idaptive

SOLUTION BRIEF

MFA Everywhere

Accelerating A Zero Trust Approach for Stronger Security

Stolen Passwords at Center of Breaches

It's no surprise that data breaches and cyber attacks continue to garner worldwide media attention. In fact, compromised identities are at the center of these major cyber attacks and thus pose the greatest threat to your enterprise. Verizon's 2017 Data breach Investigations Report found that 80% of hacking-related breaches leveraged weak, stolen or compromised credentials[1]. And not surprisingly, Verizon's 2018 Data Breach Investigations Report continued to state the persistence of stolen credentials topping the list of causes for data breaches. Identity theft has increased in record numbers and has been the primary focus for hackers. This is because it's much easier to steal a trusted insider's credentials and bypass traditional cyber security controls than it is to break through the firewall. Instead of burrowing through firewalls, attackers simply walk in the front door with stolen keys — usernames and passwords. Once logged in, attackers branch out through the enterprise.

As users increasingly embrace mobile devices and organizations move applications into the cloud, the risk grows. Attackers have even more user, system and application identities to target. How can organizations secure enterprise identities against cyberthreats that target today's hybrid IT environment of mobile, cloud and on-premises resources?

MFA Everywhere Reduces Risk

Multi-factor authentication (MFA) is quickly emerging as the solution of choice. And yet, even MFA is only as good as the breadth of applications and systems it supports. Attackers target all users. Stealing an end-user's password allows them a foothold inside the organization, from which they seek out privileged accounts to get to servers and data. JP Morgan was breached because, of its thousands of servers, malware penetrated about 80 servers not protected by MFA. Even though JP Morgan was mostly protected by MFA, it was still 100% vulnerable to automated malware that entered via a compromised user identity.

Organizations need MFA everywhere — across users, and across all systems — VPN, cloud and on-premises applications, and endpoints. Only then can MFA protect organizations against the leading point of attack in data breaches — compromised credentials. Companies that deploy a comprehensive security platform with MFA as an integral component can build an identity-based security perimeter that enforces access while also enabling the use of hybrid clouds, software-as-a-service (SaaS) applications and a growing inventory of mobile business apps. The result will be stronger and more reliable security, sustainable regulatory compliance and dramatically reduced risk of being victimized by a costly data breach.

One of the simplest, yet most powerful, ways to confirm identity is to leverage MFA. Not only can you reduce your attack surface, but you are enabling IT organizations to adopt a Zero Trust Security model by requiring a higher level of identity assurance

[1] Verizon, 2017 Data Breach Investigations Report

Ready to learn more?

Please contact us at
hello@idaptive.com