Application Note

Network Observability: A Critical Tool in Achieving GDPR Compliance and Avoiding Fines

How to Avoid GDPR Compliance Issues Through Network Observability

www.cpacket.com

Highlights

- Learn what is GDPR and why it is important to be GDPR compliant
- Learn why network observability is critical for GDPR compliance
- Learn how cPacket Networks can help companies be GDPR compliant and avoid fines

Introduction

In recent years, the General Data Protection Regulation (GDPR) has garnered significant attention in the business world. This document will dive into some specifics of GDPR, including why it's crucial for both local and international companies to comply with its regulations. Additionally, it explores technical requirements and consequences of non-compliance while highlighting how network observability can aid companies in adhering to GDPR guidelines and avoiding severe penalties.

What is GDPR?

The General Data Protection Regulation (GDPR) is the latest data protection and privacy regulation from the European Union that went into effect on May 25, 2018 (see Diagram 1). It provides a set of standards for protecting individuals' personal data, providing transparency and control over the use of that data.

The GDPR applies to any organization that stores or processes personal data from EU citizens, regardless of geographic location. This means it affects all businesses, both inside and outside the EU, that handle information about EU citizens.

GDPR also sets requirements for organizations on how they must collect, store and share personal data. Some examples of these requirements would include as ensuring that people are informed when their data is collected, maintaining secure systems; limiting retention times; asking for consent before collecting data, and giving people access to their own data if they request it.

Additionally, it requires organizations to notify authorities in case of a data breach and undertake other measures to ensure compliance with GDPR regulations. The GDPR sets out seven key principles: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, Integrity, confidentiality (security), and accountability.

Diagram-1: GDPR Overview

Why Companies Must Comply with GDPR

Every company that does business with the European Union is required to be compliant with the GDPR (General Data Protection Regulation). This regulation was put in place to protect the data of EU citizens and ensure that companies handle, store, and process data in a secure manner.

The GDPR sets forth strict guidelines for how companies should collect, use and manage personal data. Companies need to ensure that they have effective measures in place to protect their customers' information from unauthorized access or disclosure. They must also inform customers about how their information is being used and give them the right to view, delete or request corrections to their records.

The regulation sets out strict rules for how companies must store, process, and use personal data. By adhering to these standards, businesses can provide greater security for sensitive information and reduce the risk of a data breach or other loss of personal data. GDPR also requires companies to update their policies and procedures as needed to remain compliant with new regulations or changes in technology.

Failure to comply with GDPR requirements can result in significant fines or other penalties from supervisory authorities. Therefore, it is important for businesses to take the necessary steps to ensure that they are up-to-date on GDPR regulations and understand how best to meet their obligations under the law.

This document explores how a properly architected network observability platform can help companies avoid costly fines by being GDPR compliant.

Why US Companies Must Comply with GDPR

Although the General Data Protection Regulation (GDPR) is a European Union (EU) regulation, it has far-reaching implications for companies around the world, including those in the United States. The GDPR applies to any organization that processes or handles the personal data of EU citizens, regardless of where that organization is based.

The United States has a patchwork of privacy laws that vary by state. While most states do not yet have comprehensive privacy legislation, some are leading the charge in enacting laws to protect the personal data of their residents. For example, California is at the forefront with its robust Consumer Privacy Act (CCPA) that’s like GDPR. Other states, such as Washington and Nevada, have also passed similar laws which give consumers more control over their personal information. Additionally, certain states such as Maryland have adopted specific industry-specific regulations to ensure businesses operating within the state handle their customers' data properly. It is important for organizations to understand and comply with any applicable regulations in order to protect their customers and avoid costly fines or penalties.

For US companies, complying with GDPR regulations is not only necessary to avoid hefty fines and legal consequences but also to maintain trust and credibility with their customers. With the increasing frequency and sophistication of cyber-attacks and data breaches, consumers are becoming more concerned about how their personal information is being handled and protected.

By complying with GDPR regulations, US companies can demonstrate their commitment to protecting customer data privacy rights. This helps build trust between businesses and their customers, ultimately leading to stronger customer relationships and increased brand loyalty.

GDPR Fines and Penalties

Organizations that fail to comply with GDPR regulations are subject to significant fines. The size of the fine varies depending on the severity of the breach and can range from 10 million euros or 2% of a company's annual global revenue, whichever is higher. In some cases, fines can reach up to 20 million euros or 4% of a company's annual global revenue, whichever is higher. In addition to potential fines, organizations could also face other consequences such as criminal prosecution if there is evidence that data was deliberately mishandled. It is important for companies to ensure compliance with GDPR regulations to avoid any associated penalties or investigations by authorities. Chart 1 below is a list of the top GDPR fines handed out to companies that had GDPR violations.

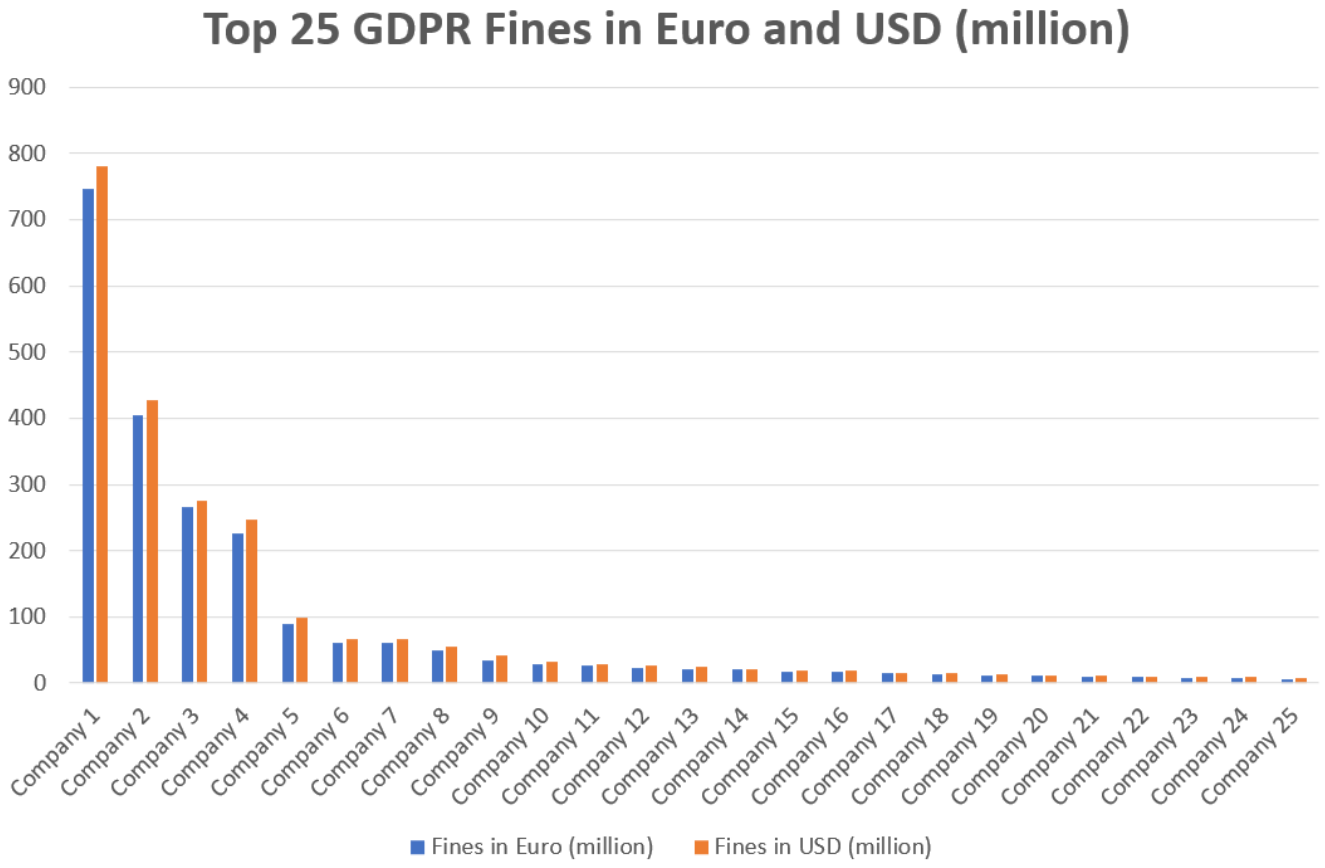


Chart-1: Top 25 GDPR Fines

GDPR is Important to Financial Services Companies

GDPR is a set of regulations designed to protect the data of EU citizens and ensure that organizations that collect such data do so responsibly. This makes GDPR especially critical for financial services companies such as banks, financial services providers, and insurance companies as they often deal with customers' sensitive information.

Financial services companies must secure customer information such as credit card details, financial records, and transactions for several reasons.

Firstly, these types of sensitive information are highly valuable to cybercriminals who can use them for fraudulent activities such as identity theft, credit card fraud, or unauthorized access to bank accounts. This puts customers at risk of financial loss and damages the reputation of the financial services company.

Secondly, financial services companies are legally obligated to protect their customers' sensitive data. There are strict regulations in place such as the Gramm-Leach-Bliley Act (GLBA), Payment Card Industry Data Security Standard (PCI DSS), and the General Data Protection Regulation (GDPR) which require companies to implement appropriate security measures to safeguard customer data.

Thirdly, failure to secure customer information can result in severe financial penalties and legal consequences. In addition to fines levied by regulatory authorities for non-compliance with data protection laws, financial services companies may face class-action lawsuits from affected customers.

Fourthly, securing customer information is essential for maintaining trust between financial services companies and their customers. Customers expect that their confidential data will be kept safe when they entrust it to a financial institution. Any breach of this trust can lead to reputational damage and loss of business.

Under GDPR guidelines, financial services companies must adhere to strict security measures in order to keep customer information secure. This includes implementing encryption protocols, maintaining audit trails, and providing customers access to their personal data upon request. Additionally, these organizations must also be prepared to report on any breach or incident within 72 hours as per GDPR Article 33.

GDPR Technical Requirements

Keeping your networks performing smoothly is essential to ensuring an optimal user experience and keeping revenue losses at bay. Unfortunately, identifying the source of network issues can be a stressful struggle that requires timely resolution. With cPacket's observability solution, IT teams are able to pinpoint problems quickly - whether on-premises, in the data center, or cloud - so downtime is minimized and services run without disruption.

Companies must implement appropriate technical and organizational measures to ensure a secure environment for personal data in accordance with the GDPR. This includes measures such as:

- Encryption of all data at rest and in transit
- Access control systems that monitor who is accessing what information
- Regular vulnerability scanning and malware prevention protocols
- Network segmentation to protect sensitive data
- Privacy by design, ensuring that any new applications or services are compliant with GDPR regulations.

It is essential for companies to assess the security risks they face and take the necessary steps to protect personal data while meeting all requirements of the GDPR. The notification must include all relevant details about the breach, including its nature, the categories of personal data affected, and the measures taken to mitigate potential harm. Companies must also provide individuals with timely update notifications if more information becomes available after reporting.

Network Observability is Critical for GDPR Compliance

Network observability is an important component of compliance with GDPR regulations. This type of monitoring helps organizations gain the visibility they need to better manage and protect their data. Network observability provides a continuous overview of the data traffic within an organization's network, allowing them to detect activities that may be noncompliant with GDPR regulations such as unauthorized access or data leakage.

It also helps organizations quickly identify any technical issues that may negatively impact their network, ensuring they can take appropriate action as soon as possible. With comprehensive network observability solutions in place, businesses can ensure that they are adequately protecting users' personal information while meeting all requirements of the GDPR.

Network Packets are the Single Source of Truth for GDPR Compliance

Network packets are the most fundamental form of data in any network observability platform. These small chunks of data carry a wealth of information and can be used to analyze network activity, detect suspicious behavior, identify performance issues, and more. Network packets are the single source of truth for many GDPR compliance requirements.

By leveraging packet-level visibility, companies can satisfy GDPR requirements while protecting the privacy of customers and employees.

Accurate Network Information is Essential

Accurate network information is essential for GDPR compliance. This means for any proper analysis of network activities, there can't be missing network packets due to drops or network blind spots where network packets aren't being captured. Without accurate network data, companies may not be able to accurately identify and protect personal data that is stored or processed in their networks. Additionally, if there is inaccurate information about the structure of the network, it can make it difficult to ensure that all security measures are being implemented properly and consistently.

Accurate network information is also critical for troubleshooting problems, as inaccurate information can lead to misdiagnosis and missed opportunities to prevent breaches from occurring. Inaccurate data can also cause issues with reporting obligations as required by GDPR regulations – if companies don't have a clear picture of what data they possess, they may not be able to provide complete and accurate reports to regulators.

Packet Loss and Network Blind Spots are Detrimental to Network Observability Solutions

When it comes to cybersecurity, GDPR compliance requires organizations to have access to complete network packet data for analysis in order to identify potential issues. However, packet loss can compromise the integrity of this data and make it harder for cybersecurity tools to perform their job properly. Packet loss is a huge issue in large enterprise networks as it can occur due to congestion or even due to faults in the underlying infrastructure. This means that any gaps or lost packets could mean that critical network data is not collected, leaving organizations vulnerable to security breaches.

Incorrect or incomplete network information can create legal risks since companies are responsible for the accuracy of their networks. If the wrong data is collected or used, organizations could face penalties or other repercussions from regulators due to their failure to comply with GDPR requirements.

Historical Network Packet Data is Critical After a Cyber Security Breach

Cyber security is an important component of GDPR compliance. The regulation aims to protect the privacy and personal data of individuals within the European Union (EU). Cyber attacks, such as data breaches, can compromise this sensitive information, leading to severe consequences for both businesses and individuals.

The availability of historical network packet data after a cyber security breach is critical for post-breach analysis. By having this data, organizations can go back through their networks and identify any patterns or activities that may have caused or been associated with the breach. With this information, they can get a better understanding of the attack vector used, as well as how far into their networks the attacker was able to get. This will also allow them to isolate any compromised systems and shut down any malicious activity quickly.

Having full packet capture provides organizations with forensic evidence that can be used to help track down and prosecute attackers. In addition, having access to accurate historical network packet data allows organizations to review their security measures and make changes if necessary, in order to ensure that similar incidents do not occur in the future.

Companies Need the Right Network Observability Solution

To ensure GDPR compliance and avoid network blind spots, companies need a network observability solution that can provide visibility into all aspects of their network. This solution should be able to monitor traffic in and out of the network without network blind spots and without any packet losses. It should also have the ability to detect any suspicious activity that could indicate unauthorized access or sharing of personal data.

The observability solution should also offer comprehensive reporting features so companies can easily generate reports for regulatory bodies if needed.

With a robust network observability solution in place, organizations can reduce blind spots while meeting GDPR compliances and protecting the privacy of customers and employees.

cPacket Network Observability Solution Can Help Companies Save Money by Avoiding GDPR Fines

cPacket Networks Network Observability solution is an invaluable tool for companies looking to avoid hefty non-compliance fines as outlined by GDPR. The platform provides a comprehensive, packet-level view of traffic flowing through the network, enabling organizations to detect suspicious activity and potential malicious actors quickly.

With its on-premise, data center, and multi-cloud network observability capabilities (see Diagram 2), IT teams can capture and store network packets anywhere without any network blind spots. This is critical for GDPR compliance as having complete historical packet data for analysis is essential to identify any potential issues that may exist.

Furthermore, cPacket's network observability platform allows organizations to visualize and monitor the network at scale so they can get real-time insights into their infrastructure and detect any suspicious activity quickly. These advanced network observability tools are especially important for financial services companies looking to meet GDPR compliances.

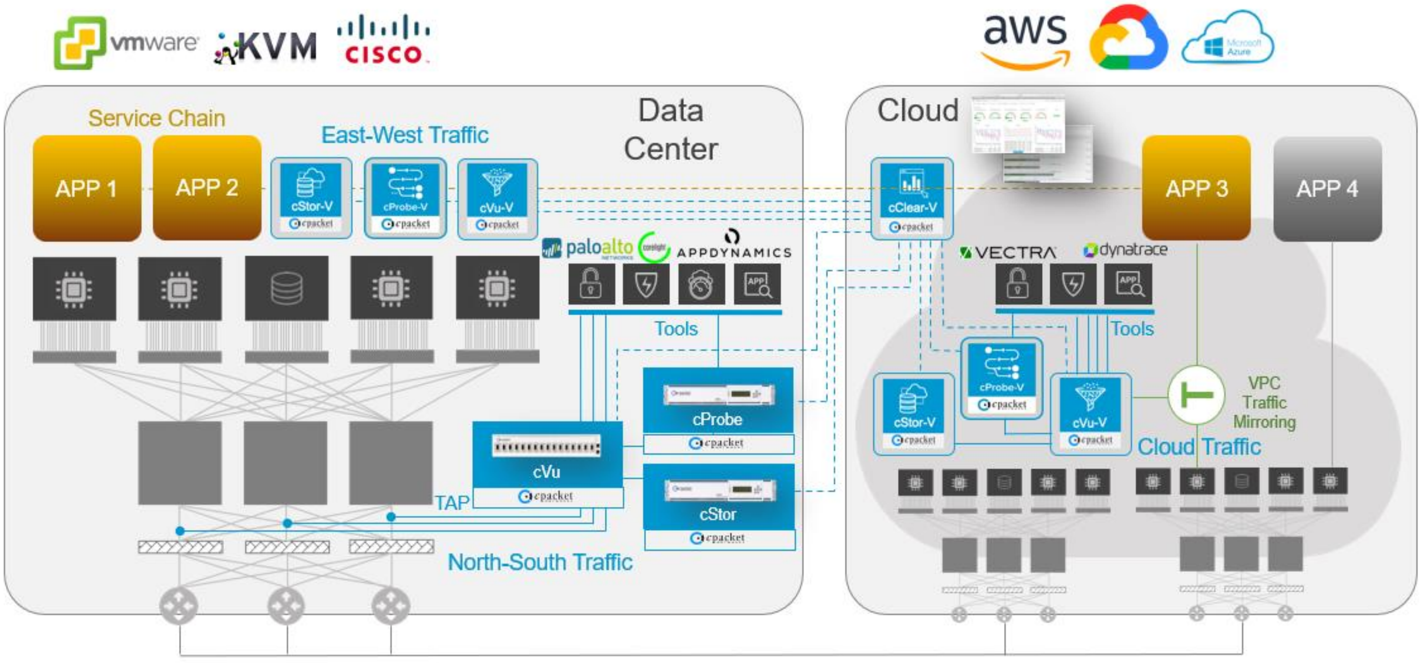


Diagram 2: cPacket Observability Platform

How cPacket Can Help Companies Be GDPR Compliant

cPacket network observability solution (see Diagram 3) offers the following key advantages for companies looking to be GDPR compliant:

- Powerful indexing capabilities for massive amounts of network packets
- Industry-leading fast search function allowing network administrators to locate network packets related to a breach in the shortest time possible
- Prevent cybersecurity incidents before they occur
- Packet slicing makes security tools more efficient
- Packets can be exported in a standard format to freely available network packet analysis tools like Wireshark
- Open API means cPacket products easily integrate with third-party network monitoring and security tools

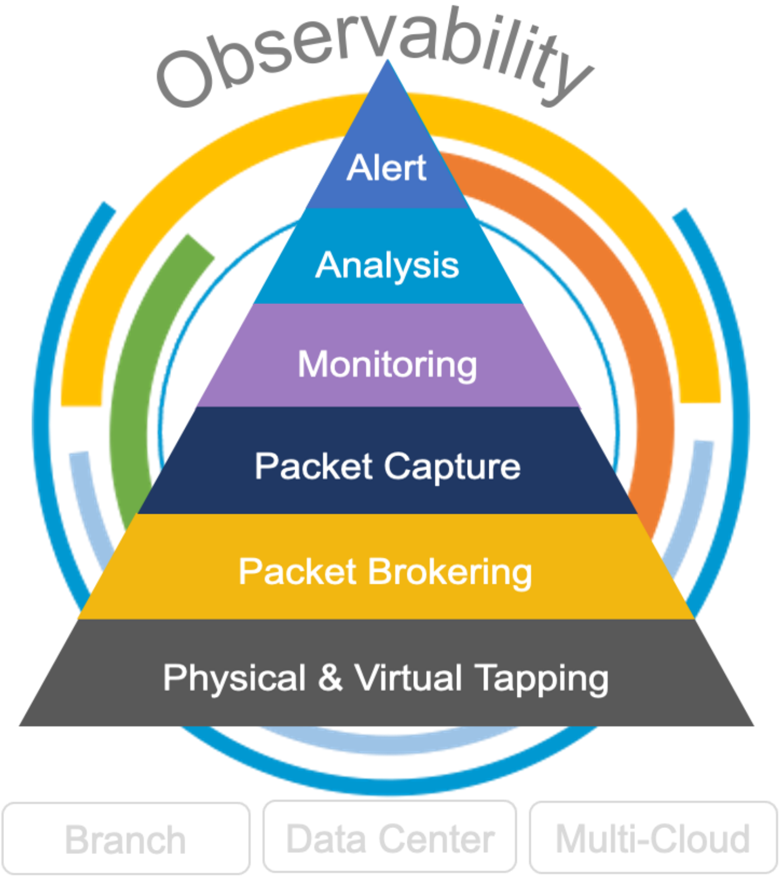
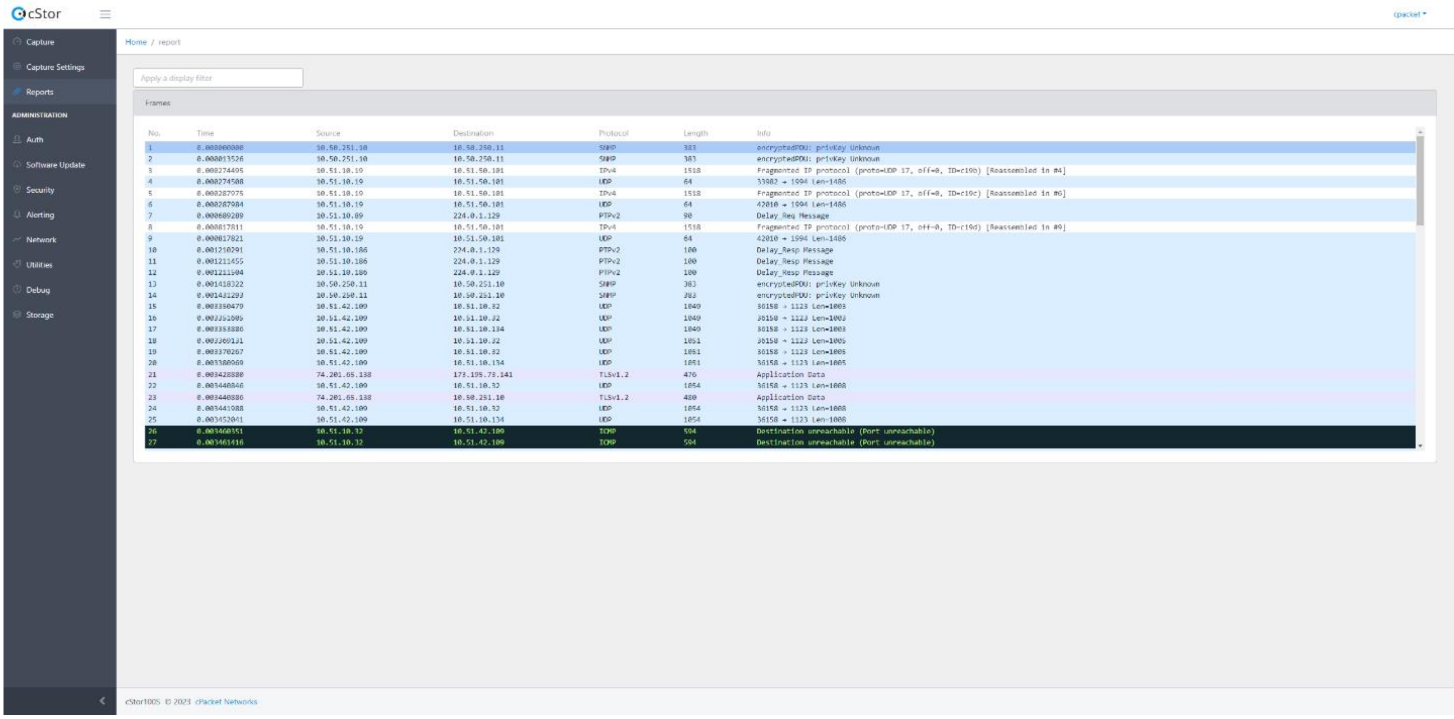


Diagram 3: cPacket Networks Observability

Organize Massive Amounts of Network Packets Quickly

Unlike other network observability solutions that can drop network packets due to the inability to handle traffic bursts, cPacket's network packet capturing and storage solution is an ideal tool for capturing network packets without packet losses. This solution uses advanced packet-capture technology at up to 100 Gbps to capture all information within a network, including application traffic, metadata, and even encrypted data. In addition, this solution will organize all the network packets captured from all the cStor packet capturing servers so they are time-synced for fast search.

Moreover, cPacket's network packet capturing and storage solution (see Diagram 4) also provides organizations with an efficient storage system that compresses large volumes of data into manageable files for archiving or analysis. The system also allows administrators to select which sets of packets need to be saved or discarded based on criteria such as protocol type or IP address. This helps ensure that all important packets are captured without wasting precious storage space or impacting performance.



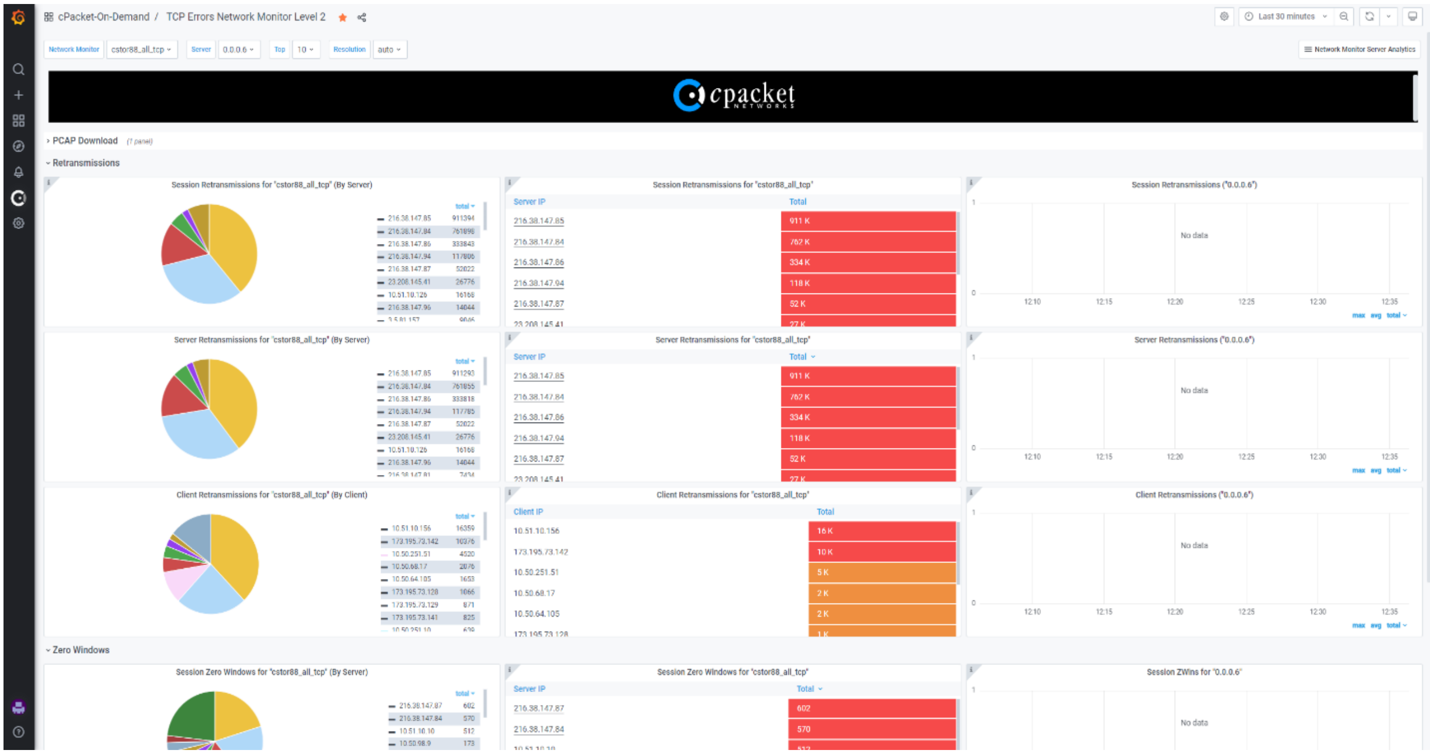
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.50.251.10	10.50.250.11	SNMP	383	encryptedPDU: privKey Unknown
2	0.000013526	10.50.251.10	10.50.250.11	SNMP	383	encryptedPDU: privKey Unknown
3	0.000274495	10.51.10.19	10.51.50.101	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=c19b) [Reassembled in #4]
4	0.000274508	10.51.10.19	10.51.50.101	UDP	64	33982 → 1994 Len=1486
5	0.000287975	10.51.10.19	10.51.50.101	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=c19c) [Reassembled in #6]
6	0.000287984	10.51.10.19	10.51.50.101	UDP	64	42010 → 1994 Len=1486
7	0.000689209	10.51.10.89	224.0.1.129	PTPv2	90	Delay_Req Message
8	0.000817811	10.51.10.19	10.51.50.101	IPv4	1518	Fragmented IP protocol (proto=UDP 17, off=0, ID=c19d) [Reassembled in #9]
9	0.000817821	10.51.10.19	10.51.50.101	UDP	64	42010 → 1994 Len=1486
10	0.001210291	10.51.10.186	224.0.1.129	PTPv2	100	Delay_Resp Message
11	0.001211455	10.51.10.186	224.0.1.129	PTPv2	100	Delay_Resp Message
12	0.001211504	10.51.10.186	224.0.1.129	PTPv2	100	Delay_Resp Message
13	0.001418322	10.50.250.11	10.50.251.10	SNMP	383	encryptedPDU: privKey Unknown
14	0.001431293	10.50.250.11	10.50.251.10	SNMP	383	encryptedPDU: privKey Unknown
15	0.003350479	10.51.42.109	10.51.10.32	UDP	1049	36158 → 1123 Len=1003
16	0.003351605	10.51.42.109	10.51.10.32	UDP	1049	36158 → 1123 Len=1003
17	0.003353886	10.51.42.109	10.51.10.134	UDP	1049	36158 → 1123 Len=1003
18	0.003369131	10.51.42.109	10.51.10.32	UDP	1051	36158 → 1123 Len=1005
19	0.003370267	10.51.42.109	10.51.10.32	UDP	1051	36158 → 1123 Len=1005
20	0.003380060	10.51.42.109	10.51.10.134	UDP	1051	36158 → 1123 Len=1005
21	0.003428880	74.201.65.138	173.195.73.141	TLSv1.2	476	Application Data
22	0.003440846	10.51.42.109	10.51.10.32	UDP	1054	36158 → 1123 Len=1008
23	0.003440886	74.201.65.138	10.50.251.10	TLSv1.2	480	Application Data
24	0.003441988	10.51.42.109	10.51.10.32	UDP	1054	36158 → 1123 Len=1008
25	0.003452041	10.51.42.109	10.51.10.134	UDP	1054	36158 → 1123 Len=1008
26	0.003460351	10.51.10.32	10.51.42.109	ICMP	594	Destination unreachable (Port unreachable)
27	0.003461416	10.51.10.32	10.51.42.109	ICMP	594	Destination unreachable (Port unreachable)

Diagram 4: cPacket cStor Packet Capturing

Industry-Leading Network Packet Fast Search Function

The ability to quickly and accurately sort through network packets is essential in any post-breach incident analysis, especially when it comes to meeting GDPR's 72 hours deadline requirement. Unlike other solutions that might take hours to sort through massive amounts of network packet data, cPacket's cClear (see Diagram 5) and cStor products provide the perfect solution for organizations looking to identify the source of any security breach or policy violation.

Both solutions come equipped with a powerful quick search function that allows security teams to immediately locate the relevant network packets, significantly reducing the time needed for a full investigation. This allows companies to quickly act on any incidents, minimizing potential damage and preventing costly fines associated with non-compliance.



Network Monitor: cstor88_all_tcp | Server: 0.0.0.6 | Top: 10 | Resolution: auto

Session Retransmissions for "cstor88_all_tcp" (By Server)

	total
216.38.147.85	911394
216.38.147.84	761898
216.38.147.86	333843
216.38.147.94	117806
216.38.147.87	52022
23.208.145.41	26776
10.51.10.126	16168
216.38.147.96	14044
3.5.81.157	9046

Session Retransmissions for "cstor88_all_tcp"

Server IP	Total
216.38.147.85	911 K
216.38.147.84	762 K
216.38.147.86	334 K
216.38.147.94	118 K
216.38.147.87	52 K
23.208.145.41	27 K

Session Retransmissions ("0.0.0.6")

Server Retransmissions for "cstor88_all_tcp" (By Server)

	total
216.38.147.85	911293
216.38.147.84	761855
216.38.147.86	333818
216.38.147.94	117785
216.38.147.87	52022
23.208.145.41	26776
10.51.10.126	16168
216.38.147.96	14044
216.38.147.81	7434

Server Retransmissions for "cstor88_all_tcp"

Server IP	Total
216.38.147.85	911 K
216.38.147.84	762 K
216.38.147.86	334 K
216.38.147.94	118 K
216.38.147.87	52 K
23.208.145.41	27 K

Server Retransmissions ("0.0.0.6")

Client Retransmissions for "cstor88_all_tcp" (By Client)

	total
10.51.10.156	16359
173.195.73.142	10376
10.50.251.51	4520
10.50.68.17	2076
10.50.64.105	1653
173.195.73.128	1066
173.195.73.129	871
173.195.73.141	825
10.50.251.10	639

Client Retransmissions for "cstor88_all_tcp"

Client IP	Total
10.51.10.156	16 K
173.195.73.142	10 K
10.50.251.51	5 K
10.50.68.17	2 K
10.50.64.105	2 K
173.195.73.128	1 K

Client Retransmissions ("0.0.0.6")

Session Zero Windows for "cstor88_all_tcp" (By Server)

	total
216.38.147.87	602
216.38.147.84	570
10.51.10.10	512
10.50.98.9	173

Session Zero Windows for "cstor88_all_tcp"

Server IP	Total
216.38.147.87	602
216.38.147.84	570
10.51.10.10	512

Session ZWins for "0.0.0.6"

Diagram 5: cPacket cClear

Prevent Cybersecurity Incidents Before They Occur

cPacket Network Observability platform is an innovative tool that helps organizations stay ahead when it comes to cybersecurity. With this platform, organizations can detect potential security breaches before they happen and take the necessary steps to prevent them from occurring. It provides comprehensive visibility across the network, giving IT teams real-time insights into areas that could potentially be vulnerable and allowing them proactively address any issues.

Furthermore, cPacket's Network Observability platform offers powerful analytics capabilities for deep packet inspection and analysis so organizations can quickly identify suspicious activity and determine if there are any possible risks in their infrastructure. With all these features, cPacket's Network Observability platform can help organizations strengthen their cybersecurity posture, improve overall efficiency, and reduce security incidents.

Packet Slicing Can Make Security Tools More Efficient

The cPacket network observability solution provides administrators with the ability to configure simple packet slicing that removes payload from packets at predefined or user-defined offsets, which can be enforced on a port level or port group. Additionally, Smart filters can be set up to select packets that match specific IP addresses, ports, protocols, or other patterns in the header or payload.

The 'Special Action Filter' feature is another unique and powerful tool available in cPacket's solution. It ensures granular traffic pruning for performance monitoring and network troubleshooting needs by utilizing cPacket's innovative Smart Filter technology. This technology allows full packet inspection of every byte in both the header and payload at wire-speed, making dynamic truncation an easy and more powerful alternative to simple packet slicing at fixed offsets.

Dynamic truncation is another innovative cPacket feature which removes TCP or UDP payloads while leaving the header intact, which makes it ideal for removing Personally Identifiable Information (PII) for GDPR compliance or other compliance purposes in finance and healthcare industries. By doing so, cPacket's solution only passes relevant packet data to upstream security tools, making them more efficient since they process only packet headers without sensitive personal information. Furthermore, packets can be stored without sensitive payload information for compliance purposes.

cPacket Can Supercharge Network Analysis Tools like Wireshark

As network operators, it is crucial to protect the privacy of personal data transmitted across networks. Failure to do so can result in hefty fines under the General Data Protection Regulation (GDPR). This is where Wireshark comes in as a valuable tool for network operators.

Wireshark is a widely popular open-source network analysis tool that enables users to monitor and troubleshoot network packets in real-time or offline. cPacket’s cStor has Wireshark built into the platform for instant access and quick analysis of network packets.

Additionally, cClear and cStor offer extensive customization options for packet capture settings such as protocol type or IP address which allows users to optimize their resources by selecting exactly what needs to be saved or discarded.

cClear and cStor can export network packets into a standard PCAP format. The exported PCAP files can then be easily imported into Wireshark so administrators can gain further insight into the current state of their networks and take necessary actions to reduce potential security threats or improve performance.

Benefits of cPacket's Integration with Third-Party Cybersecurity Tools

In today's fast-paced business environment, cybersecurity is an indispensable aspect of operations. With cyber threats becoming increasingly sophisticated, it's crucial to have reliable cybersecurity tools in place. However, the effectiveness of a cybersecurity tool depends on the network packets available for analysis. Packet capture is a critical element of network security as it enables administrators to monitor and analyze network traffic for potential threats.

Many packet-capturing solutions struggle with high volumes of traffic or sudden bursts leading to packet drops that compromise stored data. Fortunately, cPacket's high-performance solution offers a comprehensive packet capture solution that captures packets at wire-speed up to 100 Gbps without any loss even during periods of high traffic volume or sudden bursts. This ensures that all relevant data is captured and analyzed in real time for effective threat detection and response.

cPacket's Network Observability tools are designed to integrate seamlessly with third-party network monitoring and security solutions via standard APIs (see Diagram 6). This integration allows organizations to monitor their networks using their choice of cybersecurity tools, providing a comprehensive view of the current state of their networks. Additionally, users can customize alert conditions, such as setting up notifications when certain criteria are met - like an unexpected spike in traffic or intrusion attempts.

Security tools often charge companies for the total amount of bandwidth sent to them, regardless of whether it includes relevant packets or not. cPacket's Network Observability solutions provide a cost-effective alternative as they allow organizations to filter out irrelevant packets and only send the required ones for analysis. This helps them save on bandwidth consumption, leading to improved resource management and cost reduction. With this feature, companies can also ensure greater efficiency while staying compliant with GDPR rules and regulations.

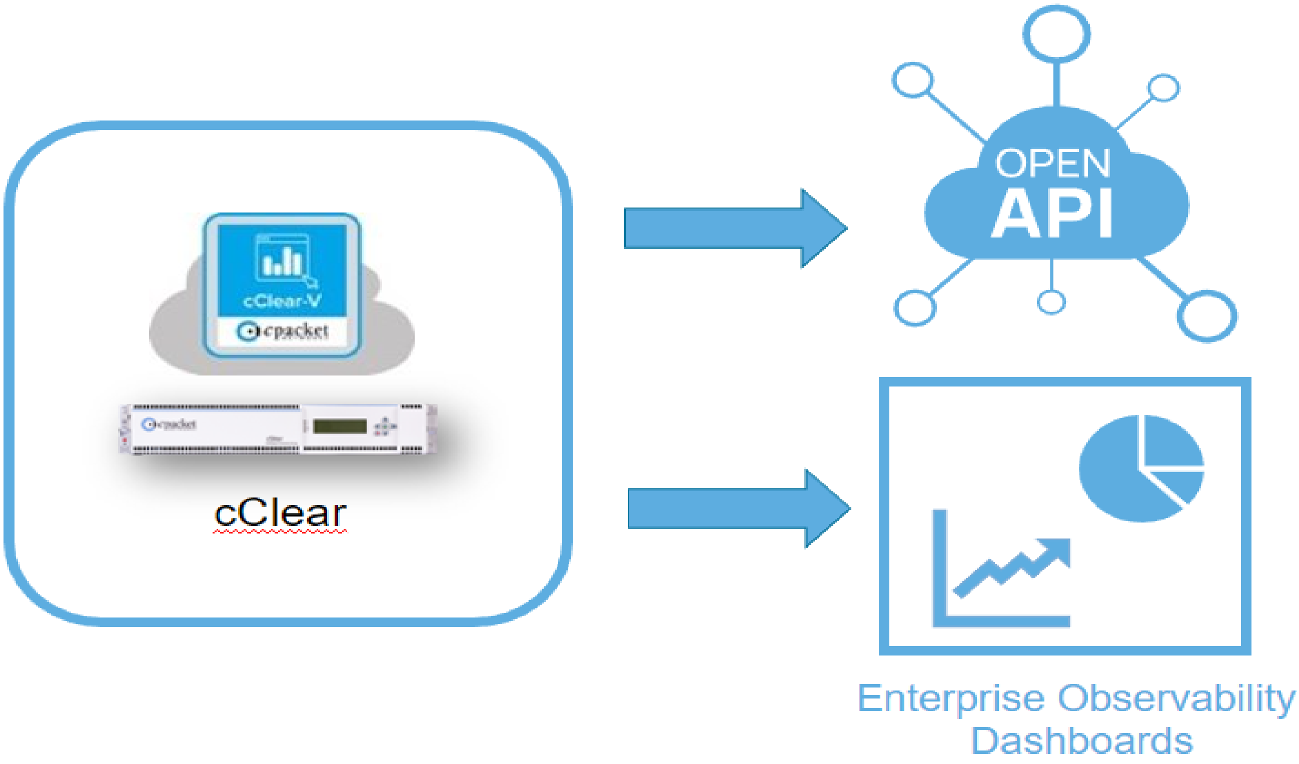


Diagram 6: cPacket Integration with Third-Party Tools

Conclusion

cPacket's network observability platform is an effective solution for organizations looking to avoid GDPR non-compliant fines by identifying security vulnerabilities before any cybersecurity breaches occur. By utilizing its advanced packet-capturing capabilities, cPacket can provide companies with all the necessary historical packet data for post-breach analysis, which can help them identify and address any issues that may have led to the breach. This not only helps companies save money by avoiding or reducing GDPR non-compliant fines but also enables them to improve their overall security posture. Furthermore, cPacket's packet-capturing solution provides companies with complete visibility into their networks, allowing them to quickly detect and respond to any potential security threats in real time.

Please contact cPacket today to get more information. We look forward to hearing from you.