corelight

White Paper

Why Fintech is embracing metadata over full packet capture

smartPCAP

THE TOTAL NETWORK VISIBILITY CHALLENGE

For years, the financial services industry has assumed that the only way to achieve total network visibility is through full packet capture (PCAP). Traditional PCAP provides comprehensive visibility by storing all packets that cross the network. However, this reliable yet outdated solution introduces significant inefficiencies. Corelight offers a new perspective on PCAP, reducing storage infrastructure and maintenance needs while simplifying data searching.

Would you be interested in a modern approach to capturing relevant data?

DRAWBACKS OF FULL PACKET CAPTURE

Full packet capture (PCAP) offers an end-to-end recording of network activity, akin to a moment-in-time snapshot. However, with thousands of devices, you could accumulate millions or even tens of millions of captures, consuming immense disk space, requiring extra cooling, and slowing down queries.

An analogy for full packet capture is CCTV surveillance footage: how efficiently can you find a ten-second clip among thousands of hours of recordings? How much storage is needed to retain useful information over weeks or months? How much of this stored video is actually useful? The solution relies on static filters and may struggle with new network segments, traffic pattern changes, or encrypted sessions with no way to decrypt. How much heating and cooling is required? How much rack space is consumed by full PCAP solutions that lack intelligence?

SMART PCAP BENEFITS

Storage efficiency: reduces storage by 80-90%

Optimized performance: speeds search times by up to 50x

Selective capturing: enables user-defined packet capturing

Rich metadata: uses only 1-2% of network throughput

Streamlined maintenance: minimizes storage infrastructure and cooling

SMART PCAP. CORELIGHT'S APPROACH TO ACHIEVING TOTAL VISIBILITY

Corelight, an industry-leading NDR platform provider, offers Smart PCAP to address the drawbacks of traditional full PCAP solutions. Smart PCAP complements Corelight network transaction logs, enabling packet capture for specific subsets of network data.

Smart PCAP can be configured to trigger packet captures based on IPs, protocols, or ports, or by matching a traffic profile or IDS signature. For instance, Smart PCAP can collect packet captures relevant to financial transactions, trading environments, and backend systems, while also gathering metadata on network data that doesn't meet the Smart PCAP conditions.

A Corelight solution with Smart PCAP not only captures necessary PCAPs but, together with our Open NDR Platform, provides rich metadata for all network traffic, occupying just 1-2% of actual network throughput.

With this rich metadata and detections for encrypted traffic, SecOps teams have an index 1-2% the size of a full packet capture, enabling searches up to 50x faster.

CONCLUSION

Traditional full packet capture solutions offer visibility of everything that traversed the network but don't offer anything better for regulatory requirements or any way to see encrypted connections, resulting in massive, expensive, and slow-to-search data.

In contrast, Corelight with Smart PCAP allows selective packet capturing based on user-defined parameters, alongside our rich NDR and IDS solutions. This approach saves 80-90% on packet capture storage and accelerates incident response by up to 50x compared to traditional full packet captures.

corelight

To learn more, request a demo at **https://corelight.com/contact**

info@corelight.com | 888-547-9497