HYPR | The Cyber Hut

A JOURNEY TO ZERO TRUST WITH ZERO PASSWORDS

Authored by: Simon Moffatt, The Cyber Hut

Contents

1 Why Zero Trust Needs Zero Passwords

From Boundary-Based Access... 03
... To Identity-Based Access 03
Why No Passwords 04

2 Identify and Protect User Interactions Passwords

Workstation Login 04
VPN and Remote Access 05
Single Sign On 05

3 Don't Forget Administrators

Policy Design 06

4 Extend, Expand and Future Proof

Support IT Operations 07
Migrate From Legacy MFA 07
Centralize Control and Visibility 07

5 Deliver Continuous Security

Support Post-Authentication Verification 08

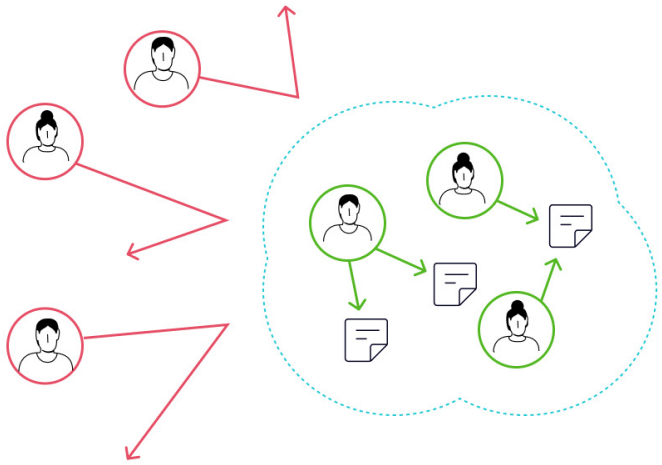
In Summary 09

1 Why Zero Trust Needs Zero Passwords

From Boundary-Based Access...

The modern enterprise is a complex mix of both business agility and technological stagnation, heavily reliant on complex supply chains, data integrations and application meshes.

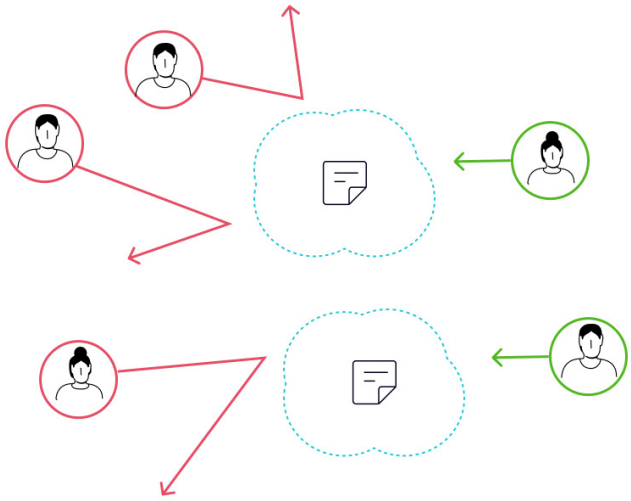
Many identity and cybersecurity platforms often have long lifespans — which on one hand can generate economies of scale with regards to integration and repeatability, yet can result in rigidity and a lack of modular adaptability in the face of emerging threats and changing business patterns.



...To Identity-Based Access

Zero Trust is a changing business security architecture allowing organizations to deliver services faster and more securely by placing less emphasis on the location of people, data and services and **more emphasis on identity and context**.

Organizations can do this by placing less trust on location — of people, their devices and the data they wish to access — and more emphasis on identity-based security, especially the surrounding context.



Why No Passwords

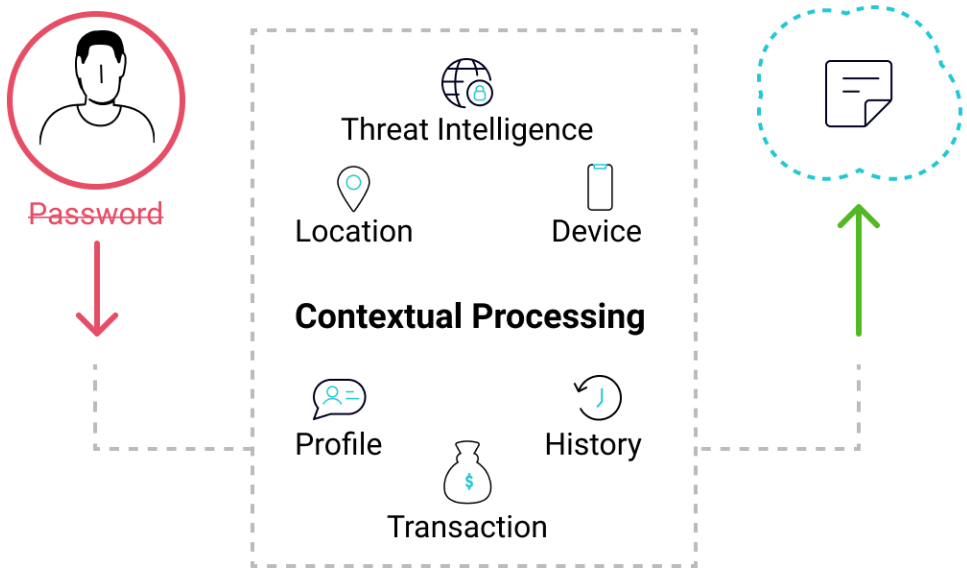
With an identity-centric model of security, there is greater emphasis on the user interactions required for verification.

The number of authentication and authorization triggers **increase**.

The focus on identity also introduces contextual analysis – where non-identity data can help evaluate the level of risk associated with the user and the transaction they are trying to perform.

User verification relying solely on the password not only amplifies the risk associated with weak password security, but places an unnecessary burden on usability.

We are moving to an environment of continual security and passwords will inhibit this modern user journey.



Why Now?

- Evolving Threats
- Distributed Working Patterns
- API Economy
- Increased Business Agility
- Complex Supply Chains

2 Identify and Protect User Interactions

In order to secure the distributed and porous nature of the modern enterprise, we need to undergo a process of mapping identity assets and entry points. Where are identities and passwords being used and why?

Workstation Login

The workstation will be the main entry point into the corporate network – whether it is located within the confines of the controlled network or not. The reliance on passwords as the main authentication approach, while familiar, does not provide the necessary security or usability requirements the modern enterprise will need.

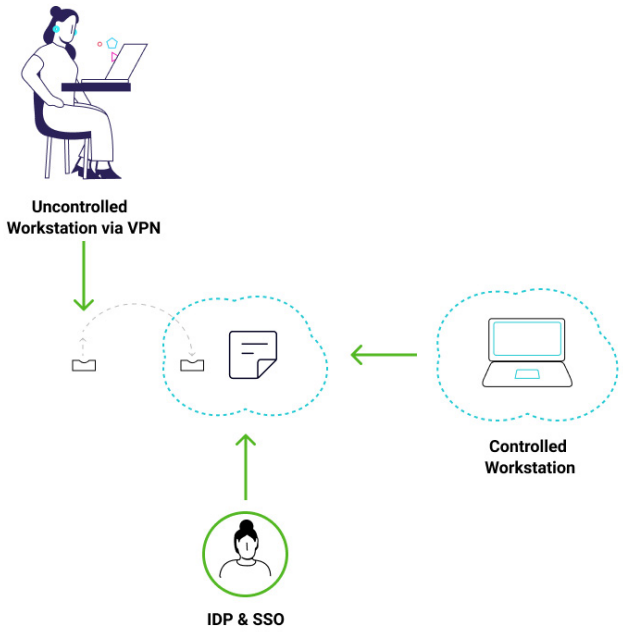
The workstation has a high frequency usage pattern so the migration to passwordless needs to provide simple enrollment, self-explanatory usage and flexible recovery.

- Expect QR-code based workstation login
- Consider access requests when the workstation is offline
- Support self-sufficiency for enrollment and recovery

VPN and Remote Access

While many organizations are redesigning their network infrastructure to be less reliant on virtual private networks (VPN), they still provide a popular means for home and distributed worker access to centralized and controlled resources.

As the enforcement point of identity and device authentication moves from being centralized to being more distributed, the addition of passwordless MFA to these remote entry points is key. The VPN client may well be located on an uncontrolled device, perhaps a personally owned laptop. As the control point is now the client and not the device, increased security via MFA becomes essential.



Single Sign On

The use of identity providers and centralized single sign-on services (SSO) allows organizations to expand access control policies and authentication baselines to a range of integrated applications – from cloud SaaS, legacy on-premises or modern microservices-based systems.

The goal is to broaden application coverage of passwordless MFA by integrating with existing IDP infrastructures. This should likely be via a decoupled and standards-based architecture, allowing the SSO platform to focus on application integration and session management, without the concern of device and user coverage requirements of passwordless MFA.

The identity verification aspect moves from being tied to applications, to being managed by the IDP but implemented by the passwordless infrastructure.

3 Don't Forget Administrators

The bulk of passwordless adoption will be for typical employees in the workplace or for consumers and customers in the external digital transformation environment. However, Zero Trust architectures place a greater emphasis on access control policy design.

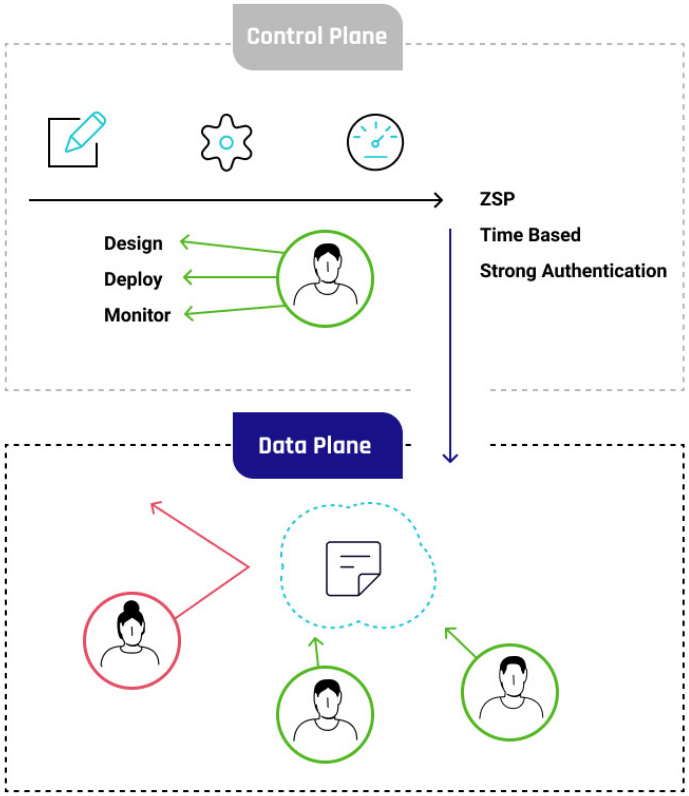
Policy Design

This **policy-lead architecture** will see the separation of the "data plane" where end users access resources and the "control plane" where administrators create policies and monitor the underlying access control infrastructure.

The protection of this control plane should take inspiration from the standard privileged access management use cases such as **zero standing privileges, time-bound access** and the use of **strong authentication** with **continual monitoring**.

These PAM principles along with basic hygiene regarding Zero Trust system management helps to reduce impact from "keys to the castle" attacks.

The design, deployment and monitoring of Zero Trust access control policies should be protected by strong authentication – an authentication mechanism that will be triggered frequently for identity verification, policy change, rollout and other high risk events associated with the deployment of **enforcement policies** to **endpoints, agents, gateways** and **protected applications**.



- ZTNA often leverages policy-based decisioning for identity authentication, device authentication and transaction processing
- Strong driver to integrate the passwordless verification process into those management actions

4 Extend, Expand and Future Proof

The success of Zero Trust and passwordless adoption will come from a long tale of integration and sustained success supported by quantitive and qualitive metrics.

Support IT Operations

IT operations – especially when focused upon employee and workspace infrastructure management – are under constant review with regards to efficiency, productivity and cost reduction.

Any new security technology adoption needs to be able to support and promote one of those three key pillars of operational efficiency.

- Reduce call center activity from external users
- Reduce help desk password reset costs from staff
- Increase self sufficiency by end users as they handle enrollment, additions and device migrations in a more simple manner

Migrate From Legacy MFA

Many enterprises will likely have existing multi-factor authentication (MFA) components in place. They are likely to be used by pockets of individuals, for specific applications or siloed use cases. The rise of passwordless MFA is driven by a ubiquitous need and much broader and more consistent rollout and adoption plan.

Existing MFA capabilities will need to be migrated from, in a staged way that provides self-service enrollment and migration as well as zero touch and low-code changes for integrated IDPs and downstream applications.

- Collapse existing infrastructure as it pertains to existing MFA solutions
- Identify and document use of **SMS OTP**, **email OTP, hardware tokens** and **fobs** for **OTP** generation

Centralize Control and Visibility

The use of ubiquitous passwordless MFA for employee and consumer login, administrator MFA and high risk event processing, places greater emphasis on having not only decoupled integration against identity providers and application enforcement systems, but also a centralized control and visibility plane.

- Provide **central management** to integrate passwordless in a distributed set of systems
- Leverage **logs, analytics** and **metrics** to validate rollout success and increased security analysis (SIEM)

5 Deliver Continuous Security

Zero Trust and an identity-centric security model, amplifies the frequency of identity verification and authentication triggers.

Authentication becomes the pinch point not only for directory-based authentication for employees, but also for high-risk event processing in the consumer space, step-up authentication for partners and federated use cases, and distributed data and service access for the workplace.

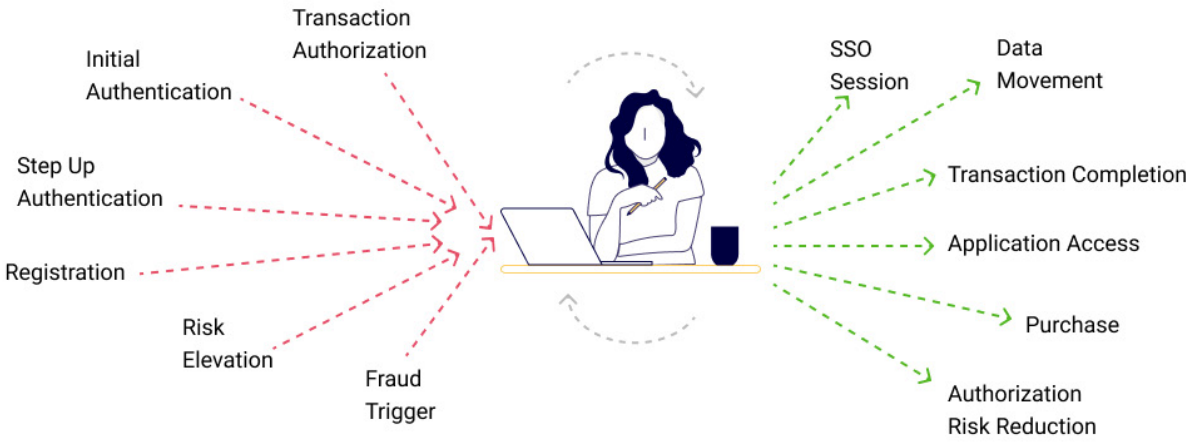
The choice of passwordless MFA therefore, needs to contend with integration requirements that emerge from a range of different sources, many of which are post authentication in nature. The ability to expose passwordless services via centralized APIs or with standards-based integration, provides a foundation for mass adoption into a range of systems with high risk processing requirements.

- Leverage API access to passwordless triggering
- Use standards such as OIDC/OAuth2 and SAML for increased authentication coverage

Support Post-Authentication Verification

Many authentication modals can now be accessed from a post-authentication event, such as application access, making a purchase or performing a high risk transaction.

- Consider exposing authentication functionality to generic event triggers



In Summary

Passwordless MFA is a key control for 2022 and beyond. The rise of distributed working, emerging threats and digital transformation is driving a need for Zero Trust identity-centric security patterns that place greater emphasis on secure, yet usable authentication experiences.

The migration from legacy and siloed MFA into a decoupled passwordless approach, allows a future based on ubiquitous continual security that can be applied to a host of new identity verification use cases.

About the Author

Simon Moffatt is Founder and Analyst at The Cyber Hut. Simon provides the overall strategy and content management, analyzing unique positions with many different lenses. He is a published author and contributor to identity and security standards at the likes of NIST and the IETF. He has a 20+ year career working within the identity and access management and cybersecurity sectors – for vendors, system integrators and within industry. Simon is a CISSP, CCSP, CEH and CISA, a Member of the British Computer Society and a Fellow of the Chartered Institute of Information Security.

About The Cyber Hut

The Cyber Hut is a leading boutique industry analyst firm focused on identity, access and cyber security technology.

Web: www.thecyberhut.com
LinkedIn: www.linkedin.com/company/tch-research
Twitter: www.twitter.com/thecyberhut

THE PASSWORDLESS COMPANY

Contact: 1-866-GET-HYPR [US]

Learn more: www.hypr.com

HYPR reimagines multi-factor authentication to protect workforce and customer identities at the highest level of assurance. With HYPR True Passwordless™ MFA, you can change the economics of attack, improve your security posture, and enhance digital engagement with every login experience.