1KOSMOS

Modernizing Identity and Access Management

Emergence of Decentralized Identity and its Role in the New Framework for Managing Investment in Cybersecurity

Whitepaper

Introduction of Business Challenge

The rise of remote workers and borderless trade has opened the door to heightened cybersecurity threats. More geographically dispersed workers, customers, and supply chain partners comprising the *"extended enterprise"* are logging into corporate services remotely, placing significant stress on security and service desk teams already stretched thin.

At the same time, hackers have become more adept at exploiting cyber vulnerabilities with tactics such as phishing, SIM swaps and push bombing exposing organizations to massive economic loss and disruption.

Information Technology (IT) and security leaders cannot reach a consensus with other C-Suite members and the Board of Directors on the value that cybersecurity brings to the business. All find it difficult to articulate the metrics they are expecting from cybersecurity efforts.

Open to debate are the operational efficiency, risk reduction, audit and compliance, end-user experience, business adoption, and, most prominently, cost metrics to gauge value and organizational maturity. Just as complicated is how to deploy human resources optimally across a broad array of teams designed to manage the corporate IT network. These include Information Security, Cloud Security, Information Assurance and Security (IAS), Cybersecurity, Digital Identity, Fraud Prevention, Human Resources, and Audit and Compliance.

The great debate surrounds what ROI (Return on Investment) should be expected from the many investments in systems and tools. But also, what is the cost of doing nothing? If you do not do anything, there may be a chance for troubling audit findings, making the more significant challenge of understanding and agreeing on what to prioritize in addition to how to measure and benchmark progress to industry cohorts.

Emergence of a New Framework for Managing Investment in Cybersecurity

To frame strategy and execution to reduce cyber risks and thwart ongoing attacks, a new Digital Identity framework has evolved around four tenants colloquially called the ***"Four R's":*** Realization, Readiness, Resilience, and Remediation. As we will see, digital identity runs as a common thread through each of the four, and password-based security, the Achilles heel, can set organizations up for failure from the start. In collaboration with Sam, 1Kosmos has adopted the 4 Rs framework to truly address two areas that are important for C-suites; maturity and value.

Realization

How well do you understand your environment as an IT and Security executive? How many types of identities do we have? What are the authoritative sources for each? It is crucial to have a comprehensive understanding to satisfy management and access to systems, including considerations such as classifying IT assets to help prevent cyber incidents. This is not just about data, but encompasses continuous monitoring of infrastructure, cloud, devices, network, application, and most importantly people.

Resilience

Micro-segmentation and network hardening are critical, but zero trust strategies and implementing least privilege represent operational challenges. Part of resiliency is making it simple, easy, repeatable, and secure simultaneously. Another critical ingredient is regular cybersecurity training to ensure everyone uniformly understands and can implement zero trust strategies. But, at a higher level, this really asks, "Are we applying the least privilege to everything that requires authentication and authorization?"

Readiness

How ready are you for unforeseen changes, unexpected multinational and geopolitical situations, and attacks from within? Are you running routine simulation exercises to test and refine the organization's response to various scenarios?

Remediation

When a cyber incident does happen, how quickly can the organization respond to contain and recover with as minimal impact on the organization and brand as possible? Does the organization have a firm grasp on important metrics such as "time to detect a breach," "time to contain a breach," and "time to recover from a breach."

The Challenge Managing Access to IT Networks Built Over Decades

Migrating and merging the disparate technologies comprising modern-day enterprise computing infrastructure requires a lot of effort. But there is a misconception that when a few target systems are merged, the result is a single platform. This is usually not true because cloud providers still utilize disparate Identity Providers (IDP).

When it comes to managing authentication for the extended enterprise, most organizations struggle with a cobbled-to-gether infrastructure – generations of Identity and Access Management (IAM), Identity Governance and Administration (IGA), Single Sign-on (SSO), Privileged Access Management (PAM), and Identity as a Service (IDAAS) systems working with as many operating systems and all wrestling over access control and user data, slowing digital transformations.

As a result, IT and security teams and the service desk as well are strapped, and users are dissatisfied. Progress cannot come fast enough or stop the threats that keep evolving. This has caused a lot of people to realize the transformative benefits of consolidating IDPs. Cost, management, and overhead operations are all considerations. However, at a more strategic level, this ushers into consideration a new enterprise architecture for identity that is shifting toward decentralization.

This shift will bring unparalleled privacy controls and portable credentials, promising an improved and more secure user experience, ensuring an identity is present at every transaction. But how can IT and security teams adjust on the fly? Even when you merge into a single IDP platform, it does not mean you have a guarantee that moving forward because of mergers, acquisitions, and divestitures, you do not end up with multiple and competing architectures again.

A shift toward decentralized identity entails a strategy and supporting platform that can adapt with the business to accommodate new organizational structures, users in all corners of the globe, and a broad array of devices that will require anytime access. At the same time, it must not introduce new security vulnerabilities, privacy concerns, or compliance challenges.

How can identity be orchestrated across these multiple IDPs to make the experience seamless? And how will critical privileged systems that require the highest authentication assurance levels fit into the picture?

Problem Posed by 60-Year-Old Password-Based Security

Password-based technology dates to the 1960s, and along with MFA (Multi Factor Authentication), SSO, and the cadre of platforms introduced earlier, it failed badly to protect individuals, organizations, and government agencies from costly cyber attacks.

As an outdated but familiar approach, passwords create a complicated and costly mix of people, processes, and technology to support a perpetual cat-and-mouse game with red versus blue teams vying to prevent and gain access to knowledge, inherence, and possession factors.

According to the 2024 Verizon Data Breach Investigations report, almost **40%** of threat actors gain unauthorized systems access through login credentials. Further, **68%** of breaches involved the "human element."

The evidence is clear.

Passwords pose an unfair cognitive load on users to remember countless "hard to guess, easy to remember" secrets dozens of times each day while juggling second factor devices and often multiple authenticator apps. But mostly, passwords have left organizations reeling from social engineering, phishing, and increasingly deepfake attacks on account credentials while cyber criminals have become ever more adept at push bombing and SIM swaps to defeat multi-factor authentication (MFA).

The antiquated construct of an individual represented as a user ID and password in a centralized user store must evolve to a more durable construct. This decentralized identity offers much higher protection and fidelity, such as live biometrics matched to verified government-issued credentials. This approach ensures much higher levels of trust behind remote logins to help prevent fraud and unauthorized access.

At the user interface, every credential using a password is weak because it can be intercepted and coerced, and caches can be cracked. Users interact with the SSO system and then use second factors to authenticate. Other systems fall outside the reach of SSO. Still, others might require secrets to be shared – the so-called knowledge-based factors. Users often juggle multiple authenticator apps and hundreds of passwords, each slowing access to digital services. Each one is an exceptionally weak link exposing cyber vulnerability.

The Emergence of Decentralized Identity

Make access easy. Take out the friction and stop fraud at new account origination, during login, and especially at the transaction level. It all sounds so simple, but the seed of cyber vulnerability in identity and access management starts with username and password.

Decentralized identity solves the "Trust on First Use" (TOFU) challenge, which occurs when users transition to new systems and must provide a username and password. From that point forward, the limited fidelity of the username and password combination representing the user presents a fundamental problem because any time a password is leveraged, the user's true identity cannot be known.

The idea behind decentralized identity is to not only eliminate passwords from the user interface but to replace them in the user store by:

One.

Creating a reusable, attribute-rich, and tamper-evident digital identity (AKA Digital Identity Wallet) replacing the user ID and password construct.

Two.

Make this identity as private and independent as users themselves by removing administrative access to it.

Three.

Use the attributes that comprise the digital identity to authenticate the individual into online service.

This modernized approach to identity and access management does not simply obfuscate or hide the password behind a biometric. It evolves the "atomic unit" representing an individual from the frail username/password combination stored in a centralized user store to an attribute-rich decentralized identity protected by public-private key cryptography, sharding, and decentralized storage.

With decentralized identity, users are not issued a user ID or password on first access. Instead, they typically click a link sent to any device and complete a customizable identity verification journey that can include biometric capture, credential scans, and validation, or virtually any combination of traditional identity verification methods deemed appropriate for their role, risk level, employee grade, etc.

The 1Kosmos platform verifies identity (not just an authentication factor like a password, PIN, or security question) at the initial login and re-verifies identity anytime a new login or step-up authentication is needed.

Users register their biometric data, such as fingerprints or facial scans, which are then encrypted and securely stored on a private blockchain. Facial biometric capture is certified against deepfake injection and presentation attacks to PAD-1 by the independent testing organization iBeta. Passwordless MFA is further certified by FIDO to their FIDO2 specification and by Kantara to the government standard "NIST (National Institute of Standards and Technology) 800-63-3" and UK-DIATF IDSP and ASP. Further, 1Kosmos holds SOCII and ISO27001 certifications.

The unique privacy-by-design architecture centered around a private and permissioned ledger provides 1Kosmos an architectural advantage in performing passwordless MFA and enabling the use of reusable verified credentials (e.g., zero-knowledge proofs) while giving users sole access and control of their data, thus eliminating privacy concerns related to a centralized user store.

Current customers include several multinationals with operations in financial services, banking, telecommunications, manufacturing, and several other industry verticals that offer emerging growth opportunities. Use cases include remote and in-person identity verification and authentication for logical and physical access.

1Kosmos has a global installed base and performs hundreds of millions of daily authentications. In one recent case study, it was deployed for passwordless authentication into a remote access system in **less than four weeks for 40,000 users** and demonstrated **$4 million in annual savings** – roughly $1,000,000 in efficiency **for every 10,000 employees**, by reducing login times and reducing workload on the service desk (e.g., password reset requests).