Flowmon

Driving Network Visibility

Don’t forget to include your network in

GDPR Compliance Strategy

The General Data Protection Regulation (GDPR) will strengthen and unify data protection for individuals within the European Union (EU), whilst addressing the export of personal data outside the EU. This directive is very much about processes - some of which inherently need to be supported by technologies. There is no single tool or platform, and incorporating dozens of technologies isn’t the right way to go. Both financially and technically-wise.

Flowmon represents a smart and cost-efficient alternative that helps to fight data breaches with an unprecedented combination of powerful features and ease of use. Read further to learn how to avoid unnecessary penalties, ensure your data security and protect your business critical processes.

DATA BREACHES PREVENTION

ALERT ON ZERO DAY VULNERABILITIES

PROVIDE EVIDENCE FOR DETAILED FORENSICS

RESTORE BUSINESS AS USUAL QUICKLY

www.flowmon.com

Flowmon
Driving Network Visibility

GDPR COMPLIANCE STRATEGY

HOW WILL GDPR AFFECT YOU?

The General Data Protection Regulation will become effective on May 25th 2018. It is set to have an impact on all member states of the European Union, as well as on nations handling the data of EU citizens. As you know from dozens of GDPR related content, it is not about EU-based companies only and the impact of the GDPR is global.

GDPR will impact organizations in two ways as it relates to security and visibility. Companies based in the EU, or companies outside the EU doing business with EU residents:

- need to ensure that their handling of EU residents' personal data, at-rest or in-motion, complies with the GDPR
- must also ensure that no personal data is transported to countries outside of the EU that are deemed to have lower standards, except by design.

www.flowmon.com

FLOWMON ENABLES YOU TO COMPLY

When GDPR goes into effect organizations will have just 72 hours to report detected breaches to the relevant authorities. If not, they can be fined up to €20 million or 4% of total revenue (the higher from those two is applied). However, providing evidence for compromised records in a short time will force companies to have the visibility needed for any investigation. And flow monitoring is an effective way to gain visibility. Of course, network monitoring tools are not a primary tool ensuring GDPR compliance. However, it is a mandatory prerequisite to detect, investigate and report data breaches, as required by GDPR.

APPLY ADAPTIVE SECURITY MODEL TODAY

Unlike traditional flow-based monitoring tools, Flowmon goes beyond L3/L4 traffic monitoring and provides extensive L7 auditing features such as access to websites, file sharing via SMB protocol, DHCP and DNS troubleshooting and others. On the top of monitoring flow data is proactively used to protect your network.

Flowmon brings three strong pillars to your organisation:

- **Quality flow data** - records about all communications across the network enriched with L7 information
- **Powerful intelligence** - network behavior analysis reveals deviations from standard behavior
- **On-demand packet capture** - triggered manually or automatically, provides bulletproof evidence for investigation of security incidents and their subsequent reporting

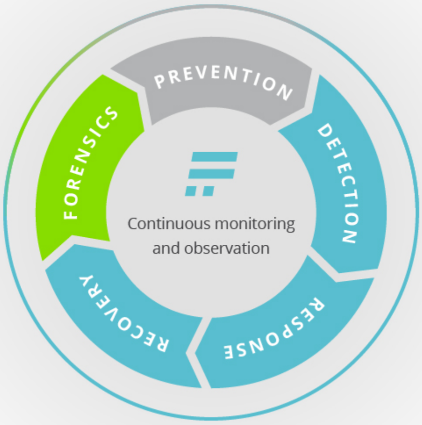
The Gartner security model reminds us that blocking and prevention techniques are not enough today. Organisations must approach security as a well-constructed process to keep up with the growing volumes of clever and automated threats. Flowmon's Adaptive Security Model applies the idea of a constant-learning approach allowing a deep understanding of network behavior.

Computer networks have become a nervous system of every organisation. Paying attention to this part of business IT really pays off. Flowmon solution allows a way not only to detect threats bypassing firewalls and signature-based protection. They also significantly simplify response to new and persistent threats, speed up the recovery process and provide important information for forensics that empowers better prevention. Thus they play a key role in strengthening the entire security circle of an organisation.

PREVENTION
90% of the security budget - mainly perimeter security - where only 25% of attacks target this point in the network.

FORENSICS
Flowmon stores the full statistical history of communication and provides on-demand and auto-triggered recording of detected incidents. It‘s is a reliable source-of-truth and enables you to understand the characteristics of an attack and to discover bottlenecks, predict upcoming attacks and to insure better prevention.

DETECTION
Early detection with Flowmon Anomaly Detection System covers gaps left by standard prevention technologies and represents the people, time, skillset which are lacking to identify a problem before it causes major impacts on company productivity.



RECOVERY
Eliminate unnecessary costs on IT operations and insure time-efficient disaster recovery with Flowmon, which helps you to conduct an assessment of the scope of the attack. This includes understanding what parts of the network have been compromised, what needs to be re-installed, recovered and adjusted. Flowmon enables effective collaboration between all IT teams.

RESPONSE
Fundamental network and security tools that many of us already use in day-to-day operations have the capabilities necessary to block or restrict suspicious traffic. Use the whole potential of such technlogies you have already implemented with Flowmon to provide a flexible incident response at no additional costs.

FLOWMON IS AN ESSENTIAL PART OF YOUR GDPR SECURITY STRATEGY

Flow-based network traffic monitoring tools provide IT professionals with detailed network visibility to streamline troubleshooting, network operations, optimize the performance of an entire IT environment and provide necessary detail for the investigation of operational as well as security incidents.

Flow data provides information from layer 3 and layer 4 which means IP addresses, ports, protocol, timestamps, number of bytes, packets, flags and several other technical details. So you have something like a list of phone calls for each communication in your network. You always know who communicates with whom, when, how long, how often, using which protocol, port, etc. By collecting, storing and analyzing this aggregated information, network administrators, security engineers or operations managers benefit from efficiency and no need to store the payload, which is often encrypted (=useless) nowadays. Besides standard flow data, Flowmon Probes can extend the visibility into L7 protocols such as (HTTP, DNS, DHCP, SMB, VoIP, ...) so the detail is even deeper. And in case packet capture is needed, Flowmon Probe can capture the traffic on-demand or automatically when security event is detected.

Also, using flow data statistics for security opens new possibilities for security engineers. The Network Behavior Anomaly Detection technology provides them with advanced network security monitoring for the automatic detection of suspicious activities, attacks and advanced threats that bypass traditional solutions.
Flowmon Solution helps organizations in network performance monitoring, security, user-experience monitoring and DDoS protection. About half of 700 customers worldwide use Flowmon for network security forensic investigations which is critical for GDPR compliance in pre-incident and post-incident ways:

- Validation that the organization has taken sufficient steps to ensure necessary network visibility for investigation and reporting of security incidents including details. All within 72 hours as expected by the legislation.
- Post-incident investigation using flow data together with on-demand full packet capture data. Both of them provide evidence what data was affected, how and help to identify if intellectual property was compromised.

Support of GDPR-related use-cases is only the tip of the iceberg. Flowmon Solution provides a fully featured NPMD toolset helping IT operations and security teams to ensure a reliable and secure network infrastructure.

OUR CUSTOMERS' EXPERIENCE

As we can see in this example from a real Flowmon customer, it is not only about GDPR compliance. First, it is about protection of your network and your business.

The target organization was a European hospital with over 1500 employees. Naturally, the hospital devoted much energy to the protection of its systems and data. Since it was a modern thinking organization, it had already invested in a next-generation firewall, different email and web filters, end-point data-loss prevention system and antivirus software, network access control and an Active Directory for authentication.

A malicious email was received by an employee bypassing all preventive tools. Using social-engineering the email convinced the user to install Ransomware. This Ransomware spread around the network, including stations that had access to a visual documentation storage system. Among others, this "warehouse" kept all CT and X-ray scans of thousands of their patients. The Ransomware was able to encrypt almost half of the data, preventing doctors to access such a crucial source of information. Doctors could not intervene in patients whose lives depended on the precise estimation of their condition that could only be achieved by body scans. No important decisions on surgeries or treatments could have been taken without a clear understanding of the client's health status.

The customer's detection capabilities focused only on perimeter and end-points, thus creating a vacuum space of no protection in between. Additionally, they utilized only traditional approaches with signatures - ineffective against this new type of Ransomware. Flowmon filled the blank spaces by operating on the network between the perimeter and end-points so it was capable of seeing malicious activity inside the monitored network. The power of an anomaly detection system lies in the fact it does not rely on signatures, and therefore it can discover currently unknown attacks. It will alert you: "This station is acting unusually. It is sending too much data, communicating to different systems, contacting outside IPs, etc." Which is how our customer detected the attack. Thanks to Flowmon's capabilities to identify an unknown attack based on heuristics and advanced anomaly detection mechanisms, the customer could react in a matter of minutes. This early warning, near real-time system saved time for their engineers to detect the root--cause of the problem. Which, without Flowmon, would have taken anywhere from an hour to a whole day.

In addition, Flowmon can orchestrate systems such as Network Access Control (NAC), authentication services, Firewalls, etc. to block or disconnect infected stations from the network so the response can be fully automatized. Flowmon also helps to thoroughly understand the characteristics of an intrusion throughout the whole process and across all IT departments. Based on the investigation, the customer introduced even more restrictive access rights to the storage, and applied rules that would specifically report on this type of incident and preventively block the source of encryption as a fully automated action.

Download free TRIAL and experience how Flowmon can help your organization to comply GDPR.