Simplifying secure identity and access for over 27 million users

IBM Office of the CIO establishes future-proof digital authentication with IBM Security Verify

by Lance E. Osborne

7-minute read

The expression "caught between a rock and a hard place" comes to mind when describing two challenges that the IBM Office of the CIO was struggling with. First, imagine having to provide identity and access authentication services for over half a million IBM employees around the world, with a highly customized, single tenant, on-premises platform. And at the same time, having to provide similar identity and access services for over 26 million global IBM clients with a separate, antiquated first-generation identity as a service (IDaaS) solution.

Now you might begin to understand what the IBM Office of the CIO was up against: two separate identity and access management (IAM) platforms offering different technologies and different levels of maturity, reliability, and functionality.

The scale of the challenge can be hard to imagine. IBM's Assured Identity and Cybersecurity Operations team supported 5,000 applications, more than 600 federated client companies and their workforces, and over 150,000 authorization groups. In one quarter

of 2021, IBM authentication services supported 35.7 million logins.

And in today's competitive environment, the playing field was constantly changing. As Daniel Opoku-Frempong, Director of the Assured Identity and Cybersecurity Operations team, points out, "The IBM CIO organization provides critical identity services for the entire IBM workforce, millions of clients and now Kyndryl, too."

Transforming IBM's authentication services would require significant infrastructure modernization and consolidation to efficiently deliver large-scale reliability and security. Opoku-Frempong describes the difficulty: "We needed to orchestrate a foundational change in how we captured, engaged, managed and administered user identity and access across our millions of users

around the world. We could no longer defend the poor return on investment and the slow speed to market that haunted every workflow touched by the old solutions."

Ed Klenotiz, Assured Identity Architect, and his colleagues got the ball rolling. "We completed a competitive analysis of the leading vendors to power both business-to-employee and business-to-business identity services," he says. "Leveraging a standard, cloud-based authentication platform would be a critical first step to modernizing identity services for both IBM employees and our customers, at scale."

And just as IBM would recommend to its own clients, the Assured Identity and Cybersecurity Operations team captured all their identity and access requirements and compared several solutions from across the market.

"The IBM Security Verify capabilities enabled us to provide our customers with extensible features for enhanced security with flexible MFA methods, password management enhancement, user ID lifecycle management and self-care, application management, flexible user notification of changes, and event notification service."

Lee Ann Rodgers, IBMid Program Manager, Assured Identity and Cybersecurity Operations, IBM

Applying the power of a modern IAM solution

After gathering requirements and considering all the options, the Assured Identity and Cybersecurity Operations team chose IBM Security™ Verify (SaaS) for their combined millions of internal and external users. The number-one reason? Top of the list was because the APIs enabled a seamless application migration. And number two? They'd be able to customize the user interface to fit their exact requirements without draining their development resources.

By embracing IBM Security Verify as the standard cloud IAM services platform for all B2E and B2B identities, IBM would be poised to deploy more modern identity capabilities with enhanced security, scale, and user experience.

"With the new solution, we could expand internal user choice for authentication," says Opoku-Frempong.

"Two-factor authentication (2FA) significantly protects against password compromise but it's often cumbersome for users. So, we implemented adaptive features of 2FA that used back-end analytics to determine when and where to require additional authentication. The shift to IBM Security Verify 2FA capabilities offered enhanced choice for IBMers to authenticate via passwordless options, such as QR code and FIDO2 for TouchID and Windows Hello. That was a sea change just by itself."

But there were other pressures. Historically, the IBM CIO team had invested in developing its corporate directory to comply with the International Traffic in Arms Regulations (ITAR) a United States regulatory regime to restrict and control the export of defense and military related technologies. Ripping and replacing the old IAM solution across the globe and all at once was out of the question. The IBM Security Verify engineers had anticipated this requirement. The Security Verify Bridge coupled with the Bridge for Directory Sync enabled the IBM CIO team to apply its legacy investment and the associated processes. And as a secondary benefit, this enabled them to develop a carefully staggered migration plan with minimal impact.

Opoku-Frempong continues: "There were other migration capabilities that made the transition smoother. IBM Security Verify's enhanced API library enabled self-service application migration by our application owners, minimizing impact to other workloads. Moreover, the enhanced layer of control around privileged API access gives us tighter security control over the environment, further minimizing attack vectors. That's definitely a win-win for us."

...and we're just getting started

Opoku-Frempong and his team had quite a lot to celebrate. By adopting IBM Security Verify, they were able to improve the user experience while also tightening the security for those same users and the company's network, data, and applications, at scale. Lee Ann Rodgers, IBMid Program Manager, puts it this way: "The IBM Security Verify capabilities enabled us to provide our customers with extensible features for enhanced security with flexible MFA methods, password management enhancement, user ID lifecycle management and self-care, application management, flexible user notification of changes, and event notification service."

Plus, there's a vision for the future now, a promise for more value. As IBM's identity and access authentication journey continues, the IBM workforce and IBM clients can expect more benefits:

- A transformed user experience without passwords
- Enhanced protection for privileged users across multicloud environments
- Flexible multi-factor authentication (MFA) methods, improved password management, and user ID self-care and lifecycle management

- Integration with devices and mobile device management solutions to support IBM's zero-trust strategy
- IBM Security Verify microservices architecture for improved solution fault tolerance and scalability
- Multi-site plans for enhanced reliability
- Continued focus on the user and branding experience with strengthened commitment to security and privacy.

Gary Schmader, Sr. Manager of Assured Identity, sums it up: "We are relying on our own commercially available solution for a mission-critical need, on a grand scale. With IBM Security Verify, to anyone who interacts with IBM, we can now provide frictionless, secure, state-of-the-art access to information resources ... and we're just getting started."

> "With IBM Security Verify, to anyone who interacts with IBM, we can now provide frictionless, secure, state of the art access to information resources."

Gary Schmader, Sr. Manager, Assured Identity and Cybersecurity Operations, IBM

For more information, please contact your IBM Business Partner:

Sweet Spot International

403-461-6227 | swifthillb@sweetspotint.onmicrosoft.com

https://saas-ssi.com/

About IBM

IBM is the global leader in hybrid cloud and AI, serving clients in more than 170 countries. More than 3,500 clients use our hybrid cloud platform to accelerate their digital transformation journeys and, in total, more than 30,000 of them have turned to IBM to unlock value from their data—this client list includes nine out of ten of the world's largest banks. With this foundation, we continue to leverage Red Hat® OpenShift® as the leading platform to address our clients' business needs: a hybrid cloud platform that is open, flexible, and secure. Guided by principles of trust, transparency and support for a more inclusive society, IBM also is committed to being a responsible steward of technology and a force for good in the world.

Solution component

- IBM Security™ Verify (SaaS)