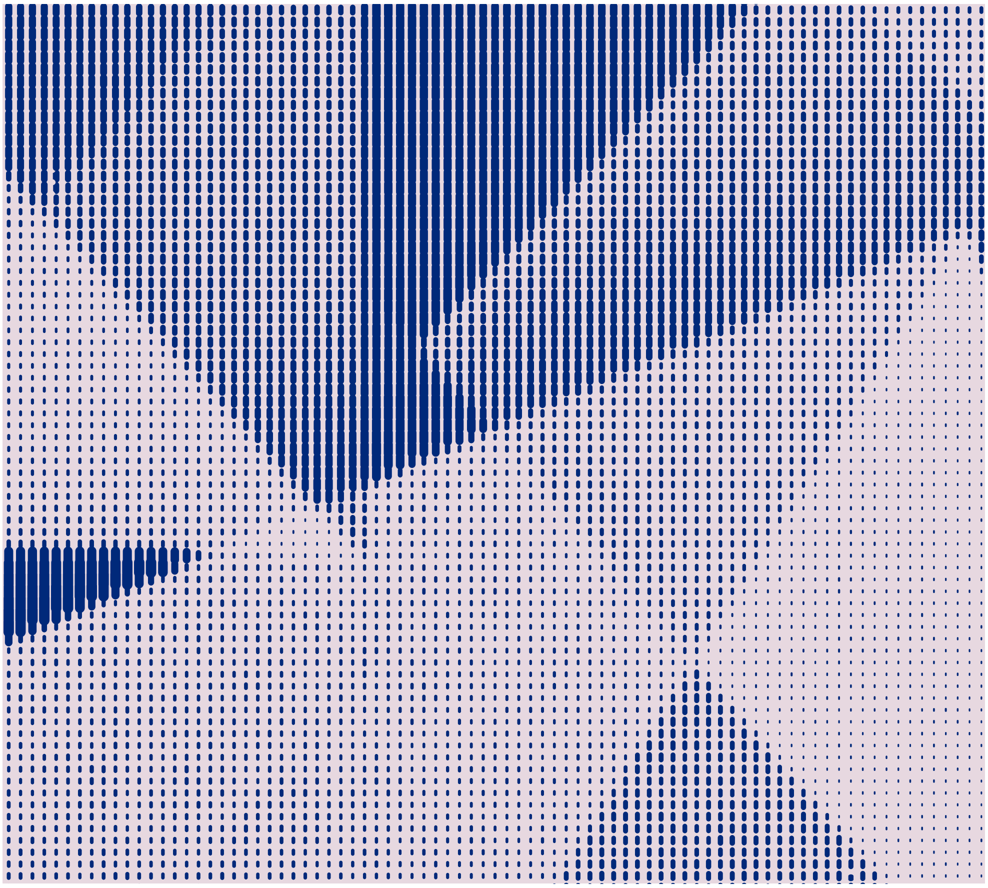
Whitepaper

June 2021

Gartner Is Mapping the Future of Secure Access. Okta Is Helping Organizations Get There

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871



okta

At Okta, it's our job to keep our eye on the horizon of identity and access management, so we have strong ideas about where it's headed. That's just one thing we have in common with Gartner, the global leader for research, analysis, and advisory services. And at Gartner's Identity and Access Management Summit this year, we got to see just how closely our projections align.

In May 2021, business, IT, and security leaders convened to discuss top priorities and best practices in identity. Okta both attended and presented, participating through a virtual sponsor booth and by hosting a roundtable discussion with attendees.

That put us in an ideal position to hear firsthand about the issues that are top of mind for leaders today, and we noticed a recurring theme—one that's very much in line with Okta's view of best practice for securing data, streamlining processes, and modernizing access.

The word that surfaced again and again was consolidation. Conversations across a range of contexts focused on the need to centralize, converge, and integrate, and they arrived at some conclusions:

- **Identity solutions need to be both future-proof and backwards-compatible.** They need to function alongside the systems and applications that businesses currently depend on, but they also need to be extensible so they can evolve and scale as technologies change.
- **There has to be a better way to create unified, consistent digital identities for users.** It's imperative that the right individuals have the right level of access to the right data at the right time.
- **Organizations need a single strong identity platform to provide all this.** Identity isn't seen as a commodity anymore, but as a central pillar in a modern tech and security stack.

In short, identity needs to be simplified: leaders agree it's currently too complex for many organizations—if all these pieces are so critical, they shouldn't be so difficult to connect.

Three specific initiatives respond to these general themes, and it's no surprise that they trended at Gartner's summit:

- Privileged access management (PAM)
- Identity governance and administration (IGA)
- Passwordless authentication

We are familiar with these trends—they follow the lead of Okta's strategic thinking and innovative service offerings. Here's a closer look at why these three initiatives are so important, and how Okta has been answering the call.

Privileged access to the most sensitive resources

Many of the attendees at Gartner's identity summit had recently shifted on a large scale to distributed operations and service delivery. Naturally, they unanimously supported ongoing digitization and modernization initiatives.

But of course, with large-scale technology adoption, the need to protect critical computing resources—such as restricted systems, restricted functions, and confidential data—has become both more urgent and more complex. This pushes PAM to top priority for leaders. According to Gartner senior director Felix Gaehtgens, "PAM is all about securing the keys to your kingdom."

But how does PAM work? "Superusers," such as system administrators or CIOs, tend to have privileged credentials for privileged accounts and can access an organization's most critical systems and resources. This makes them the highest value targets for malicious attacks. Traditionally, PAM has involved isolating superuser accounts within an encrypted repository or vault and protecting them with a range of complex and cumbersome identity protocols to ensure compliance.

Common principles and best practices for PAM include:

- The principle of least privilege, which ensures that users, applications, and devices are given access only to the resources they need to perform their roles.
- The principle of just-in-time-access, which ensures access is only granted for a short period of time, rather than extended indefinitely.

Introducing a consolidated PAM solution

In the past, Okta supported these initiatives by integrating with PAM providers and adding a range of supportive solutions: single sign-on helped reduce identity sprawl and strengthen credentials; adaptive multi-factor authentication and risk-based authentication assessed the context of every login request. Meanwhile, lifecycle management automated provisioning and deprovisioning and limited the risk of ghost accounts.

But Gartner's identity summit reiterated the importance of having a single identity partner to provide a consolidated identity stack. So it's a good thing that Okta Privileged Access is already in the works.

Launching in Q1 2022, Okta Privileged Access taps into the power of the Okta Identity Cloud to provide a comprehensive and user-friendly PAM solution. Fine-grained and role-based security policies, centralized management at the infrastructure level, and tightly-scoped ephemeral credentials for limited sessions combined in a single product offering. It ensures automation and velocity at scale, while mitigating error-prone manual processes and risk.

Identity governance for employees and contractors

PAM protects superuser accounts—but what about security and access for everyone else? Workforces and their work environments have changed dramatically. Employees sign in from anywhere, and partners and contractors have access needs that may be as extensive as full-time and in-house teams.

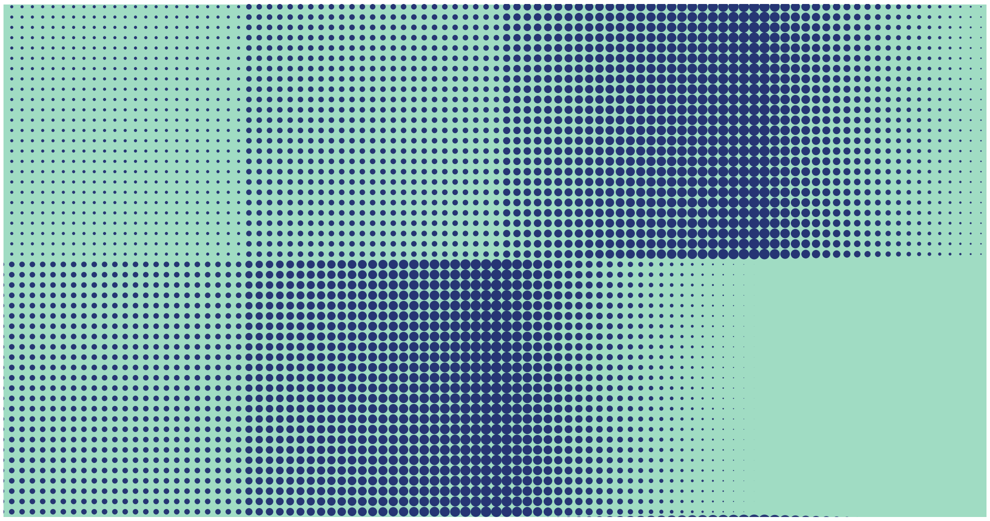
Organizations leverage IGA solutions to orchestrate user management and access control. They coordinate multiple technologies and features, such as administration, analytics, identity management, and role-based access policies, to enable process automation and compliance. The problem is that conventional IGA systems are designed for on-prem applications and infrastructure—and they have always been costly and complex to deploy. They no longer meet the business needs of today's dynamic cloud environments.

Tellingly, Gartner predicts that IGA will be the single largest identity investment most organizations will need to make in the months ahead—but it will also be one of the riskiest solutions to deploy. Gartner maintains that an IGA deployment should be 80% automation, but typical tool-centric approaches lack consolidation and unification, and could undermine the solution's success.

Integrated IGA is on its way

Once again, the summit's focus on IGA was timely; Okta recently announced the rollout of a new cloud-based, integrated IGA solution, coming in Q1 2022. Okta Identity Governance delivers self-service identity governance and administration for all users through a single control plane. It stretches across all systems—from apps, to APIs, to servers—analyzing the right level of access to resources and the right level of automation for every use case.

At the same time, streamlined reporting supports compliance programs, empowering organizations to do away with time-consuming data wrangling and costly consultants.



Stronger security with passwordless authentication

Throughout Gartner's identity summit, business, IT, and security leaders clearly shared Okta's opinion that identity is now inextricably tied to security. Modern organizations see the need to adopt a Zero Trust model, where all network traffic is viewed as untrusted and user identities must be verified through robust context awareness and risk-based authentication.

As security moves to the level of login, it's imperative that organizations part with their obsolete passwords. The vast majority of data breaches originate with these outmoded credentials, which can be stolen or lost; and once they've been compromised, brute force attacks such as password spray and credential stuffing can be conducted at scale with botnets. Hackers looking to stage an account takeover (ATO) attack also favor phishing and spear phishing as powerful threat vectors, tricking users into handing over their identity information.

The attendees at Gartner's summit agreed: getting rid of passwords is the future of security. But as an added bonus, it makes life a lot simpler for your workforce. Passwords have long pained workers and administrators, whose productivity suffers as a result of constant resets.

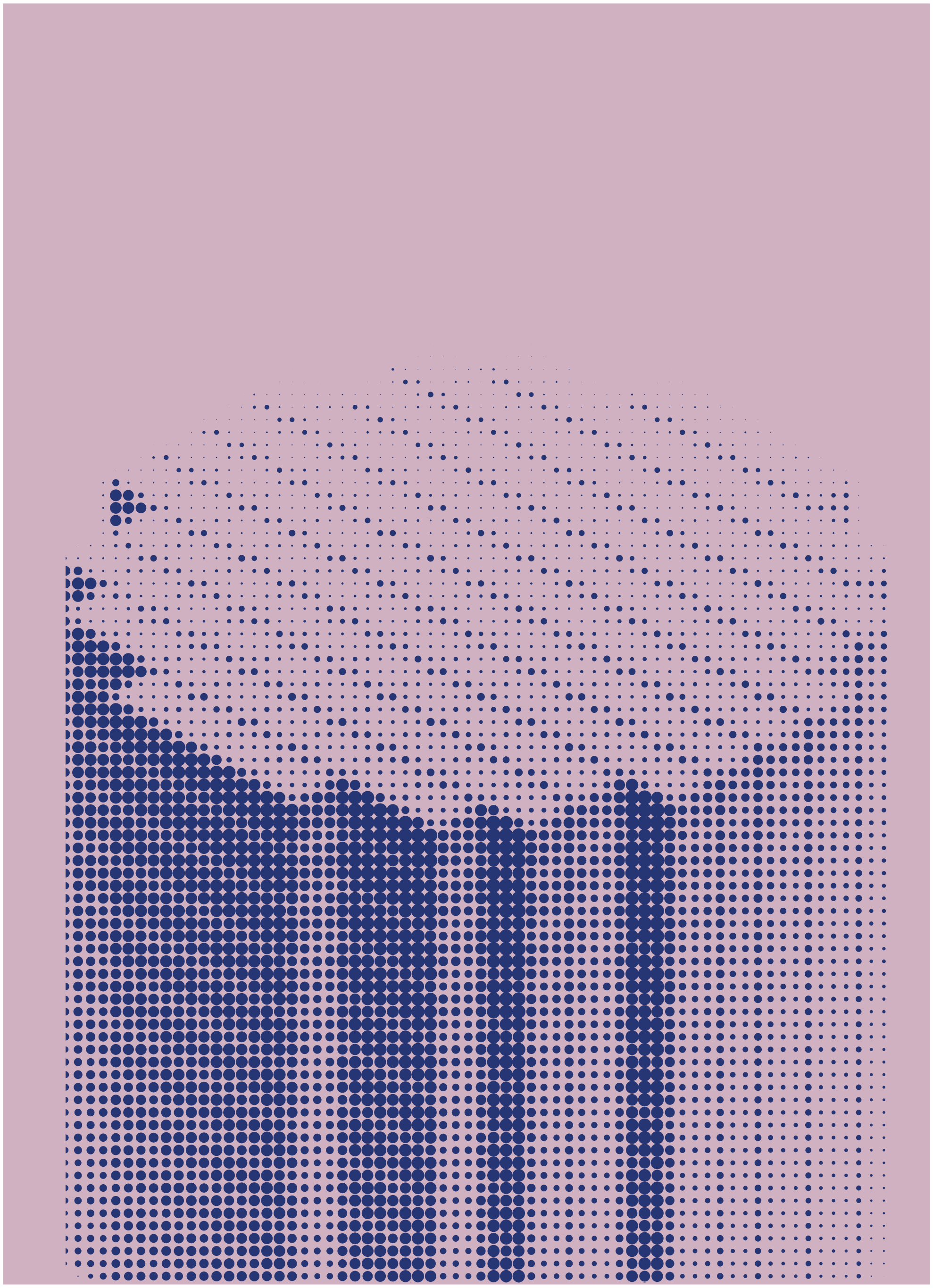
There's a streamlined approach to authentication

There are many ways to adopt passwordless authentication for the workforce and lay a strong foundation for a modern Zero Trust security framework:

- Okta FastPass provides device-based authentication for Windows, iOS, Android, and MacOS with no dependency on on-prem directories or specific endpoint management tools.
- Email magic links enable employees to simply click on an embedded link in a verified email to validate the login request and continue the process.
- Factor Sequencing is a defined chain of passwordless factors that combine with user, device, and location context.
- WebAuthn allows for phishing-proof, biometric-based auth using the FIDO2.0 standard.
- PIV/Smart cards are used mostly by federal stakeholders to facilitate authentication with an x509 certificate.
- Desktop Single Sign-On permits passwordless logins for AD domain-joined machines.

- Device Trust integrations utilize endpoint management solutions' mobile SSO features.

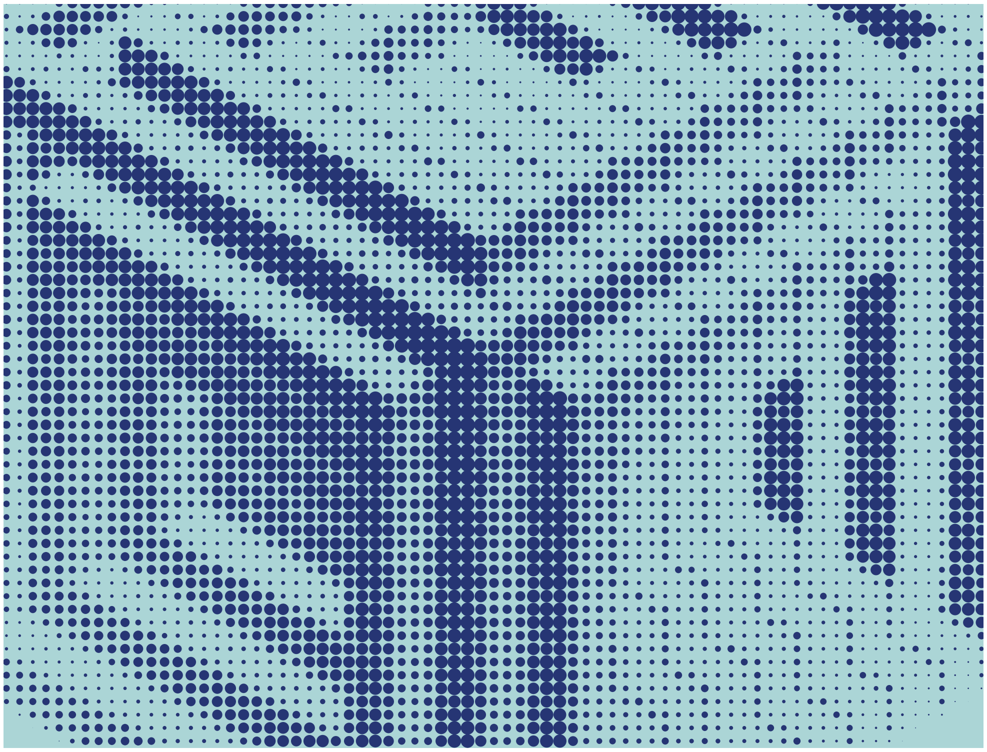
For some, passwordless authentication may sound theoretical, but it's actually practical, simple, and secure, and leading organizations have already adopted it. For Gartner's summit, we spoke to our longtime customer, Moody's, about the future of identity for their global investor services enterprise—and for them, the shift to passwordless is as imminent as it is inevitable.



The central role of identity in modern organizations

One lesson from Gartner's identity summit rang clear: organizations understand that the future of security starts with identity, and that unified, consolidated solutions are its foundation. Okta forecast this future—and that prepared us to help organizations navigate it, now. As we've demonstrated, we don't just track trends; we set them, with innovative solutions like Okta Privileged Access, Okta Identity Governance, and passwordless authentication that readily anticipate what's next on the horizon.

Now is a pivotal moment to elevate the role of identity in your organization's security stack. For help finding the solution that fits your organization's future, get in touch.



About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 7,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 10,000 organizations, including JetBlue, Nordstrom, Slack, Teach for America, and Twilio, trust Okta to help protect the identities of their workforces and customers. For more information, visit **okta.com**.