Progress® | Flowmon

Ransomware

Early detection and response

Stop ransomware in its infancy.
Isolate the problem. Respond with Confidence.

Inability to access critical digital assets can have catastrophic consequences for business operations. Thus, Ransomware is one of the most common, and yet scariest, online assaults.

Flowmon is a network detection and response tool utilizing an AI-powered engine combined with a number of advanced techniques to detect the footprints of an ongoing ransomware attack in its early stages. It helps security leaders to cover visibility gaps by monitoring east/west traffic, understand the problem and respond manually or automatically before the ransomware starts spreading across digital assets and harms the business.

"Thanks to Flowmon we are able to reveal threats and malicious behavior within the internal network. And what is the most important experience - we have significantly reduced incident resolution times."

Vittorio Cimin, CIO of Bricofer

Bricofer

BENEFITS

Cut threat hunting time

Noise-free presentation of events enables real-time threat hunting and convenient post-compromise analysis.

Minimize breach impact

Flowmon monitors and analyzes network traffic to alert you to security compromises at early stages so that you may act before the danger escalates.

Speed up time to value

Streamlined deployment, user enablement, predefined views, dashboards, and reports. From deployment to data on the dashboard in just 30 minutes.

Respond manually or automatically

Understand context, impact, root cause, and priority to respond manually or automatically via integrations with NAC, Firewall, or SIEM systems.

Enhance SSL/TLS visibility

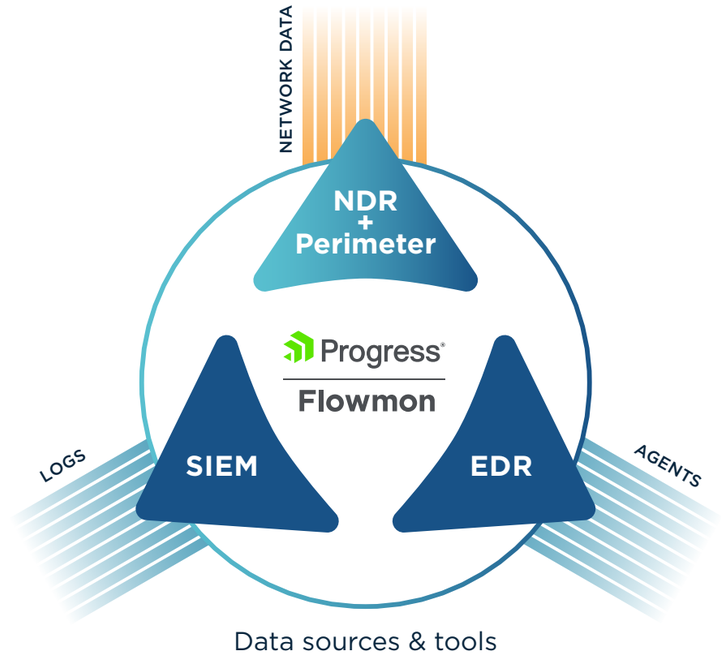
Detect suspicious behavior without decrypting encrypted traffic and inspecting the payload.

Detect and Respond

Due to the spread of BYOD, Internet of Things and cloud adoption, today's infrastructure is sprawling far beyond the perimeter, challenging end-point security tools to provide sufficient visibility. The ever-changing nature of ransomware oftentimes allows it to slip under the radar of the perimeter, bypass end-point security, and get lost in a bunch of false positives or hide in blind spots in network visibility.

This is why security teams turn to a security model that extends log management and end-point protection with network detection and response tools. Known as the SOC visibility triad, this approach compensates for the weak points of its individual parts (EDR, NDR, SIEM) and gives full visibility across complex IT environments. Using these tools together significantly reduces the chance that attackers evade detection and accomplish their goals.

As a leading network detection and response tool, Flowmon is one of the pillars of the SOC triad. It allows IT professionals to switch from "prevent and protect" to an active "detect and respond" approach and fight the risks that bypass signature-based solutions.



Data sources & tools

30 min
From deployment to dashboard insights

Day Zero
Respond to ransomware threats on Day Zero

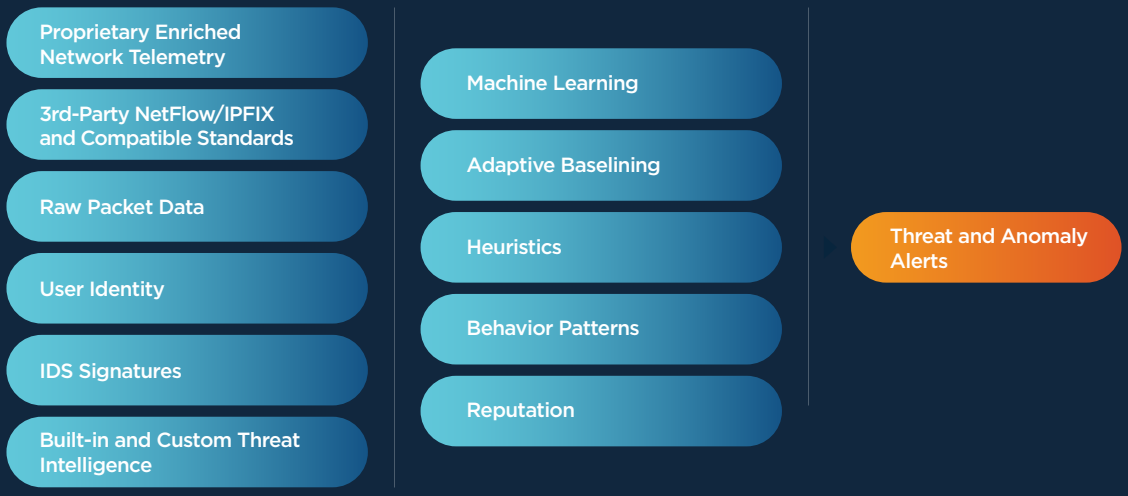
16x
Up to 16x faster time to resolution

Continuous visibility to find indicators of compromise quickly

Flowmon supplies security experts with continuous visibility across networks while detecting anomalies and indicators that point at ransomware attacks. It alerts administrators on abnormal behavior in network traffic, giving them the ability to detect ransomware before digital assets suffer lockdown, trace the attackers' footprints across the system, and respond manually or automatically via integrations with NAC, Firewall, and SIEM systems.

The solution does not use just one detection mechanism, but several, all working at the same time, including machine learning, heuristics, behavior patterns, adaptive baselining, reputation databases, and signature-based detection.

They cover a wide number of scenarios by examining the network from several points of view. For instance, threats that would escape detection by reputation databases will be revealed by entropy modeling. Because the solution uses network traffic metadata for its analysis, it has no problem delivering the same level of detection accuracy in encrypted traffic as well.



WITH FLOWMON, NETWORK AND SECURITY EXPERTS CAN BENEFIT FROM

Automated response
via integration with network access control or firewalls.

Continuous monitoring
of all networks across on-demand, datacenter, cloud, and hybrid infrastructure.

Leading threat detection
that detects atypical behavior that occurs in data streams using various methods.

East-west traffic visibility
to cover gaps left by traditional approaches.

www.flowmon.com