Centrify
ZERO TRUST SECURITY

SOLUTION BRIEF

MFA Everywhere — for Much Stronger Security

Data breaches and cyber attacks continue to garner worldwide media attention.

Compromised identities are at the center of major cyber attacks and thus pose the greatest threat to your enterprise.

Multi-factor authentication (MFA) everywhere reduces the risk of compromised credentials.

Stolen Passwords at Center of Breaches

Gartner estimated that worldwide information security spending would grow from $76.64 billion in 2015 to $104.99 billion in 2019, at a compound annual growth rate of 7.8%[1]. The vast majority of this spending has been directed at perimeter defenses. But perimeter defenses are only part of the solution. Verizon's 2017 Data breach Investigations Report found that 80% of hacking-related breaches leveraged weak, stolen or compromised credentials[2]. 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 all users — end and privileged users, and across all systems — VPN, cloud and on-premises applications, servers and privileged commands. 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 and privilege policies 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.

1 Gartner Inc., Forecast Analysis: Information Security, Worldwide, 4Q15 Update, March 22, 2016
2 Verizon, 2017 Data Breach Investigations Report

Centrify delivers Zero Trust Security through the power of Next-Gen Access. Centrify verifies every user, validates their devices, and limits access and privilege. Centrify also utilizes machine learning to discover risky user behavior and apply conditional access — without impacting user experience. To learn more visit www.centrify.com.