CERTES NETWORKS

THE FINTECH TIMES

Publication: The Fintech Times
Date: 10.08.2019
URL: https://thefintechtimes.com/data-financial-services/
Title: Banking on Security: Keeping Data Secure in Financial Services
Author: Simon Hill, Legal & Compliance, Certes Networks

Banking on Security: Keeping Data Secure in Financial Services

By Simon Hill, Legal & Compliance, Certes Networks

The protection of sensitive data in line with regulations, both for banks and other financial services organisations, is currently a big challenge. The way these organisations operate has changed dramatically in recent years, due mostly to the fact that financial institutions are not only heavily regulated by data privacy requirements, but they are also under mounting pressure to be open to consumers and businesses about how they are protecting their data from potential breaches.

The increasing expectations of consumers means that banks and financial institutions are trying to achieve a balancing act: how can they protect data privacy, while at the same time remaining transparent about how data is being protected? However, it doesn't have to be a play-off between meeting these customer expectations and meeting cyber security and compliance requirements: banks and financial services organisations can utilise technology to the fullest extent while still protecting data.

The balancing act

To achieve this balance, banks and financial services organisations need to take control of their security posture and assume the entire network is vulnerable to the possibility of a cyber-attack. Robust encryption and controlled security policies should be a central part of an organisation's cyber security strategy. Through generating and defining policies, network policy enforcement allows organisations to ensure that only authorised applications and users are communicating with one another, while enabling them to meet their own governance, security and compliance requirements.

Rather than waiting for a cyber-attack to happen, new technology tools are now available to gain a deeper understanding of policy deployment and analyse every application that tries to communicate across the network, all the while monitoring all traffic and limiting the pathways potential threats can travel.

Banks and financial services organisations need to take control of their security posture and assume the entire network is vulnerable to the possibility of a cyber-attack.

Conclusion

Banks and financial services organisations should not have to worry about keeping data secure and protected. Adopting new ways of thinking about how these organisations can strengthen the protection of data requires well-defined policies, strict key assignments and authorisation of who sends and receives data. But, most importantly, the ability to enforce policies to better monitor and observe applications and suspicious activity on the network will require sophisticated technology and tools that are currently available today.
