Threat actors constantly modify code and use advanced techniques to hide in network traffic. But they still leave footprints scattered all over the network. Where siloed tools deliver only partial information on breaches, Flowmon’s detection and security analytics make it possible to piece together all anomalies, zone in and get a clear picture of the risk.

Today, security experts look for a technology that observes indicators of compromise at every stage from reconnaissance to lateral movement or data exfiltration, pieces the information together and presents it as one clear picture to help to see which events pose the highest risk and require the most attention.

197 days

The average time to detect a data breach.

Source: 2018 Cost of a Data Breach Study, Ponemon Institute

70%

of the companies would have known about the data breach if they had looked at their logs.

Source: 2019 Data Breach Investigations Report, Verizon

"The Flowmon solution is widely used in our company both by network and security engineers. Everyone receives the most important information necessary for their work."

Source: Unknown
Flowmon shields you from the noise and clutter of data and presents a holistic view of the situation from the network perspective.

The network never lies - external data breaches cannot occur without communication, and not even encryption will hide them.

The solution enables you to respond in early stages of breaches, whether it is a known or unknown malware or a targeted attack. Most importantly it will help you to reduce dwell time and streamline threat detection and response.

**USER BENEFITS**

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

- **Threat hunting time reduction**
  Events are presented in meaningful context to support real-time threat-hunting and recorded in full for convenient post-compromise analysis.

- **Reduction of risk**
  Prevent breaches by identifying non-compliant, high-risk assets.

- **Breach impact minimization**
  Flowmon monitors network traffic to proactively alert on a compromise at an early stage so that breach dwell time can be reduced.

- **Breaking NetOps and SecOps silos**
  Response time is reduced when both teams collaborate on prevention, detection and response.

**FORENSICS**

Flowmon stores full traffic statistics for weeks or even months, and auto-triggers the recording of detected anomalies to provide full packet trace of the event. This provides a wealth of insight about the communication and enables post-compromise analysis of the incident.

**RECOVERY**

Flowmon helps to assess the attack scope and impact to draft a robust recovery plan. This includes identifying parts of the network which were compromised, assets and users affected, and what needs to be re-installed or recovered.

**DETECTION**

Perimeter and endpoint security can only protect against threats of known signature. The rest require a layered security model that can monitor the gap between perimeter and endpoint and pick up early indicators of compromise on the network level.

**RESPONSE**

While the NetOps team will appreciate Flowmon’s data on network structure during sizing, capacity planning or performance management, SecOps teams will use the same data to identify non-approved service traffic. Flowmon helps to assess the attack scope and impact to draft a robust recovery plan. This includes identifying parts of the network which were compromised, assets and users affected, and what needs to be re-installed or recovered.

- **30 min**
  From deployment to dashboard insights

- **Day Zero**
  Respond to advanced persistent threats on Day Zero

- **16x**
  Up to 16x faster time to resolution

**What is considered to be an unknown threat**

The traditional way of detecting threats is based on signatures - a characteristic piece of code that can be recognized by detection software. However, some threats are too new or too rare for the signature to be available.

Malware constantly adapts to outrun the rate at which signature databases can be updated. Similarly, advanced persistent threats and targeted attacks are purposely designed to penetrate the victim’s defences, often with substantial backing from powerful organizations or states.

However, Flowmon does not rely on signatures and has ways of detecting them.
Flowmon does not use just one detection mechanism, but several, all working at the same time. 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.

Once a threat is detected, the user is alerted and can immediately see the event and what it represents in the given context. Such insight is necessary for immediate and deliberate decision-making and prioritization. Flowmon can automatically trigger a response via integration with other security tools to block or quarantine the threat. The event is logged and recorded for full forensic drilldown.

www.flowmon.com