CASE STUDY

Cybersecurity Firm Standardizes on Accolade Adapters to Deploy Proprietary Signature Generation & Matching Algorithms

Accolade Technology

SUMMARY

Cybersecurity firm integrates ANIC-40Ku adapter into their security monitoring appliance.

KEY CHALLENGES

- Need new platform to deploy signature generation and matching algorithms
- Require custom features to meet key product requirements
- Require cost effective, lossless packet capture solution with full service support

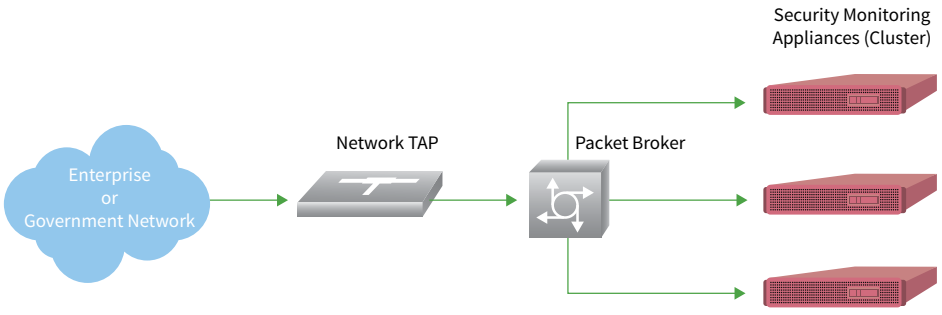
WHY ACCOLADE?

- Willing to add custom features to ANIC-40Ku in order to meet unique customer requirements
- Provide hardware based flow classification
- Provide full featured IP packet processing adapter

ANIC FEATURES USED

- Customer specific functionality
- 100% packet capture
- Timestamping
- Packet Merging
- Packet Steering
- Flow classification

The firm is a pioneer in appliance based cybersecurity with decades of experience selling to enterprise and government organizations. Its network security monitoring appliances are deployed inside the firewall to detect various attacks such as zero-day exploits, malware and insider threats. The appliances provide continuous visibility across the network and rely on sophisticated forensic analysis to mitigate threats. A key component of the forensic analysis is the ability to generate and match internally developed signatures. Over the years, the firm has developed various proprietary signature generation and matching algorithms which are effectively the firm's "secret sauce" and main competitive advantage.



TECHNICAL CHALLENGE

The firm's proprietary signature generation and matching software was initially developed to run on x86 processors. However, over time plain software running on x86 CPUs was no longer enough. Three distinct dynamics forced the company to re-evaluate its initial development strategy: 1) The sophistication and frequency of cyber threats increased exponentially, 2) The number of applications deployed in networks exploded, and 3) the firm's proprietary algorithms became more sophisticated and resource intensive. If the firm was to maintain its lead in the cybersecurity market its approach to signature generation and matching had to be radically rethought.

Cybersecurity Firm Standardizes on Accolade Adapters to Deploy Proprietary Signature Generation & Matching Algorithms

THE SOLUTION

A number of different design options were explored, but ultimately the firm settled on "porting" its algorithms to run on an FPGA since it would provide the needed performance boost and flexibility for signature generation and matching.

Initially the firm surveyed vendors that provide "raw" FPGA boards or in other words just an FPGA on a PCIe adapter with no accompanying intellectual property. This approach was not practical because the firm only had one FPGA designer on staff and couldn't rely on him to do all the design, integration and support work. This left only one option, namely find a full service FPGA adapter vendor that would provide comprehensive integration support services as well as intellectual property for critical functions such as time stamping, packet merging, packet steering and flow classification. With this caveat the field of available vendors was narrowed considerably, but there was still one critical requirement that needed to be met.

Because the signature generation and matching algorithms were a core part of the firm's intellectual property it could not reveal those to any third party (including its end customers) and thus any FPGA adapter it chose had to include the provision for the firm's own design engineer to add FPGA code. It could not initially find a single suitable vendor that would allow someone other than the vendor's own designers to add FPGA code to the adapter. In the end, Accolade was flexible and willing to add custom hooks into the ANIC-40Ku which would permit the firm to add its proprietary FPGA code directly on to the adapter right alongside the FPGA code developed by Accolade's FPGA designers. This was the clinching factor which compelled the firm to standardize on Accolade's FPGA-based, packet capture adapters for its network security monitoring appliances.

The table below details the firm's selection criteria.

CRITERION	REQUIREMENT	ACCOLADE FIT
Custom Functionality	FPGA adapter vendor must create a provision that allows the firm's FPGA designer to add code directly to the adapter	Accolade was flexible and willing to add custom hooks in to ANIC-40Ku to accommodate customer request
Future Proof	Additional custom features may be required in the future	Accolade provided one key custom feature and was willing to provide additional features as needed in the future
Flow Classification	The firm could only provide limited flow classification features due to software limitations	ANIC adapter flow classification was far superior to what the firm could do in software
Cost Effective	The selected solution must meet specific budgetary requirements	The ANIC solution was the lowest cost of all that met every criterion
Zero Packet Loss	No packet loss could be tolerated even with 64 byte packets	All ANIC adapters perform 100% lossless packet capture
Timestamp	Each packet had to be timestamped with nanosecond precision	All ANIC adapters offer nanosecond precision timestamping

Accolade Technology

Headquarters:
124 Grove Street, Suite 315
Franklin, MA 02038

phone: 877 653 1261
email: inquire@accoladetechnology.com
www.accoladetechnology.com