SOLUTION BRIEF

HYPR

Passwordless Multi-Factor Authentication for the Supply Chain

HYPR Key Benefits

- Deploy passwordless MFA everywhere, including desktop through 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
- Reduce risk through continuous monitoring and adaptive, risk-based authentication
- Integrate quickly with existing systems, IdPs and applications

1 https://www.securitymagazine.com/articles/98615-98-of-organizations-have-been-impacted-by-a-cyber-supply-chain-breach

2 https://www.ibm.com/reports/threat-intelligence?_ga=2.91902362.1231815805.1679347335-1473918378.1679347335

3 https://www.csoonline.com/article/3677228/supply-chain-attacks-increased-over-600-this-year-and-companies-are-falling-behind.html

While security impacts to the supply chain have been a growing concern for well over a decade, the global pandemic pushed this into high gear. Regardless of the business sector, producers, suppliers, shippers and sellers require flawless execution of the supply chain to avoid shortages and product defects. Even a minor mis-orchestration can cost billions of dollars. For critical product sectors that rely on the supply chain, lives can be put at risk if products become scarce.

By the Numbers

98% of organizations surveyed have been negatively impacted by a cybersecurity breach that occurred in their supply chain.[1]

Supply chain issues from the pandemic were made worse by the fact that manufacturing was the most attacked industry in North America.[2]

633% year-over-year growth in supply chain attacks.[3]

Supply chain attack risks are at an all-time high, and the authentication process into systems has become the attack vector of choice because of its efficacy. Attack methodologies are dynamic and risk profiles can change per person and per encounter. The growing public awareness of the threats, increased oversight from regulators and the fact that attackers have more resources and tools at their disposal, creates the perfect storm where organizations must take action to ensure the ongoing operation of their infrastructure while also guarding against unacceptable authentication risk.

Targeting the Supply Chain

As clear from the statistics above, attacks on the supply chain and its components are on the rise. A confluence of factors make this attack surface attractive as a target.

- **Multiple parties involved:** The supply chain involves various stakeholders such as suppliers, manufacturers, distributors, and retailers. Each of these parties needs access to sensitive information and they are usually interconnected. This makes it difficult to control who has access to what information.

Significant Attacks Impacting the Supply Chain

2022 — LastPass, one of the world's largest password managers with 25 million users, disclosed that a hacker gained access to developer account credentials and used them to infiltrate their software supply chain and exfiltrate portions of their proprietary source code.

2020 — Attackers compromised SolarWinds, a software vendor that provides network management tools to thousands of organizations, and used this access to distribute malware. As many as 250 organizations were affected, and the attackers took advantage of multiple supply chain layers.

2017 — The NotPetya attack was launched against software provider MeDoc, a tool used by thousands of businesses in Ukraine. The attack distributed malware through a software update, which then spread throughout the supply chain. NotPetya caused more than $10 billion in damage and disrupted operations for multinational corporations such as Maersk, FedEx and Merck.

- **Lack of standardization:** The lack of standardization in the supply chain industry means that different parties may use different authentication methods, making it challenging to ensure a consistent level of security.
- **Data breaches:** With the rise in cyber attacks, data breaches can occur at any point in the supply chain. If a hacker gains access to one part of the chain, they may be able to access sensitive information from other parts of the chain, leading to significant security concerns.
- **Cost:** Implementing secure authentication systems can be costly, especially for small businesses in the supply chain. This cost may make it difficult for smaller companies to adopt the latest authentication technologies.
- **Lack of awareness:** Some parties in the supply chain may not be aware of the importance of secure authentication and the need for ongoing, automated risk assessments, making it challenging to implement secure authentication systems across the entire supply chain.

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 cybersecurity threats. Moreover, the inherent interconnections of operations and infrastructure throughout the supply chain means that a successful attack, even through an outside partner or provider, can quickly laterally migrate across the entire chain. This has dramatically changed the attack surface of the typical enterprise that relies on the supply chain as a core function of their business delivery.

For strong protection, ensure MFA is enabled on all accounts and devices that support the functionality. Utilization of MFA is especially important for administrative users with access privileges above that of a standard user. MFA should be required when accessing applications and systems from the Supplier's corporate network as well as remotely.

Passwordless MFA for the Supply Chain

HYPR's passwordless MFA empowers organizations with strong, risk-based, passwordless authentication whether it is to an endpoint or to the cloud. CISA and the OMB, "urge all organizations to implement phishing-resistant MFA as part of applying Zero Trust principles." HYPR is fast, secure, and convenient, which makes it an ideal security solution for environments that rely on or are connected to supply chain operations.

HYPR significantly reduces authentication-based risk since it eliminates the use of passwords and employs a sophisticated risk engine that constantly looks for anomalous events and policy deviations. Organizations that deploy phishing-resistant, passwordless authentication benefit on multiple fronts.

Why HYPR

HYPR's FIDO Certified passkey-based MFA easily integrates with your existing technology to provide a best-of-breed, risk-based security approach. For the operator, it provides a seamless, fast and consistent user experience across the organization, from the endpoint to the cloud .

Supply chain environments face a multitude of challenges with passwords and legacy MFA, cutting across security, operations, productivity, engagement and user adoption. HYPR protects your users, services and brand reputation now, with the flexibility and forward compatibility to meet future evolving conditions.

HYPR has a demonstrated track record securing organizations globally, with deployments in some of the most complex and demanding environments. HYPR's solutions have been independently validated to return a 324% ROI.

HYPR

THE IDENTITY ASSURANCE COMPANY

www.hypr.com | hypr.com/contact

Increased Security

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.

Improved User Experience

Passwordless authentication simplifies the login process and on average reduces the number of login streams by 75%, eliminating the need for users to remember complex passwords or reset them periodically. This streamlines the user experience, user satisfaction and overall productivity.

Quantifying Risk

Risk profiles can shift at a moment's notice. HYPR's risk-based authentication enables a constant and proactive measurement of risk by user and/or action. This can not only stop risky behaviors before they happen, but also leverages a cooperative security model that strengthens the entire security ecosystem.

Compliance With Security Requirements

Supply chain organizations are required to comply with various regulations such as NIST, HIPAA and PCI DSS, among others. Further, many security-conscious organizations are now requiring that their supply chain providers implement phishing-resistant MFA at all points of access. This includes secure, risk-based login to the desktop and workstation, which often falls outside traditional authentication defense controls. HYPR passwordless MFA helps meet these compliance requirements and also helps organizations align with recommended security frameworks such as Zero Trust and MITRE ATT&CK.

Cost Savings

Password-related issues such as helpdesk 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 highly prevalent in the supply chain. HYPR decouples authentication from the identity provider and other suites that can only scale to their own product. HYPR ensures the same frictionless, consistent and secure passwordless authentication experience via VPN, VDI and RDP access from anywhere.