Publication: Security Boulevard
Date: 14.10.2019
URL: https://securityboulevard.com/2019/10/network-security-observability-visibility-why-they-are-not-the-same/
Title: Network Security Observability & Visibility: Why they are not the same
Author: Sean Everson, Chief Technology Officer, Certes Networks

Network Security Observability & Visibility: Why they are not the same

Sean Everson, Chief Technology Officer, Certes Networks

In today's increasingly complex cyber landscape, it is now more important than ever for organisations to be able to analyse contextual data in order to make informed decisions regarding their network security policy. This is not possible without network observability. Organisations can now see inside the whole network architecture to explore problems as they happen. Observability is a property of the network system and should not be confused with visibility which provides limited metrics for troubleshooting.

With observability, organisations can make the whole state of the network observable and those limitations no longer exist. Observability provides the contextual data operators need to analyse and gain new and deeper insights into the network. This enables teams to proactively make more informed decisions to improve network performance and to strengthen their overall security posture because context is now available to troubleshoot incidents and make policy changes in real-time.

Unfortunately, observability is often miscommunicated and misunderstood, as visibility is repackaged by some vendors and sold as observability, when the two are not the same. Visibility and monitoring have an important role to play but observability is different. Visibility and the metrics it provides limits troubleshooting, whereas observability provides rich contextual data to gain deeper insights and understanding based on the raw data collected from the network or system.

With research showing that the average lifecycle of a data breach is 279 days, it is clear that organisations are slowly putting observability into practice and adopting 'observability as a culture'. In the case of some well-known breaches, however, the timescales were much longer than that. The Marriott International breach, which was discovered in November 2018, saw hackers freely access the network since 2014. During this time, no unusual activity was detected and no alerts of the hacker's access were raised.

Additionally, in the British Airways data breach in 2018, data was compromised over a two-week period, affecting 500,000 customers. This resulted in the Information Commissioner's Office (ICO) announcing that it intended to fine British Airways £183.39M for infringements of the General Data Protection Regulation (GDPR).

These two examples alone demonstrate how essential it is for organisations to begin to value the ability to understand their systems and behaviour by making their network observable.

Understanding Observability

Simply defined, observability is a measure of how well something is working internally, concluded from what occurs externally. Observability is creating applications with the idea that someone is going to observe them with the aim of strengthening and making system access decisions. The right combination of contextual data can be used to gain a deeper understanding of network policy deployment and every application that tries to communicate across the network. With an observability capability, attackers will therefore have a hard time attempting to make lateral 'east-west' movements or remaining hidden in the data centre or across the WAN. In turn, observability can provide a global view of the network environment and visual proof that the security strategy is effective and working.

Unfortunately, it's not uncommon for infiltrations to go undetected in networks for days, weeks or months. This means infiltrations are going undetected for longer and networks systems are more increasingly vulnerable. To effectively do this, all roles need to see inside the entire architecture. And, when this capability is built in, it is observability that enables greater insight into the overall reliability, impact and success of systems, their workload and their behaviour.

Conclusion

Research shows that companies who are able to detect and contain a breach in less than 200 days spend £1 million less on the total cost of a breach. That's a figure no organisation can – or should – ignore. Organisations need a cyber security solution that can be measured and traced. Observability provides the contextual data so organisations can take measurable steps towards controlling system access of the network environment. With this type of observable analysis, organisations can gain deeper insights into how to enhance their security policy and detect unwanted access as it occurs.
