Microsoft and Yubico Part 1 - Enterprise Strong Authentication with YubiKey

Overview

In Verizon's 2019 Data Breach Investigations Report it shows that stolen credentials are again this year involved in a significant number of breaches. This is a common trend year over year where stolen or weak credentials are somehow involved in a breach.

The 2019 Verizon report also categorizes and ranks Hacking being involved in 52% of the breaches. Following that statistic, the top hacking action performed was using stolen credentials.

![Breaches Diagram]


The report suggests that implementing MFA solutions is an effective method to protect credentials. This cannot be overstated in today's world where much of the attention and time is given to attack vectors that are theoretically possible but rarely exploited. Organizations need to refocus and make sure that they have first covered the most likely threats. This means, enabling MFA needs to be immediately placed as a top priority for securing your organization to mitigate the risk of account takeover. According to Alex Weinert, Director of the Microsoft Identity Division - Security and Protection Team, in his 'Your Password Doesn’t Matter' blog, he states:

"Based on our [Microsoft’s] studies, your account is more than 99.9% less likely to be compromised if you use MFA."

While most MFA solutions significantly address a lot of the security concerns, all MFA solutions may not be the right fit for your organization. An important consideration for MFA solutions is also the user experience. Ease of use, uniformity, speed, portability, and availability are just some aspects to consider with the user experience. As your organization
develops your strategy for MFA, also consider the direction your organization is headed for authentication. We all should be learning from the yearly Verizon DBIR reports and remove altogether the opportunity for passwords to be involved in breaches.

To understand why user experience is also critical we should also learn from the Ponemon Institute's 2019 State of Password and Authentication Security Behaviors Report about risky password practices, time spent managing/using passwords, and overall perceptions about passwords. Ideally, the MFA vision your organization is working towards is passwordless.

An astute observer will rightly recognize that passwords are commonly entrenched in the enterprise and cannot be immediately replaced. There are many circumstances where a passwordless sign-in alternative is not yet available. Since not all organizations, applications, and scenarios can immediately move to a passwordless sign-in, it is best to start posturing your user-base towards that future. Organizations should now look at MFA in a new light and see not only how it secures their organization, but how it can also be used to get ready for a passwordless future. Today, there are still gaps in capabilities which prevent most organizations from implementing passwordless. Organizations need to develop a strategy which focuses on how they can start positioning themselves towards passwordless today using MFA. This repositioning will enable a smoother passwordless transition once the full set of capabilities are in place and passwords can finally be eliminated.

**Microsoft and YubiKeys**

In the Azure and Microsoft ecosystem, for both on-premises and cloud environments, FIDO2 can be leveraged to solve many of your password concerns by allowing an organization to go passwordless in many scenarios. FIDO2 is an open standard, co-developed by Yubico, Microsoft, and other members of the FIDO Alliance. FIDO2 was developed to support both passwordless and two-factor authentication scenarios, providing organizations options in their identity and authentication strategy.

Yubico has enabled their products to support the FIDO2 spec allowing the keys to be used to secure accounts and go passwordless. FIDO2 hardware security keys by Yubico provide some of the strongest MFA protections available since the solution is resistant to malware,
phishing, Man-In-The-Middle, and brute force attacks. In addition to supporting the FIDO2 spec, the YubiKey 5 series line of keys has been enabled with many additional capabilities to solve other common authentication challenges. The YubiKey 5 series also includes support for FIDO U2F, OATH One-Time Passcodes, certificate-based authentication and other protocols that are commonly used in the Microsoft ecosystem. Organizations can use a single YubiKey to unlock many different doors providing a more seamless user experience during their long road to passwordless.

Two Organizations Enabling Strong Authentication

This series is divided by types of organization to isolate different components that are common to many organizations. The first organization is cloud native, only having resources in the cloud, and the second is an organization having resources both in the cloud and on-premises. Even if your organization is not cloud native, it is best to read all of the guidance related to the cloud native organization, since the guidance is cumulative and will apply across both organization types.

Continue reading the series with: Microsoft and Yubico Part 2 - Enterprise Strong Authentication for Cloud Native Organizations