ixia
A Keysight Business

We Make
Networks
Stronger

IXIA AND THE EU GENERAL DATA PROTECTION REGULATION:

This Decade's Y2K

"Security should be based on a risk assessment, however, not of the risks the organization faces, but the risks for the **rights and freedoms of natural persons**."—GDPR (paraphrased)

The GDPR is complex and evolving. Although there are no easy solutions to address all of the requirements, using Ixia products and solutions can help put you in the best position to meet the security standards.

GDPR At-a-Glance

The European Union (EU) General Data Protection Regulation (GDPR), as of May 2018, will lead to a greater degree of data protection harmonization for individuals across the EU. Organizations began the transition to GDPR compliance in 2016 and have until May 25, 2018 for full implementation of measures needed to comply. Ixia products can help ensure that customers' visibility architectures facilitate compliance, either on-premises, within the cloud, or as a hybrid deployment.

GDPR will impact organizations in two ways as it relates to security and visibility. First, companies that are based in the EU, or, if outside the EU, are doing business with EU residents, will need to ensure that their handling of EU residents' personal data, at-rest or in-motion, complies with the GDPR. They 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.

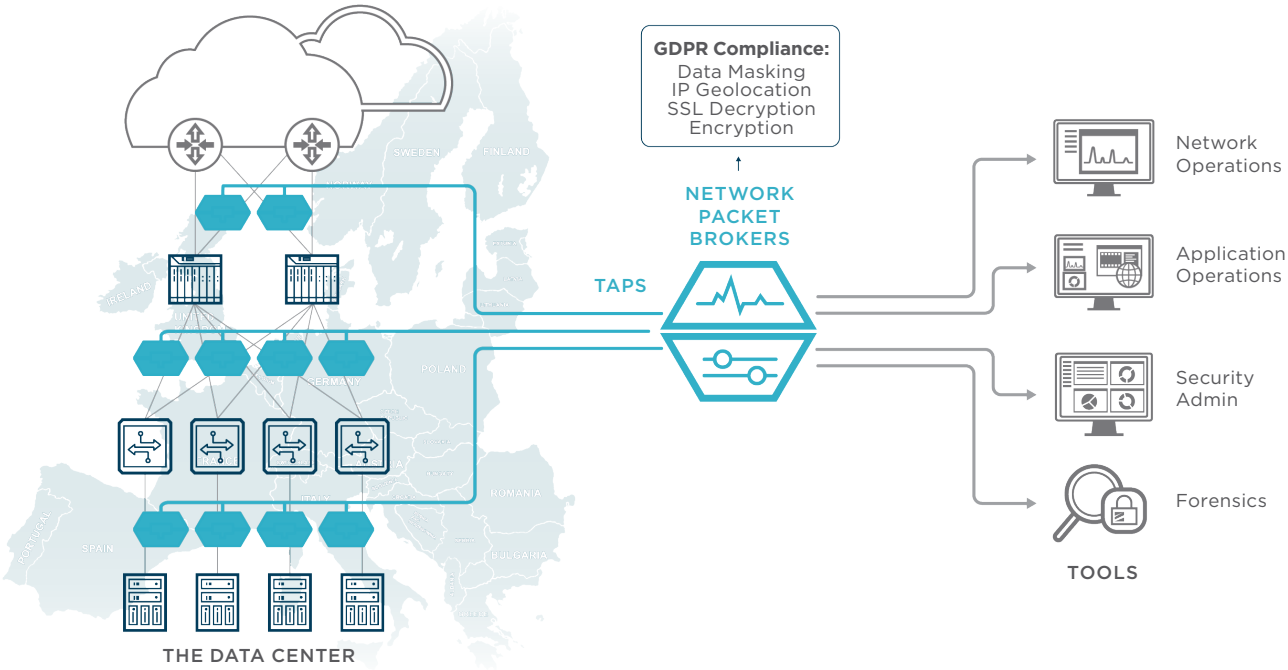
This, of course, implies advanced planning. For example, employees of an EU-based company may be pointed to non-EU Software as a Service (SaaS). This requires that the organization have confidence in the security of the SaaS application. And, the term “personal data” is wide-ranging, relating to any private or professional data, including names, addresses, photos, email addresses, bank details, social postings, medical information, or, in some cases, even Internet Protocol (IP) address.

GDPR Impact on Visibility Architectures

The GDPR will have a major impact on the types of personal data that may be collected and recorded, as well as where this data can go. Any visibility architecture must ensure that a company knows which countries their data is going to, and if the data is not encrypted, must make doubly sure that it is protected. On-premises and private cloud architectures will probably be the easiest to handle. Under the GDPR, one basic precept is that businesses implement technical and organizational measures to provide appropriate protection to the personal data they hold or process. Protection standards outlined in the GDPR include pseudonymization or encryption, where possible, to reduce privacy risks.

LEARN MORE

IXIA VISIBILITY ARCHITECTURE



Ixia GDPR Compliance Visibility Architecture for a Physical Data Center

The fact that IP addresses can be considered personal data adds a wrinkle to this. In some ways, this almost turns traditional approaches to visibility upside down, since, instead of opening up the network to further analysis with increasingly powerful tools, a balance is now required in restricting the flow of confidential data. In implementing a visibility architecture, IP addresses should be protected. Ixia already has a solution for this with its AppStack capabilities, which includes the Data Masking Plus feature, available on the Ixia Vision network packet brokers (NPBs). The technology to deliver these capabilities is either built in on Vision NPBs or delivered through a software module.

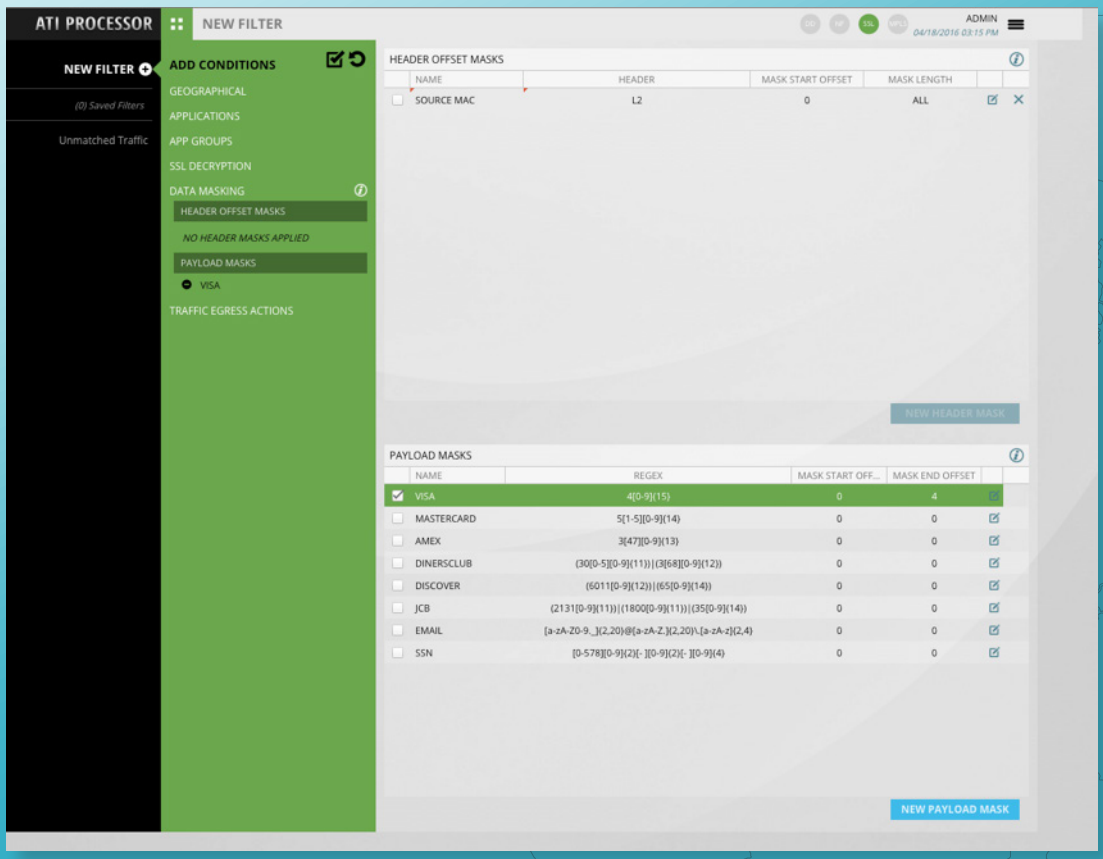
LEARN MORE

NETWORK VISIBILITY

Data Masking Plus was originally developed to secure Personally Identifiable Information (PII) data but is ideal for GDPR compliance. The administrator can set any data pattern or offset for masking, such as a credit card record, a Social Security number, or the IP address, with a simple, best-in-class graphical user interface (GUI). AppStack also supports geolocation of user data, which further helps identify traffic originating in the EU. Data masking and geolocation combined with or without encryption of the data itself will help facilitate GDPR compliance.

LEARN MORE

SECURITY REPORT 2017

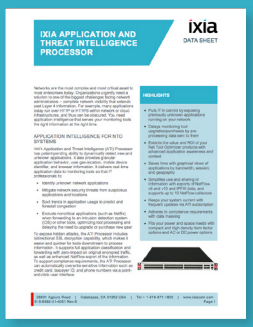


Data Masking Setting

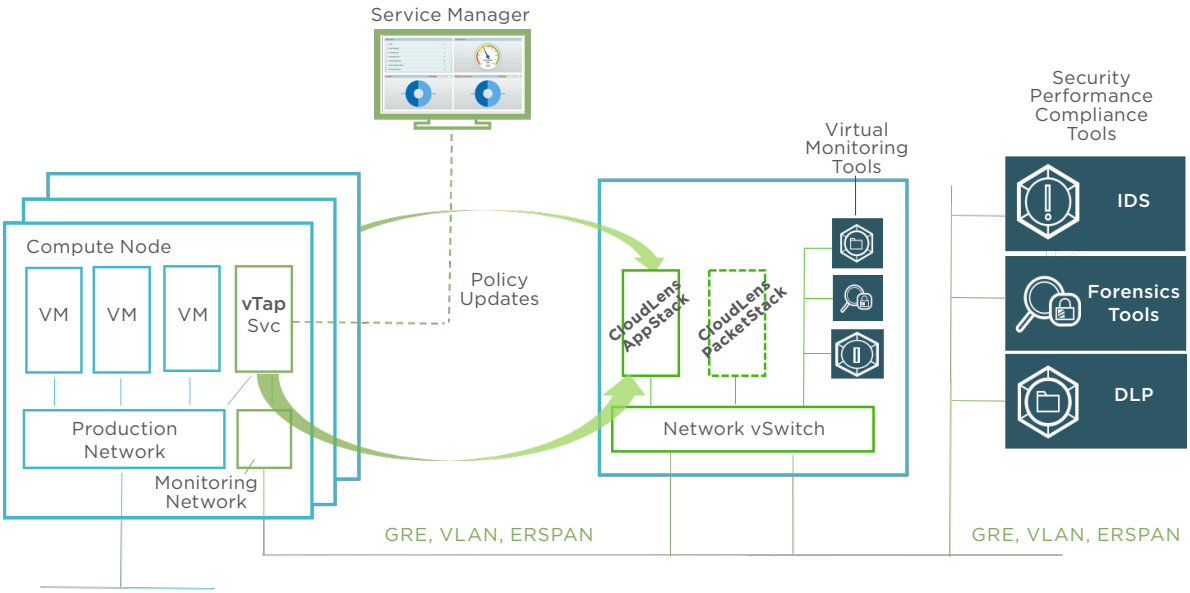
Masking also operates hand-in-hand with Secure Sockets Layer (SSL) decryption, implemented by organizations for security purposes, such as identifying cyber-threats in malicious payloads, and also a part of AppStack. Once the payload is decrypted, any sensitive data can be masked and not exposed.

Across the ocean in the U.S. and elsewhere, things get interesting, since any organization touching data belonging to EU citizens must offer the same protection. Organizations must, therefore, implement processes and technology to comply with the GDPR, since it is difficult to segregate data from one customer or another, for all practicality, this applies to the overall infrastructure. For example, a bank's automated teller machine (ATM) may serve both U.S. and EU citizens. The AppStack enabled solution described above meets the requirements of both regions.

DOWNLOAD NOW



APPLICATION AND THREAT INTELLIGENCE PROCESSOR DATA SHEET



CloudLens Private Implementation for GDPR

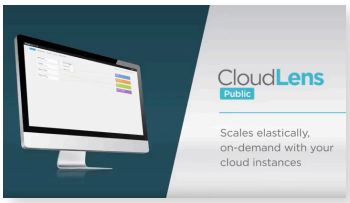
The Cloud

Extending beyond the corporate data center, hybrid environments introduce additional challenges. Where an organization processes personal data both on-premises and in a cloud, encryption between the two domains is practically mandatory. Data masking is extended to the private cloud via Ixia CloudLens™ Private, ensuring that those responsible for building visibility within a private cloud will also maintain GDPR compliance.

For private cloud implementations, CloudLens Private can virtually tap (vTap), monitor, and tunnel traffic to a Vision network packet broker with AppStack capabilities. Alternately, CloudLens Private also offers AppStack capabilities, providing a complete virtual infrastructure. Here, the same data masking and geolocation identification can take place similar to what occurs in a physical network.

For public cloud implementations, CloudLens Public operates on AWS. AWS is compliant with the CISPE Code of Conduct which may become a framework for GDPR security compliance. Additionally, Amazon has announced that AWS provides a number of services and tools that will enable you to build a GDPR-compliant infrastructure when it becomes enforceable on May 25, 2018.

WATCH THE VIDEO

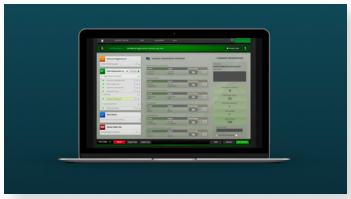


CLOUDLENS PUBLIC

Is Your Network Ready for GDPR?

In addition to visibility across physical and virtual networks, many organizations want to validate that their network is robust and defends against data breaches. Ixia's test architecture with BreakingPoint® enables organizations to ensure correct implementations and configurations of their security solutions. BreakingPoint simulates a live network by originating both legitimate traffic with embedded PII as well as malware from various geographies to assess that the security solution stops the malware but allows the valid traffic. BreakingPoint can also be used to test for GDPR-specific compliance with customized test packs.

LEARN MORE



BREAKINGPOINT

BREAKINGPOINT VE

ixia
A Keysight Business

EU–US Privacy Shield and CISPE

As clarification, note that the GDPR is not the same as the EU–US Privacy Shield which is a bi-lateral agreement to facilitate the exchange of personal data to the United States while remaining compliant with EU privacy laws. The Privacy Shield replaced the EU-US Safe Harbor Privacy Principles, also known as the Safe Harbor Agreement. How the two will relate and what changes will be made has yet to be decided, but one way of looking at it is that the Privacy Shield allows US companies or EU companies working in the US to meet GDPR requirements that relate to transferring information from the EU to the US.

Another acronym in use is Cloud Infrastructure Services Providers in Europe (CISPE). This is an association comprised of 20+ international and EU-based cloud service providers that have developed a data protection code of conduct that may become a framework for GDPR security compliance. What this means is that the underlying cloud infrastructure will most likely conform to GDPR security standards, but it is still the burden of the enterprise/SaaS company, which must implement their own policies to comply with their responsibilities while operating in the cloud.

AWS, the platform for CloudLens Public, is compliant with the CISPE Code of Conduct.

LEARN MORE

OFFICIAL EU GDPR PAGE

Conclusion

Compliance requires up-front infrastructure and process planning, and the GDPR mandates “data protection by design and data protection by default.” It also places equal responsibility on what is termed the “data controller,” which controls the data, and the “processor,” which processes the data on behalf of the controller, to keep data secure. For example, a SaaS company that serves the end customer is a data controller, while the cloud service provider is a processor. The GDPR will have a major impact on both of their processes, and organizations must have a keen understanding of the cloud provider’s shared responsibility model and proper engineering to ensure that data and applications remain in region, where required.

Organizations must automate as much as possible to overcome the lack of skilled resources that span networking, operations, and security, while education in data protection and privacy is critical. The more automation, the less chance for error. Ixia is committed to working with organizations to understand necessary changes in their security and visibility architectures.

CONTACT US

REQUEST AN IXIA DEMO TODAY

IXIA WORLDWIDE
26601 W. AGOURA RD.
CALABASAS, CA 91302

(TOLL FREE NORTH AMERICA)
1.877.367.4942

(OUTSIDE NORTH AMERICA)
+1.818.871.1800
(FAX) 1.818.871.1805
www.ixiacom.com

IXIA EUROPE
CLARION HOUSE, NORREYS DRIVE
MAIDENHEAD SL6 4FL
UNITED KINGDOM

SALES +44.1628.408750
(FAX) +44.1628.639916

IXIA ASIA PACIFIC
101 THOMSON ROAD,
#29-04/05 UNITED SQUARE,
SINGAPORE 307591

SALES +65.6332.0125
(FAX) +65.6332.0127