Whitepaper

Fortifying The New Perimeter:

How Zumigo Powers Identity-First Security with Real-Time, Authoritative Verification and Authentication

Zumigo

Whitepaper

Fortifying the New Perimeter: How Zumigo Powers Identity-First Security with Real-Time, Authoritative Verification & Authentication

The New Reality of Network Vulnerabilities Requires New Security Approach

The proliferation of cloud computing, remote work, and mobile access has rendered traditional network-centric security models obsolete. The security perimeter has dissolved, making the user's identity the single most critical and most vulnerable control plane for enterprise systems.

The traditional model of enterprise security, defined by firewalls and virtual private networks (VPNs) built around a physical network, must be upgraded to respond to this shift. This reality has ushered in a new security architectural consideration: to secure the perimeter, instead of adding barriers that can be breached with malware, phishing or social engineering by hacking identities, you have to ensure the identity accessing your system actually belongs to a legitimate consumer.

This Identity-First Security approach places the verification and authentication of the identity of the consumer at the core of the security architecture. Access is granted based on who the consumer is and what their context is (their device, location, and behavior), not where they are located.

This approach requires new architectural considerations:

1. **Low-Friction, Seamless Approach:** Security must be invisible and effortless so that people will actually use it and not abandon the process.
2. **Real-Time, Authoritative Information:** Verification must be immediate and based on the freshest and most authoritative data for maximum accuracy.
3. **Comprehensive digital identity intelligence:** Different artifacts of an identity should be verified, and the layering options should meet business requirements.
4. **Easy to Deploy:** Solutions must be simple to deploy and integrate, regardless of the business's existing network or system architecture.

With this in mind, Zumigo architected its solution to provide a multi-layered verification and authentication framework that utilizes real-time digital risk signals, including account and device intelligence, payment, email, geo location, and others to successfully implement this essential identity-first model. Businesses can expect to:

1. Reduce and prevent identity-related risks and loss from identity fraud (including account takeover attacks, stolen credentials, and synthetic IDs), and identity access-derived network attacks (including phishing and social engineering).
2. Improve security posture to better manage risk without unnecessary consumer/user friction.
3. Reduce consumer abandonment of web and app services and improve their digital experience with the business.

Zumigo

Consideration 1: Strong and Frictionless Authentication

The fundamental challenge to Identity-First Security is that traditional authentication (relying on passwords and one-time passcodes, or OTPs) is inherently weak and violates the "frictionless" mandate.

Zumigo addresses this with a suite of passwordless authentication solutions that are seamless and non-invasive to the consumer experience:

- **Mobile Network Authentication:** This is a passive, background check that verifies device possession and ownership using direct Mobile Network Operator (MNO) signals and can be achieved via two technologies: Silent Network Authentication (SNA) or SIM-Based Authentication (SBA). Both will confirm that the user is who they claim to be without slowing them down.
- **FIDO-Based Passkeys:** Zumigo facilitates the secure binding of cryptographic passkeys to the user's mobile device (leveraging the secure enclave), eliminating password vulnerability entirely while providing the strongest possible security assurance.
- **Trust Transfer:** Zumigo enables the ability to securely transfer verified identity trust from a mobile device to a desktop or tablet session via QR code, by authenticating the ownership using Mobile Network Authentication or the installed passkey. This approach seamlessly maintains the Zero Trust chain across all user devices.
- **Social Log-in:** For convenience, Zumigo enables secure log-in using existing social credentials.

Consideration 2: Continuous Real-Time Authoritative Information

For an Identity-First strategy to work, security must be continuous and contextual based on real-time, authoritative sources, not just a one-time event. Simple checks fail to catch sophisticated threats like SIM Swap and Synthetic Identity Fraud.

Zumigo addresses this by providing risk scoring based on layered verification information that are not based on outdated predictive models:

- **MNO Real-Time Signals:** Zumigo gathers authoritative, deterministic data from MNOs, including SIM Swap alerts, number Porting status, and Deactivation status. These signals provide immediate, unforgeable context for risk assessment.
- **Data Fusion:** Zumigo aggregates MNO data with crucial intelligence on device fingerprinting, behavioral biometrics, email validity, geo location, IP listing, and payment information. This data fusion generates a single, holistic risk score that reveals threats hidden in siloed systems.
- **Contextual Risk Scores:** Real-time, multi-layered scoring is aggregated to determine the risk of various fraud threats, including Account Takeovers (ATOs) or Synthetic ID, allowing the enterprise to manage risk proactively.

Consideration 3: Comprehensive data and risk signals

No single piece of information is sufficient to confirm digital identity or prevent modern fraud. Fraudsters are adept at compromising one or two data elements (like a password and an email address), but they cannot simultaneously falsify or control every signal across the digital, physical, and network layers. Zumigo brings together a comprehensive suite of data and signals to assess identity risk across the entire journey:

Data Element	Why it is Crucial for Verification/Authentication	Examples of Fraud Risks Mitigated
Mobile Number and Account Information	Verifies that the user physically possesses the device *and* that their claimed name and identity are linked to the authoritative mobile carrier account record.	**SIM-Swap Fraud:** Detects when a number has recently been moved to a new SIM card. **Account Takeover (ATO):** Confirms possession before sending secure codes or granting access.
Device Fingerprinting and Biometrics	Fingerprinting creates a unique ID for the device accessing the system, detecting shared access or spoofing. Biometrics like liveness check confirms the physical presence of a *human* user.	**Bot Attacks:** Identifies automated scripts and emulators (device fingerprinting). **Deepfakes and Spoofing:** Identifies when criminals use stolen photos or videos to fool verification systems (biometrics).
PII Match and Verification	Confirms that the provided name, date of birth (DOB), social security number (SSN), address and other PII match existing, trusted records (e.g., credit bureaus).	**Data Falsification:** Detects inconsistencies on application forms. **Identity Theft:** Verifies that the PII is real and associated with the claimed individual.
Email Validity and Verification	Assesses the email address's domain reputation, creation date (tenure), and association with past fraud incidents.	**Phishing and Spam:** Identifies throwaway or disposable emails often used for fraud. **Account Takeover:** Determines if the email is a high-risk vector for password resets.
Payment and Banking	Verifies that the bank account or payment card details belong to the identity presented during a transaction. This is often done via micro-deposits or matching cardholder name and billing address.	**Payment Fraud:** Prevents the use of stolen credit cards or banking credentials for immediate transactions. **Money Laundering:** Confirms the flow of funds originates from a verified, known financial instrument.
Government-Issued Documents	Provides legal assurance by validating the identity against a primary, government-issued document (e.g., driver's license) and verifying with a selfie/liveness check.	**Synthetic Identity:** Prevents fraudsters from creating identities by fabricating documentation. **Impersonation:** Ensures the user's face matches the photo on the official ID.
Network Activity	Analyzes anomalies in access patterns across a network of businesses as well as for an individual business.	**Credential Stuffing:** Detects abnormal, high-velocity log-in attempts across accounts, a signal that indicates that the attempts are originating from fraud rings.

Data Element	Why it is Crucial for Verification/Authentication	Examples of Fraud Risks Mitigated
IP-Based Geolocation	Determines the physical location of the device/user. Crucial for compliance (e.g., gambling, international sales) and for detecting suspicious transactions.	**Fraudulent Transactions:** Flags activities originating from a location that does not match what's associated with the payment instrument **Suspicious Logins:** Detects impossible travel (login from New York followed by a login from London five minutes later).

Consideration 4: Ease of Deployment and Accessibility

To achieve widespread adoption of seamless verification workflows, the solution must be easy for business units to deploy and manage without extensive IT support. Zumigo ensures this accessibility through flexible deployment options:

- Businesses can deploy via API integration for complex, custom scenarios.
- Available via major e-commerce platforms for easy downloads and deployment.
- The Zumigo low-code/no-code platform allows fraud and compliance teams to visually build, test, and deploy complex, risk-tiered workflows without relying on custom coding, drastically improving agility and reducing the cost of deployment.

Summary: Make identity your strongest defense

The identity-centric model is mandatory for modern security. By eliminating reliance on compromised passwords and fragmented identity checks, Zumigo provides the critical intelligence layer necessary for the enterprise to manage risk effectively. By making verified and authenticated identity the core defense, businesses realize significant benefits:

- **Reduced Identity-Related Risks and Loss:** Proactive defense against ATOs, synthetic identities, and phishing attacks.
- **Improved Security Posture:** A continuously authenticated identity perimeter that better manages risk without introducing unnecessary consumer friction.
- **Reduced Consumer Abandonment:** Maximizing conversion rates through the adoption of seamless, passwordless user experiences.

To secure their digital systems in the mobile and cloud environment, enterprises must recognize that verified identity is the new, strongest perimeter defense.

About Zumigo

Zumigo powers digital identity verification in the world's largest enterprises to protect transactions, accounts and trust, using real-time intelligence across mobile, email, device, financial, account, and other information sources. Its modernized, multi-layer approach fortifies the identity perimeter against today's complex fraud and promises a streamlined consumer journey from onboarding to transactions. Learn more: www.zumigo.com.