Progress® | Flowmon

Encrypted **Traffic Analysis**

Detect risks in encrypted traffic.
Understand the scope.
Respond immediately.

Encryption is on the rise and for a good reason, too - the protection of customer information and business-sensitive data is of great concern to all businesses today.

Although it is necessary for data protection, encryption creates certain obstacles for security teams, who are still required to protect their networks in spite of the lack of visibility. Moreover, encryption can be used by attackers to mask their intentions, and weak encryption can even be exploited to their advantage. It is estimated that up to 50 % of all known cyber attacks use encryption, and there is universal agreement that encrypted traffic is an important source of security risks.

In spite of this, many businesses still lack the means to monitor encrypted traffic, where up to a half of organizations cannot detect malicious SSL traffic. The Flowmon solution addresses this need and offers the necessary insight while remaining scalable, easily integrable and, most importantly, respectful of privacy.

50%

of all known cyber attacks use encryption to evade detection.

According to IDG Connect

70%

of organizations fear the exposure of sensitive personal data due to decryption

According to IDG Connect

What Encrypted Traffic Analysis does

Flowmon provides administrators with the insight required to counter malware and cyber threats that take advantage of encryption to sneak in. Here are a few examples of what ETA can monitor and detect:

COMPLIANCE	CYBERSECURITY
Expired and non-compliant SSL certificates to show which applications need an update	Malware-infected stations diagnosed by anomalies in SSL parameters
Encryption strength by monitoring key length and algorithm	Malware C&C center communication revealed by JA3 fingerprinting
Unwanted TLS versions that contain vulnerabilities	Man-in-the-middle attacks manifested by unusual or illegitimate certificates
Non-compliant clients accessing unwanted sites discovered by server name identification	Suspicious packet size indicating data exfiltration

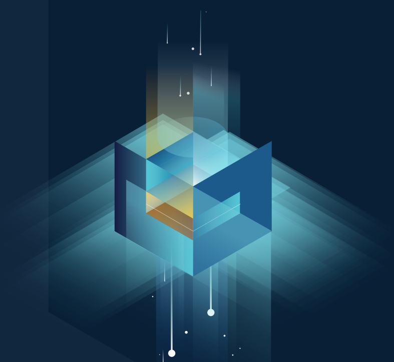
> “Our priority was to improve the visibility of our infrastructure, as in our manufacturing segment network outages automatically lead to financial losses. So we decided that besides the tools such as Cisco Prime we would invest in a flow data monitoring solution.”

Peter Skorvanek
Network Administrator at KIA
Motors Slovakia

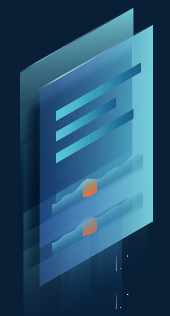
BENEFITS OF ETA

Breach impact minimization
Flowmon monitors network traffic and proactively alerts on potential compromise, so that the breach can be contained in time.

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



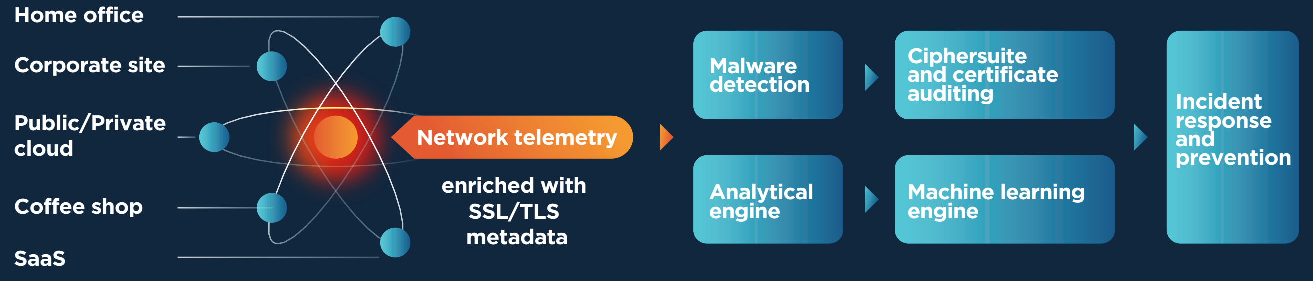
Fast time to value
Streamlined deployment, user enablement, predefined views, dashboards and reports. From deployment to data on the dashboard in just 30 minutes.



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

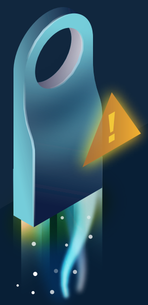
How Encrypted Traffic Analysis works

Flowmon's encrypted traffic analytics collects network traffic metadata in the IPFIX format using passive probes and enriches it with TLS protocol information (among others). These attributes of the encrypted session between clients and servers are available regardless of the client's physical location or whether the server runs in the cloud or datacenter. This provides a wealth of information about the traffic and allows for the identification of out-of-date SSL certificates, policy non-compliant certificates, encryption strength and old TLS versions that may contain faults or vulnerabilities. Furthermore, the solution's machine learning engine uses this data to perform behavior analysis and anomaly detection to identify malware and other threats.

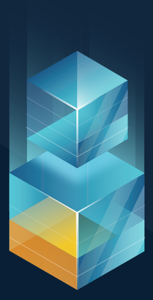


This approach does not violate privacy, nor does it degrade performance. It provides insightful analytics regardless of the volume. Moreover, since the data is stored in aggregated form, it saves a considerable amount of storage space without impeding information fidelity.

FEATURES

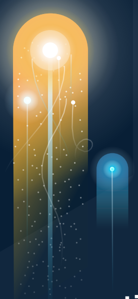


Privacy preserving
Using network traffic metadata does not require decryption and causes no privacy compromise.



Heterogeneous environments
On-premise, remote, hybrid or cloud makes no difference. It provides the same insights.

Zero latency impact
ETA is unobtrusive to the network. It provides monitoring with no impediment to operation.



Reduce response time
Provide an overview of all relevant events and detections without any clutter or information noise.

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

Decrypt or analyze?

Many threats misuse SSL/TLS to mask their activities, and ignoring them is a risk that no organization can afford to take. While decryption is one way of tackling this, it doesn't scale down in terms of cost efficiency and robustness to meet the needs of the majority of organisations. It is not always the most effective approach, nor is it always necessary.
Information about encryption is already contained in the network data and can be used for security and compliance purposes, performance monitoring and troubleshooting. Since this method is passive and scalable, it is particularly well-suited for real-time monitoring.

In short, using metadata:
Preserves privacy / doesn't affect latency / scales with the network / is best practice and value in the majority of cases.

www.flowmon.com