nPulse Technologies and McAfee

Delivering Dramatically Shorter Incident Response Times

Network Forensics for the 10Gig World

OVERVIEW

Capabilities

- Capture and index all network traffic for back-in-time analysis
- Quickly pivot from McAfee ESM's security alerts to full packet data
- Reconstruct session-level activity behind an alert
- Determine the nature, extent and duration of successful attacks

Benefits

- Dramatically shorten security incident response and resolution times
- Better understand security incidents to isolate root causes and improve future defenses
- Increase reach and value of existing tools without retraining analysts or changing proven workflow

Results

A seamless integration of two of the leading cybersecurity tools on the market today

YOUR CHALLENGE

In today's sophisticated, dynamic and continually evolving threat landscape, security professionals are well aware that the enterprise is continually targeted. Enterprise networks hold enormously valuable, sensitive, proprietary, confidential information, making them irresistible targets to attackers.

Well-maintained perimeter defenses will stop many of these attacks, but inevitably some will get through. Once a breach is detected, the challenge is to determine the extent of the damage, isolate the means of entry, and patch it to avoid future repeats. It is also critical to know how long the breach has been present, what data may have already left the network, and how many other hosts may already have been compromised.

OUR SOLUTION

nPulse's Capture Probe eXtreme (CPX) is the industry performance leader in packet capture, historical search, and traffic analysis. It delivers the fastest packet indexing solution at up to 30 million packets per second, enabling users to significantly reduce incident response times even when faced with massive-scale searches. The integration through CPX's Pivot2Pcap API with McAfee's ESM provides deeper insight into network traffic and activities through simple drill-down access to captured, indexed and stored connection and packet information on the largest and busiest 10Gbps networks. By allowing McAfee ESM users to quickly locate and decode an entire session, nPulse's CPX provides greater visibility into potential malicious activities and payloads while also eliminating the time required to manually collate all of the packets within the session. With CPX, McAfee customers can expand searches to view network activities before and after a security event, further enhancing visibility that can be crucial for rapid incident response investigations.

By capturing and indexing full packets reliably at extremely rapid speeds, nPulse's CPX platform provides a powerful complement to McAfee's ESM comprehensive security management capabilities. In addition to receiving precise alerts and correlated threat information from McAfee ESM, analysts can also get a fine-grained view of the specific packets and sessions behind a possible attack to confirm what may have happened, to respond rapidly and effectively, and to apply this information to enhancing future protective strategies.

McAfee Enterprise Security Manager

Effective security starts with real-time visibility into all activity on all systems, networks, databases, and applications. McAfee Enterprise Security Manager enables your business with true, real-time situational awareness and the speed and scale required to identify critical threats, respond intelligently, and ensure continuous compliance monitoring. Security teams now have access to real-time, risk relevant information to obtain a stronger security posture while shortening response time.

Advanced risk and threat detection — Enterprise Security Manager connects evolving threat data with a real-time understanding of the risk, asset importance, and security posture throughout the enterprise. This dynamic context, combined with a highly intelligent correlation engine, provides risk scoring and threat prioritization that continually adapts to the enterprise environment.
In addition, available integration with McAfee Global Threat Intelligence (GTI) and McAfee ePolicy Orchestrator (McAfee ePO) software help you detect, correlate, and remediate threats in minutes across your entire IT infrastructure.

McAfee Key Advantages

- Actionable information in minutes instead of hours
- Massive data collection across a wide range of information sources
- Real-time threat and risk data integration and event correlation
- Immediate access to years of event and flow data
- Supports monitoring and reporting against more than 240 regulations
- Integrated tools for improved security workflow
- Flexible, hybrid delivery options include physical and virtual appliances
- High-availability options

CPX Key Advantages

- Continuous, lossless packet capture with nanosecond time-stamping at recording speeds up to 20 Gbps
- Real-time indexing of all captured packets using time-stamp and connection attributes
- Export of flow index in NetFlow v5, v9 and IPFIX formats for use with other flow analysis tools
- Ultrafast search and retrieval of target connections and packets using patent-pending indexing architecture
- Web-based, drill-down GUI for search and inspection of packets, connections, and sessions
- Session decoder support for viewing and searching web, email, FTP, DNS, chat, SSL connection details, and file attachments
- Packet payload search using regular expressions (regex)
- Up to 144 TBytes of traffic recording in one appliance, or expandable to petabytes with fiber-attached storage option
- Data storage and export in industry-standard PCAP format
- Pivot2Pcap RESTful API for integration with customer utilities and other monitoring/security appliances

Policy-aware compliance management — As compliance requirements evolve, so must your SIEM. Enterprise Security Manager makes compliance management easy with hundreds of pre-built dashboards, complete audit trails, and reports for PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, SOX, and others. Full support for the Unified Control Framework also allows you to report your policies against more than 240 global regulations and control frameworks. Critical facts in minutes, not hours — The highly tuned ESM appliance can collect, process, and correlate billions of events from multiple years and keep all information available locally for immediate ad-hoc queries, forensics, rules validation, and compliance.

nPulse Technologies CPX Packet Capture & Analysis

CPX is an ultrafast, multipetabyte traffic recording and analysis platform for Security Operations Center (SOC) environments. The high-speed, continuous recording solution provides deep, fully indexed storage of network traffic for direct analysis or use with other security or monitoring applications. CPX delivers an easily searched, multi-level view of network packets, connections and session data.

Even on the busiest networks, CPX captures 100% of the traffic, time stamping every packet with nanosecond resolution, and extracting flow identification parameters. As traffic is streamed to disk, CPX generates packet connection- and time-based indexes that allow rapid search and retrieval of targeted traffic from many terabytes of capture records.

The browser-based drill-down interface allows remote analysis of selected packets and sessions without the need to export entire PCAP files. All packet data is stored, and can be retrieved, in industry-standard PCAP format. In addition, packets, session data, and extracted files are available via the API in industry-standard formats for thorough analysis by external tools.

About nPulse Technologies, Inc.

nPulse Technologies is the performance leader in network forensics. Leading financial institutions, government agencies, telecommunications carriers and other organizations rely on nPulse solutions to enhance security monitoring, shorten incident response times, and increase returns on existing security investments.

For network forensic analysts looking to significantly reduce incidence response time, nPulse solutions enable expeditious reconstruction of the kill chain. Unlike competitive solutions that are unable to operate at 10Gbps sustained and take hours to analyze network traffic, our solutions are designed to perform at 10Gbps full duplex, capturing, inspecting, and exposing indications of compromise within minutes, all at a fraction of the cost.

For more information, visit www.npulsetech.com.