General Data Protection Regulation

INTRODUCTION

The General Data Protection Regulation (GDPR) is a landmark piece of regulation that will radically transform the data protection landscape of not just Europe, but the world.

GDPR creates one standard for European data protection and introduces a number of new security demands for any organisation with customers within the EU—including mandatory breach reporting and greater transparency into personal data processing—all backed by administrative fines that reach as high as four percent of global revenue.

The risk of those fines will shoot information security issues from the IT department all the way to board level, and for many organisations data protection officers will have to be appointed to oversee continuing compliance. But while the rights of European citizens are at the heart of GDPR, proactive compliance isn't quite that simple.

From data protection to investigation automation to robust breach reporting, ExtraHop can help your organisation stay ahead of GDPR and the paradigm shift it represents.

GDPR TERMINOLOGY

In the text of GDPR, data refers to the personal data of European residents specifically—that is to say, anything which could be personally identifiable and tied to the data subject, or person whose data it is. That refers to the standard fare of names and addresses but GDPR also demands that specific attention be paid to sensitive data like ethnicity, political stances, health records, genetic data, criminal records, sexual history, religion or membership in certain organisations.

The data controller is the body which decides why and how the data is used, or processed, and the data processor is the one who actually processes the data—but neither needs to actually be located within the European Union's 28 member states. If you're processing the personal data of Europeans, GDPR applies to you.

Controllers and processors must make security decisions by weighing the risks for rights and freedoms of the data subject were that data to be exposed, taking into account the sensitivity of the data and how that data could be exploited. GDPR offers a number of examples including discrimination, identity theft, reputational or financial loss, damage to professional secrecy, "or any other significant economic or social disadvantage."

And for all of this you will have to demonstrate compliance. Complying is not just about being secure, it's about showing that you're secure. That means documented security policies, breach reports, and regular audits to show that you're methodically taking steps towards compliance.

HOW EXTRAHOP SUPPORTS YOUR GDPR INITIATIVE

No vendor can make you fully compliant with everything packed into all 88 pages of GDPR, but ExtraHop is an ideal solution in three critical areas:

Start of the Art Security

While GDPR doesn't lay out many concrete methods to make yourself secure, "state of the art" is well expressed in Article 32 ("Security of Processing"). It states that controllers and processors must implement security controls according to the data being processed and "appropriate to the risk."

Assessing that risk means knowing what data is actually flowing through your system, why it's being used, and how you're going to keep it secure. ExtraHop delivers real-time insight into the most comprehensive source of all that information: the network.

ExtraHop automatically discovers and classifies every asset on your network, automatically grouping assets by importance to your business, and delivers full visibility of all transactions in flight right down to the packet level. Machine learning drives behavioral analytics that spot suspicious behaviour in real time, and you can click from an anomaly straight to the precise packets for fast, accurate forensic investigation.

One key facet of GDPR compliance is the ability to quickly and reliably pinpoint which assets handle personal data, as well as the ability to assure your customers (and, in the event of a breach, the regulatory authorities) that your organisation has implemented a higher level of security for those assets. Only ExtraHop automates the prioritization and grouping of assets within an enterprise, allowing you to focus deep analytics and security resources on your most critical systems, applications, and devices.

Because ExtraHop processes network traffic in real time instead of performing reactive log analysis, not only do you avoid the risk of capturing unnecessary personal data due to default logging capabilities but you also receive far more comprehensive data at a line rate of 40Gbps. As soon as ExtraHop detects suspicious behavior involving a critical asset, your response team will see the anomaly, its correlation with other anomalies throughout your enterprise, and the relevant packet details extracted with surgical precision.

Wire data also enables a higher degree of fidelity than log- or agent-based analytics, especially in security: wire data is impossible to modify or delete, and ExtraHop offers full decryption capabilities so even attackers using SSL/TLS or Perfect Forward Secrecy encryption have nowhere to hide. As ExtraHop integrates with leading security orchestration tools, anomaly detection can also launch an automated response such as a system quarantine which dramatically reduces the risk to customer data while you address the threat.

This 3-in-1 workflow—threat detection, correlation across the attack chain, and investigation automation—significantly cuts down on the impenetrable noise of false positives while helping you invest security resources, analytical capabilities, and human energies where they're needed, i.e. "appropriate to the risk."

Assessing risk also means taking into account the sensitivity of any given data were it to be exposed. To that end, Article 32 encourages pseudonymising and encrypting personal data so that in the event of a breach, attackers will find themselves clutching a worthless prize, one which they cannot read, decrypt or most importantly, profit from. The only way to guarantee that personal data is always encrypted/pseudonymised is to monitor transactions in flight across the network, and only ExtraHop provides that visibility in real time.

Of course, even the most robust and proactive security can only get you so far in today's climate of ever-more-sophisticated cyber threats. GDPR doesn't need you to successfully fend off every breach, however, only to ensure that when (not if) you are attacked the damage is limited—and then you'll have to come clean. Which brings us to...

Reporting

Where GDPR transcends 'good security practice' is in its reporting requirements. The GDPR text is resolute here. Article 33 ("Notification of a personal data breach to the supervisory authority) states that the local regulator must be told within 72 hours of discovery of a data breach. Article 34 ("Communication of a personal data breach to the data subject") states that for certain data breaches likely to result in a high risk to the data subject, data subjects must be told without undue delay of the data breach.

With ExtraHop you'll be able to detect breaches in real time while cutting down on false positives, allowing for the quick response and comprehensive reporting that GDPR compliance requires.

Simply put, ExtraHop gives you more information, faster. When an attacker breaches your environment ExtraHop will detect the anomalous behavior, correlate that anomaly with any other unusual behavior, and map the threat across the cyber attack chain—all in real time. Your security team will be able to track the threat as it moves through your network, enabling rapid containment, full visibility into every relevant transaction, and significantly faster root-cause analysis.

In order to avoid GDPR's astronomical fines as well as the hit to your reputation, when that breach does happen your report should confidently answer three distinct questions: How quickly did you spot the breach? How effectively did you contain the damage? How completely do you understand what happened and why, so you can assure your customers it won't happen again?

ExtraHop is unmatched in the combination of machine-driven threat detection, automated investigation, and objective forensic analysis. No other solution will give you the same rapid, high-fidelity insight needed for a fast response and thorough post-breach reporting.

Shadow IT

One of the more troublesome aspects of GDPR compliance is the implicit demand (reasonable though it may seem on the surface) that organisations know exactly what's communicating on their networks. Because this goes for apps and devices as much as it does for data, many organisations are fretting over BYoD, IoT devices, or which of their average 608 cloud applications will hamstring their path to GDPR compliance.

Because ExtraHop automatically discovers and classifies assets whether on-premises, virtual, or hosted in the public or private cloud, organisations can see everything touching the network—including those pesky pieces of shadow IT. You'll see all your environment's interlaced relationships and dependencies in real time as well as a packet-level record of historical events, so you can track which devices, applications, and systems are communicating with which (as well as what they're saying).

Cloud apps, BYoD devices, and IoT tools should be collecting no more data than they need to do their job. But if they are, ExtraHop can tell you. When, for example, a strange device starts accessing personal data, you'll know what that data is, who's attempting to move it, and through which channel.

Another angle of shadow IT, at least from the perspective of your own organisation, is the matter of third parties and applications where you have no direct control over data processing practices. Article 32 specifically states that the tools used to process data must not in themselves be a risk to the rights of the data subject.

You'll need to make sure the apps and tools you use, as well as any third parties you deal with, are on a similar security footing to yours, and that they too comply with GDPR requirements. These small chinks in the armor can undo an otherwise well-protected organisation, so locking these down is critical.

ExtraHop delivers the same level of comprehensive visibility into cloud-hosted and third party apps as into local systems, so you can select vendors without putting your organisation at any additional risk.

AT THE END OF THE DAY...

There are no quick fixes to GDPR. This is a piece of regulation designed to bring about a spiritual change in data protection just as much as a technical one. But the guiding principle for GDPR compliance is to understand data itself, and any notion of security will be incomplete without keeping a close eye on where data, personal or otherwise, is heading.

ExtraHop will give you profound insight into your environment, enabling a more complete understanding of your network and the personal data that travels across it. You'll have the security, speed, and depth of knowledge that GDPR compliance requires, and the command over your data that today's threats demand. No one solution or strategy can make you fully GDPR compliant, but ExtraHop will take you much of the way.

ABOUT EXTRAHOP NETWORKS

ExtraHop makes data-driven IT a reality. By applying real-time analytics and machine learning to all digital interactions, ExtraHop delivers instant and unbiased insights. IT leaders turn to ExtraHop first to help them make faster, better-informed decisions that improve performance, security, and digital experience. Just ask the hundreds of global ExtraHop customers, including Sony, Lockheed Martin, Microsoft, Adobe, and Google.

520 Pike Street, Suite 1700
Seattle, WA 98101
877-333-9872 (voice)
206-274-6393 (fax)
info@extrahop.com
www.extrahop.com