Using Machine Learning (AI) to Detect and Neutralize Threats

Darktrace boosts automated threat detection with Network Critical SmartNA-PortPlus API integration

Summary

Machine learning and AI are changing the game for network security appliances. Not only can new security appliances learn patterns and adapt to changes without human intervention, they respond and report faster because there is no need for manual re-configuration when responding to new challenges. In order to fully realize the promise of AI in security tools, visibility tools need to automatically adapt to requests from security tools without human intervention. The new SmartNA-PortPlus from Network Critical has an integrated API for direct machine to machine communication.

Using Machine Learning (AI) to Detect and Neutralize Threats

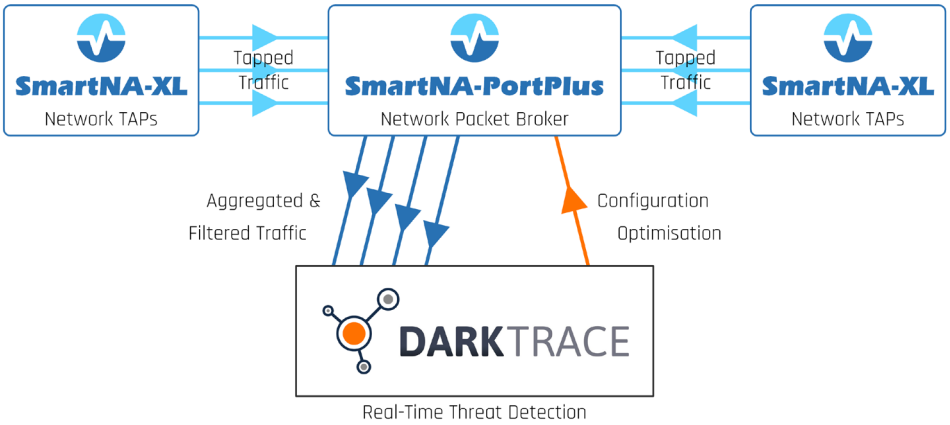
The fundamental technology underlying Darktrace is powered by advanced, unsupervised machine learning, which is capable of learning what is normal and what is abnormal inside a network on an evolving basis, without using training data or customized models. This allows it to detect cyber-attacks that may not have been observed before, the 'unknown unknowns'. The SmartNA-PortPlus packet broker from Network Critical provides a seamless integration that is controlled by software in the Darktrace tool completing a dynamic machine driven visibility and security architecture.

Legacy approaches to cyber security embody the second revolution: people describe what an attack looks like and then ask the computer to look for a match to that description. Darktrace turns this paradigm on its head, embodying the third machine revolution: the computer autonomously finds anomalous areas within large data sets, and makes intelligent judgements accordingly. This self-learning capability is transformative, allowing organizations to embrace interconnected networks, while defending their critical data and reputation. The SmartNA-PortPlus API integration allows the computer to also autonomously control traffic flows from network links picking and choosing the data it needs and eliminating other traffic.

Traffic Filters and Port Maps

Specialized tools that actively capture and monitor network traffic need to be connected to links in order to access traffic. Network Critical's TAPs and Packet Brokers make this connection between network links and monitoring tools, accurately duplicating data flows and passing information to the appropriate tools. Often, however, the tools receive much more traffic data than they actually need or irrelevant traffic data that must be filtered out. Packet Brokers like the SmartNA-PortPlus from Network Critical filter out unnecessary traffic and map only the appropriate network traffic from live links to specific ports on security tools. This greatly enhances the speed, efficiency and cost effectiveness of the security tool.

Network Critical
The Window to your Network™



Typically, port maps determine what traffic is sent to certain ports on tools and traffic filters eliminate irrelevant traffic. Generally, these maps and filters are manually configured and, once set, the configurations remain static until someone changes them.

SmartNA-PortPlus Automates Maps and Filters

The SmartNA-PortPlus provides an integrated Application Programming Interface (API) that allows Darktrace to write software that automatically controls the SmartNA-PortPlus filtering and port mapping functions from the Darktrace tool without human intervention. This integration between Darktrace and the SmartNA-PortPlus allows the intelligence in the tool to control the information that it receives from the network.

Using the integrated API on the SmartNA-PortPlus, Darktrace, can quickly detect and report on traffic anomalies and can automatically adapt to changes in traffic patterns without manual intervention. The Darktrace Enterprise Immune System, uses unsupervised machine learning and Artificial Intelligence (AI) to understand all about an organization. Observing users and devices, cloud containers and workflows, it learns 'on the job' what is normal for the organization. Over time, Darktrace adapts as the organization changes without requiring reconfiguration or tuning. However, in order to automatically adapt responses, the tool must be able to automatically manage the traffic input from the network. Automating and integrating traffic visibility allows Darktrace to fully realize the promise of advanced machine learning technology built into their tool.

The integration between Darktrace and Network Critical creates a complete visibility architecture that is:

- Adaptive - evolves with your organization.
- Self Learning - constantly refines its understanding of normal.
- Probabilistic - works out likelihood of serious threat.
- Real-time - spots threats as they emerge.
- Hands off – the Darktrace tool automatically adapts and updates the traffic flow it receives from the Network Critical packet broker layer, thus increasing its efficiency and improving the overall threat detection capability.

SmartNA PortPlus Overview

The SmartNA-Port Plus provides a scalable range of access and visibility from 48 ports up to 194 ports at speeds of 1/10/25/40 and 100 Gbps connecting critical monitoring and security tools. Packaged in a compact single RU chassis the SmartNA-PortPlus offers immediate value for today and an efficient path to the inevitable adds and changes required for future growth.

Beyond server ready high speed connectivity for security and monitoring tools, the SmartNA-PortPlus is also a feature rich traffic manager. Advanced features such as aggregation, filtering, port mapping and load balancing allow users to leverage their tool investments.

The Drag'n' Vu Graphical User Interface (GUI), is a sophisticated computational engine for configuration and management. In addition to the manual GUI, the SmartNA-PortPlus features an integrated API that allows tool manufacturers to write customized programs that automate many critical filtering and mapping tasks. This integration helps monitoring tools perform more efficiently by providing just the right information to the right port at the right time with no human intervention. The SmartNA-PortPlus API supports standard HTTP communication protocol and JSON data format. These formats are both widely supported by major programming languages and other software, making integration easy. Additionally, the API offers access to all the information and configuration settings supported in the standard GUI.

As monitoring tools advance from manual configuration to machine learning and AI driven dynamic network protection, it is critical that the visibility architecture integrates more closely with the monitoring tools. The Smart NA-PortPlus with integrated API is leading the way to machine driven configuration changes for improved threat response times and more robust network security.

For more information, visit www.networkcritical.com

Network Critical
The Window to your Network™

www.networkcritical.com