SOLUTION BRIEF

HYPR

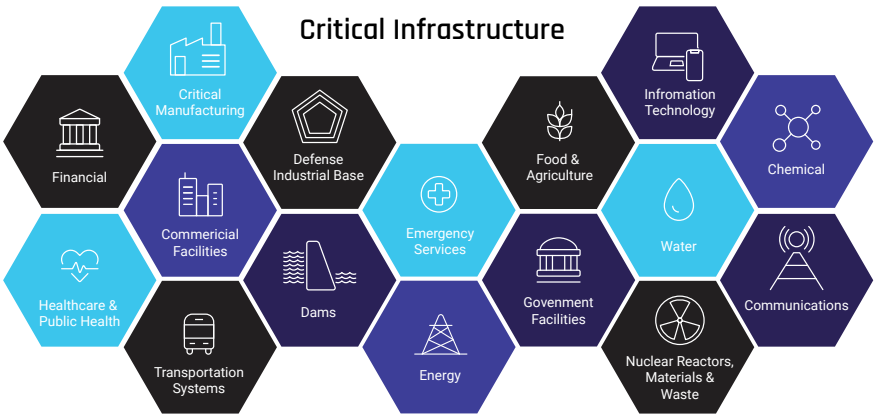
Passwordless MFA for Critical Infrastructure

Reduce risk and meet regulatory requirements with phishing-resistant, passwordless multi-factor authentication from HYPR

HYPR Key Benefits

- Deploy phishing-resistant MFA everywhere, from the desktop to cloud applications
- Protect against phishing, MitM and other credential attacks
- Improve user experience
- Achieve regulatory compliance
- Reduce IT and help desk costs
- Secure remote access
- Integrate quickly with existing systems, IdPs and applications

In today's digital world, critical infrastructure is the backbone of the economy, and its security and safety are vital for the nation's well-being. The Cybersecurity & Infrastructure Security Agency (CISA) defines critical infrastructure as sixteen distinct operating sectors. Essentially, they are industries that modern society cannot live without.



These systems are grounded in operational technology (OT) infrastructure. While in the past IT and OT systems were separated by an air gap, both intentional and unintentional convergence has occurred, now making both susceptible to attack.

Critical Infrastructure Authentication Risks

Critical infrastructure is exposed to various types of authentication security threats that target the password. Common attack method include:

- Phishing: Trick users into revealing their login credentials by posing as a legitimate source.
- Brute force: Crack passwords by trying every possible combination until they find the correct one.
- Man-in-the-middle attacks: Intercept communications between two parties to steal authentication credentials.
- Social engineering: Leverage psychological manipulation to gain access to critical systems.
- Malware: Attackers install malware on systems to steal login credentials or bypass authentication.

Recent Password-Based Security Breaches on Critical Infrastructure

- A 2021 attack against the Oldsmar, Floridas water treatment plant raised the level of sodium hydroxide to potentially fatal levels. It was determined that this breach was due to leaked credentials and an out of date operating system.
- Also in 2021, a password-based breach into the "third network" of the Colonial Pipeline caused the pipeline, which supplies more than half of the petroleumto the northeastern United States, to be completely shut down.
- From 2018-2020, the APT28 hacking group carried out a broad scale campaign against US targets, including the energy sector. The primary methods of attack were through email and VPN. APT28 has a history of hacking critical infrastructure. Sandworm planted malware on the networks of US electric utilities in 2014, then carried out the first-ever cyberattack-induced blackouts in Ukraine in 2015 and 2016.

The 2023 IBM Security Threat Intelligence Index found brute-force attacks and weak or default passwords to be among the most common OT threat alerts, with spear phishing the most frequent initial access vector for OT breaches.

The Authentication Inflection Point

Traditional password-based security, including multi-factor authentication, has become more prone to attack. One-time passwords and other phishable MFA technologies cannot combat modern cybersecurity threats. In critical infrastructure environments, this is especially dangerous due to the convergence of IT and OT and the severe damage that can result from a single security lapse.

Passwordless MFA for Critical Infrastructure

HYPR's passwordless multi-factor authentication empowers organizations with strong security when accessing critical infrastructure systems. In fact, CISA and the OMB, "urge all organizations to implement phishing-resistant MFA as part of applying Zero Trust principles." This security method is fast, secure and convenient, which makes it an ideal solution for critical infrastructure environments.

HYPR significantly reduces authentication-based risk since it eliminates the use of passwords altogether. Government organizations, healthcare providers, financial institutions and energy companies are required to comply with strict data protection regulations. Passwordless MFA helps organizations comply with these regulations by providing secure access control that meets critical infrastructure security and usability requirements.

Critical infrastructure organizations that deploy phishing-resistant passwordless authentication benefit on multiple fronts.

Increased Security

Passwordless, phishing-resistant MFA eliminates the risk of credential breaches, which are a major security concern in critical infrastructure settings. It ensures that users are who they claim to be, reducing the risk of unauthorized access to critical systems and information.

Improved User Experience

Passwordless authentication simplifies the login process, eliminating the need for users to remember complex passwords or reset them periodically. This streamlines the user experience, user satisfaction and overall productivity.

Compliance With Regulations

Critical infrastructure organizations are required to comply with various regulations such as NIST, HIPAA and PCI DSS, among others. HYPR Passwordless MFA helps meet these regulatory requirements and also helps

80%
of OT/ICS organizations
had an incident in the last year.[1]

65%
of IT/OT security professionals
in the U.S. say
their IT and OT networks are
now more interconnected.[2]

organizations align with recommended security frameworks such as Zero Trust and MITRE ATT&CK.

Cost Savings

Password-related issues such as help desk requests, password resets, and lost productivity can be costly for organizations. HYPR helps reduce these costs, enabling organizations to redistribute resources to other important areas with an independently verified 324% ROI.

Secure Remote Access

Passwordless authentication can be highly beneficial in remote access scenarios, which are prevalent in critical infrastructure environments. Whether on an oil drilling turret in the middle of the North Atlantic, onsite in a mining operation or in a sprawling electricity generating facility, HYPR ensures the same frictionless and secure passwordless authentication experience via VPN, VDI and RDP.

Why HYPR

HYPR's True Passwordless Security is FIDO Certified and leverages open standards. It easily integrates with your existing technology to provide a best-of-breed security approach that is fully scalable. For the operator, it provides a seamless, fast and consistent user experience that's unparalleled across the entire organization from the endpoint to the cloud.

Critical infrastructure environments face a multitude of challenges with passwords and legacy MFA, cutting across security, operations, productivity, engagement and user adoption.

As history has demonstrated, security threats and operating environments are dynamic. HYPR has a demonstrated track record securing organizations globally, with deployments in some of the most complex and demanding environments including finance and banking, critical infrastructure and government. HYPR's solutions have been independently validated to return a 324% ROI.

1 https://claroty.com/press-releases/80-of-critical-infrastructure-organizations-experienced-ransomware-attacks-last-year

2 https://www.cybersecuritydive.com/news/IT-OT-cybersecurity-air-gaps/588947/

HYPR
THE IDENTITY ASSURANCE COMPANY
www.hypr.com | hypr.com/contact

HYPR creates trust in the identity lifecycle. HYPR Identity Assurance provides the strongest end-to-end identity security for your workforce and customers, combining phishing-resistant passwordless authentication with adaptive risk mitigation, automated identity verification and a simple, intuitive user experience. HYPR's solutions have been independently validated to return a 324% ROI.