Centrify Confirms the Enterprise Security Industry Has Failed to Stop Breaches

Submitted by: Origin Comms Ltd
Tuesday, 14 February 2017

Organisations spend $75B on security, yet Centrify-commissioned Forrester study reveals 83 per cent are at high risk, and being breached at an alarming rate

Centrify (https://www.centrify.com), the leader in securing hybrid enterprises through the power of identity services, commissioned a new Forrester study (https://www.centrify.com/lp/forrester-stop-the-breach-IAM-maturity-model?utm_campaign=forrester%20stop%20the%20breac that revealed the enterprise security industry is failing, with organisations being breached at an alarming rate. The study found that two-thirds of organisations experienced an average of five or more security breaches in the past two years, and hackers compromised more than one billion identities in 2016 alone.

“Cybersecurity breaches are causing more havoc and affecting more industries than ever before,” said Tom Kemp, CEO of Centrify. “Despite over $75 billion spent on cybersecurity in 2016, the products and services from major security companies have failed to stop breaches from occurring, and in fact, the problem is getting worse. This clearly indicates that traditional approaches are flat out not working in this age of access.”

For years now, organisations have relied on a well-defined boundary, supported by digital walls and gatekeepers, to protect their assets. But today, with the rapid introduction of new technologies, platforms, applications and practices, that border has disintegrated, resulting in significant exposure for the global enterprise. With 90 percent of all enterprises moving to the cloud, and billions of users accessing data across millions of applications, enterprises face an increasingly complex digital canvas of identities. These identities live in and out of the enterprise, creating a new dimension in security. Most accessed by one simple permission: the password.

“Organisations need to completely rethink their security approach, and in today’s world of access they must increase their Identity and Access Management (IAM) maturity to more effectively reduce the likelihood of a data breach,” said Kemp. “Centrify’s mandate is to ensure the breach stops here by providing a single platform to secure each user’s access to apps and infrastructure in today’s boundaryless hybrid enterprise.”

In fact, the study concluded that 83 per cent of organisations do not have a mature approach to Identity and Access Management (IAM) resulting in two times more breaches and $5 million more in costs. The study further concluded that 91 per cent of organisations with the most mature IAM stances gravitate toward integrated IAM platforms, rather than relying on multiple point solutions, and spend 40 per cent less on technology. The more mature IAM approach showed direct correlation to reduced security risk, improved productivity, increased privileged activity management and greatly reduced financial loss over their less mature counterparts.

The Impact of IAM Maturity

The Forrester research study, which surveyed more than 200 enterprise IT security decision-makers in charge of identity and access management, revealed that:

- Organisations with the highest IAM maturity experience half the number of breaches as the least mature. For instance, they are 46 per cent less likely to suffer a server or application breach, 51 per cent less likely to suffer a database breach and 63 per cent less likely to suffer cloud infrastructure breach.
- Organisations that secure both regular and privileged access are less likely to experience a breach compared to those organisations that adopt fewer best practices. Forrester estimates that 80 per cent of security breaches involve privileged credentials that typically belong to the IT professionals who administer the systems, databases and networks of an organisation.
- Organisations with the least IAM maturity averaged over 12 breaches, more than twice the number of breaches of the most mature, and endure more than $5 million more in financial damage.
- Mature companies spend more on overall IT security versus the least mature companies, but actually spend less on IAM technology as a percentage of their entire budget—40 per cent less. This translates into an additional cost savings of $2,582,000, which not only makes these organisations more capital efficient, but also allows them to better streamline their IT infrastructure by eliminating redundant IAM technologies.

In this study, Forrester concluded that a maturity hierarchy exists in the marketplace. The most mature groups employ more IAM approaches as well as use integrated IAM technology platforms to reduce security risk and may avoid millions in data breach costs over their less mature counterparts.

Download the full study here
(https://www.centrify.com/lp/forrester-stop-the-breach-IAM-maturity-model?utm_campaign=forrester%20stop%20the%20breac

About Centrify

Centrify redefines security from a legacy static perimeter-based approach to protecting millions of scattered connections in a boundaryless hybrid enterprise. As the only industry recognized leader in both Privileged Identity Management and Identity-as-a-Service, Centrify provides a single platform to secure each user’s access to apps and infrastructure through the power of identity services. This is Next Dimension Security in the Age of Access. Centrify is enabling over 5,000 customers, including over half the Fortune 50, to defend their organizations. To learn more visit www.centrify.com.

Media contact:
Amanda Hassall, Consultant, Origin
amanda@origincomms.com
Tel: +44 1628 822741/+44 7855 359889
Tw: @mandyhassall

Distributed via Press Release Wire (https://pressreleases.responsesource.com/) on behalf of Origin Comms Ltd

Copyright © 1999-2024 ResponseSource, The Johnson Building, 79 Hatton Garden, London, EC1N 8AW, UK

e: info@responsesource.com t: 020 3426 4051 f: 0345 370 7776 w: https://www.responsesource.com