Ping Identity, the provider of Identity Defined Security, announces updates to its multi-factor authentication (MFA) solution, PingID, providing new methods to mitigate risk and strengthen security for enterprises.

PingID’s new features include ways to evaluate user and device risk before access is granted, as well as support for Fast Identity Online (FIDO) standards to increase resistance to advanced phishing attacks. With phishing resistant and user-friendly authentication methods—including biometric authenticators, such as facial recognition and fingerprint matching—enterprises are able to create policies to enforce MFA only when warranted by an increased level of risk.
Risk-based security

Verizon’s 2019 Data Breach Investigations Report found that 32% of breaches involved phishing and 29% of breaches involved the use of stolen credentials. For this reason, enterprises can benefit from an MFA solution that evaluates user and device risk to provide an extra layer of protection against phished and stolen credentials.

Risk-based security is especially critical to maintain employee productivity and seamless online customer experiences. As a result, MFA has become more highly recommended by security frameworks like Zero Trust, those promoted by the National Institute of Standards and Technology and the International Organisation for Standardisation, as well as regulations like the PCI Data Security Standard.

Leveraging facial recognition

PingID further improves the balance of security and convenience provided to end users through multi-factor authentication as follows: Generally available in the next month, PingID support for Windows Hello and Mac Touch ID will support FIDO-compliant authentication methods. This will help users leveraging facial recognition and fingerprint matching on their devices.

These capabilities help to securely access web applications that have implemented the FIDO standard. Additionally, PingID integration with FIDO-compliant security keys, such as Yubikeys, can be leveraged for web authentication and Windows login. Becoming generally available in the same time period, hardware OATH compliant tokens will be able to be used as an authentication factor when users are unable to use a mobile device.
Virtual private network

PingID will have the ability to support a quick and easy way to implement MFA

PingID can now configure the number of attempts consumers logging in to a provider’s website have to enter a one-time passcode (delivered by SMS or Email), as well as set the amount of time they are locked out of their accounts if failing to provide the right one-time passcode.

Additionally, generally available in the next month, PingID will have the ability to support a quick and easy way to implement MFA for Virtual Private Network access when users are working remotely, simplifying deployment of MFA for enterprise administrators.

Corporate Resources

PingID is now offering features in private preview that evaluate the location where a user requests access to corporate resources, and compares it to the location of the previous request. If the distance between the two geographies exceeds the threshold of what is possible by human travel, access can be automatically denied.

Also in private preview, PingID assesses the reputation of the IP address from which a user requests access. Organisations can mandate specific MFA methods when the malicious activity-based risk score associated with an IP address exceeds a certain benchmark.

Multi-factor authentication

Hackers are evolving their tactics to access accounts and steal data every single day"
“PingID is a core product that enterprises have been using for years, and its new features make it stronger and smarter than ever,” said Steve Shoaff, chief product officer, Ping Identity.

Organisations interested in securing their enterprise with multi-factor authentication can sign up for a free trial of PingID. Also, be sure to check out the blog titled ‘Five Preventable Breaches Make the Case for MFA Everywhere’ to learn more about attacks that can be prevented with multi-factor authentication.
Ping Identity, the pioneer in Identity Defined Security, announced a cloud-based multi-factor authentication (MFA) and single sign-on (SSO) bundle provides security from identi...

The rise of access control in the cloud

Among the cloud’s many impacts on the physical security market is a democratisation of access control. Less expensive cloud systems ar...

How are standards changing physical security?

The definition of a standard is “an authoritative principle or rule that usually implies a model or pattern for guidance, by compariso...

Ping Identity to talk about best practices towards digital transformat...

Ping Identity, global provider of Identity Defined Security solutions, announced its participation at Identiverse 2019, slated to take place...