GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Author: Canner, Ben

Title: "7 Access Management Best Practices for Enterprises"

Website: solutionsreview.com

Organization: Solutions Review

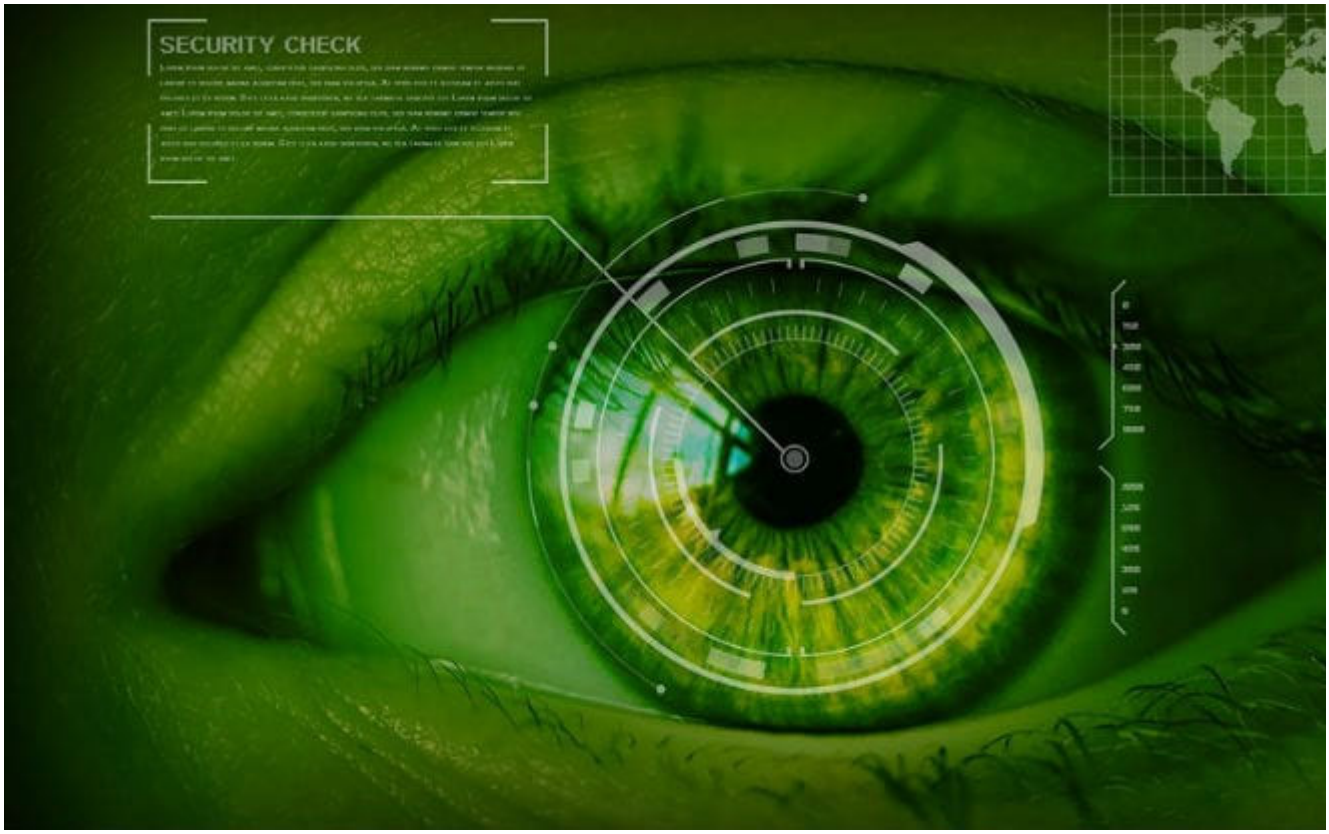
Date: 28 May 2019

URL: https://solutionsreview.com/identity-management/7-access-management-best-practices-for-enterprises/

Accessed: 15 October 2019

Synopsis: What are the 7 access management best practices for enterprises? How can your enterprise ensure full-fledged identity and access management and cybersecurity across a growing IT infrastructure? We explore this and more below!

7 Access Management Best Practices for Enterprises



What are the 7 access management best practices for enterprises? How can your enterprise ensure full-fledged identity and access management and cybersecurity across a growing IT infrastructure? We explore this and more below!

The 7 Access Management Best Practices

1. Centralization

One of the most overlooked access management best practices—indeed cybersecurity best practices—is centralization.

Imagine your network as it exists currently. Consider all of the users, applications, databases, data traffic flows, portals, and more that comprise it. Now imagine trying to keep an eye on all of these moving parts simultaneously, all the while acknowledging the inevitability of scaling, consider their identity security.

Legacy identity management solutions can't possibly provide the centralized view necessary to keep all of this information straight. So your enterprise needs to consider deploying a solution which centralizes your view, controls, and authority over users' identities. Otherwise, you'll always find yourself on the back foot.

2. Role-Based Access Control

Among the access management best practices listed here, role-based access control appears the most complicated. However, when broken down to layman's terms it actually proves incredibly simple.

Role-based access control (RBAC) refers to restricting your enterprise users' permissions to their roles within your business infrastructure. In other words, RBAC only permits users access to what they absolutely need to perform their job functions. For example, an ordinary member of your accounting office shouldn't have access to your digital financial accounts.

In addition, RBAC also helps facilitate identity security, business processes, and cybersecurity visibility. As part of your access management best practices, your enterprise should assign clear, delineated roles to all users.

Ideally, this includes your privileged users as well as your regular users. Moreover, no role should receive permissions outside their roles; if projects demand the assignment of temporary privileges, those privileges should expire within a set time limit.

3. Zero Trust Identity Security

Zero Trust works to upset the traditional model of access management best practices. The traditional method of access management basically checked users at the door but then gave them free rein afterward.

On the other hand, zero trust works more like an airport. You don't just go through one checkpoint at the door; you go through multiple checkpoints to evaluate your identity and your security. Only then does airport security allow you to board.

Put simply, zero trust identity security states your enterprise IT security shouldn't trust any user or application under any circumstances. Your enterprise shouldn't trust anything trying to connect to your network and databases and thus constantly verify its legitimacy before granting access. Are you employing zero trust identity security? You should be.

4. The Principle of Least Privilege

Some may consider the Principle of Least Privilege exclusively privileged access based. However, it actually serves as one of the most crucial access management best practices for enterprises—and often one of the most neglected.

In many ways, the Principle of Least Privilege parallels role-based access control (which we explored above). Both work to limit the privileges your users possess in your IT environment. In fact, the Principle of Least Privilege states employees should only possess the permissions necessary to perform their job processes. Yet role-based access focuses on identity governance whereas the Principle of Least Privilege focuses on initial permissions granted.

For example, imagine your most powerful privileged user in the Human Resources department. The Principle of Least Privilege states that while they may have great liberty in the HR network, they should have limited or no access to your financial

records. After all, those don't correspond to their job titles.

In conclusion, you need to follow the Principle of Least Privilege now, before the worst should happen to your business.

5. Automated Onboarding

Part of the key to access management best practices is starting on the right foot. If your enterprise struggles with ensuring employees begin their roles with the right permissions then you'll have a hard time solidifying business processes and ensuring cybersecurity. Instead, your employees and IT team must spend valuable time and resources ironing out the necessary permissions and ensuring they work properly before an employee truly starts working.

With an identity and access management solution, you can automate the onboarding process; this ensures employees start off on the right foot with the right permissions. This takes the burden off your IT team to onboard each new employee. Moreover, it also shortens the onboarding process from a matter of months to a matter of hours. Plus, automated onboarding forces your IT team to determine the necessary permissions for each role, heightening your identity governance capabilities.

6. Orphaned Account Detection and Removal

Conversely to the above point, failing to offboard your employees properly creates new identity management nightmares in the long term. Without deprovisioning and removing accounts as employees leave your enterprise, their accounts can linger unseen on the network. They become orphaned accounts, which can go ignored for years until hackers use them to bypass your digital perimeter.

Many enterprises don't have an identity and access management solution which can detect and remove orphaned accounts. In fact, many don't possess the willpower or the time to actually seek out all of the orphaned accounts lurking in their environments.

Therefore, your enterprise needs to seek out an identity and access management solution which helps discover and remove orphaned accounts on your network; achieving the highest possible level of cybersecurity visibility should become a top priority for your business. Additionally, your solution should automate and mandate the offboarding process to ensure no orphaned accounts slip past your identity security. The best way to solve the orphaned account problem is straightforward prevention.

7. Multifactor Authentication

The inadequacy of single-factor authentication serves as the central theme in our previous articles on enterprise access management best practices. Passwords, the foundation of most single-factor authentication schemes, consistently prove unreliable for enterprise identity security. Hackers of even nominal skill can easily crack, guess, or circumvent password-based logins.

Additionally, users often use weak passwords or worse yet repeat their passwords across multiple sites. The latter in particular bolsters hackers' cyber attacks by giving them ammunition for credential stuffing attacks. Often, employees don't enjoy using

a password-based single-factor authentication system; passwords are often forgotten and require time and resources to recover.

Therefore, your enterprise needs to embrace deploying and maintaining multifactor authentication as part of your access management best practices. The more steps between the access request and your digital assets you implement, the more secure they remain.

Multifactor authentication steps can include biometrics, geofencing, time of access request monitoring, hard tokens, SMS messaging systems, and even passwords. If your employees find multifactor authentication an impediment to their business processes, you can weigh the prospect of step-up authentication instead.

Want to learn more about access management, identity security, and identity governance? Check out our 2019 Buyer's Guide! We provide details on the top vendors in the field, their capabilities, and our own Bottom Lines!

- About
- Latest Posts

Ben Canner

Ben Canner is an enterprise technology writer and analyst covering Identity Management, SIEM, Endpoint Protection, and Cybersecurity writ large. He holds a Bachelor of Arts Degree in English from Clark University in Worcester, MA. He previously worked as a corporate blogger and ghost writer. You can reach him via Twitter and LinkedIn.