positive one.”

With over three million citizens in the state interacting with the agency’s systems, the security architect team also integrated public-facing systems with the Security Access Management tools to control access and deprovision users who’ve been inactive for a period.

Streamlined provisioning and administration

“Before we had this system, supervisors had to manually submit PDF forms through email to request access for their employees, a process that would take days or weeks,” says the architect. “Now all requests and approval processes are online, and it takes hours to get users provisioned to the applications they need. It not only makes things faster, it increases our internal customers’ satisfaction.”

Additionally, the IBM identity management system automatically handles deprovisioning based on inactivity, employee termination and job transfers, which increases the security for agency applications while minimizing the cost of having administrators pull reports and manually deprovision users. The agency estimates that its administrators are reclaiming over 80 percent of the time they would typically have spent on such routine activities.

Outside partner organizations can also register users for authorized access to the agency’s systems through the portal. “They give us all their information before they get access, meaning somebody at their organization has approved that they are a valid user,” the architect says. “That’s how we distinguish that authorized user from some random person trying to self-register. It’s extremely critical from a security perspective. We have an audit trail showing who approved it, so we’re decentralizing identify management by putting the responsibility on them, exactly as we do our internal users.”

Solution components

- IBM Security Access Manager for Web
- IBM Security Identity Manager
- IBM® WebSphere® Portal
- IBM Security Access Manager for Enterprise Single Sign-On

Take the next step

To learn more about the IBM identity management system, please contact your IBM marketing representative or IBM Business Partner, or visit the following websites:

ibm.com/software/products/access-mgr-web
ibm.com/software/products/identity-manager
ibm.com/software/products/websphere-portal-family
ibm.com/software/products/access-mgr-esso

Connect with us

Produced in the United States of America. December 2015. IBM, the IBM logo, ibm.com and WebSphere are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml. This document is current as of the initial date of publication and may be changed by IBM at any time. The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. It is the user’s responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.