Flowmon
Networks

Flowmon Packet Investigator

Flowmon Packet Investigator (FPI) is an automated network traffic auditing tool that records and interprets full packet data.

Where flow data is not sufficient, and more detail is needed, the Investigator captures all the packets of traffic surrounding the event for in-depth troubleshooting.

What sets the Investigator apart, is built-in expert knowledge. It not only provides extensive details but automates the analysis, assessing the captured events, looking for error codes, and providing explanations and suggestions for a remedy.

EXAMPLES WHERE FPI CAN HELP

Network connectivity-related issues

Communication blocked by the firewall, destination unreachable, TCP errors, etc.

Malfunction or misconfiguration

Of critical network services such as ARP, DNS, DHCP

Client/server encryption incompatibility

SSL/TLS version, encryption algorithms, certificates, etc.

Application protocol stack issues

HTTP, SAMBA, FTP, IMAP, POP, etc.

90%

of MTTR is spent trying to figure out that there is indeed a problem.

Source: Zeus Kerravala, ZK Research

35%

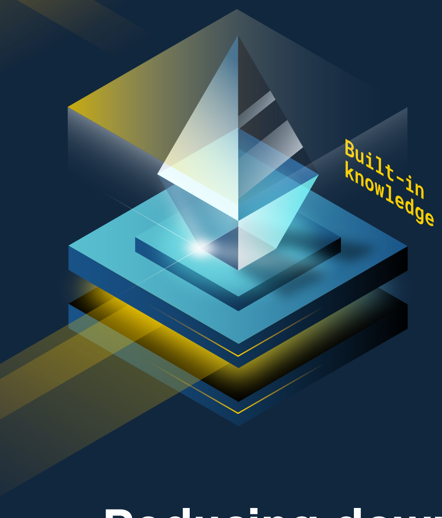
of network management time is spent on reactive troubleshooting.

Source: Network Management Megatrends 2018, EMA

BENEFITS

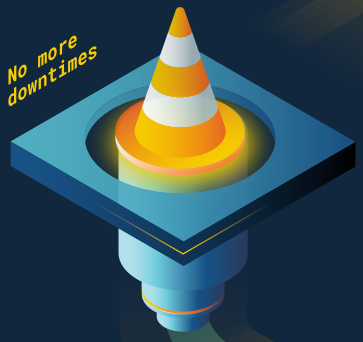
Automating analytics

Autonomous investigation of the root cause of operational issues, saving hours or days.



Expert experience

In-built expert knowledge of error codes, their circumstances, and suggestions for remedial action.

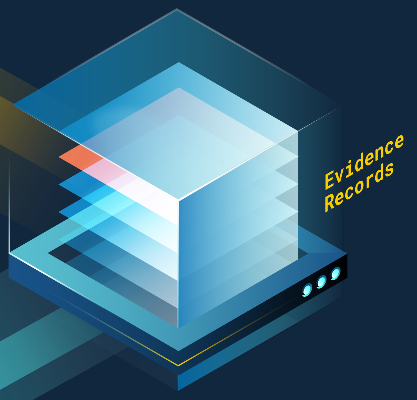


Reducing downtimes

Detect an anomaly, capture and investigate the root cause and get a suggestion for remedial action automatically, in seconds.

Hard evidence anytime you need

Reduce noise by recording only what is essential and store it for post-compromise analysis and auditing.



Reducing # of tools

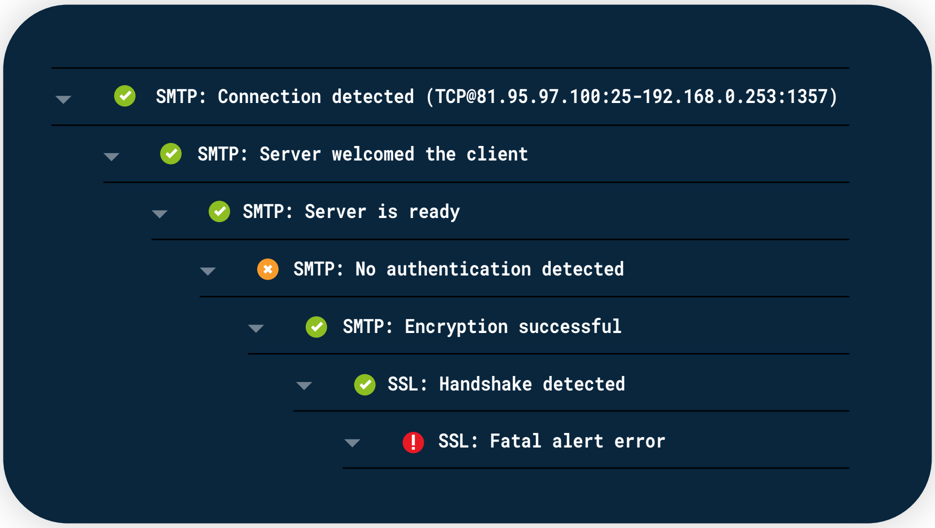
Availability, capacity, troubleshooting, compliance, and forensics - with Flowmon, all under one hood without switching between UIs.

Intelligent Decision-Tree Analysis

The Investigator digests PCAP files, which can be imported or recorded upon event detection, alert or custom trigger. It processes them using an analytical engine to locate the root-cause of operational issues and suggests remedial actions.

Investigation
The PCAPs are automatically analyzed for deviations from the RFC specifications of the respective protocols and their combinations, and any error codes or other failures are recorded. The list of currently supported protocols includes all of the most common services used by enterprises, such as TCP, IP, HTTP/S, IMAP, SMTP, DNS, DHCP, SMB, and many more.

In-built expertise
The Investigator draws on databases of error codes and translates them into a clear message. For example, when a client attempts to negotiate an encryption channel with the server but, due to certificate mismatch, the communication fails.



```
▾ ✓ SMTP: Connection detected (TCP@81.95.97.100:25-192.168.0.253:1357)
    ▾ ✓ SMTP: Server welcomed the client
        ▾ ✓ SMTP: Server is ready
            ▾ ✗ SMTP: No authentication detected
                ▾ ✓ SMTP: Encryption successful
                    ▾ ✓ SSL: Handshake detected
                        ▾ ! SSL: Fatal alert error
```

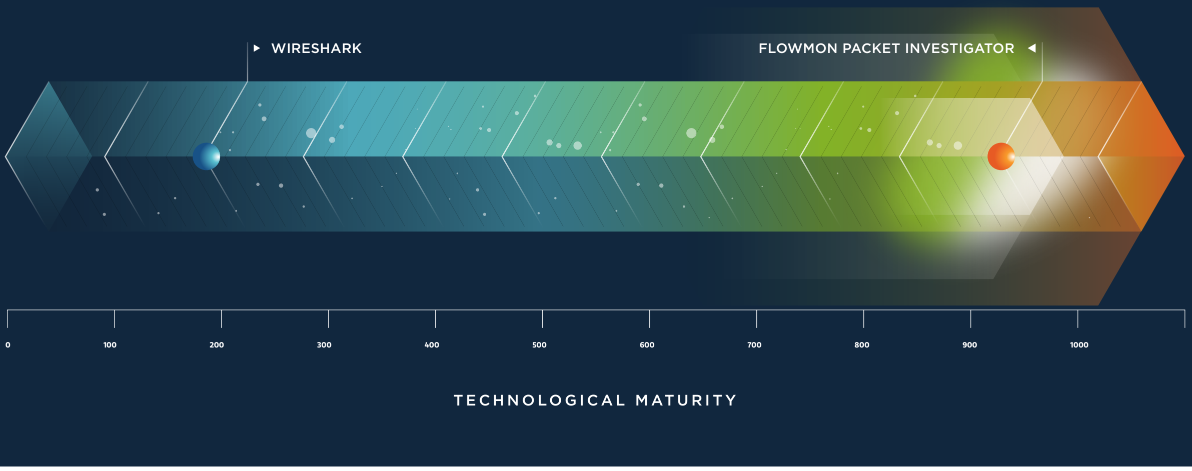
Instant knowledge
The results are presented on a dashboard showing the number of issues and their severity, allowing the user to immediately focus on relevant errors and act without delay.

Flowmon’s team of networking experts with decades of combined experience in the field are constantly working to expand the built-in expertise with interpretations of error codes and suggestions for remedial actions.

FPI vs. Wireshark

Wireshark is the most popular packet analyzer out there. It is available as open-source and is used by millions of users.

Unlike Wireshark, the FPI uses sensors distributed over the network, allowing packet capture to be triggered remotely and at any time and dedicated network sensors allow support of up to 100G speeds. Instead of manual analysis, it uses an analytical engine to process the packets and automatically displays any issues found.
While expert users possess the knowledge to learn all they need using Wireshark, it may be difficult and time-consuming to use for less experienced admins. This is where the FPI comes to its own - it supplies the expertise and automates the labor.



Recording

On-demand capture is a powerful tool that stores relevant packets, even at 100G speeds, instead of capturing everything and consuming resources unnecessarily.

A variety of capturing triggers is available, from planned triggers based on a set of rules like MAC address, IP address, subnet (CIDR), protocol, port, VLAN tag, or MPLS label to manual or fully automated triggers.

Automated trigger
Consider this example: Flowmon ADS detects an Indicator of Compromise where a device is trying to access a domain known for malware distribution. This event triggers packet capture and thus ensures that full packet data is available for thorough analysis.

Rolling buffer
The rolling buffer allows a set of packets per flow to remain buffered for a defined period and recorded on-demand. This approach is a lightweight alternative to continuous packet capture that ensures that no packets are lost.

www.flowmon.com