Tech Brief

HYPR Alignment With the MITRE ATT&CK Framework

Background on MITRE ATT&CK

In 2013, MITRE — a not-for-profit corporation established to advance national security and act as an independent adviser for the public interest — released a framework outlining the stages and tactics associated with cyberattacks. Adversarial Tactics, Techniques, and Common Knowledge, or MITRE ATT&CK as it is more commonly referred to, consists of fourteen categories with techniques (and sub-techniques) under each. Over the years, ATT&CK has grown into a comprehensive knowledge base, which is open to anyone and MITRE actively encourages contributions and feedback. Its key goal is to bring the security community together to help identify, address and thwart attack methods before they are used in the wild.

Below is a representation of the fourteen categories and subcategory techniques that comprise MITRE ATT&CK:

The MITRE ATT&CK Framework[1]

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	42 techniques	16 techniques	30 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques

[1] https://attack.mitre.org/#

The Role of Authentication in ATT&CK

The frequency and severity of threats that leverage the authentication attack vector make authentication methodologies a continued area of concern for the security community. The bedrock of the most common authentication methods involves a combination of passwords and/or shared secrets. As time and attack methodologies progress, the industry continues to add layers of security on top of the password including hard tokens, one-time passwords and more. Nevertheless, the layers of security have not kept pace to arrest the evolving dynamic attack surface and methodologies.

MITRE ATT&CK specifies many of the techniques that hackers obtain and employ using compromised credentials to successfully launch attacks. They all come back to the password.

How You Can Combat Authentication-Based Attacks

HYPR True Passwordless™ MFA completely eliminates all passwords and shared secrets from the authentication process. This means that many of the attack methods associated with credential-based attacks are no longer viable.

Below, you'll find a reference table which highlights the attack categories and techniques called out in the MITRE ATT&CK framework and how HYPR helps you solve for them.

Initial Access

Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

Initial Access				
Technique ID	**Sub-Technique ID**	**Name**	**Description**	**How HYPR Protects Against This ATT&CK Technique**
T1133		External Remote Services	Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as Windows Remote Management and VNC can also be used externally.	HYPR supports passwordless MFA for RDP, VPN and VDI. This means that phishing-resistant MFA can be used for external facing remote services. This is specifically relevant for remote workforces and distributed environments.

Initial Access				
Technique ID	**Sub-Technique ID**	**Name**	**Description**	**How HYPR Protects Against This ATT&CK Technique**
T1566		Phishing	Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.	HYPR's passwordless MFA is phishing resistant by design. There are no passwords or shared secrets used on the front end or on the back end. Phishing-resistant MFA is not only recommended as part of MITRE ATT&CK, but is also recommended by CISA, OMB and other regulatory agencies.
	0.003	Spearphishing via Service	Adversaries may send spearphishing messages via third-party services in an attempt to gain access to victim systems. Spearphishing via service is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of third-party services rather than directly via enterprise email channels.	HYPR's passwordless coverage is from the desktop to the cloud which includes third party services as well as SSO providers.
T1199		Trusted Relationship	Adversaries may breach or otherwise leverage organizations who have access to intended victims. Access through trusted third party relationship exploits an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a network.	The HYPR solution provides passwordless MFA which includes role-based access control. This means that once authenticated, users can gain access in accordance with their unique role. Gaining the right access rather than giving full access to everything aligns with the Zero Trust framework.
T1078		Valid Accounts	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access and remote desktop. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.	It is common for valid accounts, whether they are remote access, VPNs or even applications to be used in an attack by way of valid but stolen or compromised user credentials. HYPR eliminates the password and shared secrets and uses passwordless MFA. There is nothing to steal or compromise thus making the need to guard credentials irrelevant. HYPR can be used in conjunction with other security products in order to provide an additional feed for a more comprehensive view of stealthy and sophisticated attacks that are architected to evade point security products.
	0.001	Default Accounts	Adversaries may obtain and abuse credentials of a default account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Default accounts are those that are built-into an OS, such as the Guest or Administrator accounts on Windows systems. Default accounts also include default factory/provider set accounts on other types of systems, software, or devices, including the root user account in AWS and the default service account in Kubernetes.	Same as previous. Furthermore, HYPR works in conjunction with AWS as well as SSO operators and Identity platforms.
	0.002	Domain Accounts	Adversaries may obtain and abuse credentials of a domain account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Domain accounts are those managed by Active Directory Domain Services where access and permissions are configured across systems and services that are part of that domain. Domain accounts can cover users, administrators, and services.	HYPR uses passwordless multi-factor authentication to secure domain accounts and as such, there are no credentials to steal. HYPR works in conjunction with AD, LDAP and standalone accounts to provide the same level of security and usability. HYPR can also secure non-domain joined accounts as necessary.

Initial Access				
Technique ID	**Sub-Technique ID**	**Name**	**Description**	**How HYPR Protects Against This ATT&CK Technique**
	0.004	Cloud Accounts	Adversaries may obtain and abuse credentials of a cloud account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Cloud accounts are those created and configured by an organization for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application. In some cases, cloud accounts may be federated with traditional identity management systems, such as Windows Active Directory.	HYPR secures cloud accounts by using passwordless multifactor authentication, and as such, there are no credentials to steal. HYPR works in conjunction with AD, LDAP and standalone accounts to provide the same level of security and usability.

Credential Access

Credential access represents techniques that can be used by adversaries to obtain access to or control over passwords, tokens, cryptographic keys, or other values that could be used by an adversary to gain unauthorized access to resources. Credential access allows the adversary to assume the identity of an account, with all of that account's permissions on the system and network, and makes it harder for defenders to detect the adversary. With sufficient access within a network, an adversary can create accounts for later use within the environment.

Credential Access				
Technique ID	**Sub-Technique ID**	**Name**	**Description**	**How HYPR Protects Against This ATT&CK Technique**
T1557		Adversary-in-the-Middle	Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation. By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions.	HYPR's passwordless MFA eliminates AiTM when FIDO2 protocols are being used (also referred to as MitM). The elimination of one-time passwords, and push notification ensures that there is nothing to steal via this tactic. Private keys are always stored in the secure enclave or TPM of the smartphone or like device, and users must initiate any authentication request thus eliminating MitM and push fatigue (MFA prompt bombing) types of attacks.
T1110		Brute Force	Adversaries may use brute-force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes.	Brute-force attacks are typically used where the hacker has a library of passwords that they can try until they hit upon one that grants them access. Since there are no passwords or shared secrets anywhere in HYPR's authentication process, brute force attacks are eliminated whether accessing the endpoint device such as the desktop, all the way to the cloud.

Credential Access				
Technique ID	**Sub-Technique ID**	**Name**	**Description**	**How HYPR Protects Against This ATT&CK Technique**
	0.001	Password Guessing	Adversaries with no prior knowledge of legitimate credentials within the system or environment may guess passwords to attempt access to accounts. Without knowledge of the password for an account, an adversary may opt to systematically guess the password using a repetitive or iterative mechanism. An adversary may guess login credentials without prior knowledge of system or environment passwords during an operation by using a list of common passwords. Password guessing may or may not take into account the target's policies on password complexity or use policies that may lock accounts out after a number of failed attempts.	With HYPR Passwordless MFA, all passwords and shared secrets are eliminated, making password guessing impossible.
	0.002	Password Cracking	Adversaries may use password cracking to attempt to recover usable credentials, such as plaintext passwords, when credential material such as password hashes are obtained. OS Credential Dumping can be used to obtain password hashes, this may only get an adversary so far when Pass the Hash is not an option. Further, adversaries may leverage Data from Configuration Repository in order to obtain hashed credentials for network devices.	With HYPR Passwordless MFA, all passwords and shared secrets are eliminated, making password cracking impossible.
	0.003	Password Spraying	Adversaries may use a single or small list of commonly used passwords against many different accounts to attempt to acquire valid account credentials. Password spraying uses one password (e.g. 'Password01'), or a small list of commonly used passwords, that may match the complexity policy of the domain. Logins are attempted with that password against many different accounts on a network to avoid account lockouts that would normally occur when brute forcing a single account with many passwords.	With HYPR Passwordless MFA, all passwords and shared secrets are eliminated, making password spraying impossible.
	0.004	Credential Stuffing	Adversaries may use credentials obtained from breach dumps of unrelated accounts to gain access to target accounts through credential overlap. Occasionally, large numbers of username and password pairs are dumped online when a website or service is compromised and the user account credentials accessed. The information may be useful to an adversary attempting to compromise accounts by taking advantage of the tendency for users to use the same passwords across personal and business accounts.	Similar to brute-force attacks, since there are no passwords or shared secrets anywhere in HYPR's authentication process, credential stuffing attacks are eliminated whether accessing the endpoint device such as the desktop or remote access point, SSOs, native apps or cloud apps.
T1555		Credentials from Password Stores	Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications that store passwords to make it easier for users to manage and maintain. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.	HYPR eliminates all password stores, thus user credentials and authentication cannot be achieved via this method.

Credential Access

Technique ID	Sub-Technique ID	Name	Description	How HYPR Protects Against This ATT&CK Technique
	0.001	Keychain	Adversaries may acquire credentials from Keychain. Keychain (or Keychain Services) is the macOS credential management system that stores account names, passwords, private keys, certificates, sensitive application data, payment data, and secure notes. There are three types of Keychains: Login Keychain, System Keychain, and Local Items (iCloud) Keychain. The default Keychain is the Login Keychain, which stores user passwords and information. The System Keychain stores items accessed by the operating system, such as items shared among users on a host. The Local Items (iCloud) Keychain is used for items synced with Apple's iCloud service.	HYPR operates on a variety of platforms including Windows, iOS and Linux. By using HYPR's passwordless MFA, Keychain is no longer a vector for acquiring credentials in the Apple environment.
	0.002	Securityd Memory	An adversary may obtain root access (allowing them to read securityd's memory), then they can scan through memory to find the correct sequence of keys in relatively few tries to decrypt the user's logon keychain. This provides the adversary with all the plaintext passwords for users, WiFi, mail, browsers, certificates, secure notes, etc.	HYPR eliminates all password stores, thus user credentials and authentication is not stored in securityd memory.
	0.003	Credentials from Web Browsers	Adversaries may acquire credentials from web browsers by reading files specific to the target browser. Web browsers commonly save credentials such as website usernames and passwords so that they do not need to be entered manually in the future. Web browsers typically store the credentials in an encrypted format within a credential store; however, methods exist to extract plaintext credentials from web browsers.	Because HYPR's coverage is from the desktop to the cloud, the same level of security is applied from the time the user logs in to the endpoint device. As such, credential acquisition in the browser or on the device whether encrypted or decrypted is impossible.
	0.004	Windows Credential Manager	Adversaries may acquire credentials from the Windows Credential Manager. The Credential Manager stores credentials for signing into websites, applications, and/or devices that request authentication through NTLM or Kerberos in Credential Lockers (previously known as Windows Vaults).	Because HYPR's coverage is from the desktop to the cloud, Credential Manager (Windows Vaults) is not needed due to the retirement of passwords and shared secrets. For the edge cases where it is still used for certain legacy applications, securing the device where Credential Manager is ordinarily housed is secured with passwordless MFA.
	0.005	Password Managers	Adversaries may acquire user credentials from third-party password managers. Password managers are applications designed to store user credentials, normally in an encrypted database. Credentials are typically accessible after a user provides a master password that unlocks the database. After the database is unlocked, these credentials may be copied to memory. These databases can be stored as files on disk.	Same as previous.
T1187		Forced Authentication	Adversaries may gather credential material by invoking or forcing a user to automatically provide authentication information through a mechanism in which they can intercept.	With HYPR, only the user self invokes authentication. A forced authentication that is initiated automatically from an unknown source is eliminated.

Credential Access

Technique ID	Sub-Technique ID	Name	Description	How HYPR Protects Against This ATT&CK Technique
T1606		Forge Web Credentials	Adversaries may forge credential materials that can be used to gain access to web applications or Internet services. Web applications and services (hosted in cloud SaaS environments or on-premise servers) often use session cookies, tokens, or other materials to authenticate and authorize user access.	HYPR's passwordless MFA protects from the desktop to the cloud. This includes eliminating passwords and shared secrets relating to authentication to web/cloud-based applications and services.
T1056		Input Capture	Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. Credential API Hooking) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. Web Portal Capture).	Since HYPR's passwordless MFA eliminates the need to input passwords or shared secrets, there is no ability to harvest any inputs including credentials entered via web portal capture, password filtering or pluggable authentication modules.
T1111		Multi-Factor Authentication Interception	Adversaries may target multi-factor authentication (MFA) mechanisms, (I.e., smart cards, token generators, etc.) to gain access to credentials that can be used to access systems, services, and network resources. Use of MFA is recommended and provides a higher level of security than user names and passwords alone, but organizations should be aware of techniques that could be used to intercept and bypass these security mechanisms.	While traditional multi-factor authentication methods are better than just using a password, there are documented instances where the hacker has bypassed MFA controls and has harvested credentials in order to gain authentication. HYPR eliminates these hackable layers of authentication, such as a token generators, smart cards, etc., from the authentication process, replacing them with phishing and bypass-resistant passwordless authentication.
T1621		Multi-Factor Authentication Request Generation	Adversaries may attempt to bypass multi-factor authentication (MFA) mechanisms and gain access to accounts by generating MFA requests sent to users.	Any form of password or credentials can be harvested...even one time passwords. HYPR takes MFA one step further by eliminating all forms of passwords and shared secrets, rendering MFA bypass attacks which include phishing, push fatigue and other forms of bypass tactics ineffective and obsolete. Further, with HYPR, any request for authentication must be invoked by the user, thus eliminating MFA prompt bombing.
T1552		Unsecured Credentials	Adversaries may search compromised systems to find and obtain insecurely stored credentials. These credentials can be stored and/or misplaced in many locations on a system, including plaintext files (e.g. Bash History), operating system or application-specific repositories (e.g. Credentials in Registry), or other specialized files/artifacts (e.g. Private Keys).	HYPR eliminates passwords, making unsecured credentials, credentials in files or in registries a thing of the past. Access is tied to the individual rather than a string of characters or the device. This changes the economics of an attack since there is no repository of credentials to steal and use.
	0.004	Private Keys	Adversaries may search for private key certificate files on compromised systems for insecurely stored credentials. Private cryptographic keys and certificates are used for authentication, encryption/decryption, and digital signatures. Common key and certificate file extensions include: .key, .pgp, .gpg, .ppk., .p12, .pem, .pfx, .cer, .p7b, .asc.	HYPR uses asymmetric key encryption with the private key securely stored in the TPM or secure enclave of the device. Only the public key is revealed or granted to services. This changes the economics of an attack since the highest security portion of each individual user's device must be cracked to get the private keys.

Credential Access				
Technique ID	**Sub-Technique ID**	**Name**	**Description**	**How HYPR Protects Against This ATT&CK Technique**
	0.006	Group Policy Preferences	Adversaries may attempt to find unsecured credentials in Group Policy Preferences (GPP). GPP are tools that allow administrators to create domain policies with embedded credentials. These policies allow administrators to set local accounts.	HYPR works in conjunction with AD, LDAP for group policy enforcement. It can also work without either of the aforementioned for populations that may be non-domain based users. RBAC is built into the product to ensure each individual has the correct policy and access to the relevant group. Changes for onboarding, role reassignment or termination can be easily accomplished along with a complete and digitally-signed audit trail.

About HYPR

HYPR creates trust in the identity lifecycle. HYPR's Identity Assurance solution provides the strongest end-to-end identity security, combining modern passwordless authentication with adaptive risk mitigation, automated identity verification and a simple, intuitive user experience. With a third-party validated ROI of 324%, HYPR easily integrates with existing identity and security tools and can be rapidly deployed at scale in the most complex environments.