

New Research Study Commissioned by Centrify Reveals That Organisations Adopting Next-Gen Access Solutions are Twice as Confident Accelerating New Business Models and Customer Experiences to Market

Submitted by: Origin Comms Ltd

Monday, 23 July 2018

Respondents with Zero Trust models leveraging Next-Gen Access report reduced overall risk and lower security-related costs

Bracknell UK — July 23, 2018 — Centrify (<https://www.centrify.com>), a leading provider of Zero Trust Security through the power of Next-Gen Access, today announced results of a commissioned study conducted by Forrester Consulting on behalf of Centrify, which finds that organisations powering Zero Trust Security with Next-Gen Access solutions reported twice the confidence to accelerate new business models and customer experiences. The study of 311 IT decision-makers in North America and the UK finds that 67 per cent of all enterprise resources are exposed to access-related risk, and that a Zero Trust Security approach is the best strategy to control access to enterprise resources.

The study revealed that Next-Gen Access is the engine that powers Zero Trust Security, stating that, “NGA technologies enable the layers necessary for a successful Zero Trust strategy.” Organisations using Next-Gen Access solutions – including Identity-as-a-Service (IDaaS), Enterprise Mobility Management (EMM), and Privileged Access Management (PAM) – also reported topline benefits including being 66 per cent more confident in adopting mobile work models, and 44 per cent more confident in securing DevOps environments. Those same respondents reported bottom line benefits of mitigating overall risk by 37 per cent and reducing security costs by 31 per cent.

According to Forrester, 58 per cent of global enterprises have experienced a breach in the past 12 months. According to the study, “Security leaders are urgently scrambling to defend every entry point, but traditional approaches to security, based on keeping out the ‘bad guys,’ while letting in the good guys, have proven ineffective.” In response, many security leaders are turning to Zero Trust approaches that remove trust from the equation completely, shunning the traditional “trust but verify” approach and replacing it with a “never trust, always verify” mandate.

“The dissolving network perimeter is causing a complete rethink in how we approach security, taking into account a new enterprise reality defined by the cloud, mobility, and increasing demands for agility,” said Tom Kemp, CEO of Centrify. “This study reveals that two-thirds of enterprise resources are exposed to access-related risk, largely because organisations are approaching security in a way that no longer works and with solutions that are ineffective. Zero Trust Security, powered by Next-Gen Access, reduces risk and costs, while ushering in a new era in customer experiences and business models.”

“Zero Trust is the best strategy to control access,” the study states. “Successful access control is a key pillar in Forrester’s Zero Trust model for securing today’s enterprises. A Zero Trust strategy, as the name implies, rests on security leaders not making any trust assumptions throughout their security architecture.”

To enforce user access, a Zero Trust strategy requires that an organisation’s security must have the capability to:

- Verify the identity of every user through a combination of identity governance, single sign-on, and multifactor authentication (MFA) to eliminate the risk of credential compromise.
- Validate every device with mobile device management to enforce secure policy, with local administrator privilege management to eliminate local admin compromise, and with device identity management to ensure that only trusted devices are allowed to access resources.
- Limit access and privilege using privileged access management to ensure a user has just enough access and only the necessary privileges to perform their job during any given time.
- Continually learn and adapt using behaviour-based analytics and privileged access auditing/monitoring to automatically improve and personalise access policies.

Centrify's Next-Gen Access delivers a unified, industry-recognised solution that uniquely converges IDaaS, EMM and PAM to address these four pillars of Zero Trust Security. This seamless integration secures access across applications, endpoints and infrastructure for all users, without sacrificing best-of-breed features.

About This Study:

Forrester Consulting conducted an online survey of 311 IT decision-makers in North America and the UK belonging to organisations with 1,500 or more employees to evaluate identity and access management practices. Survey participants were required to have authority over identity and access management decisions in their organisation.

For more information, download the full study here

(<https://www.centrify.com/lp/forrester-adopt-next-gen-access-to-power-zero-trust-strategy/>)

#

About Centrify

Centrify delivers Zero Trust Security through the power of Next-Gen Access. The Centrify Zero Trust Security model assumes that users inside a network are no more trustworthy than those outside the network. Centrify verifies every user, validates their devices, and limits access and privilege. Centrify also utilises machine learning to discover risky user behaviour and apply conditional access — without impacting user experience. Centrify's Next-Gen Access is the only industry-recognised solution that uniquely converges Identity-as-a-Service (IDaaS), enterprise mobility management (EMM) and privileged access management (PAM). Over 5,000 worldwide organisations, including over half the Fortune 100, trust Centrify to proactively secure their businesses.

Centrify is a registered trademark of Centrify Corporation in the United States and other countries. All other trademarks are the property of their respective owners.

For further information please contact:

Louise Burke

Origin Comms

louise@origincomms.com

+44 (0) 7917 176095