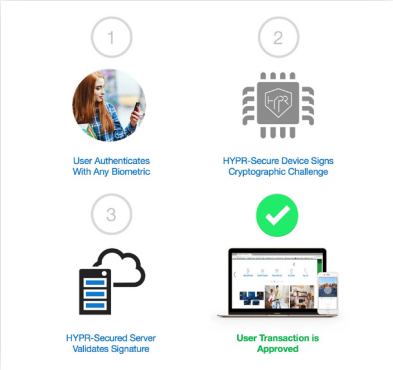
BIOMETRICS SECURITY MANAGEMENT

The co-mingling of personal and professional (corporate) applications has increased the risk and likelihood of passwords being lost, forgotten, stolen, and exposed due to brute force attacks. As a result, biometric technologies such as facial, voice, fingerprint, and palm recognition continue to emerge as securely viable, operationally efficient, and cost-effective solutions.

HYPR-Secure Biometric FIDO Authentication



- Utilize Biometrics for Access and Authentication
- Improve ROI by eliminating Passwords and Shared Secrets
- Reduce the likelihood of a Data Breach by protecting the identities

Use Cases and Challenges	Outcomes and Benefits
Costs are becoming increasingly expensive with password resets. On average this ranges from $35-50 per password reset.	Biometrics reduces costs and provides a better ROI by eliminating the need for password resets.
Complexities and constraints associated with limited personnel due to budget and finding proper skill sets for managing and monitoring password vaults.	Password-less Management is a secure, centralized repository with automated responses for self service password resets through the use of Biometrics.
Silos have been created with Identity and Password Management technologies due to Cloud and SaaS sprawl. This has led to a lack of visibility and monitoring for potential threats to critical assets and intellectual property.	Implementation and ongoing administration becomes seamless and fully integrated with existing Identity technologies such as MFA and PAM. Whereas, monitoring for identity and credential theft becomes instantaneously detected, quarantined, and remediated.
Password-less management seems to be a utopian idea with little to no security. This makes it challenging to convince and prove the security and operational effectiveness.	Through the use of Biometrics, cryptographic keys are generated upon user initiation. These keys are associated with the endpoint and user identity. A service lookup is performed for either access validated or denied.

BIOMETRICS SECURITY MANAGEMENT

What We Do

With the ever evolving migration to the cloud, organizations are reconsidering how they manage passwords, password resets, enhance end user experience, and protect themselves against social engineering and brute force attacks. Since there are a multitude of performance and security variables, BNS UEP provides organizations an architectural blueprint and engineering services for Biometrics.

How We Do It

Our mantra is to simplify and migrate from the often difficult and complex password management lifecycle (monitor, detect, respond) to passwordless management. This is accomplished by utilizing Biometrics and by baselining and modeling a subset of individual users, user groups, and endpoints. Eventually, the rollout and onboarding process accounts and encompasses for all identities and endpoints.

Why It Matters

Biometrics and password-less management reduces the costs and security complexities and challenges associated with managing and administering password resets, privileged access, end user experience, operational efficiencies, and securing critical assets. According to the 2019 Verizon Cyber-Security Report, Privileged Misuse and Web Application attacks accounts for the Top 3 Data Breach Patterns in every industry. Therefore, by utilizing Bio-Metrics with MFA and an Identity Provider this will reduce your attack surface and the likelihood of losing critical assets, user identities, credit card information, patient healthcare records, and even worse the inability to pay employees and staff due to credentials and payment systems being compromised.