vehere

Case study

Telecommunications

Summary

Industry/Organisation

Telecommunications

Challenges

- Gain visibility into what's happening on the network
- Speed up triage – reduce time to respond to security incidents
- Comply with regulatory mandates
- Protect the system from constantly-evolving threats

Solution

PacketWorker 10G

Benefits

- Real-time insights into applications, actors and, actions
- Prompt incident response and discovery by leveraging comprehensive indexing and searching capabilities
- Improved performance of application monitoring and network behaviour analytics for non-standard management-plane traffic
- Reduction in total cost of ownership for security implementation

vehere

"We needed to ensure compliance with regulatory requirements and enhance visibility with respect to management-plane applications."

- Name withheld, Client

"Vehere's PacketWorker is extremely powerful when it comes to detecting abnormal activities that can threaten our cybersecurity framework."

- Name withheld, Client

Background

The security leadership of a leading telecommunications company was looking to curtail costs and improve the efficiency of the cyber threat detection solution that was deployed for their management-plane networks. The incumbent vendor's solution was at its end-of-life stage and the cost of refreshing the technology was proving to be higher than budgeted.

Gaining visibility into the network

Burgeoning growth in terms of customer base and data usage had meant that the company's network had become more complex and the throughput had exceeded 10 gigabytes per second across majority of their router interfaces. Adding to their woes was the fact that the solutions available at their disposal did not really have much to offer in terms of detection for management-plane applications. Subsequently, the company began to look for a technology that could help them make sense of the 'unknowns' and provide a response to the questions that were being raised as a result of the security incidents they were encountering. The company was found to be lacking the ability their sectoral peers had in terms of discovering and triaging a security incident. Not only did this indicate the waning power of the company's risk management framework but also its potential inability to deal with a material attack, if and when it happened. There was a strong likelihood that the company was on the verge of inviting customer ire because of the aforementioned failings.

vehere

"We have ensured stringent compliance with established sectoral regulations ever since PacketWorker was installed."

- Name withheld, Client

Solution – PacketWorker 10G

By leveraging the deep packet inspection and analytics capabilities of PacketWorker, the company gained incisive insights into their management-plane traffic and by utilising signature-less techniques they were able to detect security risks and shield the network from sophisticated cyber threats. PacketWorker is an effective cyber threat detection and response solution that helps organisations minimise risk of expensive breaches by accurately detecting and enabling swift responses to thwart cyber threats. PacketWorker facilitates the efficient resolution of identified security incidents using concrete evidence, actionable intelligence and response workflow integrations. The solution is true big data architecture that is built around a search engine to speed up retrieval of information and execute complex analytical tasks such as identifying instance of spikes and slow and low-flying traffic, correlating them across multiple activities and finding similar patterns to tell normal and malicious behaviour apart.

Visibility and answers

PacketWorker empowered the company to get cyber threat alerts on a real-time basis. PacketWorker's unique ability allowed the company's security and risk management teams to proactively assess security postures and formulate detection rules and use advanced predictive analytics to detect unknowns. Capitalising on a powerful deep packet and payload inspection, PacketWorker offered full visibility into network traffic along with the ability to analyse encrypted communications using mathematical models. Security analysts leveraged the visual play-book and time-travel capabilities to determine root causes of incidents and retrieve actionable intelligence – from session correlations and graphic analyses – to improve the organisational security posture. Furthermore, all this was done without disrupting ongoing business processes.

Accelerated resolutions

With PacketWorker, the company managed to trim their incident resolution time from days to hours and simplified an analyst's interaction with network data. An easy point-and-click interface was used to lay down complex behaviour-based rules, which enabled the security operations team to deliver predictable and repeatable outcomes, irrespective of the skill set of the user. The result: maximised efficiency and reduced dwell-time. PacketWorker used big data analytics to eliminate considerations pertaining to events or log rates and obviate the need for deploying collectors for different applications and processes. The platform ran on readily-available structured data that it gathered from the source of truth – packets on the network.