www.pipelinepub.com
Volume 18, Issue 1

Frictionless Security without Passwords

By: Lucas Budman

Everybody hates passwords. They slow us down. They can be complicated. And of course, we must remember *so many of them*.

Cyber threat actors are the exception. Hackers love passwords—after all, passwords are easy to discover and exploit. And they're plentiful.

In other words, hackers don't break in, they login with stolen passwords. In fact, 81 percent of data breaches start this way, making passwords the biggest attack vector in the modern enterprise. And even though more than $16 billion was spent on identity and access management (IAM) solutions in 2020, the problem continues to worsen. Existing two-factor and multi-factor authentication (MFA) tools are simply insufficient; they may improve a poor security posture, but they do nothing to prevent phishing attacks, credential stuffing, or man-in-the-middle SIM swaps. They do, however, cause significant user friction and workflow interruption, which hinders their adoption and use.

A renewed interest in passwordless solutions

A recent Forrester report notes the increased criticality of IAM for securing access, ensuring business continuity, and supporting remote workers while battling evolving threats across dispersed on-premises and cloud-based workloads. The push to fully remote workforces and the strain of layoffs, rehires, contractors, and role changes exposed the frailty of homegrown, manual identity governance and paved the way for renewed interest in passwordless solutions.

But as organizations know all too well, the identity management and authentication landscape is incredibly costly and complex, and as the Forrester analysts note, the adoption of too many security solutions in a short span can lead to unforeseen integration challenges, tools that don't map well to existing business processes, and wasteful or overlapping capabilities.

For those companies committed to supporting the shift to hybrid work, innovative and robust passwordless enterprise technologies can help protect the business from rapidly increasing cybersecurity threats while ensuring a seamless experience for employees who can easily and securely log in from anywhere in the world without the need for antiquated and insecure passwords. As Walter Yosefat of Wyndham Destinations remarked, "As a CIO, my vision has been to live in the day when user IDs and passwords are no longer needed and I'm just known to my apps and systems without the need to continually assert it."

Successful passwordless deployments must reduce complexity, end fragmented user experiences, and streamline use-case support to drive down cost. After all, a great technology is only meaningful if it's useful—and used. To remove the threat from compromised credentials and support a secure, easy-to-use solution, organizations must:

1. Eliminate credentials altogether with a fully passwordless experience based on true identity and industry standards like FIDO and FIDO2
2. Deploy continuously validated identity based on behavioral ***and*** environmental signals
3. Create a friction-free user experience

Aligning with the Zero Trust model

The best solutions available today align to the Zero Trust model. They continually receive signals from a user's smartphone, computer, network, and proximal environment to make highly secure decisions on identity and authentication. They also use sophisticated multipath optimization technology to find the most secure path to communicate identity to systems, applications, and resources. But perhaps most importantly, winning solutions offer pre-built, standards-based integrations across the entire identity stack to support full-spectrum authentication. Remote onboarding and identity proofing, workstations, SSO/apps, servers, VPNs, Windows, Mac, and privileged access should all be supported, as should physical access via badge readers. Benefits include fast secure deployment, shorter procurement cycles, easier maintenance schedules, lower product subscription costs, lower integration costs, more accurate IAM policy management, and centralized reporting.

Solutions must also be more than just a biometric alternative to passwords; they must offer frictionless access, coupled with behavior pattern analysis and the ability toremove access from unintended users. Done right, an advanced passwordless solution removes the zero-sum trade-off between better security and a better user experience. It allows individuals to authenticate into workstations, physical doors, and other sensing assets simply by being close to them and uses AI/ML to approximate distance from sensing objects without requiring traditional pairing or additional user interaction. End-to-end use case support allows enterprises to consolidate

solutions, remove complexity, reduce costs, and deliver better security outcomes, while robust administration tools and workflow-based execution easily support complicated security and access requirements. Here's how:

Enterprise-wide coverage

The passwordless solution can't be tied to just one application or system; it must be available everywhere a user works.

Presence-based authentication

The solution must be able to authenticate users seamlessly at workstations *and* physical entries using proximity and biometric data.

Continuous identification

It's not enough to validate users at sign in; solutions must continually authenticate them throughout the entire work session.

Self-service tools

Enabling users to enroll and manage their devices from anywhere (based on internal security policies) reduces IT help desk tickets.

Speed and scalability enable passwordless solutions to become the single most secure authentication layer to all digital and physical workflows in the enterprise. Deep technology collaborations with manufacturers and operating system vendors overcome usability challenges, and strong AI/ML functionality allows the solution to improve with each user interaction. Best of all, the superior end-user experience facilitates broad adoption so the tech actually gets used.

Weighing the tradeoffs

Forrester analysts also encourage buyers to consider the security and ease-of-use tradeoffs between biometrics, smartphone as token, or hardware tokens and to pay attention to vendor support for OSes, browsers, and endpoint devices. They note that a passwordless approach must still support an overall MFA strategy with a means for risk-based, step-up authentication that takes into account the need to secure access to apps built to support only passwords.

Additionally, to provide more granular and dynamic network access, Zero Trust edge mandates that most network traffic and activity be tied to well-identified, authenticated, and authorized users. As the Forrester report notes, cloud-based solutions enable organizations to implement and enforce least-privilege-based, just-in-time access to storage, compute, and network resources.

Beyond usability and security, continuous authentication solutions must respect user privacy. Users should have complete control over and visibility into the data that are collected and how it is used. Modeling should be done in a privacy-preserving manner with clear outcomes defined, and AI/ML models should be used strictly to facilitate authentication the user initiated and not for any other data collection or user monitoring.

Striking the right balance

Continuous passwordless identity should strike a balance between a frictionless end-user experience and highly accurate security to lay the foundation for data-breach risk-reduction strategies that improve cyber resilience and reduce user frustration at the same time. Organizations that prioritize the passwordless approach will leapfrog current technologies and lead the pack with the best credential defense available.

Their workflows will become more streamlined, their overall cyber investments will shrink, and their users will be much, much happier.