TELESOFT

CASE STUDY

DIGITAL ESTATE VISIBILITY

INDUSTRY: Telecommunications

CUSTOMER PROFILE AND CHALLENGE:

One of our larger customers, operating within the Telecommunications industry for a considerable length of time, had understandably gone through a number of Mergers and Acquisitions (M&As) over the years. This had broadened their digital estate considerably.

Whilst M&As are relatively commonplace and organisations understand the risks associated with an M&A, oftentimes acquisitions can pose threats to an organisation's network security. Additionally, if the network infrastructure is not fully understood prior to an M&A, it can be very challenging and time consuming to map out the extended network after integration.

Furthermore, the larger the network, the less visibility of all the digital assets there is, for smaller networks there are generally less security tools, teams and controls. Deep visibility enables a greater accuracy valuing digital assets and business operations, whilst better quantifying the cyber risk individually and cumulatively of the two parties.

It's widely assumed that an organisation's network administrators and IT security teams know and can see into every corner of their network. Unfortunately, this isn't the case, and only through correct usage of the appropriate capability could our customer fully understand their digital estate.

DEPLOYMENT — FLOWPROBE

1. How can I better understand my entire network?

The insight data offers into an organisation's operations, its customers, its competitors and its supply chain, is truly invaluable. However, this information can only be utilised if it can be seen. The FlowProbe extracts metadata from 100% of the network flows, ensuring that visibility is maintained across every network communication session.

By monitoring and understanding the flow sessions across a network, an organisation can begin to fully understand its network, the devices within it and how, why and when they communicate. This deep understanding enables identification of anomalous activity, such as a device initiating and maintaining communications with another device, possibly in a different geographical location which it has not previously communicated with.

HEADQUARTERS
Telesoft Technologies Ltd
Observatory House, Stour Park
Blandford DT11 9LQ UK
+44 (0)1258 480880
+44 (0)1258 486598
sales@telesoft-technologies.com

AMERICAS
Telesoft Technologies Inc
430 National Business Parkway
Suite 480, Annapolis Junction
MD 20701
USA
salesusa@telesoft-technologies.com

ASIA
Telesoft Technologies Ltd
Tapasya Corp Heights
Ground Floor, Sector 126
Noida, 201301
+91 120 612 7725
salesindia@telesoft-technologies.com

2. How can I use this information to identify new additions to our digital estate?

Un-sampled flow monitoring was utilised in order to fully map and understand the existing network topology - ie understanding where devices were located and who they communicated with. Once understood, access control lists and network segregation could be introduced. This ensured that different geographical areas of the network could communicate with other preauthorised areas only, essentially turning digital assets in to entities and dictating who should/not be communicating with whom.

This enabled identification of new communications to anywhere within the exisitng network, particularly where communications were originating from different geographical regions and attempting to communicate with the headquarters - this can be normal activity for an organisation, but a simple way to identify and understand such communications. When triggered, the SOC teams utilising the TDAC would be alerted, enabling them to investigate and understand if this was malicious acitivity or a legitimate communication from an organisation recently acquired through an M&A.

SUMMARY

By utilising our FlowProbe and fully understanding their network infrastructure, the customer was able to ensure that its CTOs and CISOs were able to carry out the important function of protecting their digital estate, comprised of known and new, unknown assets being acquired through M&As.

Once the solution was in place and the network was fully understood, any new organisations being introduced to the network following M&As were readily identified by the system, ensuring a holistic view of the entire network and therefore a much more secure and understood environment.

TELESOFT

Telesoft Technologies, the Telesoft Technologies logo design, ThinkEngine, Triton, HINTON, OKEFORD, TDAPI, MPAC, MILBORNE, C-CURE and ARNE are trademarks or registered trademarks of Telesoft Technologies Ltd or its subsidiaries. All other brand or product names may be trademarks of their respective companies. All rights reserved.

DX-TTL-GEN-MK-GU-35772-01
Telesoft Public

telesoft-technologies.com
© Copyright 2020 by Telesoft Technologies.
All rights reserved. Commercial in Confidence.